Secret-key rates and privacy leakage in biometric systems

Secret-Key Rates and Privacy Leakage in Biometric Systems

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de rector magnificus, prof.dr.ir. C.J. van Duijn, voor een commissie aangewezen door het College voor Promoties in het openbaar te verdedigen op dinsdag 2 juni 2009 om 16.00 uur

door

Tanya Ignatenko

geboren te Minsk, Wit-Rusland

Dit proefschrift is goedgekeurd door de promotor:

prof.dr.ir. J.W.M. Bergmans

Copromotor:
dr.ir. F.M.J. Willems

This research was kindly supported by SenterNovem, The Netherlands, as a part of IOP Generieke Communicatie Progam.

Ignatenko, Tanya

Secret-key rates and privacy leakage in biometric systems / by Tanya Ignatenko. - Eindhoven : Technische Universteit Eindhoven, 2009.
A catalogue record is available from the Eindhoven University of Technology Library
ISBN: 978-90-386-1832-6

Samenstelling van de promotiecomissie:

prof.dr.ir. J.W.M. Bergmans, promotor
Technische Universiteit Eindhoven, The Netherlands

dr.ir. F.M.J. Willems, copromotor
Technische Universiteit Eindhoven, The Netherlands

prof.dr. P. Narayan, extern lid
University of Maryland, USA

prof.dr. A.A.C.M. Kalker, extern lid
Harbin Institute of Technology, China

prof.dr.ir. J.P.M.G. Linnartz, lid TU/e
Technische Universiteit Eindhoven, The Netherlands

prof.dr. M.C. Gastpar, extern lid
University of California at Berkeley, USA

prof.dr.ir. C.H. Slump, extern lid
University of Twente, The Netherlands

prof.dr.ir. A.C.P.M. Backx, voorzitter
Technische Universiteit Eindhoven, The Netherlands

Моему дорогому Серёже
To my dear Sergey

Summary

Secret-Key Rates and Privacy Leakage in Biometric Systems

In this thesis both the generation of secret keys from biometric data and the binding of secret keys to biometric data are investigated. These secret keys can be used to regulate access to sensitive data, services, and environments. In a biometric secrecy system a secret key is generated or chosen during an enrollment procedure in which biometric data are observed for the first time. This key is to be reconstructed after these biometric data are observed for the second time when authentication is required. Since biometric measurements are typically noisy, reliable biometric secrecy systems also extract so-called helper data from the biometric observation at the time of enrollment. These helper data facilitate reliable reconstruction of the secret key in the authentication process. Since the helper data are assumed to be public, they should not contain information about the secret key. We say that the secrecy leakage should be negligible. Important parameters of biometric key-generation and key-binding systems include the size of the generated or chosen secret key and the information that the helper data contain (leak) about the biometric observation. This latter parameter is called privacy leakage. Ideally the privacy leakage should be small, to prevent the biometric data of an individual from being compromised. Moreover, the secret-key length (also characterized by the secret-key rate) should be large to minimize the probability that the secret key is guessed and unauthorized access is granted. The first part of this thesis mainly focuses on the fundamental trade-off between the secret-key rate and the privacy-leakage rate in biometric secret-generation and secret-binding systems. This trade-off is studied from an information-theoretical perspective for four biometric settings. The first setting is the classical secret-generation setting as proposed by Maurer [1993] and Ahlswede and Csiszár [1993]. For this setting the achievable secret-key vs. privacy-leakage rate region is determined in this thesis. In the second setting the secret key is not generated by the terminals, but independently chosen during enrollment (key binding). Also for this setting the region of achievable secret-key vs. privacy-leakage rate pairs is determined. In settings three and four

zero-leakage systems are considered. In these systems the public message should contain only a negligible amount of information about both the secret key and the biometric enrollment sequence. To achieve this, a private key is needed, which can be observed only by the two terminals. Again both the secret generation setting and chosen secret setting are considered. For these two cases the regions of achievable secret-key vs. private-key rate pairs are determined. For all four settings two notions of leakage are considered. Depending on whether one looks at secrecy and privacy leakage separately or in combination, unconditional or conditional privacy leakage is considered. Here unconditional leakage corresponds to the mutual information between the helper data and the biometric enrollment sequence, while the conditional leakage relates to the conditional version of this mutual information, given the secret.

The second part of the thesis focuses on the privacy- and secrecy-leakage analysis of the fuzzy commitment scheme. Fuzzy commitment, proposed by Juels and Wattenberg [1999], is, in fact, a particular realization of a binary biometric secrecy system with a chosen secret key. In this scheme the helper data are constructed as a codeword from an error-correcting code, used to encode a chosen secret, masked with the biometric sequence that has been observed during enrollment. Since this scheme is not privacy preserving in the conditional privacy-leakage sense, the unconditional privacy-leakage case is investigated. Four cases of biometric sources are considered, i.e. memoryless and totally-symmetric biometric sources, memoryless and input-symmetric biometric sources, memoryless biometric sources, and stationary and ergodic biometric sources. For the first two cases the achievable rate-leakage regions are determined. In these cases the secrecy leakage rate need not be positive. For the other two cases only outer bounds on achievable rate-leakage regions are found. These bounds, moreover, are sharpened for fuzzy commitment based on systematic parity-check codes. Using the fundamental trade-offs found in the first part of this thesis, it is shown that fuzzy commitment is only optimal for memoryless totally-symmetric biometric sources and only at the maximum secret-key rate. Moreover, it is demonstrated that for memoryless and stationary ergodic biometric sources, which are not input-symmetric, the fuzzy commitment scheme leaks information on both the secret key and the biometric data.

Biometric sequences have an often unknown statistical structure (model) that can be quite complex. The last part of this dissertation addresses the problem of finding the maximum a posteriori (MAP) model for a pair of observed biometric sequences and the problem of estimating the maximum secret-key rate from these sequences. A universal source coding procedure called the Context-Tree Weighting (CTW) method [1995] can be used to find this MAP model. In this thesis a procedure that determines the MAP model, based on the so-called beta-implementation of the CTW method, is proposed. Moreover, CTW methods are used to compress the biometric sequences and sequence pairs in order to estimate the mutual information between the

sequences. However, CTW methods were primarily developed for compressing one-dimensional sources, while biometric data are often modeled as two-dimensional processes. Therefore it is proved here that the entropy of a stationary two-dimensional source can be expressed as a limit of a series of conditional entropies. This result is also extended to the conditional entropy of one two-dimensional source given another one. As a consequence entropy and mutual information estimates can be obtained from CTW methods using properly-chosen templates. Using such techniques estimates of the maximum secret-key rate for physical unclonable functions (PUFs) are determined from a data-set of observed sequences. PUFs can be regarded as inanimate analogues of biometrics.

Samenvatting

In dit proefschrift wordt de generatie van geheime sleutels uit biometrische data en het binden van geheime sleutels aan biometrische data onderzocht. Deze geheime sleutels kunnen gebruikt worden om de toegang te regelen tot gevoelige gegevens, diensten en omgevingen. In een biometrisch secrecy-systeem wordt een geheime sleutel gegenereerd of gekozen (gebonden) tijdens een enrollment procedure waarbij de biometrische data voor de eerste keer worden geobserveerd. Deze geheime sleutel moet gereconstrueerd kunnen worden als de authentieke biometrische data voor een tweede keer geobserveerd worden tijdens de authentication procedure. Omdat biometrische metingen in het algemeen verruist zijn, extraheert een biometrisch secrecy-systeem ook zogenaamde helper-data uit de biometrische observatie tijdens de enrollment procedure. Deze helper-data maken betrouwbare reconstructie mogelijk tijdens de authentication procedure. Omdat de helper-data openbaar worden verondersteld, zouden ze geen informatie mogen bevatten over de geheime sleutel. We zeggen dat de secrecy-leakage verwaarloosbaar klein moet zijn. Belang-rijke parameters van een biometrisch sleutel-generatie schema en een sleutel-binding schema zijn de grootte van de geheime sleutel en de informatie die de helper-data bevat over de biometrische data. Deze laatste parameter wordt de privacy-leakage genoemd. In het ideale geval is deze privacy-leakage klein om te voorkomen dat de biometrische gegevens van een persoon gecompromitteerd raken. Bovendien moet de lengte van de geheime sleutel (ofwel de secret-key rate) groot zijn om de kans dat hij geraden wordt, waardoor onbevoegde toegang wordt verkregen, zo klein mogelijk te maken.

Het eerste deel van dit proefschrift richt zich op de fundamentele balans tussen secret-key rate en privacy-leakage in sleutel-generatie en sleutel-binding systemen. Deze balans wordt vanuit een informatietheoretisch perspectief bestudeerd voor vier biometrische situaties. De eerste situatie is de klassieke sleutel-generatie situatie zoals voorgesteld door Maurer [1993] en Ahlswede en Csiszár [1993]. Voor deze situatie wordt het bereikbare secret-key versus privacy-leakage gebied bepaald in dit proefschrift. In de tweede situatie wordt de geheime sleutel niet gegenereerd tijdens de enrollment-procedure maar onafhankelijk gekozen (sleutel-binding). Ook voor deze situatie wordt het gebied van bereikbare secret-key versus privacy-leakage paren hier afgeleid. In situaties drie en vier worden zero-leakage systemen beschouwd. In deze systemen mag de publieke helper-data slechts een verwaarloosbare hoeveelheid informatie over de geheime sleutel en de biometrische enrollment data bevat-

ten. Om dit te kunnen bereiken is een private sleutel nodig die alleen maar beschikbaar is voor beide terminals (tijdens enrollment en authentication). Ook hier worden sleutel-generatie en sleutel-binding onderzocht. Voor deze twee gevallen worden de bereikbare gebieden van secret-key versus private-key rate paren afgeleid. In alle vier de situaties beschouwen we twee soorten van privacy-leakage. Afhankelijk van of men nu kijkt naar secrecy-leakage en privacy-leakage afzonderlijk of in combinatie, wordt niet-conditionele of conditionele privacy-leakage beschouwd. Hierbij correspondeert niet-conditionele leakage met de mutuele informatie tussen de helper-data en de biometrische data, terwijl conditionele leakage correspondeert met deze mutuele informatie gegeven de geheime sleutel.

Het tweede deel van het proefschrift richt zich op de privacy-leakage versus secrecy-leakage analyse van fuzzy-commitment schema's. Fuzzy commitment, voorgesteld door Juels en Wattenberg [1999], is een speciale realisatie van een binair biometrisch systeem met een gekozen geheime sleutel (sleutel-binding). In dit schema wordt de helper-data gevormd door het codewoord van een fout-verbeterende code, dat ontstaan is uit de sleutel, te maskeren door er de biometrische enrollment data bij op te tellen. Omdat dit schema geen bescherming biedt tegen privacy-leakage in het conditionele geval, onderzoeken we hier niet-conditionele privacy-leakage. We beschouwen vier soorten bronnen, geheugenloze totaalsymmetrische bronnen, geheugenloze inputsymmetrische bronnen, geheugenloze bronnen, en stationaire ergodische bronnen. Voor de eerste twee klassen bepalen we het bereikbare secret-key rate versus privacy-leakage gebied. Het blijkt dat hier de secrecy-leakage niet positief hoeft te zijn. Voor de andere twee klassen kunnen we alleen bovengrenzen voor de bereikbare gebieden afleiden. Deze bovengrenzen kunnen worden verscherpt als in het fuzzy-commitment schema gebruik wordt gemaakt van systematische parity-check codes. Als we de fundamentele balans die we afgeleid hebben in het eerste gedeelte van dit proefschrift vergelijken met de balans voor fuzzy commitment, blijkt dat fuzzy commitment alleen optimaal kan zijn voor geheugenloze totaalsymmetrische bronnen als de secret-key rate maximaal is. Bovendien wordt voor geheugenloze en stationaire ergodische bronnen, die niet inputsymmetrisch zijn, aangetoond dat fuzzy commitment informatie lekt over zowel de biometrische data als de geheime sleutel.

Biometrische rijen hebben een statistische structuur (model) die vaak onbekend en vrij complex is. Het laatste gedeelte van dit proefschrift gaat over de bepaling van het maximum a-posteriori (MAP) model dat past bij een paar geobserveerde biometrisch rijen. Een universele broncodeer-methode die de naam Context-Tree Weighting (CTW) [1995] methode heeft, kan gebruikt worden om dit MAP-model te vinden. In dit proefschrift stellen we een procedure voor die het MAP-model bepaalt, gebaseerd op de zogenaamde beta-implementatie van het CTW algoritme. Daarnaast gebruiken we het CTW algoritme om biometrische rijen en paren van ri-

jen te comprimeren om zodoende een schatting te krijgen van de mutuele informatie tussen deze rijen. Omdat CTW methodes primair ontwikkeld zijn om eendimensionale data-rijen te comprimeren terwijl biometrische data vaak gemodelleerd worden als tweedimensionaal, bewijzen we eerst dat de entropie van een stationair tweedimensionaal proces uitgedrukt kan worden als een limiet van een reeks conditionele entropieën. Dit resultaat wordt vervolgens uitgebreid naar de conditionele entropie van een tweedimensionaal proces gegeven een tweede proces. Als gevolg hiervan kunnen schattingen van entropieën en mutuele informaties verkregen worden met het CTW algoritme als we behoorlijk-gekozen context-templates gebruiken. Met behulp van deze technieken worden schattingen van de maximale secret-key rate voor physical unclonable functions (PUFs) gemaakt gebaseerd op een dataset die geobserveerde paren van data-rijen bevat. PUFs kunnen beschouwd worden als levenloze analogons van biometrieën.

Contents

Chapter 1

Introduction

Big Brother is watching you (G. Orwell).

1.1 Introduction

Nowadays people live in the era of large-scale computer networks connecting huge numbers of electronic devices. These devices execute applications that use the networks for exchanging information. Sometimes the information that is transmitted within these networks and stored by the devices is sensitive to misuse. Moreover, the networks and devices cannot always be trusted. This can lead to intrusions into the privacy of users by e.g. hackers, commercial parties, or even by governmental institutions. Also illegal copying of copyrighted content, illegal use of e–payment systems, and identity theft can be foreseen. In order to prevent all such malicious actions the security of networks and devices should be adequate.

Traditional systems for access control, which are based on the possession of secret knowledge (passwords, secret keys, etc.) or on a physical token (ID card, smart-card, etc.), have the drawback that they cannot guarantee that it is the legitimate user who e.g. enters a password or presents a smart-card. Moreover, passwords can often be guessed, since people tend to use passwords which are easy to remember. Physical tokens in their turn can be lost, stolen, or copied.

Biometric systems offer a solution to most of the problems mentioned above. They could be either substituted for traditional systems or used to reinforce them. Biometric systems are based on physical or behavioral characteristics of human beings, like faces, fingerprints, voice, irises, gait, see Jain et al. [36]. The results of the measurement of these characteristics are called biometric data. Biometric data have the advantage that potentially they are unique identifiers of human beings, as was argued by Clarke [12]. They provide therefore a closer bond with the identity of their owner than a password or a token does. Moreover, biometric data cannot be stolen or lost. They potentially contain a large amount of information and therefore are hard to guess. All this makes biometrics a good candidate for substitution of traditional passwords and secret keys. A drawback of using biometrics is that the out-

come of their measurements is, in general, noisy due to intrinsic variability, varying measurement conditions, or due to the use of different hardware. However, advanced signal-processing and error-correcting techniques can be applied to guarantee reliable overall behavior.

The attractive property of uniqueness, that holds for biometrics, also results in its major weakness. Unlike passwords and secret keys, biometric information, if compromised once, cannot be canceled and easily replaced by other biometric information, since people only have limited resources of biometric data. Theft of biometric data results in a partially stolen identity, and this is, in principle, irreversible. Therefore requirements for biometric systems should include *secure storage* and *secure communication* of biometric data in the applications where they are used.

Although biometric data may provide solutions to the problems discussed above, there are situations when they cannot be used. There is e.g. a small percentage of people whose fingerprints cannot be used due to intrinsic bad quality, see Dorizzi [24]. Also DNA recognition fails for identical twins. In such situations standard cryptographic tools are needed to provide additional security.

An artificial inanimate analog of biometrics is a Physical Unclonable Function (PUF). PUFs were introduced by Pappu [52] as objects having properties similar to standard biometric modalities. They cannot easily be copied or cloned and are unique, and just like human biometrics the data that result from their measurements are noisy. The most prominent advantage of PUFs over human biometrics is that it can easily be replaced when necessary. Privacy is not a point of concern in systems based on PUFs, but note also that there is no strong bonding between a PUF and its owner.

In what follows we will first describe traditional biometric systems in more detail. In these systems biometric data are supposed to be stored in the clear although these data can provide access to data or to a service. After that, we will discuss techniques that make (complete) reconstruction of the biometric data from the stored information practically impossible. These techniques therefore prevent an attacker from getting access to data or to a service after breaking into the database or eavesdropping on the network.

1.2 Biometrics and Physical Unclonable Functions

1.2.1 Traditional Biometric Systems

The terms “Biometrics” and “Biometry” have been used since the first part of the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in biological sciences [1]. Relatively recently the term “Biometrics” has also been used to refer to the field of technology devoted to automatic identification of individuals using biological traits, such as those based

on retinal or iris scanning, fingerprints, faces, signatures, etc. Such biological traits are unique for individuals as noted in Jain et al. [36].

Traditionally, biometric recognition was used in forensic applications and performed by human experts. However, recent advantages in automated recognition resulted in the spreading of biometric applications, now ranging from border control at airports to access control in Walt Disney amusement parks (see Wayman et al. [85]).

A typical biometric system is essentially a pattern recognition system, which performs one or more identity checks based on specific physiological or behavioral characteristics possessed by individuals. There are two different ways to resolve an individual's identity, i.e. authentication and identification. Authentication (Am I who I claim I to be?) involves confirming or denying the individual's claimed identity. In identification, one has to establish the individual's identity (Who am I?). Each of these approaches has its own characteristics and could be solved best by biometric systems.

All biometric technology systems have certain aspects in common. All are dependent upon an accurate reference or enrollment data. If a biometric system is to identify or to authenticate an individual, it first must have these reference data positively linked to the subject. Modern biometric identification systems, based on digital technologies, analyze personal physical attributes at the time of enrollment and distill them into a series of numbers. Once this reference sample or template is in the system, future attempts to identify an individual rest on comparing "live" data to the reference data.

A perfect system would always recognize an individual, and always reject an impostor. However, biometric data are gathered from individuals under environmental conditions that cannot always be controlled, over equipment that may slowly be wearing out, and using technologies and methods that vary in their level of precision. Consequently, an ideal behavior of biometric systems cannot be realized in practice. Traditionally, the probability that an authorized individual is rejected by a biometric system is called False Rejection Rate (FRR), and the probability that an unauthorized individual is accepted by a biometric system is called False Acceptance Rate (FAR). There are also other performance measures that characterize biometric systems. For for an excellent overview and similar issues see Jain et al. [36], Maltoni et al. [21], or Wayman et al. [85].

Although biometric technologies have their advantages when they are applied in access control systems, privacy aspects of biometric data should not be ignored. Identification and authentication require storage of biometric reference data in some way. However, people feel uncomfortable with supplying their biometric information to a huge number of seemingly secure databases for various reasons, such as

- practice shows that one cannot fully trust an implementation of secure algorithms by third parties. Even governmental organizations that are typically

trusted by the majority of the population cannot always guarantee that important sensitive data are securely stored;

- databases might be attacked from inside, which allows an owner of a database to abuse biometric information, for example, by selling it to third parties;

- people have limited resources of biometric data, that can be conveniently used for access control. Therefore an "identity theft" of biometric information has much more serious implications than a "simple" theft of a credit card. In the latter case, one can simply block and replace this credit card, while biometric information cannot be easily revoked and replaced by other biometric information.

It is often argued that privacy need not be a real issue in biometric systems, since biometric data are not secret and can easily be captured (faces, irises) or left in public (fingerprints), see Schneier [65]. However, this information, unlike the reference data, is typically of low quality and therefore cannot be easily used for impersonation. Even if it was of good quality, which might be the case with faces, connecting it to the corresponding database is not always an easy task.

Another important point is, that obtaining biometric data of a specific person as well as any other secret information belonging to him, is always possible when sufficient effort is exerted. In contrast, compromising a database, requires a comparable effort, but then provides immediate access to the biometric data of large number of individuals. Therefore it makes sense to concentrate on protecting the database. It would be ideal if, in case the database becomes public, the biometric reference data could not be recovered.

1.2.2 Physical Unclonable Functions

Physical Unclonable Functions (PUFs) were first discovered and studied in Pappu [52]. Pappu used the name "physical one-way" functions for PUFs. Later, the name was changed to "physical random functions" and to "physical unclonable functions", see Gassend et al. [30]. This was done to avoid confusion since PUFs do not match the standard definition of one-way functions, see e.g. Schneier [64]. A PUF is defined as a function that maps challenges to responses and is embodied by a physical device. The properties of PUFs are

- the response to challenge is easy to obtain;

- they are hard to characterize, i.e. given physical measurements of a PUF, an attacker can only extract a negligible amount of information about the response to a randomly chosen challenge.

PUFs can be used to obtain unique, tamper resistant and unforgeable identifiers from physical structures. This was observed by Pappu [52]. Uniqueness implies that the number of independent degrees of freedom in the output space should be large. Tamper resistance means that the output of the physical system is very sensitive to changes in the challenge or in the system itself. Finally, unforgeable stands for the property of the system to be very difficult to clone in such a way that the cloned version produces an identical response to all challenges.

From the above we can conclude that PUFs can be regarded as a particular biometric modality that comes from inanimate objects. However, unlike standard biometric modalities, for PUF-based systems privacy is not a major point of concern. Unlike human biometrics, PUFs can be easily replaced. The main problem with using PUFs lies in their noisy nature and therefore can be formulated as extraction of secure keys out of noisy data.

In the first part of this thesis we will focus on standard biometrics and on the corresponding privacy problems, while in the second part, we will investigate PUFs without considering privacy issues.

1.3 From Traditional Biometric Systems to Biometric Secrecy Systems

1.3.1 Types of Security

To assess cryptographic protocols, two notions of security are commonly used, i.e. information-theoretical security and computational security.

Computationally secure protocols rely on such an assumption as hardness of mathematical problems, e.g. factoring and taking discrete logarithms, and assume that an adversary has bounded computing power. However, hardness of a problem is sometimes difficult to prove, and in practice certain problems are "assumed" to be hard.

Protocols whose security does not rely on computational assumptions, i.e. they are secure even when the adversary has unbounded computing power, are called unconditionally or information-theoretically secure. Information-theoretically secure protocols are more desirable, but not always achievable. Therefore, in practice, cryptographers mostly use computational security.

In the present thesis we will treat security from an information-theoretical point of view. The key mathematical concept on which information theory is built and which is also relevant for considering information-theoretical security, is entropy. The notion of entropy comes from Shannon [68]. Entropy is a measure of the information contained in a random variable. Although there are a number of alternative entropy concepts, e.g. Rényi and min-entropy (Rényi entropy of order 2) [59], and smooth

Rényi entropy [58], we will only use the classical (Shannon) notion of entropy here. Another Shannon-type concept is that of mutual information. Mutual information measures by how much the entropy of the first random variable decreases if access to the second random variable is obtained, and this notion can be defined in terms of entropies. For the exact definitions, properties and their proofs of entropy and mutual information we refer to Shannon [68] or e.g. Cover and Thomas [13].

An interesting special case of information-theoretical security is perfect security. This concept was introduced by Shannon [69]. He defined a secrecy system to be perfect if the mutual information between plaintext M and ciphertext C satisfies

$$I(M;C) = 0, \tag{1.1}$$

i.e. if a ciphertext C, which is a function of a plaintext M and a secret key K, provides no information about the plaintext M, in other words, if C and M are statistically independent. Shannon proved that perfect secrecy can only be achieved when the key-entropy and plaintext-entropy satisfy

$$H(K) \geq H(M). \tag{1.2}$$

An example of a perfectly secure system is the one-time pad system, also referred to as the Vernam cipher [82]. In one-time pad, a binary plaintext is concealed by adding modulo-2 (XOR-ing) a random binary secret key.

In practice it is quite possible and common for a secrecy system to leak some information. Although such a system is not perfectly secure, it can be information-theoretically secure up to a certain level.

1.3.2 Biometric Secrecy Systems with Helper Data

Biometric secrecy systems in which the stored reference data satisfy certain secrecy and privacy constraints can be realized using the notion of helper data. In the next subsections we will follow an intuitive discussion that will eventually introduce us to systems in which helper data are applied. After that we will discuss two applications in which helper data play a role.

Noisy Passwords and Helper Data

A perfect system for a secure biometric access control has to satisfy three requirements. Biometric data have to be private, namely, the reference information stored in a database should not reveal the actual biometric data. Reference data that are communicated from a database to a point where access can be granted have to be resilient to eavesdropping. Reference data stored in a database have to be resilient to guessing, i.e. to brute-force attacks.

A simple naive approach to satisfy both the first and the second requirements would be to use the biometric data as a password in a UNIX-password authentication scheme. In such a scheme, a user possesses a password x that gives access to his account. There is a trusted server that stores some information $y = f(x)$ about the password. The user gains access to the account only if he enters the password x', such that $f(x') = y$. The scheme has the requirement that nobody can figure out the password x from y in any way other than by guessing. To fulfill this requirement, a UNIX-password scheme relies on one-way functions. A one-way function $f(\cdot)$ is a function that is easy to compute but "hard to invert", where "hard to invert" refers to the property that no probabilistic polynomial-time algorithm can compute a pre-image of $f(x)$ with a better than negligible probability when x is chosen at random.

Thus, if we would use the UNIX-password authentication scheme and apply a one-way function to the biometric data, the storage of biometric data in the clear would be circumvented. However, there are a number of problems that would arise if we use biometric data in the UNIX scheme. First, the security properties that are guaranteed by one-way functions rely on the assumption that x is truly uniform, while we know that biometric data are far from uniform, although they do contain randomness of course. Moreover, one-way functions, as all cryptographic primitives, require their entries to be exactly reproducible for positive authentication[1], while biometric data measurements are almost never identical. Therefore additional processing (e.g. error-correction and compression) is needed to realize a biometric UNIX-like authentication scheme that can tolerate a reasonable amount of errors in biometric measurements and results in uniform entries to the one-way function. One way of operating would be to use a collection of error-correcting codes such that for each observed biometric enrollment template there is a code that contains this template as a codeword. The index to this code is then stored in the database as helper data. Upon observing the individual for a second time, the helper can then be used to retrieve the enrollment template from the authentication template. The error-correcting code should be strong enough to correct the errors between the enrollment and authentication templates. From this we may conclude that error-correcting techniques and helper data can be applied to combat errors. Subsequently compression methods can be used to achieve almost uniform entries.

Now that we have argued that helper data could be used to create a reliable system, the question arises what requirements ideal helper data should satisfy. Since helper data need to be stored (and communicated) for authentication, it would be advantageous if they could be made publicly available without compromising or leaking any information about the data that are used to get access to the system. We say that

[1] Positive authentication can also be a result of an entry that produces a collision. However, here we do not consider collisions, since this is a problem associated with the design of one-way functions and therefore beyond the scope of this thesis.

secrecy leakage from the helper data has to be negligible. Note that these data could be obtained using a one-way function as in the UNIX-scheme, but better procedures may exist as well. On the other hand, the helper data should leak as little information as possible about the observed biometric enrollment template. This would reduce privacy-related problems. Note that it might be impossible to make this leakage negligible, since helper data should contain some information about the biometric data in order to set up a reliable system. It will become clear later in this thesis that a notion of secret key sharing originated from Information Theory (see Ahlswede and Csiszár [4]) will be essential in designing and analyzing biometric systems in which public helper data is used. For these secret-key sharing systems, the problem of maximizing the size of the extracted secrets (the data needed to get access) was solved. This provides the solution for our third requirement, resilience to guessing.

In what we have discussed up to now, we have always assumed that keys were obtained as a result of a one-way operation on a password or on a biometric template. A biometric system would however be more flexible if we could choose the keys ourselves. We will show that the helper-data construction will make this possible. In the rest of the thesis we will therefore distinguish between generated-key systems and chosen-key systems. Sometimes their performance will not differ that much, but in other situations the differences can be dramatic.

In the next two subsections, we will shortly discuss two applications of biometric access with helper data. In the first application the secret key is stored in the database in an encrypted form, while in the second application the key is discarded.

Application A: Biometric Access

A general protocol for secure authentication can be schematically represented as the diagram in Fig. 1.1. A typical authentication procedure reads as follows.

During *enrollment*, the biometric data of a subject are captured and analyzed, and the template X^N is extracted. A secret K is chosen or generated from these data. Then the template X^N is linked to the key K via a helper message M. The key is encrypted using a one-way function and stored in a database as $f(K)$, together with an ID of the subject and the helper message M.

During *authentication*, the subject claims his identity (ID). His biometric data are captured and preprocessed again, resulting in the template Y^N. The key $\widehat{K}$ is estimated based on Y^N and the helper message M that corresponds to the claimed ID. This estimated key is encrypted and then matched against the encrypted key $f(K)$ corresponding to the claimed ID. Only if $f(\widehat{K})$ is the same as $f(K)$ the subject is positively authenticated.

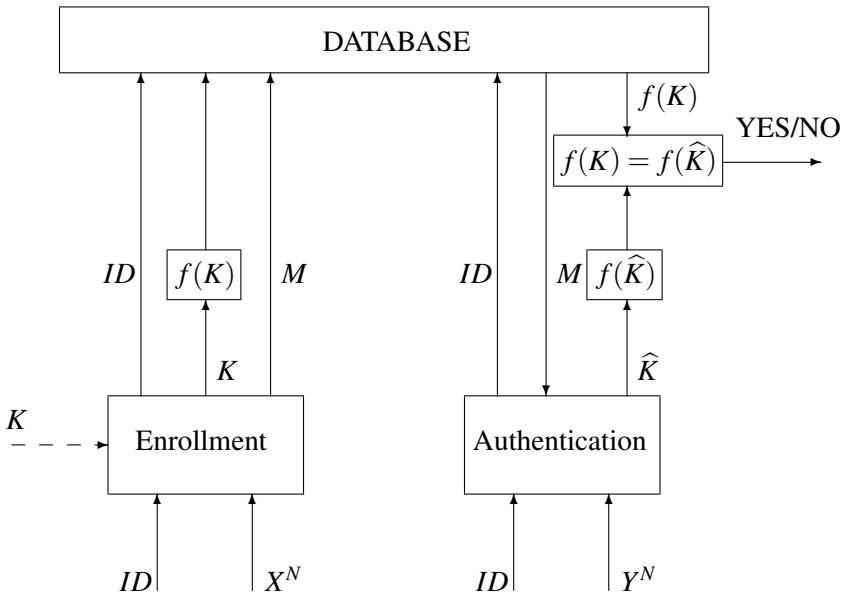


Figure 1.1: *Secure authentication. The dotted arrow indicates the possibility that the secret key is chosen, not generated from X^N.*

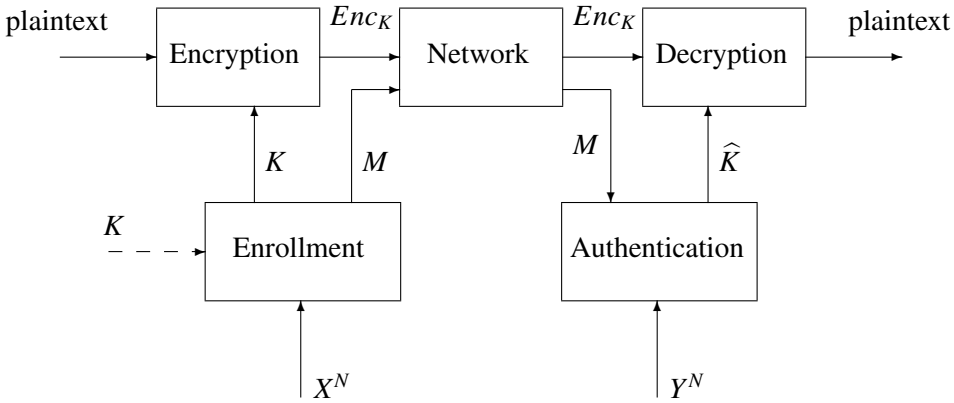


Figure 1.2: *Secure encryption. Dotted arrow indicates the possibility that the secret key is chosen, not extracted from X^N.*

Application B: Biometric Encryption

Another system of interest is a system that uses biometric based keys for encryption. A protocol for biometric based encryption is depicted in Fig. 1.2.

The first step of biometric based *encryption* is similar to the enrollment procedure in the authentication protocol, viz. biometric data of a subject are captured and

analyzed, and a template X^N is derived. Then, a secret key K is extracted/chosen and linked to the template via a helper message M. This secret is used to encrypt a plaintext m as $Enc_K(m)$ (here encryption is assumed to be symmetric). This encrypted plaintext and the helper message are either stored or transmitted, while the key is discarded.

In the *decryption* phase, in order to decrypt the plaintext, the subject provides a measurement of his biometrics. This measurement is preprocessed, resulting in a noisy template Y^N. The template and the helper message M are now used to derive a key $\widehat{K}$. The key $\widehat{K}$ is used to decrypt the encrypted plaintext $Enc_K(m)$. The decryption is successful, viz. $Dec_{\widehat{K}}(Enc_K(m)) = m$, only if $\widehat{K} = K$, since symmetric encryption is used.

Two Generic Settings

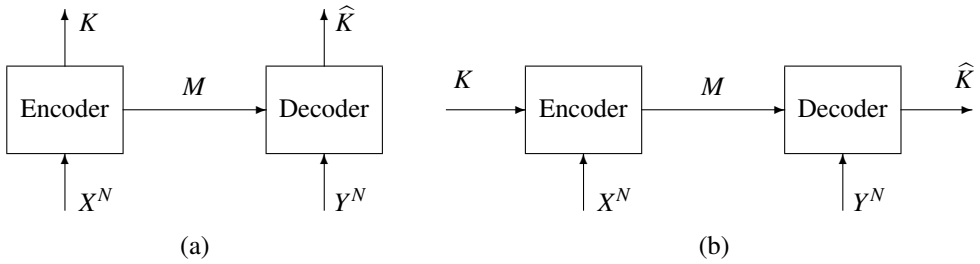


Figure 1.3: *Generic settings, generated and chosen keys.*

From the discussions above we may conclude that in order to design a good biometric secrecy system, it is enough to focus on a number of generic structures, i.e. models that constitute the core of any biometric secrecy system. These generic, secret-key sharing models can be subdivided into a class of models with generated keys, see Fig. 1.3(a), and a class of models with chosen keys, see Fig. 1.3(b). This subdivision also appears in the overview paper of Jain et al. [37]. In both models K is a randomly generated/chosen secret key, X^N and Y^N are biometric enrollment and authentication sequences having length N, M is a helper message, and $\widehat{K}$ is an estimated secret key. The channel between an encoder and decoder is assumed to be public. We only assume that passive attacks are possible, namely, an attacker can see all public information but cannot change it. The information leakage is characterized in terms of mutual information, and the size of the secret keys in terms of entropy. The generic models must satisfy the following requirements

$$\Pr(K \neq \widehat{K}) \approx 0 \quad \text{(reliability)}, \tag{1.3}$$

$$H(K)/N \approx \log|\mathcal{K}|/N \text{ is as large as possible} \quad \text{(secret-key rate)}, \tag{1.4}$$

$$I(K;M)/N \approx 0 \quad \text{(secrecy leakage)}, \tag{1.5}$$

$$I(X^N;M)/N \text{ is as small as possible} \quad \text{(privacy leakage)}. \tag{1.6}$$

Remark: In this thesis log denotes logarithm to the base 2. Moreover, further in the thesis, we denote the generated and chosen keys by S and K, respectively.

1.4 Modeling Biometric Data

Throughout this thesis we assume that our biometric sequences (feature vectors) are discrete, independent and identically distributed (i.i.d.). Fingerprints and irises are typical examples of such biometric sources. A discrete representation of other biometric modalities can by obtained using quantization. The independence of biometric features is not unreasonable to assume, since PCA, LDA and other transforms, which are applied to biometric measurements during feature extraction (see Wayman et al. [85]) result in more or less independent features. In general, different components of biometric sequences may have different ranges of correlation. However for reasons of simplicity we will only discus identically distributed biometrics here.

In Chapters 2, 4 and 6 we consider stationary ergodic biometric sources. Whether biometric data sources can be modeled as stationary and ergodic is still a research question, however, there are some indications that irises, fingerprints and DNA can be considered to be stationary ergodic, see [2]. On the other hand, PUFs are modeled as stationary ergodic processes. Indeed from Feng et al. [26] we know that the two-point intensity correlations in a speckle pattern are translation invariant. Moreover, these processes are also ergodic due to the fact that the spatial distribution of intensities is the same as the PUF ensemble distribution of intensities, see Goodman [31].

In the first part of the thesis, we assume that our biometric secrecy systems are based on a biometric source with distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$. This source produces enrollment sequences $x^N = (x_1, x_2, \ldots, x_N)$ of N symbols from the finite alphabet $\mathcal{X}$ and authentication sequences $y^N = (y_1, y_2, \ldots, y_N)$ of N symbols from the finite alphabet $\mathcal{Y}$. When a sequence pair (x^N, y^N) comes from the same person, then it is characterized in terms of joint probability distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$. In that case the biometric sequences X^N and Y^N are in general not independent of each other. However, when in the sequence pair (x^N, y^N) the sequences come from different persons, the pair is characterized in terms of $\{Q(x)Q(y), x \in \mathcal{X}, y \in \mathcal{Y}\}$, where $Q(x)$ and $Q(y)$ are marginals of $Q(x,y)$. Therefore the biometric sequences X^N and Y^N that come from different persons are assumed to be independent. These assumptions can also be observed in Schmid and Nicolo [62], where biometric system capacity is studied under global PCA and ICA encoding.

1.5 Related Work

Privacy concerns related to the use of biometric data in various secrecy systems are not new. Schneier [65] pointed out that biometric data are not standard secret keys that cannot be easily canceled. Ratha et al. [56] investigated the vulnerability points of biometric secrecy systems. In Prabhakar et al. [54] security and privacy concerns were raised. Linnartz and Tuyls [45] looked at the problem of achieving biometric systems with no secrecy leakage. Finally, at the DSP forum [83] secrecy- and privacy-protecting technologies were discussed. The extent to which secrecy and privacy problems were investigated in literature also received attention there.

Considerable interest in the topic of biometric secrecy systems resulted in the proposal of various techniques over the past decade. Recent developments in the area of biometric secrecy systems led to methods grouped around two classes: cancelable biometrics and "fuzzy encryption". Detailed summaries of these two approaches can be found in Uludag et al. [80] and in Jain et al. [37].

It is the objective of cancelable biometrics, introduced by Ratha et al. [56], [57], Ang et al. [7], and Maiorana et al. [46], to avoid storage of reference biometric data in the clear in biometric authentication systems. These methods are based on non-invertible transformations that preserve the statistical properties of biometric data and rely on the assumption that it is hard to exactly reconstruct biometric data from the transformed data and applied transformation. However, hardness of a problem is difficult to prove, and, in practice, the properties of these schemes are assessed using brute-force attacks. Moreover, visual inspection shows that transformed data, e.g. the distorted faces in Ratha et al. [57], still contain a lot of biometric information.

The "fuzzy encryption" approach focuses on generation and binding of secret-keys from/to biometric data. Implementation of "fuzzy encryption" includes methods based on various forms of Shamir's secret sharing [67]. These methods are used to harden passwords with biometric data (Monrose et al. [49], [48]). Methods based on error-correcting codes, that bind uniformly distributed secret keys to biometric data and that tolerate (biometric) errors in these secret keys, were formally defined by Juels and Wattenberg [41]. Less formal approaches can be found in Davida et al. [19], [18]. Error-correction based methods were extended to the set difference metric developed by Juels and Sudan [40]. Some other approaches focus on continuous biometric data and provide solutions which are based on quantization of biometric data as in Linnartz and Tuyls [45], Denteneer et al. [20] (with emphasis on reliable components), Teoh et al. [74], and Buhan et al. [10].

Finally, a formal approach for designing secure biometric systems for three metric distances (Hamming, edit and set), called fuzzy extractors, was introduced in Dodis et al. [22] and further elaborated in [23]. Dodis et al. [22], [23] were the first ones who addressed the problem of code construction for biometric secret-key generation in a systematic information-theoretical way. Although their works provide results on

the maximum secret-key rates in biometric secrecy systems, they also give the corresponding results for the maximum privacy leakage. In biometric setting, however, the goal is to minimize the privacy leakage. The need for quantifying the exact information leakage on biometric data was also stated as an open question in Sutcu et al. [73].

Another branch of work on "fuzzy encryption" focuses on combination of biometric and cryptographic keys. Methods in this direction include attempts to harden the fuzzy vault scheme of Juels and Sudan [40] with passwords by Nandakumar et al. [50] and dithering techniques that were proposed by Buhan et al. [9].

1.6 Thesis Organization

In the current thesis we study a number of problems related to the design of biometric secrecy systems.

First of all we address the problems of what the fundamental trade-off between the secret-key rate and the privacy leakage is in biometric secrecy systems that extract or convey secret keys, and what the methods are to achieve optimal systems. Chapter 3 is devoted to these problems and is the main chapter of this thesis.

The results obtained in Chapter 3 are further used to assess the optimality of a popular existing technique for designing biometric secrecy systems, i.e. fuzzy commitment, which was proposed by Juels and Wattenberg [41]. We study the properties of fuzzy commitment in Chapter 4.

Then we focus on a problem that needs to be addressed before any practical biometric secrecy system is built, viz. how much secret information can be extracted or conveyed with a certain biometric modality. In Chapter 5 we describe the methods that we use to estimate this amount of secret-key information. Moreover, since to design codes that achieve a nearly-optimal performance we need to know the statistics of the biometric source, we also study in this chapter the problem of how to find the model that matches best a pair of observed biometric sequences.

Then, in Chapter 6, we concentrate on the estimation of maximum secret-key rates for two-dimensional biometric sources. We use the techniques described in Chapter 5 and perform a series of experiments to estimate the secret-key rates for optical PUFs.

Next, we present in detail the content of the chapters that compound this thesis.

1.6.1 Chapter 2: Secret Sharing and Biometric Systems

Chapter 2 is mainly a review chapter that sets theoretical grounds for our investigation of secret-key rates and privacy leakage in biometric secrecy systems. In this chapter we revisit the classical Ahlswede and Csiszár [3] and Maurer [47] problem of

generating a secret from two dependent sequences but in the biometric setting. Here the biometric source is assumed to be discrete memoryless. The maximum secret-key rate that is achievable for this model is equal to the mutual information between a biometric enrollment sequence X^N and a biometric authentication sequence Y^N, i.e. $I(X;Y)$. Although this result was already proved using strong typicality by Ahlswede and Csiszár [3], we provide our version of the proof, which is based on weak typicality. This proof will be the core part of the achievability proofs given in Chapter 3 where we deal with more general biometric settings.

Then, as a warm-up, we derive a characterization for privacy leakage for the biometric secret generation systems, which achieve the maximum secret-key rates with codes determined in our achievability proof.

Moreover, we discuss how typical biometric performance measures, i.e. the FRR and the FAR, relate to the results obtained for the biometric secret generation model. We show that these error probabilities can be made arbitrarily small for positive secret-key rates smaller than or equal to $I(X;Y)$. Furthermore, we argue that the FAR for the biometric secret generation model can be characterized in terms of the identification capacity of a typical biometric identification system with no security constraints.

Finally, we extend the i.i.d. results derived in this chapter to stationary ergodic sources.

1.6.2 Chapter 3: Privacy Leakage in Biometric Secrecy Systems

In Chapter 3 we continue to study secret-key rates and privacy leakage. There, however, we concentrate on a more general situation. One of the challenges in designing biometric secrecy systems is to minimize the privacy leakage for a given secret-key rate. Therefore, in Chapter 3, we focus on finding the fundamental trade-off between secret-key rates and privacy leakage. In this chapter we assume that our biometric source is discrete memoryless.

Since biometric secrecy systems can be designed as those where secret keys are generated from biometric data but also as those where secret keys are bound to biometric data, see the overview paper of Jain et al. [37] and our discussions above, we investigate both types of systems, i.e. biometric secret generation systems and biometric systems with chosen (bound) secret keys.

We consider four biometric settings. The first one is again the standard Ahlswede-Csiszár secret-generation setting. Now, however, we have the requirements that the helper data should not only contain a negligible amount of information about the secret, but also should leak as little information as possible about the biometric data.

In the second setting we consider a biometric model with chosen keys where the secret key is not generated by the terminals but independently chosen at the encoder side and conveyed to the decoder. This model has the same requirements as biometric

secret generation model.

The other two biometric settings that we consider correspond to biometric secrecy systems with zero privacy leakage. Ideally, biometric secrecy systems should leak a negligible amount of information not only on the secret but also on the biometric data. However, in order to be able to generate or convey large secret keys reliably, we have to send some data (helper data) to the second terminal. Without any precautions, the helper data leak a certain amount of information on the biometric data. In this way biometrics solely may not always satisfy the security and privacy requirements of certain systems. However, the performance of biometric systems can be enhanced using standard cryptographic keys. In our models we assume that only the two terminals have access to an extra independent private key, which is observed together with the correlated biometric sequences. The private key is used to achieve a negligible amount of privacy leakage (zero leakage). We investigate both the secret generation model with zero-leakage and the model with chosen keys and zero-leakage.

All the four settings that we have described are studied for two types of leakage, i.e. unconditional and conditional privacy leakage. Unconditional leakage corresponds to the mutual information between the helper data and the biometric enrollment sequence and describes the information that the helper data leak about the biometric data. The second type of leakage, the conditional one, relates to the mutual information between the helper data and the biometric enrollment sequence conditioned on the secret. This type of privacy leakage is motivated by the fact that the helper data may provide more information on the pair of secret key and biometric data than on each of these entities separately. Therefore we have to consider the mutual information between the pair of secret key and biometric enrollment sequence and the helper data. This mutual information has to be as small as possible. In Chapter 3 we show that this requirement on the leakage on the pair can be reformulated in terms of conditional privacy leakage that has to be minimized and secrecy leakage that has to be negligible.

The four described biometric settings combined with two notions of privacy leakage result in eight biometric models. In Chapter 3 we determine the fundamental trade-offs between secret-key rates and privacy-leakage rates, and secret-key rates and private-key rates for all eight models. The result obtained for the first setting is similar and a special case of the secret-key part of Thm. 2.4 in Csiszár and Narayan [16].

For systems without a private key the achievable regions that we find are all equal, except for the chosen-key model with conditional leakage where the achievable region is in principle smaller. Similarly, for zero-leakage systems the achievable regions are all equal, except for the chosen-key model with conditional leakage. In the latter case, it is important to note that from the derived region we may conclude that the biometrics are actually useless. Generally, in zero-leakage systems the secret-key

rate cannot be smaller than the private-key rate.

The achievability proofs that we provide in Chapter 3 suggest that optimal codes should incorporate both vector quantization methods and Slepian-Wolf techniques.

1.6.3 Chapter 4: Leakage in Fuzzy Commitment Schemes

Chapter 4 is devoted to the analysis of the properties of fuzzy commitment, introduced by Juels and Wattenberg [41]. Fuzzy commitment is a particular realization of a binary biometric secrecy system with chosen secret keys. It became a popular technique for designing biometric secrecy systems, since it is convenient and easy to implement using standard error-correcting codes. However, fuzzy commitment is primarily designed for binary uniform memoryless biometric sequences, and it is provably secure for this case.

In Chapter 4 we focus on the achievable regions for fuzzy commitment. We investigate fuzzy commitment when the biometric data statistic is memoryless and totally-symmetric, memoryless and input-symmetric, memoryless, and stationary ergodic. Unlike in Chapter 3, where we obtain the regions of secret-key vs. privacy leakage pairs, the regions for fuzzy commitment are given for triples of achievable secret-key, secrecy-leakage, and privacy-leakage rates.

We could determine the achievable regions when data statistics are memoryless and totally-symmetric, and memoryless and input-symmetric. For the general memoryless and stationary ergodic cases we cannot determine the achievable rate-leakage regions, and we only provide outer bounds on the corresponding regions. These bounds, moreover, can be sharpened for systematic parity-check codes.

Given the achievable regions (bounds), the optimality of fuzzy commitment in terms of secret-key vs. privacy-leakage balance is assessed using the fundamental secret-key vs. privacy-leakage rate trade-offs found in Chapter 3, if we "project" the fuzzy-commitment regions on secret-key vs. privacy-leakage rate plane. It turns out that the fuzzy commitment scheme is only optimal for the totally-symmetric memoryless case and only if the scheme operates at the maximum secret-key rate. Moreover, for the general memoryless case the scheme reveals more information than necessary on both the secret and biometric data.

To assess the stationary ergodic case, we use the results obtained in Chapter 2. Then we compare the fuzzy commitment scheme to a two-layer scheme for stationary ergodic biometric sources. The latter scheme is based on a biometric secret generation model with a masking layer on top of it. It appears that the two-layer scheme enjoys better properties. Hence we may conclude that also for the stationary ergodic case the scheme reveals more than necessary information on both the secret and biometric data.

1.6.4 Chapter 5: Context Weighting And Maximizing Using Ratio Representation

In order to design codes that achieve near-optimal performance according to the guidelines stated in Chapter 3, we need to know the statistics of the biometric source. The statistics of the source is determined by the model (structure) of the biometric source and the probabilities which the biometric source uses to generate symbols. Given a model of the source we can partition an observed biometric sequence into subsequences according to the model and then calculate the empirical probabilities in these subsequences as a fraction of digits that occur in the subsequences. The main problem therefore is to find the model of the biometric source.

In Chapter 5 we derive the procedure to find the best model that matches an observed biometric sequence pair. This procedure is based on the universal source coding method, i.e. on the Context-Tree Weighting (CTW) method of Willems, Shtarkov, and Tjalkens [88]. In order to obtain an efficient procedure, we focused on the implementation of the CTW method based on ratios of block probabilities, proposed in Willems and Tjalkens [91]. Our procedure for finding the best model therefore uses these ratios. The best model for an observed biometric sequence turns out to be the maximum a posteriori (MAP) model. In Chapter 5 we describe a procedure for deriving the MAP-model for two classes of general finite context sources, i.e. for tree sources and for the so-called class III models. The general finite context sources were described in [90]. The class III weighting methods are based on a richer model than tree sources, and therefore with this class we may obtain more reliable model estimates and, consequently, parameters of the source.

1.6.5 Chapter 6: Secret-Key Rate Estimation Based on Context Weighting Methods

In Chapter 6 we study a problem that has to be addressed before any practical biometric secrecy system is built, viz. how much secret information can be extracted or conveyed with a certain biometric modality. In Chapters 2 and 4 it was argued that the maximum secret-key rate in biometric secret generation systems and biometric systems with chosen keys is equal to the mutual information between the biometric enrollment and authentication sequences. These results hold for both i.i.d. biometric sources and stationary ergodic sources. Thus we have to estimate the mutual information between the biometric enrollment and authentication sequences. In Chapter 6 we focus on stationary ergodic biometrics.

The CTW method that we discuss in Chapter 5 can be used to estimate the required mutual information. Since the CTW method finds a good coding distribution and therefore the resulting codeword has a small redundancy, the codeword length, divided by the length of the source sequence, gives a good estimate of the entropy.

Thus while estimating the mutual information we can focus on estimating the corresponding entropies.

Biometric data such as iris codes, fingerprint minutiae maps, face patterns, PUFs, etc. are often modeled as realizations of two-dimensional processes, see e.g. Jain et al. [36]. Therefore we concentrate on estimating the mutual information and, correspondingly, the entropy for two-dimensional sources.

In order to apply CTW methods, we first show that the entropy of a stationary two-dimensional source is a limit of a series of conditional entropies. A similar result was obtained by Anastassiou and Sakrison [6]. Then we extend this result to the conditional entropy of one two-dimensional source given another one. Finally, we demonstrate that the CTW method also approaches the source entropy in the two-dimensional stationary ergodic case. This result carries over to conditional entropies and joint entropies in the two-dimensional stationary ergodic case.

Using the CTW methods and the results discussed in Chapter 6, we further estimate the maximum secret-key rate of speckle patterns from optical PUFs. We use the CTW method, referred to as class IV, and the class III context weighting method to obtain maximum secret-key rate estimates. We show that class III context weighting methods give more reliable and slightly higher estimates of the secret-key capacity than class IV methods. This result can be explained by noting that, on one hand, class III context weighting methods are based on a richer model class than class IV methods, but on the other hand, the size of PUF-sequences is large enough to compensate for the model redundancy.

The estimates that we obtain in Chapter 6 can be used to evaluate not only the suitability of a biometric modality for a certain system but also the performance of existing methods for secret-key extraction and secret-key binding.

1.7 Publications by the Author

1.7.1 Book Chapters

[BC-1] T. Ignatenko, F. Willems, G.J. Schrijen, B. Škorić, and P. Tuyls, In Book Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer, 2007. Chapter 13. Entropy Estimation for Optical PUFs Based on Context-Tree Weighting Methods, pp. 217-234.
See Chapter 6.

[BC-2] P. Tuyls, G.J. Schrijen, F. Willems, T. Ignatenko, and B. Škorić. In Book Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer, 2007. Chapter 16. Secure Key Storage with PUFs, pp. 269-292.

1.7.2 Journals

[JP-1] T. Ignatenko and F. Willems, "Leakage in Fuzzy Commitment Schemes," submitted to IEEE Transactions on Information Forensics and Security, 2009.
See Chapter 4.

[JP-2] T. Ignatenko and F. Willems, "Biometric Systems: Privacy and Secrecy Aspects," submitted to IEEE Transactions on Information Forensics and Security, September 19, 2008.
See Chapter 3.

1.7.3 Conference Proceedings

[IC-1] T. Ignatenko and F. Willems, "Privacy Leakage in Biometric Secrecy Systems," Proc. of 2008 Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, 23-26 September 2008, Monticello, IL, USA.
See Chapter 3.

[IC-2] T. Ignatenko and F. Willems, "On Privacy in Secure Biometric Authentication Systems," Proc. of 2007 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2007), 15-20 April 2007, Honolulu, HI, USA, pp. 121-124 (finalist of the best student paper award).
See Chapters 2 and 4.

[IC-3] T. Ignatenko, G.J. Schrijen, B. Škorić, P. Tuyls, and F. Willems, "Estimating the Secrecy-Rate of Physical Unclonable Functions with the Context-Tree Weighting Method," Proc. of 2006 IEEE International Symposium on Information Theory, 9-14 July 2006, Seattle, WA, USA, pp. 499-503.
See Chapter 6.

[IC-4] T. Ignatenko and F.Willems, "On the Security of XOR-Method in Biometric Authentication Systems," Proc. of the Twenty-Seventh Symposium on Information Theory in the Benelux, 8-9 June 2006, Noordwijk, The Netherlands, pp. 197-204.
See Chapters 2 and 4.

[IC-5] F.M.J. Willems,T.J. Tjalkens, and T. Ignatenko, "Context-Tree Weighting and Maximizing: Processing Betas," Proc. of Inaugural Workshop ITA (Information Theory and its Applications), 6-10 February 2006, UCSD Campus, La Jolla, CA, USA.
See Chapter 5.

[IC-6] T. Ignatenko, A.A.C.M. Kalker, M. van der Veen, A. Bazen, "Reference Point Detection for Improved Fingerprint Matching," Proc. of SPIE: Security,

Steganography, and Watermarking of Multimedia Contents VIII. Vol. 6072, 15-19 January 2006, San Jose, CA, USA, pp. 173-181.

[IC-7] P. Tuyls, E.A. Verbitskiy,T. Ignatenko, D.W.E. Schobben, and T. Akkermans, "Privacy Protected Biometric Templates: Acoustic Ear Identification," Proc. of SPIE Defense and Security Symposium. Vol. 5404, 12-13 April 2004, Orlando, FL, USA, pp. 176-182.

1.8 BASIS

The work presented in this thesis was part of a larger project called Biometric Authentication Supporting Invisible Security (BASIS). BASIS was supported by SenterNovem under project number IGC03003B.

The goal of this project was to investigate the possibilities of biometric authentication for securing the access to information and services in the personal environment, with a focus on user convenience and privacy protection. The project had to address (a) the problem of transparent biometric authentication (i.e. not requiring specific user actions) as a means to enhance user convenience, (b) the problem of anonymous biometric authentication (i.e. not requiring the storage of privacy sensitive biometric data) as a means to protect the user's privacy, and (c) the specific problems of the use of biometric authentication in the home environment. Transparent and anonymous biometrics, integrated in the private network of a home environment, were supposed to increase the user acceptance of the "ambient-intelligence scenario", as it would combine user convenience with a basic notion of trust in the ambient system. At the same time, it would guarantee a sufficient level of security to the providers of information and services. These three issues were addressed in three work packages, i.e. Transparent Biometrics, Template Protection and Home Biometrics. The work in this thesis corresponds to the Template Protection work package.

The BASIS project was formed as a joint project between three universities, i.e. University of Twente (UT), Eindhoven University of Technology (TU/e), and Centrum Wiskunde and Informatica (CWI).

Chapter 2

Secret Sharing and Biometric Systems

There are two ways to live: you can live as if nothing is a miracle; you can live as if everything is a miracle (Albert Einstein).

2.1 Introduction

The problem of generating secret-keys from biometric data is closely related to the concept of secret sharing, which was introduced by Maurer [47] and (slightly later) by Ahlswede and Csiszár [3]. In the source model of Ahlswede and Csiszár [3] two terminals observe two correlated sequences X^N and Y^N and aim at producing an as large as possible common secret S by interchanging a public message M. This message, to which we refer as helper data, should only provide a negligible amount of information on the secret. It was shown that the maximum secret-key rate in this model is equal to the mutual information $I(X;Y)$ between the observed sequences. The secret sharing concept is also closely related to the concept of common randomness generation that was studied by Ahlswede and Csiszár [4] and later extended with helper terminals by Csiszár and Narayan [16]. In common randomness schemes the requirement that the helper data should provide only a negligible amount of information on the generated randomness is dropped.

In a biometric system where two terminals need to generate a common secret key S from a biometric enrollment sequence X^N and a biometric authentication sequence Y^N, the helper-message M should provide no information on the generated secret, but it is also crucial that it provides as little information as possible on the biometric data. We call this information the privacy leakage. The interest in the privacy leakage is motivated by the fact that stolen biometric data result in a stolen identity. Moreover, compromised biometrics cannot be canceled and easily substituted as people have only limited resources of biometric data. Therefore the use of biometrics raises privacy concerns, as noted by Schneier [65], Ratha et al. [56], Prabhakar et al. [54], Linnartz and Tuyls [45], in DSP forum [83], etc.

This chapter is devoted to theoretical grounds for our further investigation of secret-key rates and privacy leakage in biometric secrecy systems. In this chapter

we, first, revisit the classical Ahlswede and Csiszár [3] problem of generating a secret from two dependent sequences. We focus on the biometric setting. We provide here the results on the largest achievable secret-key rate and the corresponding privacy leakage for the case when the biometric data are discrete, independent and identically distributed (i.i.d.). Our achievability proofs are expressed in terms of the Slepian-Wolf techniques that were presented by Cover [14], in which binning of typical sequences plays an important role. We extend these results to the stationary ergodic case. In the last part of the chapter we also discuss how typical biometric performance measures, i.e. the False Rejection Rate (FRR) and the False Acceptance Rate (FAR), relate to the results obtained for the biometric secret generation model.

2.2 Biometric Secret Generation Model

2.2.1 Definitions

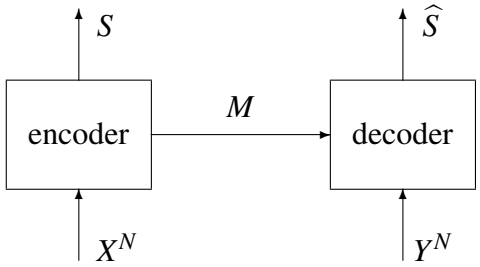


Figure 2.1: *Biometric secret generation.*

Consider a biometric system, see Fig. 2.1, which is based on a biometric source with distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$. This source produces an enrollment sequence $x^N = (x_1, x_2, \ldots, x_N)$ of N symbols from the finite alphabet $\mathcal{X}$ and an authentication sequence $y^N = (y_1, y_2, \ldots, y_N)$ of N symbols from the finite alphabet $\mathcal{Y}$. The sequence pair (x^N, y^N) occurs with probability

$$\Pr\{X^N = x^N, Y^N = y^N\} = \prod_{n=1}^{N} Q(x_n, y_n), \tag{2.1}$$

for all $x^N \in \mathcal{X}^N$ and $y^N \in \mathcal{Y}^N$, in other words, the sequence pairs (X_n, Y_n), $n = 1, 2, \ldots, N$ are i.i.d. according to $Q(x,y)$. The biometric sequences X^N and Y^N are in general not independent of each other.

Next consider an encoder that observes the enrollment sequence X^N. From this sequence the encoder generates a secret $S \in \mathcal{S} = \{1, 2, \ldots, |\mathcal{S}|\}$ and a public helper-message $M \in \mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$. The helper-message is sent to a decoder. Hence

$$(S, M) \quad = \quad e(X^N), \tag{2.2}$$

where $e(\cdot)$ is the deterministic encoder mapping. The decoder, on its turn, observes the authentication sequence Y^N and produces an estimate $\widehat{S}$ of the secret S using the received helper-message M and the observed sequence Y^N, hence

$$\widehat{S} \;=\; d(Y^N, M), \tag{2.3}$$

where $d(\cdot)$ is the deterministic decoder mapping.

It is the goal of the encoder and decoder to produce as much key information as possible, in such a way that the secret key is close to uniform, that the probability that the estimated secret $\widehat{S}$ is not equal to the secret S is close to zero and that the information that the helper-message reveals about the secret is negligible. In this thesis log denotes the base 2 logarithm.

Definition 2.1 *A secret-key rate R_s, for $R_s \geq 0$, is called achievable if for all $\delta > 0$ and all N large enough, there exist encoders and decoders such that*

$$\begin{aligned} & & \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ \frac{1}{N}H(S) + \delta &\geq \frac{1}{N}\log|\mathcal{S}| &\geq R_s - \delta, \\ & & \frac{1}{N}I(S;M) &\leq \delta. \end{aligned} \tag{2.4}$$

2.2.2 Statement of Result

The main result of this chapter is stated in the next theorem. This is actually the Ahlswede and Csiszár [3] result but put in a biometric setting.

Theorem 2.1 *For a biometric secret generation model the largest achievable secret-key rate R_s is equal to $I(X;Y)$.*

This theorem was proven by Ahlswede and Csiszár [3] using strong typicality. However, for the sake of completeness, we will give a proof of this result. Unlike the original proof of Ahlswede and Csiszár [3], our proof is based on weak typicality. This proof will be the core part of the achievability proofs presented in the later chapters of this thesis where we deal with more general biometric settings.

The difference between weak and strong typicality can be summarized in the following lines. Weak typicality requires that the empirical entropy of a sequence is close to the true entropy, while strong typicality requires that the relative frequency of each possible outcome is close to the corresponding probability. Although strong typicality is more powerful than weak typicality as a tool used to prove theorems for memoryless problems, it cannot be used for continuous alphabets while weak typicality can be. Therefore using proofs based on weak typicality make it easy to extend the results for discrete biometric sources to continuous biometric sources. Although in

this thesis we only concentrate on discrete i.i.d. data, we see the extension to sources with memory as a future research direction. Another important difference is the joint typicality property. In the case of strong typicality, joint typicality guarantees that if two sequences u^N and x^N are jointly typical, and Y^N is some random sequence drawn according to some distribution $\{Q(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$, then with probability close to one u^N, x^N and Y^N are also jointly typical if $U \to X \to Y$, see Cover and Thomas [13], p. 436. This property does not hold for weak typicality. However, as we will see in the next chapter, we can modify a typical set in such a way that a similar property also holds when weakly typical sequences are used.

2.3 Proof of Thm. 2.1

2.3.1 Jointly Typical Sequences

First, we give the definition of jointly typical sequences and their main properties, since typicality is an important notion in our proofs. For more details and the proofs of the properties see e.g. Cover and Thomas [13], Section 14.2.

Definition 2.2 (Set of jointly typical sequences, [13]) *Let $(X_1, X_2, \ldots, X_K)$ be a finite collection of K discrete random variables with some joint distribution $\{P(x_1, x_2, \ldots, x_K), (x_1, x_2, \ldots, x_K) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \ldots \times \mathcal{X}_K\}$. The set $\mathcal{A}_\varepsilon^{(N)}(X_1, X_2, \ldots, X_K)$ of ε-typical N-sequences $(x_1^N, x_2^N, \ldots, x_K^N)$ is defined as*

$$\mathcal{A}_\varepsilon^{(N)}(X_1, X_2, \ldots, X_K) \triangleq \Big\{(x_1^N, x_2^N, \ldots, x_K^N) : \Big| -\frac{1}{N}\log P(v^N) - H(V)\Big| < \varepsilon, \quad \forall V \subseteq \{X_1, X_2, \ldots, X_K\}\Big\}, \tag{2.5}$$

where v^N is a subset of N-sequences $(x_1^N, x_2^N, \ldots, x_K^N)$ corresponding to V, and $P(v^N) = \prod_{n=1}^N P(v_n)$. Moreover, let $V, W \subseteq \{X_1, X_2, \ldots, X_K\}$, then for a given w^N we define

$$\mathcal{T}_\varepsilon^{(N)}(V|w^N) \triangleq \{v^N : (v^N, w^N) \in \mathcal{A}_\varepsilon^{(N)}(V, W)\}. \tag{2.6}$$

Lemma 2.1 (Properties of jointly typical sequences, [13]) *For any $\varepsilon > 0$*

1. *$\forall V \subseteq \{X_1, X_2, \ldots, X_K\}$ and N large enough*

$$\Pr\{\mathcal{A}_\varepsilon^{(N)}(V)\} \geq 1 - \varepsilon. \tag{2.7}$$

2. *$\forall V \subseteq \{X_1, X_2, \ldots, X_K\}$*

$$|\mathcal{A}_\varepsilon^{(N)}(V)| \leq 2^{N(H(V)+\varepsilon)}. \tag{2.8}$$

3. *Let* $V,W \subseteq \{X_1,X_2,\ldots,X_K\}$, *then*

$$|\mathcal{T}_\varepsilon^{(N)}(V|w^N)| \quad \leq \quad 2^{N(H(V|W)+2\varepsilon)}. \tag{2.9}$$

4. *Let* $K=2$. *If* $(\tilde{X_1}^N,\tilde{X_2}^N)$ *are drawn according to* $P(x_1^N)P(x_2^N)$, *i.e.* $\tilde{X_1}^N$ *and* $\tilde{X_2}^N$ *are independent sequences with the same marginals as* $P(x_1^N,x_2^N)$, *then*

$$\Pr\{(\tilde{X_1}^N,\tilde{X_2}^N) \in \mathcal{A}_\varepsilon^{(N)}(X_1,X_2)\} \quad \leq \quad 2^{-N(I(X_1;X_2)-3\varepsilon)}. \tag{2.10}$$

■

2.3.2 Achievability Proof

Fix an $\varepsilon > 0$ and let $\mathcal{A}_\varepsilon^{(N)}(X)$ and $\mathcal{A}_\varepsilon^{(N)}(X,Y)$ be the sets of ε-typical and jointly ε-typical N-sequences based on the joint distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ of the XY-source. We prove the achievability with a random labeling argument.

Random labeling: The coding strategy is as follows. Let us define a random partition of space $\mathcal{X}^N$, viz. space of typical X^N-sequences, into $|\mathcal{M}|$ bins. An encoder independently assigns to each sequence x^N a helper-label (index of the bin) $m \in \{1,2,\ldots,|\mathcal{M}|\}$ with probability

$$\Pr\{M(x^N)=m\} \quad = \quad 1/|\mathcal{M}|. \tag{2.11}$$

Furthermore, we define the second random partition over $\mathcal{X}^N$ with $|\mathcal{S}|$ bins, and the encoder also assigns to each sequence x^N a randomness-label (bin-index of this second partition) $s \in \{1,2,\ldots,|\mathcal{S}|\}$ with probability

$$\Pr\{S(x^N)=s\} \quad = \quad 1/|\mathcal{S}|. \tag{2.12}$$

Encoding: The encoder observes the sequence x^N and determines the secret and helper labels s and m. If x^N is not a typical sequence, an error is declared. Moreover, the encoder checks if there exists another X-sequence with the same label pair, if so also an error is declared. The encoder sends the helper label m to the decoder.

Decoding: The decoder, after having observed y^N, looks for a unique sequence x^N with label m such that $(x^N,y^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)$. If such a sequence is found, the decoder emits its randomness-label $\widehat{s}=S(x^N)$, otherwise an error is declared.

Error probability: The first problem now is to determine the error probability averaged over the random labeling. An error at the encoder can occur in the following situations

1) if $x^N \notin \mathcal{A}_\varepsilon^{(N)}(X)$,

2) the sequence x^N with labels m and s is not unique.

Moreover, an error at the decoder would occur in the following situations

3) if $(x^N, y^N) \notin \mathcal{A}_\varepsilon^{(N)}(X,Y)$,

4) there exists a sequence $x'^N \neq x^N$ such that $M(x'^N) = M(x^N)$ and $(x'^N, y^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)$.

The decoder error probability averaged over the ensemble of random labelings satisfies

$$\begin{aligned}
\overline{P_{d,\varepsilon}} &\leq \Pr\{(X^N,Y^N) \notin \mathcal{A}_\varepsilon^{(N)}(X,Y) \cup \Big(\bigcup_{x^N \neq X^N : (x^N,Y^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)} M(x^N) = M(X^N) \Big)\} \\
&\overset{(a)}{\leq} \Pr\{(X^N,Y^N) \notin \mathcal{A}_\varepsilon^{(N)}(X,Y)\} + \sum_{x^N \neq X^N : (x^N,Y^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)} \Pr\{M(x^N) = M(X^N)\} \\
&\overset{(b)}{=} \Pr\{(X^N,Y^N) \notin \mathcal{A}_\varepsilon^{(N)}(X,Y)\} + |\{x^N \neq X^N : (x^N,Y^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)\}| \cdot \frac{1}{|\mathcal{M}|} \\
&\leq \Pr\{(X^N,Y^N) \notin \mathcal{A}_\varepsilon^{(N)}(X,Y)\} + |\{x^N : (x^N,Y^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)\}| \cdot \frac{1}{|\mathcal{M}|} \\
&\overset{(c)}{\leq} \varepsilon + 2^{N(H(X|Y)+2\varepsilon)} \cdot \frac{1}{|\mathcal{M}|} \\
&\leq 2\varepsilon, \qquad (2.13)
\end{aligned}$$

for N large enough if we we take $\frac{1}{N}\log|\mathcal{M}| = H(X|Y) + 3\varepsilon$. Here step (a) follows from the union bound, (b) follows from random labeling, and (c) follows from (2.7) and (2.9).

For the encoder error probability averaged over the ensemble of random labelings we can write

$$\begin{aligned}
\overline{P_{e,\varepsilon}} &\leq \Pr\{X^N \notin \mathcal{A}_\varepsilon^{(N)}(X) \cup \Big(\bigcup_{x^N \neq X^N : x^N \in \mathcal{A}_\varepsilon^{(N)}(X)} M(x^N) = M(X^N) \cap S(x^N) = S(X^N) \Big)\} \\
&\overset{(a)}{\leq} \Pr\{X^N \notin \mathcal{A}_\varepsilon^{(N)}(X)\} + \sum_{x^N \neq X^N : x^N \in \mathcal{A}_\varepsilon^{(N)}(X)} \Pr\{M(x^N) = M(X^N)\} \cdot \Pr\{S(x^N) = S(X^N)\} \\
&\overset{(b)}{\leq} \Pr\{X^N \notin \mathcal{A}_\varepsilon^{(N)}(X)\} + |\{x^N : x^N \in \mathcal{A}_\varepsilon^{(N)}(X)\}| \cdot \frac{1}{|\mathcal{M}|} \cdot \frac{1}{|\mathcal{S}|} \\
&\overset{(c)}{\leq} \varepsilon + 2^{N(H(X)+\varepsilon)} \cdot \frac{1}{|\mathcal{M}|} \cdot \frac{1}{|\mathcal{S}|} \\
&\leq 2\varepsilon, \qquad (2.14)
\end{aligned}$$

for N large enough if we take $\frac{1}{N}\log|\mathcal{S}| = I(X;Y) - \varepsilon$ (and $\frac{1}{N}\log|\mathcal{M}| = H(X|Y) + 3\varepsilon$). Here step (a) follows from the union bound, (b) follows from random labeling, and step (c) follows from (2.8).

Since $\overline{P_{d,\varepsilon}} + \overline{P_{e,\varepsilon}} \leq 4\varepsilon$ for N large enough, this implies that for N large enough, there exist at least two random labelings such that $P_{d,\varepsilon} + P_{e,\varepsilon} \leq 4\varepsilon$. Now we focus on these codes for the rest of the proof. Note that for these codes

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq 4\varepsilon, && (2.15)\\ H(M) &\leq \log|\mathcal{M}| = N(H(X|Y) + 3\varepsilon), && (2.16)\\ H(S) &\leq \log|\mathcal{S}| = N(I(X;Y) - \varepsilon). && (2.17) \end{aligned}$$

Since the encoder requires the secret and helper labels to be unique for x^N, we can assume that it can reconstruct the sequence based on the label pair. Now let $\widehat{X_e^N}$ be the encoder's estimate of X^N based on S and M, then we find that

$$\begin{aligned} H(X^N) &= H(X^N, S, M) \\ &= H(S) + H(M|S) + H(X^N|S,M) \\ &\leq H(S) + H(M) + H(X^N|S,M,\widehat{X_e^N}) \\ &\leq H(S) + H(M) + NP_{e,\varepsilon}\log|\mathcal{X}| + 1, && (2.18) \end{aligned}$$

where the last step follows from Fano's inequality, see e.g. Cover and Thomas [13], p. 205.

Hence the entropy of the secret is lower bounded by

$$\begin{aligned} H(S) &\geq H(X^N) - H(M) - NP_{e,\varepsilon}\log|\mathcal{X}| - 1 \\ &\overset{(a)}{\geq} NH(X) - N(H(X|Y) + 3\varepsilon) - NP_{e,\varepsilon}\log|\mathcal{X}| - 1 \\ &\geq N(I(X;Y) - 3\varepsilon - 4\varepsilon\log|\mathcal{X}| - \frac{1}{N}) \\ &\overset{(b)}{=} N(\frac{1}{N}\log|\mathcal{S}| - 2\varepsilon - 4\varepsilon\log|\mathcal{X}| - \frac{1}{N}), && (2.19) \end{aligned}$$

where (a) follows from the fact that X^N is an i.i.d. sequence and from (2.16), and (b) from (2.17).

Next we study the secrecy

$$\begin{aligned} I(S;M) &= H(S) + H(M) - H(S,M) \\ &= H(S) + H(M) - H(S,M,X^N) + H(X^N|S,M) \\ &\overset{(a)}{=} H(S) + H(M) - H(X^N) + H(X^N|S,M,\widehat{X_e^N}) \\ &\overset{(b)}{\leq} H(S) + H(M) - NH(X) + NP_{e,\varepsilon}\log|\mathcal{X}| + 1 \\ &\overset{(c)}{\leq} N(2\varepsilon + 4\varepsilon\log|\mathcal{X}| + \frac{1}{N}), && (2.20) \end{aligned}$$

where step (a) holds, since S and M are functions of X^N, and $\widehat{X_e^N}$ is a function of S and M, (b) follows from the fact that X^N is an i.i.d. sequence and from Fano's inequality, and (c) follows from (2.16) and (2.17).

Thus, letting $\varepsilon \downarrow 0$ and $N \to \infty$, we obtain the achievability from (2.15), (2.17), (2.19), and (2.20).

2.3.3 Converse

Assume that the rate R_s is achievable. Now we consider the entropy of the secret

$$\begin{aligned} H(S) &= I(S;Y^N,M)+H(S|Y^N,M) \\ &\overset{(a)}{=} I(S;M)+I(S;Y^N|M)+H(S|Y^N,M,\widehat{S}) \\ &\leq I(S;M)+H(Y^N)-H(Y^N|M,S,X^N)+H(S|\widehat{S}) \\ &\overset{(b)}{\leq} I(S;M)+H(Y^N)-H(Y^N|X^N)+\Pr\{\widehat{S}\neq S\}\log|\mathcal{S}|+1 \\ &\overset{(c)}{\leq} I(S;M)+I(X^N;Y^N)+N\Pr\{\widehat{S}\neq S\}\log|\mathcal{X}|+1 \\ &\overset{(d)}{\leq} N(\delta+I(X;Y)+\delta\log|\mathcal{X}|+\frac{1}{N}), \end{aligned} \tag{2.21}$$

where step (a) holds, since $\widehat{S}$ is a function of M and Y^N, (b) follows from the fact that S and M are functions of X^N and from Fano's inequality, (c) holds, since the encoder is deterministic and therefore $|\mathcal{S}| \leq |\mathcal{X}|^N$ (possibly) after renumbering, and step (d) follows from the fact that (X^N,Y^N) is a sequence of i.i.d. pairs and the fact that for achievable rates R_s we have that $I(S;M) \leq N\delta$ and $\Pr\{\widehat{S}\neq S\} \leq \delta$.

Then for achievable rates R_s we obtain

$$R_s - 2\delta \leq \frac{1}{N}H(S) \leq I(X;Y)+\delta+\delta\log|\mathcal{X}|+\frac{1}{N}. \tag{2.22}$$

Finally, letting $\delta \downarrow 0$ and $N \to \infty$, we obtain the converse.

2.4 Privacy Leakage for Codes Achieving the Maximum Secret-Key Rate

In biometric secrecy systems we are also interested in the amount of information that the helper data leak about the biometric data, which is called privacy leakage. We define $I(M;X^N)/N$ to be the privacy leakage per biometric source symbol. Now we concentrate on codes that we have determined in the achievability proof of Thm. 2.1. The following proposition gives us the privacy leakage per source symbol corresponding to the maximum achievable secret-key rate in the biometric secret generation model when such codes are used. A similar result for error-correcting codes was

also demonstrated in Dodis et al. [22] and Smith [72] and for binary error-correcting codes in Tuyls and Goseling [79]. The result obtained in this proposition is somewhat more general.

Proposition 2.1 *In a biometric secret generation model, for the codes that demonstrate the achievability of secret-key rate $I(X;Y)$, the privacy leakage per source symbol is equal to $H(X|Y)$.*

Proof of Prop. 2.1:
Note that, since M is a function of X^N, we have that $I(X^N;M) = H(M)$. Hence the privacy leakage is equal to the entropy of the helper data. From the achievability proof corresponding to Thm. 2.1, we can write for the entropy of the helper data, using (2.18), (2.17) and the fact that X^N is an i.i.d. sequence, that

$$\begin{aligned} I(X^N;M) = H(M) &\geq H(X^N) - H(S) - NP_{e,\varepsilon}\log|\mathcal{X}| - 1 \\ &\geq N(H(X|Y) + \varepsilon - 4\varepsilon\log|\mathcal{X}| - \frac{1}{N}). \end{aligned} \tag{2.23}$$

On the other hand, for the helper data (2.16) holds, and thus

$$I(X^N;M) = H(M) \leq N(H(X|Y) + 3\varepsilon). \tag{2.24}$$

Then, dividing both sides of the above expressions by N and letting $\varepsilon \downarrow 0$ and $N \to \infty$, we finalize the proof.

■

The above proposition gives us the privacy leakage per source symbol if we apply the coding scheme outlined in the achievability proof. However, it may be possible to achieve a privacy leakage that is smaller if an alternative coding scheme is applied. Note that in the biometric setting we are interested in a system where the helper data leak as little information as possible about the biometric data. Therefore now the question arises what the minimum achievable privacy leakage in a biometric secrecy system is for a fixed secret-key rate. The answer to this question, though, we postpone to the next chapter.

2.5 Stationary Ergodic Case

In the previous sections we considered the case when the biometric data source is i.i.d. Now we argue that the results, similar to those derived for the i.i.d. case, hold for biometric sequences that are generated by jointly stationary ergodic sources. In Csiszár and Narayan [17] it was also argued that the i.i.d. results on strong secrecy capacity for multiple terminals can be extended to the stationary ergodic case.

Let (X^N, Y^N) be a jointly stationary ergodic sequence pair and define

$$\begin{aligned} H_\infty(X) &\triangleq \lim_{N\to\infty} \frac{1}{N} H(X_1, X_2, \ldots, X_N), \\ H_\infty(Y) &\triangleq \lim_{N\to\infty} \frac{1}{N} H(Y_1, Y_2, \ldots, Y_N), \\ H_\infty(X,Y) &\triangleq \lim_{N\to\infty} \frac{1}{N} H(X_1, Y_1, X_2, Y_2, \ldots, X_N, Y_N), \\ H_\infty(X|Y) &\triangleq H_\infty(X,Y) - H_\infty(Y), \\ I_\infty(X;Y) &\triangleq H_\infty(X) + H_\infty(Y) - H_\infty(X,Y). \end{aligned} \tag{2.25}$$

Then the following theorem holds.

Theorem 2.2 *For a jointly stationary ergodic sequence pair (X^N, Y^N) the result of Thm. 2.1 holds if we replace $I(X;Y)$ with $I_\infty(X;Y)$. Moreover, for the codes that demonstrate the achievability of secret-key rate $I_\infty(X;Y)$, the privacy leakage per source symbol is equal to $H_\infty(X|Y)$.*

Proof of Thm. 2.2:

The proof of this theorem is similar to the proofs of Thm. 2.1 and Prop. 2.1. The difference is that now the definitions of typical sets are as in Cover [14].

Moreover, in both the achievability and converse proofs, the steps involving equalities $H(X^N) = NH(X)$ and $I(X^N;Y^N) = NI(X;Y)$ have to be adjusted. Using the definitions of the stationary ergodic sequences and noting that the achievability proof and the converse hold for N large enough, we substitute $NH_\infty(X)$ for $H(X^N)$ and $I_\infty(X;Y)$ for $I(X^N;Y^N)$ in (2.19), (2.20), (2.21) and (2.23).

■

2.6 FRR and FAR in Biometric Secret Generation Models

The FRR and FAR are typical performance measures for biometric systems. Recall that in standard biometric authentication systems the FRR is defined as the probability that an authorized individual cannot get access to a system, while the FAR is defined as the probability that an unauthorized individual (an imposter) is granted access.

For a biometric secret generation system, described in Section 2.2.1, we considered the probability that the estimated secret $\widehat{S}$ is not equal to the generated secret S. When these secrets are not equal, an authorized individual is rejected. Thus the probability that $\widehat{S}$ is not equal to S is equivalent to the FRR. Hence, according to the definition of achievability, we obtain that for the biometric secret generation model for rates up to $I(X;Y)$ there exist codes that achieve

$$\text{FRR} = \Pr\{S \neq \widehat{S}\} \quad \leq \quad \delta, \tag{2.26}$$

for any $\delta > 0$ and all N large enough.

Now consider an imposter who would like to obtain access to the system. He provides his biometric data during authentication. False acceptance would occur if the secret estimated by the system based on these presented data is equal to the secret generated for the authorized individual. Next we look at the probability of such an error.

The biometric secret generation system, described in Section 2.2.1, is based on a biometric source with distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$. Consider a biometric imposter sequence $\tilde{y}^N = (\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_N)$ produced by the biometric source according to $\{Q(y), y \in \mathcal{Y}\}$, where $Q(y) = \sum_x Q(x,y)$. The biometric imposter sequences have the same distribution as the biometric sequences of an authorized individual. However, since they come from different persons, we can assume that the biometric source sequences X^N and $\tilde{Y}^N$ are independent. Then the sequence pair $(x^N, \tilde{y}^N)$ occurs with probability

$$\Pr\{X^N = x^N, \tilde{Y}^N = \tilde{y}^N\} \quad = \quad \prod_{n=1}^{N} Q(x_n)Q(\tilde{y}_n). \tag{2.27}$$

In this way sequence pairs $(X_n, \tilde{Y}_n), n = 1, 2, \ldots, N$ are i.i.d. according to $Q(x)Q(y)$.

Now consider the situation when the decoder observes a biometric imposter sequence $\tilde{Y}^N$ and forms an estimate

$$\widetilde{S} \quad = \quad d(\tilde{Y}^N, M). \tag{2.28}$$

We are interested now in the probability that the imposter is granted access to the system, i.e. in the FAR. This probability is defined as $\Pr\{\widetilde{S} = S\}$. The following theorem provides us with an upper bound on the FAR that can be achieved in the biometric secret generation model.

Theorem 2.3 *For a biometric secret generation model, that is based on a source with distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$, for all $\delta > 0$ and all N large enough there exist codes with positive rates up to $I(X;Y)$ such that*

$$FAR = \Pr\{S = \widetilde{S}\} \quad \leq \quad \delta. \tag{2.29}$$

Proof of Thm. 2.3
Assume that the positive rate R_s is achievable, and consider the secret entropy

$$\begin{aligned} H(S) &= I(S; \tilde{Y}^N, M) + H(S|\tilde{Y}^N, M) \\ &\overset{(a)}{\leq} I(S;M) + I(\tilde{Y}^N; X^N) + \Pr\{\widetilde{S} \neq S\} \log |\mathcal{S}| + 1 \\ &\overset{(b)}{\leq} N\delta + \Pr\{\widetilde{S} \neq S\} \log |\mathcal{S}| + 1, \end{aligned} \tag{2.30}$$

where step (a) follows from Fano's inequality, from the fact that S and M are functions of X^N, and (b) follows from the fact that for achievable rates R_s we have that $I(S;M) \leq N\delta$ and from the fact that X^N and $\tilde{Y}^N$ are independent.

Then we can write

$$\frac{1}{N}\log|\mathcal{S}| - \delta \leq \frac{1}{N}H(S) \leq \delta + \frac{1}{N}\Pr\{\widetilde{S} \neq S\}\log|\mathcal{S}| + \frac{1}{N}. \tag{2.31}$$

Rearranging the above expression and noting that $FAR = 1 - \Pr\{\widetilde{S} \neq S\}$, we obtain

$$\text{FAR} \leq \frac{2N\delta + 1}{\log|\mathcal{S}|} \leq \frac{2\delta + 1/N}{R_s - \delta}, \tag{2.32}$$

where the last step follows from the definition of achievable rates.

Finally, letting $\delta \downarrow 0$ and $N \to \infty$, we obtain the proof.

■

The result provided in the above theorem states that we can obtain an arbitrarily small FAR in biometric secret generation systems for rates up to $I(X;Y)$. However, this is an asymptotic result, which means that arbitrarily small FARs can be obtained for infinitely long biometric sequences.

To obtain a better, non-asymptotic, characterization of the FAR, we consider the problem from a different prospective. From the achievability proof of Thm. 2.1 it follows that the estimate of the generated secret key will be equal to the generated key only if a biometric authentication sequence is jointly typical with the biometric enrollment sequence. Therefore an imposter can try to generate a biometric sequence $\tilde{Y}^N$ that is jointly typical with X^N according to the distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$. However, from the properties of jointly typical sequences, see (2.10), it follows that

$$\text{FAR} \leq \Pr\{(X^N, \tilde{Y}^N) \in \mathcal{A}_\varepsilon^{(N)}(X,Y)\} \leq 2^{-N(I(X;Y)-3\varepsilon)}. \tag{2.33}$$

Note that $I(X;Y)$ corresponds to the maximum secret-key rate achievable in the biometric secret generation system. Therefore we may conclude that generating a sequence which will be jointly typical with X^N is at least as hard as guessing the secret key (note that the secret-key rates achievable in a biometric secret generation model are smaller than or equal to $I(X;Y)$).

The result presented above holds on average for biometric sequences x^N. Moreover, we can obtain even stronger result stating that the upper bound on the FAR holds for all sequences x^N. Consider a specific biometric enrollment sequence x^N. An imposter generates a sequence $\tilde{Y}^N$ according to $\{Q(y), y \in \mathcal{Y}\}$. Then the FAR will be upper bounded by the probability that the imposter sequence $\tilde{Y}^N$ is jointly

typical with x^N. We can write

$$\begin{aligned}
\Pr\{\tilde{Y}^N \in \mathcal{T}_\varepsilon^{(N)}(Y|x^N)\} &= \sum_{y^N \in \mathcal{T}_\varepsilon^{(N)}(Y|x^N)} Q(y^N) \\
&= \sum_{y^N \in \mathcal{T}_\varepsilon^{(N)}(Y|x^N)} Q(y^N|x^N) \frac{Q(x^N)Q(y^N)}{Q(x^N,y^N)} \\
&\overset{(a)}{\leq} 2^{-N(I(X;Y)-3\varepsilon)} \sum_{y^N \in \mathcal{T}_\varepsilon^{(N)}(Y|x^N)} Q(y^N|x^N) \\
&\leq 2^{-N(I(X;Y)-3\varepsilon)}, \qquad (2.34)
\end{aligned}$$

where step (a) follows from typicality.

It is interesting to see that the upper bound on the FAR is the inverse of the identification capacity in biometric identification systems without secrecy constraints found in Willems et al. [86] and Schmid and O'Sullivan [63].

Note that the results presented in this section also hold for the stationary ergodic case.

2.7 Conclusions

In this chapter we have considered the classical Ahlswede-Csiszár secret generation model in a biometric setting. The maximum secret-key rate achievable for this model is equal to $I(X;Y)$. Although this result was proved using strong typicality before by Ahlswede and Csiszár [3], for the sake of completeness we have provided a proof here too. Our proof, which is based on weak typicality, will be the core part of the achievability proofs given in the later chapters of this thesis where we deal with more general biometric settings.

We have also demonstrated that the privacy leakage that corresponds to the maximum secret-key rate in biometric secret generation systems is roughly equal to $H(X|Y)$. A similar result but for error-correcting codes was also obtained in Dodis et al. [22], Smith [72] and Tuyls and Goseling [79]. The question whether it is possible to achieve smaller privacy leakage will be addressed in the next chapter.

Next we have investigated the question of which FRR and FAR can be achieved in biometric secret generation systems. We have shown that these error probabilities can be made arbitrarily small for positive secret-key rates of less than or equal to $I(X;Y)$.

The biometric secret generation model was studied for discrete i.i.d. biometric sources. We could also extend the i.i.d. results to stationary ergodic sources.

It should be noted that the results that we have presented in this chapter are asymptotic, and thus hold for infinitely long biometric sequences.

Chapter 3

Privacy Leakage in Biometric Secrecy Systems

Look deep into nature, and then you will understand everything better (Albert Einstein).

3.1 Introduction

3.1.1 Motivation

In the previous chapter we have started the analysis of biometric secret generation systems. We have considered the setup where the system was optimized with respect to achieving the maximum secret-key rate, and for this case we analyzed the corresponding privacy leakage. In the current chapter we consider a more general situation. As noted in the introduction to the previous chapter, the use of biometrics brings about privacy concerns, and therefore in a biometric setting the goal is to minimize the privacy leakage for a given secret-key rate. Thus we are interested in finding the trade-off between the secret-key rate and the privacy leakage.

In the overview paper of Jain et al. [37] it was noted that biometric secrecy systems can be subdivided into those that generate secret keys from biometric data and those that bind secret keys to biometric data. Therefore in this chapter we consider two types of biometric secrecy systems, i.e. systems with generated secret keys and systems with chosen (bound) secret keys.

Privacy concerns raised by Schneier [65], Ratha et al. [56], Prabhakar et al. [54], Linnartz and Tuyls [45], in the DSP forum [83], etc. led to the proposal of various techniques in the last decade. Implementations of biometric secrecy systems include methods based on various forms of Shamir's secret sharing [67]. These methods are used to harden passwords with biometric data, see e.g. Monrose et al. [49], [48]. The methods based on error-correcting codes, which bind uniformly distributed secret keys to biometric data and which tolerate (biometric) errors in these secret keys, were formally defined by Juels and Wattenberg [41]. Less formal approaches can be

found in Davida et al. [19], [18]. Error-correction based methods were extended to the set difference metric developed by Juels and Sudan [40]. Some other approaches focus on continuous biometric data and provide solutions, which rest on quantization of biometric data as in Linnartz and Tuyls [45], Denteneer et al. [20] (with emphasis on reliable components), Teoh et al. [74], and Buhan et al. [10]. Finally, a formal approach for designing secure biometric systems for three metric distances (Hamming, edit, and set), called fuzzy extractors, was introduced in Dodis et al. [22] and Smith [72] and further elaborated in [23]. Fuzzy extractors were subsequently implemented for different biometric modalities in Sutcu et al. [73], Draper et al. [25], etc.

A problem of the existing practical systems is that sometimes they lack formal security proofs and rigorous security formulations. On the other hand, the systems that do provide formal proofs actually focus on secrecy only while neglecting privacy. For instance, Frykholm and Juels [27] only provide their analysis for the secrecy of the keys. Similarly, Linnartz and Tuyls [45] offer information-theoretical analysis for the secrecy leakage but no corresponding privacy leakage analysis. Dodis et al. [22], [23] and Smith [72] were the first to address the problem of code construction for biometric secret-key generation in a systematic information-theoretical way. Although their works provide results on the maximum secret-key rates in biometric secrecy systems, they also focus on the corresponding privacy leakage. In a biometric setting, however, the goal is to minimize the privacy leakage and, more specifically, to minimize the privacy leakage for a given secret-key rate. The need for quantifying the exact information leakage on biometric data was also stated as an open question in Sutcu et al. [73]. In the current chapter we study the fundamental trade-off between the secret-key rate and privacy leakage in biometric secrecy systems.

Recently, Prabhakaran and Ramchandran [55], and Gündüz et al. [32] studied source coding problems where the issue of (biometric) leakage was addressed. In their work, though, it is not the intention of the users to produce a secret but to communicate a (biometric) source sequence in a secure way from the first to the second terminal.

3.1.2 Eight Models

In this chapter we consider four biometric settings. The first one is again the standard Ahlswede-Csiszár secret-generation setting that we considered in the previous chapter. There two terminals observe two correlated biometric sequences. It is their objective to form a common secret by interchanging a public message. This message should contain only a negligible amount of information about the secret, but, in addition, we require here that it should leak as little information as possible about the biometric data. For this first case the fundamental trade-off between the secret-key rate and the privacy-leakage rate will be determined. It should be noted that this re-

sult is in some way similar to and a special case of the SK (secret-key) part of Thm. 2.4 in Csiszár and Narayan [16].

The second setting that we consider is a biometric model with chosen keys, where the secret key is not generated by the terminals but independently chosen at the encoder side and conveyed to the decoder. This model corresponds to key-binding described in the overview paper of Jain et al. [37]. For the chosen-key setting we will also determine the fundamental rate-leakage balance.

The other two biometric settings that we analyze correspond to biometric secrecy systems with zero privacy leakage. Solely, biometrics may not always satisfy the security and privacy requirements of certain systems. In this case the performance of biometric systems can be enhanced using standard cryptographic keys. Although this reduces user convenience, since e.g. extra cryptographic keys need to be stored on external media or memorized, such systems may offer a higher level of secrecy and privacy. Practical methods in this direction include attempts to harden the fuzzy vault scheme of Juels and Sudan [40] with passwords by Nandakumar et al. [50] and dithering techniques that were proposed by Buhan et al. [9]. In our model we assume that only the two terminals have access to an extra independent private key, which is observed together with the correlated biometric sequences. The private key is used to achieve a negligible amount of privacy leakage (zero leakage). We investigate both the secret generation model with zero-leakage and the model with chosen keys and zero-leakage. For both models we will determine the trade-off between the private-key rate and the resulting secret-key rate.

For the four settings outlined above, the fundamental balance will be determined for both unconditional and conditional privacy leakage. This results in eight biometric models. Unconditional leakage corresponds to the unconditional mutual information between the helper data and the biometric enrollment sequence, while conditional leakage relates to this mutual information conditioned on the secret.

3.1.3 Chapter Outline

This chapter is organized as follows. First we start with an example that demonstrates that time sharing does not result in an optimal trade-off between secret-key rate and privacy leakage. Then in Section 3.2 we continue with the formal definitions of all the eight models discussed above. In Section 3.3 we state the results that will be derived in this chapter. We will determine the achievable regions for all the eight settings. The following section, i.e. Section 3.4, discusses the properties of the achievable regions that play a role here. Section 3.5 provides the proofs of our results. Finally, in Section 3.6 we discuss the relations between the found achievable regions and in Section 3.7 we present the conclusions.

3.1.4 An Example

Before we turn to a more formal part of this chapter, we first discuss an example. Consider an i.i.d. biometric binary symmetric double source $\{Q(x,y), x \in \{0,1\}, y \in \{0,1\}\}$ with crossover probability $0 \leq q \leq 1/2$ such that $Q(x,y) = (1-q)/2$, for $y = x$ and $Q(x,y) = q/2$, for $y \neq x$. In this example we use $q = 0.1$. In the classical Ahlswede-Csiszár [3] key-generation setting, considered in the previous chapter, the maximum secret-key rate for this biometric source is $R_s = I(X;Y) = 1 - h(q)$, where $h(\cdot)$ is the binary entropy function expressed in bits. The corresponding privacy-leakage rate in this case is $H(X|Y) = h(q)$. Then the ratio between rate and leakage is equal to $(1-h(q))/h(q) = 1.1322$.

Now suppose that we want to reduce the privacy-leakage rate to a fraction of α of its original size. We could apply a trivial method in which we use only a fraction α of the biometric symbols, but then the secret-key rate is also reduced to a fraction of α of its original size, and there is no effect on the rate-leakage ratio. A question now arises of whether it is possible to achieve a larger rate-leakage ratio at reduced leakage.

We will demonstrate next that we can achieve this goal using the binary Golay code as a vector quantizer. This code consists of 4096 codewords of length 23 and has minimum Hamming distance 3, and it is perfect, i.e. all 4096 sets of sequences having a distance of at most 3 from a codeword are disjoint and their union is the set of all binary sequences of length 23. A decoding sphere of this code contains exactly 2048 sequences and within a decoding sphere there are 254 sequences that are different from the codeword at a fixed position. This perfect code is now used as a vector quantizer for $\{0,1\}^{23}$, hence each binary biometric enrollment sequence x^{23} is mapped onto the closest codeword u^{23} in the Golay code. Now we consider the derived biometric source whose enrollment output is the quantized sequence U^{23} of X^{23} and whose authentication output is the sequence Y^{23}.

Again we are interested in the rate-leakage ratio $I(U^{23};Y^{23})/H(U^{23}|Y^{23})$ for which we can now write

$$\begin{aligned} \frac{I(U^{23};Y^{23})}{H(U^{23}|Y^{23})} &= \frac{H(Y^{23}) - H(Y^{23}|U^{23})}{H(U^{23}) + H(Y^{23}|U^{23}) - H(Y^{23})} \\ &= \frac{23 - H(Y^{23}|U^{23})}{H(Y^{23}|U^{23}) - 11}. \end{aligned} \tag{3.1}$$

Although computation shows that $H(Y^{23}|U^{23}) = 16.4733$, it is more intuitive to consider the following upper bound

$$\begin{aligned} H(Y^{23}|U^{23}) &\leq \sum_{n=1}^{23} H(Y_n|U_n) \\ &= 23h(p(1-q) + (1-p)q) \end{aligned}$$

$$\begin{aligned} &= 23h(0.1992) \\ &= 16.5683, \end{aligned} \tag{3.2}$$

where we used that $p \triangleq \Pr\{X_n \neq U_n\} = 254/2048$, since we apply the Golay code as quantizer. If we substitute this upper bound into expression (3.1) we get a lower bound for the rate-leakage ratio 1.1550, which improves upon the standard ratio of 1.1322. The exact rate-leakage ratio is equal to 1.1925 and improves more upon the standard ratio.

This example shows that the optimal trade-off between secret-key rate and privacy-leakage rate needs not be linear. Methods based on vector quantization result in better rate-leakage ratios than those simply using only a fraction of the symbols. In what follows we will determine the optimal trade-off between secret-key rate and privacy-leakage rate. It will become apparent that vector quantization is an essential part of an optimal scheme.

3.2 Eight Cases, Definitions

3.2.1 Basic Definitions

A biometric system is based on a biometric source with distribution $\{Q(x,y),\ x \in \mathcal{X}, y \in \mathcal{Y}\}$. This source produces an enrollment sequence $x^N = (x_1, x_2, \ldots, x_N)$ of N symbols from the finite alphabet $\mathcal{X}$ and an authentication sequence $y^N = (y_1, y_2, \ldots, y_N)$ of N symbols from the finite alphabet $\mathcal{Y}$. The sequence pair (x^N, y^N) occurs with probability

$$\Pr\{X^N = x^N, Y^N = y^N\} \quad = \quad \prod_{n=1}^{N} Q(x_n, y_n), \tag{3.3}$$

for all $x^N \in \mathcal{X}^N$ and $y^N \in \mathcal{Y}^N$, hence the sequence pairs (X_n, Y_n), $n = 1, 2, \ldots, N$ are i.i.d. according to $Q(x,y)$.

The sequences x^N and y^N are observed by an encoder and decoder, respectively. One of the outputs that the encoder produces is an index $m \in \{1, 2, \ldots, |\mathcal{M}|\}$, which is referred to as helper data. The helper data are made public and are used by the decoder.

We subdivide systems into those where both terminals are supposed to *generate* a secret key and systems in which a secret key is uniformly *chosen* and bound to a biometric sequence, see Jain et al. [37]. The generated secret key s and the chosen secret key k assume values in $\{1, 2, \ldots, |\mathcal{S}|\}$ and $\{1, 2, \ldots, |\mathcal{K}|\}$, respectively. The decoder's estimates $\widehat{s}$ and $\widehat{k}$ of the secret keys s and k also assume values from $\{1, 2, \ldots, |\mathcal{S}|\}$ and $\{1, 2, \ldots, |\mathcal{K}|\}$, respectively. In systems with chosen keys the secret key K is a

uniformly distributed index, hence

$$\Pr\{K = k\} \quad = \quad 1/|\mathcal{K}| \text{ for all } k \in \{1, 2, \ldots, |\mathcal{K}|\}. \tag{3.4}$$

In addition to distinguishing between generated key and chosen key systems, we can subdivide systems into systems in which the helper data are allowed to leak some information about the biometric sequence X^N and systems in which this leakage should be negligible. In the so-called *zero-leakage* systems both terminals have access to a private key p. This private key is assumed to be uniformly distributed, hence

$$\Pr\{P = p\} \quad = \quad 1/|\mathcal{P}| \text{ for all } p \in \{1, 2, \ldots, |\mathcal{P}|\}. \tag{3.5}$$

We call this key private, since we assume that the only encoder and decoder can access it.

Finally, for all four settings we consider two types of privacy leakage, (a) unconditional leakage and (b) conditional leakage. Unconditional leakage corresponds to bounding the mutual information $I(X^N;M)$, whereas conditional leakage corresponds to bounding the conditional mutual information $I(X^N;M|S)$ or $I(X^N;M|K)$. Designing a biometric system, we are interested in a secure system that leaks as little information as possible about biometric data. Therefore natural constraints involve having $I(S;M)$ or $I(K;M)$ close to zero and $I(X^N;M)$ being as small as possible, what corresponds to the unconditional case. However, since the information that the helper data provide about a pair (X^N,S) or (X^N,K) can be larger than the information that they provide on each entity separately, we are also interested to have $I(S;M)$ or $I(K;M)$ close to zero and $I(S,X^N;M)$ or $I(K,X^N;M)$ to be as small as possible. These constraints are equivalent to having $I(S;M)$ or $I(K;M)$ close to zero and $I(X^N;M|S)$ or $I(X^N;M|K)$ being as small as possible and this corresponds to the conditional case.

Note that we indeed have to consider both unconditional and conditional privacy leakage. Observe that $I(X^N;M|S) = I(X^N,S;M) - I(S;M) = I(X^N;M) + I(S;M|X^N) - I(S;M)$. Thus we see that, since $I(S;M|X^N) \geq 0$, then for negligible $I(S;M)$ we have that $I(X^N;M|S) \geq I(X^N;M)$ in secret generation systems. Similarly, we can come to the conclusion that we need to consider both unconditional and conditional privacy leakage for systems with chosen keys.

In the next sections the four resulting combinations, i.e. (1) the biometric secret generation model, (2) the biometric model with chosen keys, (3) the biometric secret generation model with zero-leakage, and (4) the biometric model with chosen keys and zero-leakage, will be proposed in detail. For each combination we consider both unconditional and conditional privacy leakage.

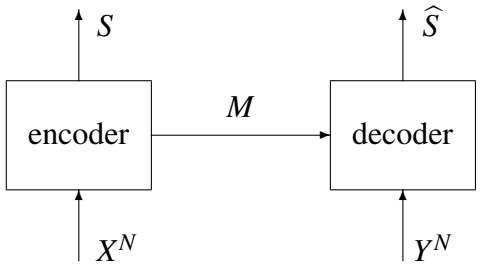


Figure 3.1: *Model for a biometric secret generation system.*

3.2.2 Biometric Secret Generation Model

In a biometric secret generation system, see Fig. 3.1, the encoder observes the biometric enrollment sequence X^N. Then from this sequence the encoder generates a secret key S and a public helper-message M, hence

$$(S,M) \quad = \quad e(X^N), \tag{3.6}$$

where $e(\cdot)$ is the deterministic encoder mapping. The public helper-message M is sent to the decoder. The decoder, on its turn, observes the authentication sequence Y^N and produces an estimate $\widehat{S}$ of the secret S using the observed data, hence

$$\widehat{S} \quad = \quad d(Y^N,M), \tag{3.7}$$

where $d(\cdot)$ is the deterministic decoder mapping.

It is the goal of the encoder and decoder to produce a common (shared) key in such a way that the probability that the estimated secret key $\widehat{S}$ is not equal to S is close to zero. Moreover, we require the information that the helper-message reveals about the secret to be negligible. In addition, we want the secret-key rate to be as large as possible and the secret key to be close to uniform. Finally, the helper data should leak as little information as possible on the biometric data. The privacy leakage can be of two types, and therefore we give two definitions of the achievable secret-key vs. privacy-leakage rate pairs, one corresponding to unconditional leakage and the other one corresponding to conditional leakage.

Definition 3.1 *A secret-key vs. privacy-leakage rate pair (R_s,R_l) with $R_s \geq 0$ is said to be achievable for a biometric secret generation model in the unconditional/conditional case if for all $\delta > 0$ and for all N large enough, there exist encoders and decoders such that*

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} \quad &\leq \quad \delta, \\ \frac{1}{N}H(S)+\delta \quad \geq \quad \frac{1}{N}\log|\mathcal{S}| \quad &\geq \quad R_s-\delta, \end{aligned}$$

$$\begin{aligned} & & \frac{1}{N}I(S;M) &\leq \delta, \\ \textit{(Unconditional)} & & \frac{1}{N}I(X^N;M) &\leq R_l+\delta, \\ \textit{(Conditional)} & & \frac{1}{N}I(X^N;M|S) &\leq R_l+\delta. \end{aligned} \tag{3.8}$$

Moreover, we define $\mathcal{R}_{sg}^u$ and $\mathcal{R}_{sg}^c$ to be the regions of all achievable secret-key vs. privacy-leakage rate pairs for a biometric secret generation model in the unconditional and conditional case, respectively.

3.2.3 Biometric Model with Chosen Keys

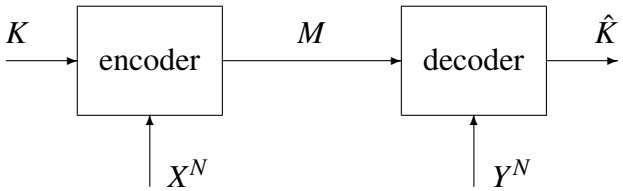


Figure 3.2: *Model for a biometric system with chosen keys.*

In a biometric system with chosen keys, see Fig. 3.2, a secret key K is a uniformly distributed random variable independent of the biometric data, see (3.4). The encoder observes this secret key K and the biometric enrollment sequence X^N and produces a public helper-message M, hence

$$M = e(X^N,K), \tag{3.9}$$

where $e(\cdot)$ is the deterministic encoder mapping. This helper-message is sent to the decoder. The decoder observes the biometric authentication sequence Y^N and produces an estimate $\widehat{K}$ of the secret key K based on the observed data, hence

$$\widehat{K} = d(Y^N,M), \tag{3.10}$$

where $d(\cdot)$ is the deterministic decoder mapping.

Again the encoder and decoder aim at creating a system in such a way that the estimated secret $\widehat{K}$ is equal to the chosen secret K with high probability. In addition, the information that the helper-message reveals about the secret should be negligible and the privacy leakage should be as small as possible. Just like before the secret-key rate should be as large as possible. Again we have two definitions of achievable pairs.

Definition 3.2 *For a biometric model with chosen keys in the unconditional/conditional case a secret-key vs. privacy-leakage rate pair (R_k,R_l) with $R_k \geq 0$ is said to*

be achievable if for all $\delta > 0$ and for all N large enough, there exist encoders and decoders such that

$$\begin{aligned} \Pr\{\widehat{K} \neq K\} &\leq \delta, \\ \frac{1}{N}\log|\mathcal{K}| &\geq R_k - \delta, \\ \frac{1}{N}I(K;M) &\leq \delta, \\ \textit{(Unconditional)} \quad \frac{1}{N}I(X^N;M) &\leq R_l + \delta, \\ \textit{(Conditional)} \quad \frac{1}{N}I(X^N;M|K) &\leq R_l + \delta. \end{aligned} \tag{3.11}$$

Moreover, we define $\mathcal{R}^u_{ck}$ and $\mathcal{R}^c_{ck}$ to be the regions of all achievable secret-key vs. privacy-leakage rate pairs for a biometric model with chosen keys in the unconditional and conditional case, respectively.

3.2.4 Biometric Secret Generation Model with Zero-Leakage

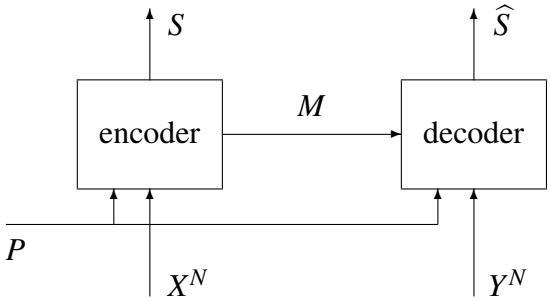


Figure 3.3: *Model for a zero-leakage biometric secret generation system.*

In a biometric secret generation model with zero-leakage, see Fig. 3.3, a private uniform random key P, see (3.5), is available to both the encoder and decoder. The encoder observes this private key P and the biometric enrollment sequence X^N and generates a secret S and a public helper-message M, hence

$$(S,M) \;=\; e(X^N,P), \tag{3.12}$$

where $e(\cdot)$ is the deterministic encoder mapping. The helper-message is sent to the decoder. The decoder also observes the private key P, the biometric authentication sequence Y^N and produces an estimate $\widehat{S}$ of the secret key S, hence

$$\widehat{S} \;=\; d(Y^N,P,M), \tag{3.13}$$

where $d(\cdot)$ is the deterministic decoder mapping.

Definition 3.3 *For a biometric secret generation model with zero-leakage in the unconditional/conditinal case a secret-key vs. private-key rate pair (R_{zs}, R_p) with $R_{zs} \geq 0$ is said to be achievable if for all $\delta > 0$ and for all N large enough, there exist encoders and decoders such that*

$$\begin{aligned} & & \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ \frac{1}{N}H(S)+\delta &\geq \frac{1}{N}\log|\mathcal{S}| &\geq R_{zs}-\delta, \\ & & \frac{1}{N}\log|\mathcal{P}| &\leq R_p+\delta, \\ \textit{(Unconditional)} & & \frac{1}{N}(I(S,M)+I(X^N;M)) &\leq \delta, \\ \textit{(Conditional)} & & \frac{1}{N}I(S,X^N;M) &\leq \delta. \end{aligned} \tag{3.14}$$

Moreover, we define $\mathcal{R}^u_{zsg}$ and $\mathcal{R}^c_{zsg}$ to be the regions of all achievable secret-key vs. private-key rate pairs for a biometric secret generation model with zero-leakage in the unconditional and conditional case, respectively.

3.2.5 Biometric Model with Chosen Keys and Zero-Leakage

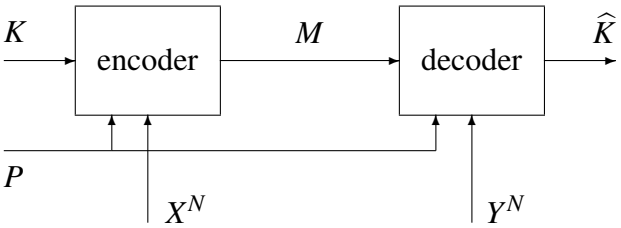


Figure 3.4: *Model for a zero-leakage biometric system with chosen keys.*

In a biometric system with chosen keys and zero-leakage, see Fig. 3.4, a private uniform random key P, see (3.5), is again available to both the encoder and decoder. Moreover, there is also an independent uniform secret key K, see (3.4), which is given to the encoder. The encoder observes the private key P, the secret key K and the biometric enrollment sequence X^N and produces a public helper-message M, hence

$$M = e(X^N, K, P), \tag{3.15}$$

where $e(\cdot)$ is the deterministic encoder mapping. The helper-message is sent to the decoder. The decoder, on its turn, observes the biometric authentication sequence Y^N and the private key P and produces an estimate $\widehat{K}$ of the secret key K, hence

$$\widehat{K} = d(Y^N, P, M), \tag{3.16}$$

where $d(\cdot)$ is the deterministic decoder mapping. Here again we have two definitions of achievable pairs.

Definition 3.4 *For a biometric model with chosen keys and zero-leakage in the unconditional/conditional case a secret-key vs. private-key rate pair (R_{zk}, R_p) with $R_{zk} \geq 0$ is said to be achievable if for all $\delta > 0$ and for all N large enough, there exist encoders and decoders such that*

$$\begin{aligned} \Pr\{\widehat{K} \neq K\} &\leq \delta, \\ \frac{1}{N}\log|\mathcal{K}| &\geq R_{zk} - \delta, \\ \frac{1}{N}\log|\mathcal{P}| &\leq R_p + \delta, \\ \textit{(Unconditional)} \qquad \frac{1}{N}(I(K;M) + I(X^N;M)) &\leq \delta, \\ \textit{(Conditional)} \qquad \frac{1}{N}I(K,X^N;M) &\leq \delta. \end{aligned} \tag{3.17}$$

Moreover, we define $\mathcal{R}^u_{zck}$ and $\mathcal{R}^c_{zck}$ to be the regions of all achievable secret-key vs. private-key rate pairs for a biometric model with chosen keys and zero-leakage in the unconditional and conditional case, respectively.

3.3 Statement of Results

In this section we present our results for all the biometric models described in the previous section. We will present eight theorems. First, however, we have to define the regions $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and $\mathcal{R}_4$. Note that depending on the model, the regions $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and $\mathcal{R}_4$ are defined for the secret-key rates R_s, R_k, R_{zs}, or R_{zk}. We only give the definitions in terms of R_s.

$$\begin{aligned} \mathcal{R}_1 \stackrel{\Delta}{=} \big\{(R_s,R_l) \;:\; & 0 \leq R_s \leq I(U;Y), \\ & R_l \geq I(U;X) - I(U;Y), \\ & \text{for } P(u,x,y) = Q(x,y)P(u|x)\big\}. \end{aligned} \tag{3.18}$$

$$\begin{aligned} \mathcal{R}_2 \stackrel{\Delta}{=} \big\{(R_s,R_l) \;:\; & 0 \leq R_s \leq I(U;Y), \\ & R_l \geq I(U;X), \\ & \text{for } P(u,x,y) = Q(x,y)P(u|x)\big\}. \end{aligned} \tag{3.19}$$

$$\begin{aligned} \mathcal{R}_3 \stackrel{\Delta}{=} \big\{(R_s,R_p) \;:\; & 0 \leq R_s \leq I(U;Y) + R_p, \\ & R_p \geq I(U;X) - I(U;Y), \\ & \text{for } P(u,x,y) = Q(x,y)P(u|x)\big\}. \end{aligned} \tag{3.20}$$

$$\mathcal{R}_4 \stackrel{\Delta}{=} \big\{(R_s,R_p) \quad : \quad 0 \le R_s \le R_p\big\}. \tag{3.21}$$

A note on auxiliary random variable U : In order to determine an achievable region, let say $\mathcal{R}_1$, we could take a test-channel with distribution $\{P(u|x), u \in \mathcal{U}, x \in \mathcal{X}\}$. For this test-channel we calculate an achievable secret-key rate vs. privacy-leakage rate pair $(I(U;Y), I(U;X) - I(U;Y))$, and it defines a point (and a region $\{(R_s,R_l) : 0 \le R_s \le I(U;Y), R_l \ge I(U;X) - I(U;Y)\}$) in the region that we seek. In this way, evaluating all possible test-channels and taking the union, we obtain the achievable region.

Theorem 3.1 (Biometric Secret Generation, Unconditional)

$$\mathcal{R}_{sg}^{u} = \mathcal{R}_1.$$

Theorem 3.2 (Biometric Secret Generation, Conditional)

$$\mathcal{R}_{sg}^{c} = \mathcal{R}_1.$$

Theorem 3.3 (Biometric Model with Chosen Secret Keys, Unconditional)

$$\mathcal{R}_{ck}^{u} = \mathcal{R}_1.$$

Theorem 3.4 (Biometric Model with Chosen Secret Keys, Conditional)

$$\mathcal{R}_{ck}^{c} = \mathcal{R}_2.$$

Theorem 3.5 (Biometric Secret Generation with Zero-Leakage, Unconditional)

$$\mathcal{R}_{zsg}^{u} = \mathcal{R}_3.$$

Theorem 3.6 (Biometric Secret Generation with Zero-Leakage, Conditional)

$$\mathcal{R}_{zsg}^{c} = \mathcal{R}_3.$$

Theorem 3.7 (Model with Chosen Keys and Zero-Leakage, Unconditional)

$$\mathcal{R}_{zck}^{u} = \mathcal{R}_3.$$

Theorem 3.8 (Model with Chosen Keys and Zero-Leakage, Conditional)

$$\mathcal{R}_{zck}^{c} = \mathcal{R}_4.$$

3.4 Properties of the Regions

In this section we present some properties of the achievable regions. Moreover, to get familiar with these regions, we give an example in which we determine the regions for a binary symmetric double biometric source.

3.4.1 Secret-Key Rates in Regions $\mathcal{R}_1$, $\mathcal{R}_2$ and $\mathcal{R}_3$

Property 3.1 *The largest possible secret-key rate in the achievable region $\mathcal{R}_1$ is equal to $I(X;Y)$. This rate is achievable with $R_l \leq H(X|Y)$.*

Proof of Property 3.1:

From Markov condition $U \rightarrow X \rightarrow Y$, it follows that

$$I(U;Y) \quad \leq \quad I(X;Y). \tag{3.22}$$

Moreover, if we take $U = X$, then we have

$$I(U;Y) \quad = \quad I(X;Y), \tag{3.23}$$
$$I(U;X) - I(U;Y) \quad = \quad H(X) - I(X;Y) = H(X|Y). \tag{3.24}$$

Hence we have that $(I(X;Y), H(X|Y)) \in \mathcal{R}_1$. This finalizes the proof.

■

Property 3.2 *The largest possible secret-key rate in the achievable region $\mathcal{R}_2$ is equal to $I(X;Y)$. This rate is achievable with $R_l \leq H(X)$.*

Proof of Property 3.2:

Property 3.2 follows if we apply the same arguments as in Property 3.1, but now for the leakage rate we have that $I(U;X) = H(X)$.

■

Property 3.3 *If $(R_s, R_l) \in \mathcal{R}_2$, then $R_s \leq R_l$.*

Proof of Property 3.3:

Follows from Markov condition $U \rightarrow X \rightarrow Y$, since now $R_s \leq I(U;Y) \leq I(U;X) \leq R_l$.

■

Property 3.4 *For the pair $(R_s, R_p) = (H(X), H(X|Y))$ we have that $(R_s, R_p) \in \mathcal{R}_3$.*

Proof of Property 3.4:

Property 3.4 follows if we let $U = X$ and fix R_p.

■

Remark 1: Note that the results on the largest possible secret-key rates in Properties 3.1 and 3.2 are actually the Ahlswede and Csiszár [3] results discussed in Chapter 2.

Remark 2: The secret-key rate achieved with private-key rate $H(X|Y)$ in Property 3.4 actually corresponds to the common randomness capacity, which is achieved with transmission rate $H(X|Y)$, studied in Ahlswede and Csiszár [4]. In our system though this secret-key rate is not the capacity.

3.4.2 Bound on the Cardinality of Auxiliary Random Variable U

Note that the achievable regions that we have presented in Section 3.3 are given in terms of auxiliary random variable U. Therefore they cannot be computed straightforwardly, since the range of U is not specified and can, in principle, be arbitrarily large. In this section we bound the range of U. This makes it possible to characterize our achievable regions.

The problem of region characterization is a typical problem studied in multiuser information theory. It involves the support lemma of Ahlswede and Körner [5] and the Fenchel-Eggleston strengthening of the Caratheodory lemma, as in Wyner and Ziv [94]. The arguments that we provide below are similar to those used in Csiszár and Körner [15], pp. 310-312, to characterize the regions for various multi-terminal source and channel coding problems. There, however, three constraints are used. Arguments with two constraints can be found in Tuncel [75], where the capacity vs. storage trade-off in identification systems was studied.

To find a bound on the cardinality of the auxiliary variable U, let $\mathcal{D}$ be the set of probability distributions on $\mathcal{X}$ and consider $|\mathcal{X}|+1$ continuous functions of $P \in \mathcal{D}$ defined as

$$\begin{aligned} \phi_x(P) &= P(x) \text{ for all but one } x, && (3.25)\\ \phi_X(P) &= H_P(X), && (3.26)\\ \phi_Y(P) &= H_P(Y), && (3.27) \end{aligned}$$

where in the last equation we use

$$\Pr\{Y=y\} = \sum_x P(x)Q(y|x), \text{ where } Q(y|x) = Q(x,y)/\sum_y Q(x,y). \qquad (3.28)$$

By the Fenchel-Eggleston strengthening of the Caratheodory lemma, see Wyner and

Ziv [94], there are $|\mathcal{X}|+1$ elements $P_u \in \mathcal{D}$ and α_u that sum to one, such that

$$\begin{aligned} Q(x) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_x(P_u) \text{ for all but one } x, && (3.29)\\ H(X|U) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_X(P_u), && (3.30)\\ H(Y|U) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_Y(P_u). && (3.31) \end{aligned}$$

Now the entire probability distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ and, consequently, the entropies $H(X)$ and $H(Y)$ are specified and therefore so are both mutual information $I(U;X)$ and $I(U;Y)$. It implies that cardinality $|\mathcal{U}| = |\mathcal{X}|+1$ suffices for the achievable regions.

3.4.3 Convexity

Now we show that the achievable regions, which are equal to $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and $\mathcal{R}_4$, are convex.

Region $\mathcal{R}_1$

We need to show that region $\mathcal{R}_1$ of achievable pairs (R_s, R_l) is convex, viz. that if $(R_s^1, R_l^1) \in \mathcal{R}_1$ and $(R_s^2, R_l^2) \in \mathcal{R}_1$, then for $0 \le \lambda \le 1$ it holds that $(\lambda R_s^1 + (1-\lambda)R_s^2, \lambda R_l^1 + (1-\lambda)R_l^2) \in \mathcal{R}_1$.

Let $(R_s^j, R_l^j) \in \mathcal{R}_1, j = 1,2$ be two achievable secret-key vs. privacy-leakage rate pairs, and U_1 and U_2 be two random variables such that

$$\begin{aligned} R_s^j &\le I(U_j;Y), \\ R_l^j &\ge I(U_j;X) - I(U_j;Y), (R_s^j, R_l^j) \in \mathcal{R}_1, j = 1,2. && (3.32) \end{aligned}$$

We define a random variable $U = (J, U_J)$, such that it takes on U_1 with probability λ and U_2 with probability $1-\lambda$, and observe that

$$\begin{aligned} I(U;Y) &= H(Y) - H(Y|U_J, J) \\ &= H(Y) - \lambda H(Y|U_1) - (1-\lambda)H(Y|U_2) - \lambda H(Y) + \lambda H(Y) \\ &= \lambda I(U_1;Y) + (1-\lambda) I(U_2;Y) \\ &\ge \lambda R_s^1 + (1-\lambda) R_s^2, && (3.33) \end{aligned}$$

and, using the result above, we also observe that

$$\begin{aligned} I(U;X)-I(U;Y) &= H(X)-H(X|U_J,J)-I(U;Y) \\ &= H(X)-\lambda H(X|U_1)-(1-\lambda)H(X|U_2)-\lambda H(X)+\lambda H(X)- \\ &\quad \lambda I(U_1;Y)-(1-\lambda)I(U_2;Y) \\ &= \lambda(I(U_1;X)-I(U_1;Y))+(1-\lambda)(I(U_2;X)-I(U_2;Y)) \\ &\leq \lambda R_l^1+(1-\lambda)R_l^2. \end{aligned} \tag{3.34}$$

Combining (3.33) and (3.34), and noting that U satisfies Markov condition $U \rightarrow X \rightarrow Y$, we conclude that $\mathcal{R}_1$ is convex.

Region $\mathcal{R}_2$

In a similar way it can be shown that the region $\mathcal{R}_2$ is convex.

Region $\mathcal{R}_3$

Now let $(R_s^j, R_p^j) \in \mathcal{R}_3, j = 1,2$ be two achievable secret-key vs. private-key rate pairs, and U_1 and U_2 be two random variables such that

$$\begin{aligned} R_s^j &\leq I(U_j;Y)+R_p^j, \\ R_p^j &\geq I(U_j;X)-I(U_j;Y), \quad (R_s^j,R_p^j) \in \mathcal{R}_3, \quad j=1,2, \end{aligned} \tag{3.35}$$

and $U = (J,U_J)$ be defined as above. We can show in the same way as before that

$$I(U;X)-I(U;Y) \leq \lambda R_p^1+(1-\lambda)R_p^2. \tag{3.36}$$

Next observe that

$$\begin{aligned} \lambda R_s^1+(1-\lambda)R_s^2 &\leq \lambda(I(U_1;Y)+R_p^1)+(1-\lambda)(I(U_2;Y)+R_p^2) \\ &= \lambda I(U_1;Y)+(1-\lambda)I(U_2;Y)+\lambda R_p^1+(1-\lambda)R_p^2 \\ &= I(U;Y)+\lambda R_p^1+(1-\lambda)R_p^2. \end{aligned} \tag{3.37}$$

Now the convexity of $\mathcal{R}_3$ follows from (3.36) and(3.37). Note that U satisfies Markov condition $U \rightarrow X \rightarrow Y$.

Regions $\mathcal{R}_4$

The convexity of region $\mathcal{R}_4$ follows from the fact that the boundary of this region is a linear function.

3.4.4 Example: Binary Symmetric Double Source

To illustrate the trade-off between the secret-key and privacy-leakage rates, and the secret-key and private-key rates, consider a binary symmetric double source with crossover probability q described in the introduction to this chapter. For such a source $I(U;Y) = 1 - H(Y|U)$ and $I(U;X) - I(U;Y) = H(Y|U) - H(X|U)$.

Mrs. Gerber's Lemma, see Wyner and Ziv [93], tells us that if $H(X|U) = v$, then $H(Y|U) \geq h(q * h^{-1}(v))$, where $a * b = a(1-b) + (1-a)b$ and $h(a) = -a\log(a) - (1-a)\log(1-a)$ is the binary entropy function. Now if $0 \leq p \leq 1/2$ is such that $h(p) = v$, then $H(X|U) = h(p)$ and $H(Y|U) \geq h(q * p)$.

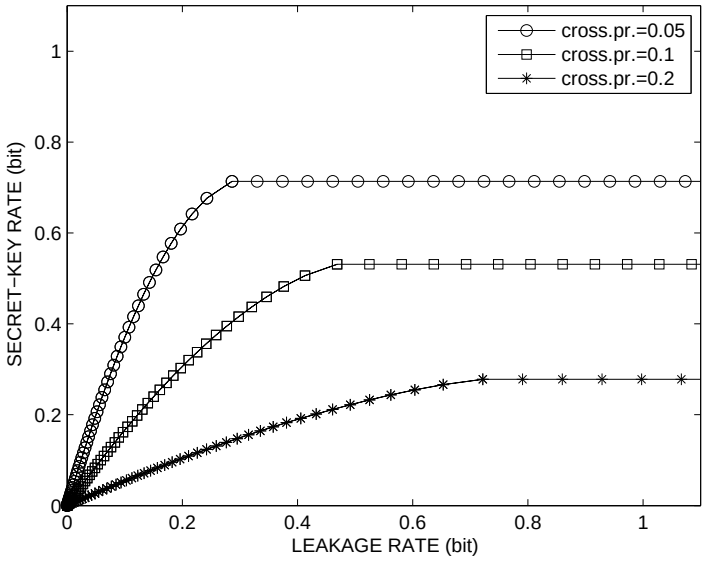


Figure 3.5: *Secret-key vs. privacy-leakage rate function $R_1(R_l)$ for three values of the crossover probability q.*

First, consider region $\mathcal{R}_1$. For this region we define the secret-key vs. leakage rate function $R_1(R_l)$ as

$$R_1(R_l) \stackrel{\Delta}{=} \max\{R_s : (R_s, R_l) \in \mathcal{R}_1\}. \tag{3.38}$$

For binary symmetric (U,X) with crossover probability p the minimum $H(Y|U)$ is achieved and, consequently,

$$\begin{aligned} R_1(R_l) &= 1 - h(q * p), \\ &\text{for } p \text{ satisfying } h(q * p) - h(p) = R_l. \end{aligned} \tag{3.39}$$

We have computed the secret-key vs. leakage rate functions for crossover probabilities $q = 0.05, 0.1$, and 0.2 using (3.39). The results are plotted in Fig. 3.5. Looking at the figure we conclude that for small q the secret-key rate is large compared to the privacy-leakage rate, while for large q the secret-key rate is smaller than the privacy-leakage rate.

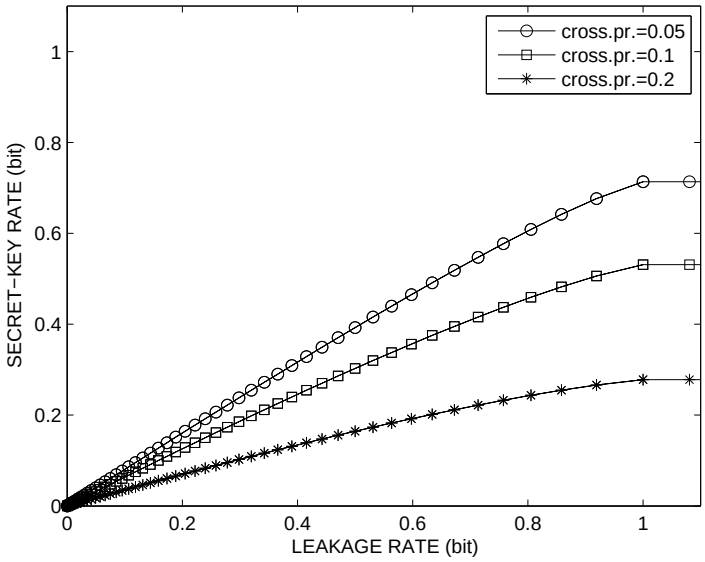


Figure 3.6: *Secret-key vs. privacy-leakage rate function $R_2(R_l)$ for three values of the crossover probability q.*

In a similar way, for region $\mathcal{R}_2$ the corresponding secret-key vs. leakage rate function $R_2(R_l)$ is defined as

$$R_2(R_l) \stackrel{\Delta}{=} \max\{R_s : (R_s, R_l) \in \mathcal{R}_2\}, \tag{3.40}$$

and then we obtain

$$\begin{aligned} R_2(R_l) &= 1 - h(q * p), \\ &\text{for } p \text{ satisfying } 1 - h(p) = R_l. \end{aligned} \tag{3.41}$$

Again we have computed the secret-key vs. leakage rate function for this case for crossover probabilities $q = 0.05, 0.1$, and 0.2 using (3.41). The results presented in Fig. 3.6 confirm our statement that the secret-key rate is always smaller than or equal to the privacy-leakage rate. Moreover, we see that compared to $R_1(R_l)$, the secret-key vs. privacy-leakage rate trade-off undergoes dramatic degradation.

Now consider region $\mathcal{R}_3$ and define the corresponding secret-key vs. private-key rate function $R_3(R_p)$ as

$$R_3(R_p) \stackrel{\Delta}{=} \max\{R_s : (R_s, R_p) \in \mathcal{R}_3\}. \tag{3.42}$$

Then for fixed private-key rates, using similar reasoning as before, it follows that

$$\begin{aligned} R_3(R_p) &= 1 - h(p), \\ &\text{for } p \text{ satisfying } h(q * p) - h(p) = R_p. \end{aligned} \tag{3.43}$$

In Fig. 3.7 we plotted the secret-key vs. private-key rate functions for crossover probabilities $q = 0.05, 0.1$, and 0.2, computed using (3.43). From this figure we observe that the private-key rate is never larger than the (chosen) secret-key rate.

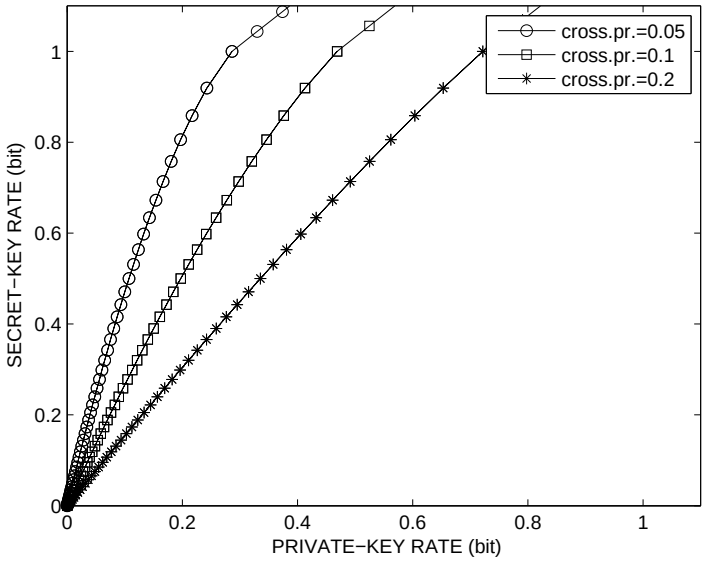


Figure 3.7: *Secret-key vs. private-key rate function $R_3(R_l)$ for three values of the crossover probability q.*

Finally, we define the secret-key vs. private-key rate function $R_4(R_p)$ corresponding to $\mathcal{R}_4$

$$R_4(R_p) \stackrel{\Delta}{=} \max\{R_s : (R_s, R_p) \in \mathcal{R}_4\}. \tag{3.44}$$

Then for fixed private-key rates we get

$$R_4(R_p) = R_p. \tag{3.45}$$

The corresponding secret-key vs. private-key rate functions are shown in Fig. 3.8. Clearly, the functions are independent of q.

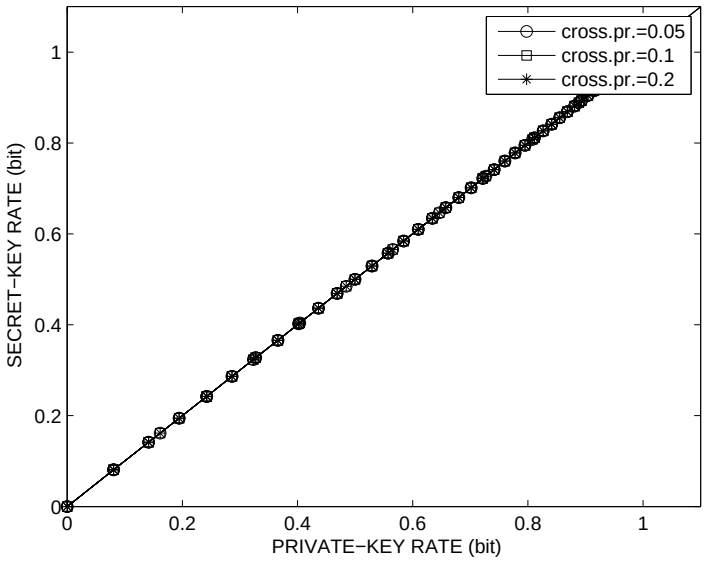


Figure 3.8: *Secret-key vs. private-key rate function $R_4(R_l)$ for three values of the crossover probability q.*

3.5 Proofs of the Results

3.5.1 Modified Typical Sets

First we define a modified typical set $\mathcal{B}_\varepsilon^{(N)}(U,X)$ and present its properties.

The modified typical set is formed in such a way that if an auxiliary random sequence, which is generated at the encoder, is typical with the sequence observed by the encoder, then also the sequence observed at the decoder should be typical with this auxiliary random sequence. Note that the sequence that the decoder observes is the output of the "channel" to which the sequence observed at the encoder is an input. This set enables a property similar to the joint typicality property of the strongly typical sets discussed in Chapter 2 and is crucial in our proof.

Definition 3.5 *Let (X,U) be a pair of discrete random variables with some joint distribution $\{P(u,x), x \in \mathcal{X}, u \in \mathcal{U}\}$, where $P(u,x) = \sum_y Q(x,y)P(u|x)$. Now for $\varepsilon > 0$ the set $\mathcal{B}_\varepsilon^{(N)}(U,X)$ of ε-typical N-sequences is defined as*

$$\mathcal{B}_\varepsilon^{(N)}(U,X) \stackrel{\Delta}{=} \Big\{(u^N,x^N) : \Pr\{Y^N \in \mathcal{T}_\varepsilon^{(N)}(Y|(u^N,x^N))|(U^N,X^N) = (u^N,x^N)\} \geq 1-\varepsilon\Big\}, \quad (3.46)$$

where Y^N is the output of a "channel" $Q(y|x) = Q(x,y)/Q(x)$ for $Q(x) = \sum_y Q(x,y)$,

where x^N is an input. Moreover, we define

$$\mathcal{B}_\varepsilon^{(N)}(U|x^N) \quad \stackrel{\Delta}{=} \quad \{u^N : (u^N,x^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)\}. \tag{3.47}$$

Lemma 3.1 (Property of $\mathcal{B}_\varepsilon^{(N)}(U,X)$) *Let (U^N,X^N) be i.i.d. with respect to $P(u,x) = \sum_y Q(x,y)P(u|x)$, then for $\varepsilon > 0$ and N large enough*

$$\Pr\{(U^N,X^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)\} \quad \geq \quad 1-\varepsilon. \tag{3.48}$$

Proof: Let (U^N,X^N,Y^N) be i.i.d. with respect to $P(u,x,y) = Q(x,y)P(u|x)$. Observe that

$$\begin{aligned}
&\Pr\{(U^N,X^N,Y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X,Y)\} \\
&\qquad \leq \sum_{(u^N,x^N)\in\mathcal{B}_\varepsilon^{(N)}(U,X)} P(u^N,x^N) + \sum_{(u^N,x^N)\notin\mathcal{B}_\varepsilon^{(N)}(U,X)} P(u^N,x^N)(1-\varepsilon) \\
&\qquad = \ 1-\varepsilon+\varepsilon\Pr\{(U^N,X^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)\},
\end{aligned} \tag{3.49}$$

then

$$\Pr\{(U^N,X^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)\} \geq 1 - \frac{1}{\varepsilon}(1-\Pr\{(U^N,X^N,Y^N)\in\mathcal{A}_\varepsilon^{(N)}(U,X,Y)\}). \tag{3.50}$$

By the weak law of large numbers $\Pr\{(U^N,X^N,Y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X,Y)\} \geq 1-\varepsilon^2$ for N large enough, and then (3.48) follows.

■

Lemma 3.2 (Property of $\mathcal{B}_\varepsilon^{(N)}(U,X)$) *If $(u^N,x^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)$ then also $(u^N,x^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X)$.*

Proof: Note that if $(u^N,x^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)$, then there exists at least one y^N such that $(u^N,x^N,y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X,Y)$ and then also $(u^N,x^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X)$.

■

Now we are ready to prove our results. The achievability proofs of the stated theorems are based on the basic achievability proof corresponding to Thm. 3.1. On its turn this proof is based on the weak typicality proof presented in Section 2.3 of Chapter 2. In the current setting, however, instead of conveying X-sequences from the encoder to decoder, auxiliary U-sequences which are typical with X-sequences, are sent from the encoder to the decoder.

3.5.2 Proof of Thm. 3.1

Remark: It should be noted that the result of Thm. 3.1 is in some way similar to and a special case of the SK (secret-key) part of Thm. 2.4 in Csiszár and Narayan [16], when $Y = Z$. In Csiszár and Narayan [16] the secret-key capacity was determined for three terminals $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ under the constraints that the public channel capacity from the first to the second and third terminals is equal to $R_1, R_1 \geq I(U;X) - \min\{I(U;Y)I(U,Z)\}$, where $U \rightarrow X \rightarrow YZ$, and that there is no communication between the second and the third terminals.

The proof of Thm. 3.1 consists of two parts. The first part concerns the achievability, and the second part relates to the converse.

(Basic) Achievability Proof for Thm. 3.1

We start our achievability proof with fixing the auxiliary alphabet $\mathcal{U}$ and the conditional probabilities $\{P(u|x), u \in \mathcal{U}, x \in \mathcal{X}\}$, and also $0 < \varepsilon < 1$. Observe that $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ is the source distribution, and let $\mathcal{A}_\varepsilon^{(N)}(U,X), \mathcal{A}_\varepsilon^{(N)}(U,Y), \mathcal{A}_\varepsilon^{(N)}(U,X,Y)$ be the sets of jointly ε-typical N-sequences corresponding to $P(u,x,y) = Q(x,y)P(u|x)$. To prove the achievability of $\mathcal{R}_1$, we use a random coding argument.

Random coding: First, we outline the coding strategy. For each index $i \in \{1,2,\ldots, M_u\}$, we generate an auxiliary random sequence u_i^N at random according to

$$P(u) \quad = \quad \sum_{x,y} Q(x,y)P(u|x). \tag{3.51}$$

Moreover, to each index i (and the corresponding randomly generated sequence u_i^N) we assign uniformly at random a secrecy label $s_i \in \{1,2,\ldots,|\mathcal{S}|\}$ with probability

$$\Pr\{S_i = s_i\} \quad = \quad 1/|\mathcal{S}| \tag{3.52}$$

and a helper label $m_i \in \{1,2,\ldots,|\mathcal{M}|\}$ with probability

$$\Pr\{M_i = m_i\} \quad = \quad 1/|\mathcal{M}|. \tag{3.53}$$

Encoding: The encoder observes a sequence x^N and looks for index i such that $(u_i^N, x^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)$. If such an index is found, it produces a secrecy label s_i and a helper label m_i. If no such index is found, an error is declared. Moreover, the encoder checks if there is only one index i with labels s_i and m_i. If not, also an error is declared. The helper label is sent to the decoder if no error occurred.

Decoding: The decoder, on its turn, having observed a sequence y^N and the helper-label m, looks for an index $\widehat{i}$ such that $m_{\widehat{i}} = m$ and $(u_{\widehat{i}}^N, y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,Y)$. If such a unique index exists, the decoder produces the secret estimate $s_{\widehat{i}}$, otherwise an error is declared.

Error probability: Now consider the error probability. Let i be the index determined by the encoder. Note that the encoder produces an error if

1) There exists no i, such that $(u_i^N, x^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)$.

2) The pair of labels (s_i, m_i) is not unique.

Moreover, an error at the decoder occurs in the following situations:

3) If u_i^N is not typical with y^N.

4) The decoder finds an index $i', i' \neq i$ such that $(u_{i'}^N, y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,Y)$ and $m_{i'} = m$.

Then we can write for the error probability averaged over the random code construction

$$\begin{aligned}
\overline{P_\varepsilon} \;\leq\; & \Pr\Big\{ \big(\bigcap_{i=1}^{M_u} (U_i^N, X^N) \notin \mathcal{B}_\varepsilon^{(N)}(U,X) \big) \cup \big(\bigcup_{\substack{i=1 \\ i\neq I}}^{M_u} M_i = M \cap S_i = S \big) \cup \\
& \qquad (U_I^N, Y^N) \notin \mathcal{A}_\varepsilon^{(N)}(U,Y) \cup \big(\bigcup_{\substack{i=1 \\ i\neq I}}^{M_u} (U_i^N, Y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,Y) \cap M_i = M \big) \Big\} \\
\leq\; & \sum_{x^N \in \mathcal{X}^N} Q(x^N) \prod_{i=1}^{M_u} \Pr\{U_i^N \notin \mathcal{B}_\varepsilon^{(N)}(U|x^N)\} + \sum_{\substack{i=1 \\ i\neq I}}^{M_u} \Pr\{M_i = M\} \cdot \Pr\{S_i = S\} + \\
& \Pr\{(U_I^N, Y^N) \notin \mathcal{A}_\varepsilon^{(N)}(U,Y) | (U_I^N, X^N) \in \mathcal{B}_\varepsilon^{(N)}(U,X)\} + \\
& \sum_{\substack{i=1 \\ i\neq I}}^{M_u} \Pr\{(U_i^N, Y^N) \in \mathcal{A}_\varepsilon^{(N)}(U,Y)\} \cdot \Pr\{M_i = M\}, \qquad (3.54)
\end{aligned}$$

where the last step follows from the union bound.

The first term of $\overline{P_\varepsilon}$ can be bounded as

$$\begin{aligned}
\overline{P_{\varepsilon,1}} \;=\; & \sum_{x^N \in \mathcal{X}^N} Q(x^N) \prod_{i=1}^{M_u} \Big(1 - \sum_{u^N \in \mathcal{B}_\varepsilon^{(N)}(U|x^N)} P(u^N)\Big) \\
\overset{(a)}{\leq}\; & \sum_{x^N \in \mathcal{X}^N} Q(x^N) \Big(1 - 2^{-N(I(U;X)+3\varepsilon)} \cdot \sum_{u^N \in \mathcal{B}_\varepsilon^{(N)}(U|x^N)} P(u^N|x^N)\Big)^{M_u} \\
\overset{(b)}{\leq}\; & \sum_{x^N \in \mathcal{X}^N} Q(x^N) \Big(1 - \sum_{u^N \in \mathcal{B}_\varepsilon^{(N)}(U|x^N)} P(u^N|x^N) + e^{-M_u 2^{-N(I(U;X)+3\varepsilon)}}\Big) \\
=\; & \sum_{(u^N,x^N) \notin \mathcal{B}_\varepsilon^{(N)}(U,X)} P(u^N, x^N) + \sum_{x^N \in \mathcal{X}^N} Q(x^N) e^{-M_u 2^{-N(I(U;X)+3\varepsilon)}} \\
\leq\; & 2\varepsilon, \qquad (3.55)
\end{aligned}$$

if we take $\log M_u = N(I(U;X)+4\varepsilon)$, for N large enough. Here step (a) follows from Lem. 3.2 and from the fact that for $(u^N,x^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X)$

$$\begin{aligned} P(u^N) &= P(u^N|x^N)\frac{Q(x^N)P(u^N)}{P(u^N,x^N)} \\ &\geq P(u^N|x^N)\frac{2^{-N(H(X)+\varepsilon)}2^{-N(H(U)+\varepsilon)}}{2^{-N(H(U,X)-\varepsilon)}} = P(u^N|x^N)2^{-N(I(U;X)+3\varepsilon)}, \end{aligned}$$

and step (b) follows from $(1-\alpha\beta)^K \leq 1-\alpha+e^{-K\beta}$, see e.g. Cover and Thomas [13], p. 353.

For the second term of $\overline{P_\varepsilon}$ we obtain

$$\begin{aligned} \overline{P_{\varepsilon,2}} &\leq \sum_{\substack{i=1 \\ i\neq I}}^{M_u} \frac{1}{|\mathcal{M}|}\cdot\frac{1}{|\mathcal{S}|} \\ &\leq \frac{1}{|\mathcal{M}|}\cdot\frac{1}{|\mathcal{S}|}\cdot M_u \\ &= 2^{-N(\frac{1}{N}\log|\mathcal{M}|+\frac{1}{N}\log|\mathcal{S}|-\frac{1}{N}\log M_u)} \\ &\leq \varepsilon, \end{aligned} \tag{3.56}$$

if we take $\log|\mathcal{M}|+\log|\mathcal{S}|-\log M_u = N\varepsilon$, for N large enough. Here the first inequality follows from random binning.

For the third term of $\overline{P_\varepsilon}$ we obtain that

$$\begin{aligned} \overline{P_{\varepsilon,3}} &\leq \max_{(u^N,x^N)\in\mathcal{B}_\varepsilon^{(N)}(U,X)} \Pr\left\{Y^N \notin \mathcal{T}_\varepsilon^{(N)}(Y|(u^N,x^N))|(U^N,X^N)=(u^N,x^N)\right\} \\ &\leq \varepsilon, \end{aligned} \tag{3.57}$$

where the first inequality follows from the definition of $\mathcal{B}_\varepsilon^{(N)}(U,X)$.

Finally, for the fourth term of $\overline{P_\varepsilon}$ we get

$$\begin{aligned} \overline{P_{\varepsilon,4}} &\overset{(a)}{\leq} \sum_{\substack{i=1 \\ i\neq I}}^{M_u} \max_{y^N} \Pr\{U_i^N \in \mathcal{T}_\varepsilon^{(N)}(U|y^N)\}\cdot\frac{1}{|\mathcal{M}|} \\ &\leq \sum_{\substack{i=1 \\ i\neq I}}^{M_u} \sum_{u^N\in\mathcal{T}_\varepsilon^{(N)}(U|y^N)} P(u^N)\cdot\frac{1}{|\mathcal{M}|} \\ &\overset{(b)}{\leq} \frac{1}{|\mathcal{M}|}\sum_{\substack{i=1 \\ i\neq I}}^{M_u} 2^{-N(H(U)-\varepsilon)}\cdot|\mathcal{T}_\varepsilon^{(N)}(U|y^N)| \\ &\overset{(c)}{\leq} \frac{1}{|\mathcal{M}|}\cdot 2^{-N(H(U)-\varepsilon)}\cdot 2^{N(H(U|Y)+2\varepsilon)}\cdot M_u \end{aligned}$$

$$\begin{aligned} &= 2^{-N(\frac{1}{N}\log|\mathcal{M}|+I(U;Y)-3\varepsilon-\frac{1}{N}\log M_u)} \\ &\leq \varepsilon, \end{aligned} \tag{3.58}$$

for N large enough if we take $\log|\mathcal{M}| = \log M_u - NI(U;Y) + 4N\varepsilon$. Step (a) follows from random binning, (b) from typicality, and (c) follows from (2.9).

Thus we see that, since $\overline{P_e} = \overline{P_{e,1}} + \overline{P_{e,2}} + \overline{P_{e,3}} + \overline{P_{e,4}} \leq 5\varepsilon$ for N large enough, there exists at least one encoder and decoder with $P_e \leq 5\varepsilon$ and we focus on the resulting code. Note that, combining all equations obtained while bounding all terms of the error probability, we have for this code

$$\begin{aligned} \Pr\{S \neq \widehat{S}\} &\leq 5\varepsilon, && (3.59)\\ H(S) &\leq \log|\mathcal{S}| = N(I(U;Y) - 3\varepsilon), && (3.60)\\ H(M) &\leq \log|\mathcal{M}| = N(I(U;X) - I(U;Y) + 8\varepsilon), && (3.61)\\ H(U) &\leq \log M_u = N(I(U;X) + 4\varepsilon). && (3.62) \end{aligned}$$

Secrecy: First, note that if no error occurs then $(u^N, x^N) \in \mathcal{A}_\varepsilon^{(N)}(U,X)$, and I uniquely defines $\widehat{U} = U$. Moreover, if an error occurs, then $\widehat{U}$ is some sequence from $\mathcal{U}^N$. Note also that $|\mathcal{T}_\varepsilon^{(N)}(X|u^N)| \leq 2^{N(H(X|U)+2\varepsilon)}$, then

$$\begin{aligned} NH(X) &= H(X^N) \\ &\leq H(X^N, U^N) \\ &= H(U^N) + H(X^N|U^N) \\ &\leq H(U^N) + P_e \log|\mathcal{X}|^N + (1-P_e)\log 2^{N(H(X|U)+2\varepsilon)} \\ &\leq H(U^N) + 5N\varepsilon\log|\mathcal{X}| + NH(X|U) + 2N\varepsilon, \end{aligned} \tag{3.63}$$

and therefore

$$H(U^N) \geq N(I(U;X) - 5\varepsilon\log|\mathcal{X}| - 2\varepsilon). \tag{3.64}$$

Next consider

$$\begin{aligned} H(S,M) &= H(U^N, S, M) - H(U^N|S,M) \\ &\overset{(a)}{\geq} H(U^N) - H(U^N|S,M,\widehat{U}^N) \\ &\geq H(U^N) - H(U^N|\widehat{U}^N) \\ &\overset{(b)}{\geq} H(U^N) - P_e \log M_u - 1 \\ &\overset{(c)}{\geq} NI(U;X) - 5N\varepsilon\log|\mathcal{X}| - 2N\varepsilon - 5\varepsilon N(I(U;X) + 4\varepsilon) - 1 \\ &\overset{(d)}{\geq} NI(U;X) - 10N\varepsilon\log|\mathcal{X}| - 2N\varepsilon - 20N\varepsilon^2 - 1, \end{aligned} \tag{3.65}$$

where in step (a) we used the fact that for a unique label pair (S,M) there is a unique index I, which defines $\widehat{U}$, in (b) Fano's inequality, in (c) we used (3.62) and (3.64), and in (d) the fact that $I(U;X) \leq H(X) \leq \log|\mathcal{X}|$.

Now consider the secrecy. Then using (3.60), (3.61) and (3.65) we obtain

$$\begin{aligned} I(S;M) &= H(S)+H(M)-H(S,M) \\ &\leq NI(U;Y)-3N\varepsilon+NI(U;X)-NI(U;Y)+8N\varepsilon-NI(U;X)+ \\ &\quad 10N\varepsilon\log|\mathcal{X}|+2N\varepsilon+20N\varepsilon^2+1 \\ &\leq N(7\varepsilon+10\varepsilon\log|\mathcal{X}|+20\varepsilon^2+\frac{1}{N}). \end{aligned} \tag{3.66}$$

Uniformity of the secret: For the entropy of the secret, using (3.65) and (3.61), we obtain that

$$\begin{aligned} H(S) &= H(S,M)-H(M|S) \\ &\geq H(S,M)-H(M) \\ &\geq NI(U;X)-10N\varepsilon\log|\mathcal{X}|-2N\varepsilon-20N\varepsilon^2-1- \\ &\quad NI(U;X)+NI(U;Y)-8N\varepsilon \\ &\geq NI(U;Y)-10N\varepsilon\log|\mathcal{X}|-10N\varepsilon-20N\varepsilon^2-1 \\ &= N(\frac{1}{N}\log|\mathcal{S}|-10\varepsilon\log|\mathcal{X}|-7\varepsilon-20\varepsilon^2-\frac{1}{N}). \end{aligned} \tag{3.67}$$

The privacy leakage: Finally, we consider the privacy leakage, and using (3.61) we get

$$I(X^N;M) \leq H(M) \leq N(I(U;X)-I(U;Y)+8\varepsilon). \tag{3.68}$$

Then letting $\varepsilon \downarrow 0$ and $N \to \infty$, we obtain the achievability from (3.59), from the equality in (3.60) and from (3.66)-(3.68).

Converse for Thm. 3.1

Assume that the secret-key vs. privacy-leakage rate pair (R_s,R_l) is achievable. First, observe that we can bound the entropy of the secret key as follows.

$$\begin{aligned} H(S) &= I(S;M,Y^N)+H(S|M,Y^N) \\ &\overset{(a)}{\leq} I(S;M,Y^N)+H(S|\widehat{S}) \\ &\overset{(b)}{\leq} I(S;M)+I(S;Y^N|M)+\delta\log|\mathcal{S}|+1 \\ &\overset{(c)}{\leq} N\delta+H(Y^N|M)-H(Y^N|M,S)+N\delta\log|\mathcal{X}|+1 \\ &\overset{(d)}{\leq} NH(Y)-H(Y^N|M,S)+N\delta\log|\mathcal{X}|+N\delta+1, \end{aligned} \tag{3.69}$$

where step (a) holds, since $\widehat{S}$ is a function of Y^N and M and since conditioning does not increase entropy, (b) follows from Fano's inequality and the fact that $\Pr\{\widehat{S} \neq S\} \leq \delta$ for achievable pairs (R_s, R_l), (c) holds, since for achievable pairs (R_s, R_l) we have that $I(S;M) \leq N\delta$ and, since the encoder mapping is deterministic and then $|\mathcal{S}| \leq |\mathcal{X}^N|$ holds (possibly) after renumbering, and step (d) follows from the facts that conditioning does not increase entropy and that Y^N is an i.i.d. sequence.

Now consider $H(Y^N|M,S)$.

$$\begin{aligned} H(Y^N|M,S) &= \sum_{i=1}^{N} H(Y_i|S,M,Y^{i-1}) \\ &\geq \sum_{i=1}^{N} H(Y_i|S,M,Y^{i-1},X^{i-1}) \\ &\overset{(a)}{=} \sum_{i=1}^{N} H(Y_i|S,M,X^{i-1}) \\ &= NH(Y_I|U_I,I) \\ &= NH(Y|U), \end{aligned} \tag{3.70}$$

where I is a random variable uniformly distributed on $\{1,2,\ldots,N\}$ and independent of (X^N,Y^N), and for $I=i$ we define $U_i = MSX^{i-1}$, $U=(U_i,i)$, $X=X_i$, and $Y=Y_i$. Here step (a) follows from the fact that $Y^{i-1} \to MSX^{i-1} \to Y_i$. We verify Markovity, bearing in mind that X^N and Y^N are i.i.d. sequences and M,S are functions of only X^N, and then

$$\begin{aligned} &\Pr\{M=m,S=s,X^{i-1}=x^{i-1},Y^{i-1}=y^{i-1},Y_i=y_i\} \\ &= \sum_{x_i\in\mathcal{X}} \sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{X_i=x_i\}\cdot\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot \\ &\quad \Pr\{Y^{i-1}=y^{i-1}|X^{i-1}=x^{i-1}\}\cdot\Pr\{M=m,S=s,Y_i=y_i|X^N=x^N\} \\ &= \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{Y^{i-1}=y^{i-1}|X^{i-1}=x^{i-1}\}\cdot \\ &\quad \sum_{x_i\in\mathcal{X}} \sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X_i=x_i\}\cdot\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\Pr\{M=m,S=s,Y_i=y_i|X^N=x^N\} \\ &= \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{Y^{i-1}=y^{i-1}|X^{i-1}=x^{i-1}\}\cdot \\ &\quad \Pr\{M=m,S=s,Y_i=y_i|X^{i-1}=x^{i-1}\}, \end{aligned}$$

thus $Y^{i-1} \to X^{i-1} \to MSY_i$, which implies that $Y^{i-1} \to MSX^{i-1} \to Y_i$.

Note also that $U_i = MSX^{i-1}$ satisfies Markov condition $U_i \to X_i \to Y_i$. Indeed,

$$\begin{aligned} &\Pr\{M=m,S=s,X^{i-1}=x^{i-1},X_i=x_i,Y_i=y_i\} \\ &\overset{(a)}{=} \sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{X_i=x_i\}\cdot\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\Pr\{Y_i=y_i|X_i=x_i\}\cdot \end{aligned}$$

$$
\begin{aligned}
&\Pr\{M=m,S=s|X^N=x^N,Y_i=y_i\}\\
&\overset{(b)}{=} \Pr\{X_i=x_i\}\cdot\Pr\{Y_i=y_i|X_i=x_i\}\cdot\Pr\{X^{i-1}=x^{i-1}\}\cdot\\
&\qquad\sum_{x_{i+1}^N\in\mathcal{X}^{N-i}}\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\Pr\{M=m,S=s|X^N=x^N\}\\
&= \Pr\{X_i=x_i\}\cdot\Pr\{Y_i=y_i|X_i=x_i\}\cdot\Pr\{M=m,S=s,X^{i-1}=x^{i-1}|X_i=x_i\}, \quad (3.71)
\end{aligned}
$$

where step (a) follows from the fact that X^N and Y^N are i.i.d. sequences, and (b) follows from the fact that M and S depend only on X^N. This implies that $U\to X\to Y$ holds. Indeed, if now $I=i$ with $\Pr\{I=i\}=1/N$ independent of (X^N,Y^N) and we define $U=(U_i,i)$, $X=X_i$, and $Y=Y_i$ for $I=i$, then we have

$$
\begin{aligned}
&\Pr\{U=(u_i,i),X=x,Y=y\}\\
&\quad= \Pr\{I=i\}\cdot\Pr\{X=x|I=i\}\cdot\Pr\{Y=y|X=x,I=i\}\cdot\\
&\qquad\Pr\{U_i=u_i|X=x,Y=y,I=i\}\\
&\quad= \Pr\{X=x\}\cdot\Pr\{Y=y|X=x\}\cdot\Pr\{I=i\}\cdot\Pr\{U_i=u_i|X=x,I=i\}\\
&\quad= \Pr\{X=x\}\cdot\Pr\{Y=y|X=x\}\cdot\Pr\{U=(u_i,i)|X=x\}. \quad (3.72)
\end{aligned}
$$

Now combining (3.70) with (3.69) and dividing both parts of the resulting inequality by N, we obtain for achievable pairs (R_s,R_l) that

$$
R_s-\delta\le\frac{1}{N}H(S)\le I(U;Y)+\delta(\log|\mathcal{X}|+1)+\frac{1}{N}, \quad (3.73)
$$

for some $P(u,x,y)=Q(x,y)P(u|x)$.

Next observe that

$$
\begin{aligned}
I(X^N;M,S) &= \sum_{i=1}^N I(X_i;M,S|X^{i-1})\\
&= NI(X_I;M,S|X^{I-1},I)\\
&\overset{(a)}{=} NI(X_I;S,M,X^{I-1},I)\\
&\overset{(b)}{=} NI(U;X), \quad (3.74)
\end{aligned}
$$

where just as before $U=MSX^{I-1}I$. Here step (a) follows from the fact that X^N is an i.i.d. sequence, and (b) holds if we set $U=(MSX^{i-1},i)$ and $X=X_i$ for $I=i$.

Then, using (3.70) and (3.74), we obtain

$$
\begin{aligned}
I(X^N;M)=H(M) &\ge H(M|Y^N)\\
&= H(M,Y^N)-H(Y^N)\\
&= H(M,S,Y^N)-H(S|M,Y^N)-H(Y^N)\\
&\ge H(M,S)+H(Y^N|M,S)-H(S|\widehat{S})-H(Y^N)\\
&\ge I(X^N;M,S)-I(M,S;Y^N)-\delta\log|\mathcal{S}|-1\\
&\ge NI(U;X)-NI(U;Y)-N\delta\log|\mathcal{X}|-1, \quad (3.75)
\end{aligned}
$$

and, dividing both parts of the above expression by N, we obtain for achievable pairs (R_s, R_l) that

$$R_l + \delta \geq \frac{1}{N} I(X^N; M) \geq I(U;X) - I(U;Y) - \delta \log |\mathcal{X}| - \frac{1}{N}, \tag{3.76}$$

where $P(u,x,y) = Q(x,y)P(u|x)$ is the same as above.

Finally, letting $\delta \downarrow 0$ and $N \to \infty$, we obtain the converse from (3.73) and (3.76).

3.5.3 Proof of Thm. 3.2

We prove this theorem by showing that $\mathcal{R}_{sg}^c = \mathcal{R}_{sg}^u$. Assume that we have a code for the unconditional case that satisfies the conditions in Def. 3.1. Then for such a code we have

$$\begin{aligned} I(X^N; M|S) &= H(M|S) - H(M|S, X^N) \\ &\overset{(a)}{\leq} H(M) - H(M|X^N) \\ &= I(X^N; M) \\ &\leq N(R_l + \delta), \end{aligned} \tag{3.77}$$

hence $\mathcal{R}_{sg}^u \subseteq \mathcal{R}_{sg}^c$. Here step (a) holds, since conditioning does not increase entropy and since S is a function of X^N.

Next assume that we have a code for the conditional case and observe that

$$\begin{aligned} I(X^N; M) &= I(X^N, S; M) - I(S; M|X^N) \\ &\overset{(a)}{=} I(S;M) + I(X^N; M|S) \\ &\overset{(b)}{\leq} N\delta + N(R_l + \delta) \\ &= N(R_l + 2\delta), \end{aligned} \tag{3.78}$$

hence $\mathcal{R}_{sg}^c \subseteq \mathcal{R}_{sg}^u$. Therefore $\mathcal{R}_{sg}^c = \mathcal{R}_{sg}^u$. Here step (a) holds, since S and M are functions of X^N, and (b) holds, since for this code $I(S;M) \leq N\delta$.

3.5.4 Proof of Thm. 3.3

Achievability Proof for Thm. 3.3

The achievability proof of this theorem is based on the achievability proof of Thm. 3.1. Here, however, we additionally use a so-called masking layer, see Fig. 3.9, on top of the biometric secret generation model. In this layer the encoder uses the generated secret key S to conceal the chosen secret key K in a one-time pad system, see Vernam [82]. This system was also applied in Ahlswede and Csiszár [3]. We denote

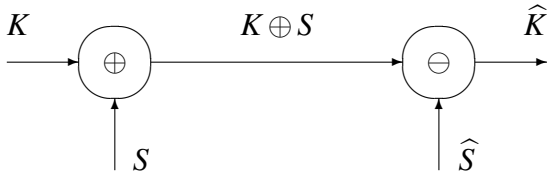


Figure 3.9: *Masking layer.*

addition and substraction modulo $|\mathcal{S}|$ by $\oplus$ and $\ominus$, respectively. Then the encoder produces extra helper data $(K \oplus S)$, which are also sent to the decoder. The decoder produces the estimate of K as $\widehat{K} = (K \oplus S) \ominus \widehat{S}$.

We take $|\mathcal{K}| = |\mathcal{S}|$ and, keeping in mind that the chosen key is uniform, we first consider the secrecy. Note that the helper data for this system are the helper data of the secret generation model and the additional helper data of the masking layer, i.e. $(M, K \oplus S)$.

$$\begin{aligned} I(K; M, K \oplus S) &= H(M, K \oplus S) - H(M, K \oplus S|K) \\ &= H(M) + H(K \oplus S|M) - H(M|K) - H(K \oplus S|M, K) \\ &\overset{(a)}{\leq} H(M) + H(K \oplus S) - H(M) - H(S|M, K) \\ &\leq \log|\mathcal{S}| - H(S|M) \\ &= \log|\mathcal{S}| - H(S) + I(S; M) \\ &\overset{(b)}{\leq} H(S) + N\delta - H(S) + N\delta \\ &= 2N\delta, \end{aligned} \tag{3.79}$$

here step (a) follows from the fact that M and K are independent, and (b) follows from Thm. 3.1, since S is the secret corresponding to the biometric secret generation model, and then $\log|\mathcal{S}| \leq N(H(S) + \delta)$ and $I(M; S) \leq N\delta$ hold.

Observe also that $\widehat{K} = K$, only if $\widehat{S} = S$. Therefore from Thm. 3.1 it follows that $\Pr\{\widehat{K} \neq K\} \leq \delta$.

Next observe that

$$\begin{aligned} 0 \leq I(X^N; K \oplus S|M) &= H(K \oplus S|M) - H(K \oplus S|X^N, M) \\ &\overset{(a)}{\leq} \log|\mathcal{S}| - H(K|X^N, M) \\ &\overset{(b)}{=} \log|\mathcal{S}| - H(K) \\ &\overset{(c)}{=} 0, \end{aligned} \tag{3.80}$$

where step (a) follows from the fact that S is a function of X^N, (b) holds, since K is independent of X^N and also of M, and (c) holds, since K is uniform.

Now we use the result of (3.80) in the following expression

$$\begin{aligned} I(X^N;K\oplus S,M) &= I(X^N;M)+I(X^N;K\oplus S|M) \\ &= I(X^N;M), \end{aligned} \tag{3.81}$$

hence the privacy leakage here is the same as in the biometric secret generation model.

Finally, combining all the obtained results together, we see that for the achievable pairs of the first layer (R_s,R_l), it holds that

$$\begin{aligned} \frac{1}{N}\log|\mathcal{K}| = \frac{1}{N}\log|\mathcal{S}| &\geq R_s-\delta, \\ \frac{1}{N}I(K;M,K\oplus S) &\leq 2\delta, \\ \Pr\{\widehat{K}\neq K\} &\leq \delta, \\ \frac{1}{N}I(X^N;K\oplus S,M) &\leq R_l+\delta. \end{aligned} \tag{3.82}$$

Now, taking into account that for the pairs (R_s,R_l) Thm. 3.1 holds, we conclude that secret-key vs. privacy-leakage rate pairs that are achievable for the biometric secret generation system are also achievable for the system with chosen keys.

Converse for Thm. 3.3

Assume now that the pair (R_k,R_l) is achievable. Consider first the entropy of the secret key

$$\begin{aligned} \log|\mathcal{K}| = H(K) &= I(K;M,Y^N)+H(K|M,Y^N) \\ &= H(M,Y^N)-H(M,Y^N|K)+H(K|M,Y^N) \\ &\overset{(a)}{\leq} H(Y^N)+H(M|Y^N)-H(M|K)-H(Y^N|K,M)+H(K|\widehat{K}) \\ &\overset{(b)}{\leq} NH(Y)-H(Y^N|K,M)+N\delta+\delta\log|\mathcal{K}|+1 \\ &\overset{(c)}{\leq} NI(U;Y)+N\delta+\delta\log|\mathcal{K}|+1, \end{aligned} \tag{3.83}$$

where $U=KMX^{I-1}I$, and I is a uniform random variable, which assumes values in $\{1,2,\ldots,N\}$ and is independent of (X^N,Y^N). Here step (a) follows from the fact that $\widehat{K}$ is a function of Y^N and M, (b) holds, since conditioning does not increase entropy, since Y^N is an i.i.d sequence, since for achievable pairs (R_k,R_l) we have that $I(K;M)\leq N\delta$ and $\Pr\{\widehat{K}\neq K\}\leq\delta$ and due to Fano's inequality, and step (c) follows if we apply similar reasoning as those used to show (3.70), here however $Y^{i-1}\to X^{i-1}\to MKY_i$ holds, which implies that $Y^{i-1}\to MKX^{i-1}\to Y_i$. Indeed, since

X^N and Y^N are i.i.d. sequences, and M is a function of K and X^N only, and K is independent of X^N and Y^N, we have

$$\begin{aligned}
&\Pr\{M=m,K=k,X^{i-1}=x^{i-1},Y^{i-1}=y^{i-1},Y_i=y_i\}\\
&= \sum_{x_i\in\mathcal{X}}\sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{X_i=x_i\}\cdot\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\\
&\quad \Pr\{Y^{i-1}=y^{i-1}|X^{i-1}=x^{i-1}\}\cdot\Pr\{M=m,K=k,Y_i=y_i|X^N=x^N\}\\
&= \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{Y^{i-1}=y^{i-1}|X^{i-1}=x^{i-1}\}\cdot\\
&\quad \sum_{x_i\in\mathcal{X}}\sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X_i=x_i\}\cdot\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\Pr\{M=m,K=k,Y_i=y_i|X^N=x^N\}\\
&= \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{Y^{i-1}=y^{i-1}|X^{i-1}=x^{i-1}\}\cdot\\
&\quad \Pr\{M=m,K=k,Y_i=y_i|X^{i-1}=x^{i-1}\},
\end{aligned}$$

Note that $U_i = KMX^{i-1}$ satisfies Markov condition $U_i \to X_i \to Y_i$, and, consequently, $U \to X \to Y$ holds. Indeed, verify that

$$\begin{aligned}
&\Pr\{M=m,K=k,X^{i-1}=x^{i-1},X_i=x_i,Y_i=y_i\}\\
&\overset{(a)}{=} \sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X^{i-1}=x^{i-1}\}\cdot\Pr\{X_i=x_i\}\cdot\Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\Pr\{Y_i=y_i|X_i=x_i\}\cdot\\
&\qquad \Pr\{M=m,K=k|X^N=x^N,Y_i=y_i\}\\
&\overset{(b)}{=} \Pr\{X_i=x_i\}\cdot\Pr\{Y_i=y_i|X_i=x_i\}\cdot\Pr\{X^{i-1}=x^{i-1}\}\cdot\\
&\qquad \sum_{x_{i+1}^N\in\mathcal{X}^{N-i}} \Pr\{X_{i+1}^N=x_{i+1}^N\}\cdot\Pr\{M=m,K=k|X^N=x^N\}\\
&= \Pr\{X_i=x_i\}\cdot\Pr\{Y_i=y_i|X_i=x_i\}\cdot\Pr\{M=m,K=k,X^{i-1}=x^{i-1}|X_i=x_i\}, \quad (3.84)
\end{aligned}$$

where step (a) follows from the fact that X^N and Y^N are i.i.d. sequences, and (b) holds, since M depends only on X^N and K and K is independent of Y^N.

Now, dividing both parts of (3.83) by N, we obtain for achievable pairs (R_k,R_l) that

$$R_k - \delta \le \frac{1}{N}\log|\mathcal{K}| \le \frac{1}{1-\delta}(I(U;Y)+\delta+\frac{1}{N}), \quad (3.85)$$

for some $P(u,x,y) = Q(x,y)P(u|x)$.

Next consider the privacy leakage.

$$\begin{aligned}
I(X^N;M) &= H(K,M)-H(K|M)-H(M|X^N)\\
&\ge H(K,M)-H(K)-H(K,M|X^N)\\
&= I(K,M;X^N)-\log|\mathcal{K}|\\
&\ge N(I(U;X)-\frac{1}{1-\delta}(I(U;Y)+\delta+\frac{1}{N})), \quad (3.86)
\end{aligned}$$

where U is defined as above, and the last step follows from similar reasoning that were used to derive (3.74).

Then, for achievable pairs (R_k, R_l), we get

$$R_l + \delta \geq \frac{1}{N} I(X^N; M) \geq I(U;X) - \frac{1}{1-\delta}(I(U;Y) + \delta + \frac{1}{N}), \tag{3.87}$$

for the same $P(u,x,y) = Q(x,y)P(u|x)$ as above.

Thus, combining the results in (3.85) and (3.87) and letting $\delta \downarrow 0$ and $N \to \infty$, we obtain

$$\begin{aligned} R_k &\leq I(U;Y), && (3.88)\\ R_l &\geq I(U;X) - I(U;Y), && (3.89) \end{aligned}$$

which finalizes the converse.

3.5.5 Proof of Thm. 3.4

The proof of this theorem repeats the proof of Thm. 3.3. The difference is that we consider now the privacy leakage defined for the conditional case. We only provide the differences here.

Achievability Proof for Thm. 3.4

Here we again use a masking layer on top of the biometric secret generation model, as in Thm. 3.3. Then the helper data for this system become $(M, K \oplus S)$, where M are the helper data from the secret generation model and $(K \oplus S)$ are the helper data from the masking layer. Consider now the privacy leakage in the conditional case.

$$\begin{aligned} I(X^N; K \oplus S, M|K) &= H(K \oplus S, M|K) - H(K \oplus S, M|K, X^N) \\ &= H(S, M|K) - H(S, M|K, X^N) \\ &\overset{(a)}{\leq} H(S) + H(M) \\ &\overset{(b)}{\leq} N(I(U;X) - I(U;Y) + 8\varepsilon + I(U;Y) - 3\varepsilon) \\ &= N(I(U;X) + 5\varepsilon), \end{aligned} \tag{3.90}$$

which allows us to conclude that the privacy leakage $I(U;X)$ is achievable. Here step (a) holds, since S and M are independent of K, since conditioning does not increase entropy and since S, M are functions of X^N, and step (b) follows from the achievability proof of Thm. 3.1, i.e. from (3.60) and (3.61).

Converse for Thm. 3.4

Assume now that the pair (R_k, R_l) is achievable, then

$$\begin{aligned} I(X^N;M|K) &= H(X^N|K) - H(X^N|K,M) \\ &\overset{(a)}{=} I(K,M;X^N) \\ &\overset{(b)}{\geq} NI(U;X), \end{aligned} \tag{3.91}$$

for some U, such that $P(u,x,y) = Q(x,y)P(u|x)$, defined in the converse proof of Thm. 3.3. Here step (a) holds, since K and X^N are independent, and (b) follows from the same reasoning used to derive (3.74).

Then for achievable pairs (R_k, R_l) we get

$$R_l + \delta \geq \frac{1}{N} I(X^N;M|K) \geq I(U;X). \tag{3.92}$$

Letting $\delta \downarrow 0$ and $N \to \infty$, we obtain the converse.

3.5.6 Proof of Thm. 3.5

Achievability Proof for Thm. 3.5

Later, in the achievability proof corresponding to Thm. 3.6, where we consider the conditional case, we will prove that the achievable region $\mathcal{R}^c_{zsg}$ is equal $\mathcal{R}_3$. Given this result, the achievability part of this theorem is proven by showing that $\mathcal{R}^u_{zsg} \supseteq \mathcal{R}^c{}_{zsg}$. Assume that we have a code for the conditional case that satisfies the conditions of Def. 3.3. Then observe that

$$\begin{aligned} I(X^N;M) + I(S;M) &= I(X^N,S;M) - I(S;M|X^N) + I(S;M) \\ &\leq N\delta + N\delta \\ &= 2N\delta. \end{aligned} \tag{3.93}$$

Hence from (3.93) we may conclude that $\mathcal{R}^u_{zsg} \supseteq \mathcal{R}^c_{zsg}$.

Converse for Thm. 3.5

Assume that the secret-key vs. private-key rate pair (R_{zs}, R_p) is achievable. Consider first the entropy of the secret.

$$\begin{aligned} H(S) &= I(S;P,M,Y^N) + H(S|P,M,Y^N) \\ &\overset{(a)}{\leq} I(S;M) + I(S;P|M) + I(S;Y^N|M,P) + H(S|\widehat{S}) \\ &\overset{(b)}{\leq} N\delta + H(P) + H(Y^N|M,P) - H(Y^N|M,P,S) + \delta \log|\mathcal{S}| + 1 \\ &\overset{(c)}{\leq} N(1+\delta)R_p + NH(Y) - H(Y^N|M,P,S) + 2N\delta + N\delta \log|\mathcal{X}| + N\delta^2 + 1, \end{aligned} \tag{3.94}$$

where step (a) holds, since $\widehat{S}$ is a function of Y^N, P and M, (b) follows from the fact that, for achievable pairs (R_{zs}, R_p), we have that $I(S;M) \leq N\delta$ and $\Pr\{\widehat{S} \neq S\} \leq \delta$, from the fact that conditioning does not increase entropy, and from Fano's inequality, and (c) follows from the facts that conditioning does not increase entropy and that Y^N is an i.i.d. sequence, since $|\mathcal{S}| \leq |\mathcal{X}|^N \cdot |\mathcal{P}|$ (possibly) after renumbering and from the definition of achievable pairs (R_{zs}, R_p).

Now consider $H(Y^N|M,S,P)$.

$$\begin{aligned} H(Y^N|M,S,P) &= \sum_{i=1}^{N} H(Y_i|M,S,P,Y^{i-1}) \\ &\geq \sum_{i=1}^{N} H(Y_i|M,S,P,Y^{i-1},X^{i-1}) \\ &\stackrel{(a)}{=} \sum_{i=1}^{N} H(Y_i|M,S,P,X^{i-1}) \\ &= NH(Y|U), \end{aligned} \tag{3.95}$$

where I is a random variable uniformly distributed on $\{1,2,\ldots,N\}$ and independent of (X^N, Y^N), and we define $U = MSPX^{I-1}I$. Here step (a) follows from the fact that $Y^{i-1} \to X^{i-1} \to MSPY_i$, which implies that $Y^{i-1} \to MSPX^{i-1} \to Y_i$. Note also that $U_i = MSPX^{i-1}$ satisfies Markov condition $U_i \to X_i \to Y_i$, and, consequently, $U \to X \to Y$ holds. Markovity can be verified in the same way as before.

Now, combining (3.94) and (3.95), we obtain for achievable pairs (R_{zs}, R_p)

$$\begin{aligned} R_{zs} - 2\delta \leq \frac{1}{N}\log|\mathcal{S}| - \delta \leq \frac{1}{N}H(S) \quad \leq \\ I(U;Y) + (1+\delta)R_p + 2\delta + \delta\log|\mathcal{X}| + \delta^2 + \frac{1}{N}, \end{aligned} \tag{3.96}$$

for some $P(u,x,y) = Q(x,y)P(u|x)$.

Next observe that

$$\begin{aligned} I(X^N;M,S,P) &= \sum_{i=1}^{N} I(X_i;M,S,P|X^{i-1}) \\ &= NI(X_I;M,S,P|X^{I-1},I) \\ &\stackrel{(a)}{=} NI(X_I;S,M,P,X^{I-1},I) \\ &\stackrel{(b)}{=} NI(U;X), \end{aligned} \tag{3.97}$$

where as before $U = MSPX^{I-1}I$. Here step (a) holds, since X^N is an i.i.d. sequence, and (b) holds if we set $U = (SMPX^{i-1}, i)$ and $X = X_i$ for $I = i$.

Now we can write

$$\begin{aligned}
N\delta &\geq I(X^N;M)+I(S;M)\\
&\geq I(X^N;M)\\
&= I(X^N,P,S;M)-I(P,S;M|X^N)\\
&= H(M)-H(M|X^N,P,S)-H(P|X^N)-H(S|P,X^N)+H(P,S|X^N,M)\\
&\overset{(a)}{\geq} H(M)-H(P)\\
&\geq H(M|Y^N)-H(P)\\
&= H(M,Y^N)-H(Y^N)-H(P)\\
&= H(S,P,M,Y^N)-H(S,P|M,Y^N)-H(Y^N)-H(P)\\
&= H(S,M)+H(P,Y^N|S,M)-H(P|M,Y^N)-H(S|P,M,Y^N)-H(Y^N)-H(P)\\
&= I(S,M;X^N,P)+H(P|S,M)+H(Y^N|S,M,P)-H(P|M,Y^N)-\\
&\quad H(S|P,M,Y^N)-H(Y^N)-H(P)\\
&\overset{(b)}{\geq} I(S,M;X^N|P)+I(S,M;P)+H(P|S,M)+NH(Y|U)-H(P|M,Y^N)-\\
&\quad H(S|\widehat{S})-NH(Y)-H(P)\\
&\overset{(c)}{\geq} I(S,M,P;X^N)-NI(U;Y)-\delta\log|\mathcal{S}|-1-H(P)\\
&\overset{(d)}{\geq} N(I(U;X)-I(U;Y)-(1+\delta)R_p-\delta-\delta\log|\mathcal{X}|-\delta^2-\frac{1}{N}),
\end{aligned} \tag{3.98}$$

where as before $U=MSPX^{I-1}I$. Here step (a) holds, since P is independent of X^N and since S and M are functions of X^N and P, (b) follows from (3.95), from the facts that conditioning does not increase entropy, that Y^N is an i.i.d. sequence and that $\widehat{S}$ is function of M,P and Y^N, (c) holds, since X^N and P are independent, since for achievable pairs (R_{zs},R_p) it holds that $\Pr\{S\neq\widehat{S}\}\leq\delta$, and due to Fano's inequality, and (d) follows from (3.97), from the fact that $|\mathcal{S}|\leq|\mathcal{X}|^N\cdot|\mathcal{P}|$ holds (possibly) after renumbering, and from the definition of achievable pairs (R_{zs},R_p).

Then, rearranging and dividing both parts of (3.98) by N and recalling (3.96), we obtain for $\delta\downarrow 0$ and $N\to\infty$ that

$$R_{zs} \leq I(U;Y)+R_p, \tag{3.99}$$

$$R_p \geq I(U;X)-I(U;Y), \tag{3.100}$$

for the same $P(u,x,y)=Q(x,y)P(u|x)$ as before. This yields the converse.

3.5.7 Proof of Thm. 3.6

We only need the achievability proof here, the converse for this theorem is the same as for Thm. 3.5.

Achievability Proof for Thm. 3.6

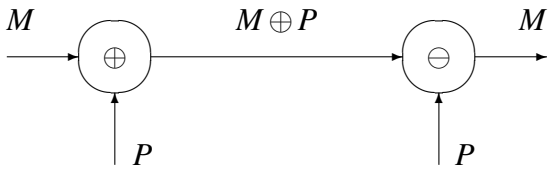


Figure 3.10: *Helper data masking interlayer.*

The achievability proof of Thm. 3.6 is an adapted version of the basic achievability proof. The difference is that now the secret is the index of u^N. Then the secret-key rate R_{zs} becomes equal to $I(U;X)$ and the corresponding helper-label rate (as before) is equal to $I(U;X)-I(U;Y)$. Note that the index uniquely defines u^N and then u^N is uniform and so the secret is. Moreover, to make the helper data completely uninformative, we use a private key P to mask the helper data in a one-time pad way, see Fig. 3.10. Thus the helper data become $M \oplus P$, where $\oplus$ denotes addition modulo $|\mathcal{P}|$. Observe that the private-key rate $I(U;X)-I(U;Y)$ suffices. Indeed,

$$\begin{aligned} I(X^N; M\oplus P) &= H(M\oplus P) - H(M\oplus P|X^N) \\ &\overset{(a)}{\leq} \log|\mathcal{M}| - H(P|X^N) \\ &\overset{(b)}{=} N(I(U;X)-I(U;Y)+8\varepsilon) - H(P) \\ &= N(I(U;X)-I(U;Y)+8\varepsilon) - \log|\mathcal{P}| \\ &= 0, \end{aligned} \tag{3.101}$$

if we take $I(U;X)-I(U;Y)+8\varepsilon = \frac{1}{N}\log|\mathcal{P}|$ for N large enough. Here step (a) holds since M is a function of X^N, and (b) follows from the basic achievability proof and from the fact that P is independent of X^N.

Observe also that this system has zero-leakage (note that in this setting we have strong secrecy, i.e. the leakage is exactly equal to zero)

$$\begin{aligned} I(X^N, S; M\oplus P) &= H(M\oplus P) - H(M\oplus P|X^N, S) \\ &\overset{(a)}{\leq} \log|\mathcal{P}| - H(P|X^N, S, M) \\ &\overset{(b)}{=} 0, \end{aligned} \tag{3.102}$$

where step (a) holds, since M is a function of X^N, and (b) holds, since P is independent of X^N and S, and uniform.

Note that for the private-key rate $R_p = I(U;X)-I(U;Y)$, we can write $R_{zs} = I(U;X) = I(U;Y)+R_p$. Then we conclude that the pair $(I(U;Y)+R_p, I(U;X)-I(U;Y))$ is achievable for $\varepsilon \downarrow 0$ and $N \to \infty$.

Observe next that if $(I(U;Y)+R_p, I(U;X)-I(U;Y)$ is achievable, then also pairs $(I(U;Y)+R_p+\alpha, I(U;X)-I(U;Y)+\alpha), \alpha>0$ are. Indeed, if we take the private key of rate $I(U;X)-I(U;Y)+\alpha$, then the part of the private key, which has rate $I(U;X)-I(U;Y)$, suffices to conceal the helper data, and we can use the other part of the private key, which has rate α, as a secret key. Thus we increase the secret-key rate by α, which results in $R_{zs}=I(U;Y)+R_p+\alpha$.

3.5.8 Proof of Thm. 3.7

Achievability Proof for Thm. 3.7

The achievability proof is based on Thm. 3.5. The difference is that here, as in Thm. 3.3, we additionally use a masking layer to conceal a chosen secret key K with the generated secret key S. The addition and substraction in this masking layer are modulo $|\mathcal{S}|$. The chosen key is uniform and we take $|\mathcal{K}|=|\mathcal{S}|$. The helper data for this system become $(M\oplus P, K\oplus S)$, where $M\oplus P$ are the masked helper data as in Thm. 3.5 and $(K\oplus S)$ are the helper data from the masking layer. Now for the secrecy we obtain

$$\begin{aligned} I(K;S\oplus K, M\oplus P) &= I(K;M\oplus P)+I(K;S\oplus K|M\oplus P) \\ &\overset{(a)}{=} H(S\oplus K|M\oplus P)-H(S\oplus K|M\oplus P,K) \\ &\leq \log|\mathcal{S}|-H(S|M\oplus P,K) \\ &\overset{(b)}{\leq} H(S)+N\delta-H(S|M\oplus P) \\ &= I(S;M\oplus P)+N\delta, \end{aligned} \tag{3.103}$$

here step (a) follows from the fact that K is independent of M and P, (b) holds, since S is the generated secret key for which Thm. 3.5 holds, and hence $\log|\mathcal{S}|\leq H(S)+N\delta$, and since S is independent of K.

Now for the privacy leakage we write

$$\begin{aligned} I(X^N;S\oplus K, M\oplus P) &= I(X^N;M\oplus P)+I(X^N;S\oplus K|M\oplus P) \\ &= I(X^N;M\oplus P)+H(S\oplus K|M\oplus P)-H(S\oplus K|M\oplus P,X^N) \\ &\overset{(a)}{\leq} I(X^N;M\oplus P)+H(S\oplus K)-H(K|P,X^N) \\ &\overset{(b)}{\leq} I(X^N;M\oplus P)+\log|\mathcal{S}|-H(K) \\ &\overset{(c)}{=} I(X^N;M\oplus P), \end{aligned} \tag{3.104}$$

where step (a) follows from the fact that M and S are functions of X^N, (b) holds, K is independent of X^N and P, and (c) holds, since K is uniform.

Note also that $K = \widehat{K}$ only if $S = \widehat{S}$, and then due to Thm. 3.5, $\Pr\{K \neq \widehat{K}\} \leq \delta$.

Finally, combining all the results together, we see that for the achievable pairs of the first layer (R_{zs}, R_p) it holds that

$$\begin{aligned}
\frac{1}{N}\log|\mathcal{K}| = \frac{1}{N}\log|\mathcal{S}| &\geq R_{zs} - \delta, \\
\frac{1}{N}I(K; S\oplus K, M\oplus P) &\leq 2\delta, \\
\frac{1}{N}I(X^N; S\oplus K, M\oplus P) &\leq \delta, \\
\Pr\{\widehat{K} \neq K\} &\leq \delta, \\
\log|\mathcal{P}| &\leq R_p + \delta. \qquad (3.105)
\end{aligned}$$

Then taking into account that for the pairs (R_{zs}, R_p) Thm. 3.5 holds and letting $\delta \downarrow 0$ and $N \to \infty$, we may conclude that secret-key vs. private-key rate pairs achievable for the biometric secret generation model with zero-leakage in the unconditional case are also achievable for models with chosen keys and zero-leakage in the unconditional case.

Converse for Thm. 3.7

Now assume that the secret-key vs. private-key rate pair (R_{zk}, R_p) is achievable. We start with the entropy of the secret key.

$$\begin{aligned}
\log|\mathcal{K}| = H(K) &= I(K; P, M, Y^N) + H(K|P, M, Y^N) \\
&\overset{(a)}{\leq} I(K; M) + I(K; P|M) + I(K; Y^N|M, P) + H(K|\widehat{K}) \\
&\overset{(b)}{\leq} N\delta + H(P) + H(Y^N|M, P) - H(Y^N|M, P, K) + \delta\log|\mathcal{K}| + 1 \\
&\overset{(c)}{\leq} N\delta + NR_p + N\delta + NH(Y) - H(Y^N|M, P, K) + \delta\log|\mathcal{K}| + 1 \\
&\overset{(d)}{\leq} NI(U; Y) + NR_p + 2N\delta + \delta\log|K| + 1, \qquad (3.106)
\end{aligned}$$

where $U = MKPX^{I-1}I$ and I is a random variable uniformly distributed on $\{1, 2, \ldots, N\}$ and independent of (X^N, Y^N). Here step (a) holds, since $\widehat{K}$ is a function of Y^N, P and M, (b) holds, since for achievable pairs (R_{zk}, R_p) we have that $I(K; M) \leq N\delta$ and also $\Pr\{\widehat{K} \neq K\} \leq \delta$, since conditioning does not increase entropy and due to Fano's inequality, (c) follows from the definition of achievable pairs (R_{zk}, R_p), from the facts that conditioning does not increase entropy and that Y^N is an i.i.d. sequence, and in step (d) we used the fact that $Y^{i-1} \to MKPX^{i-1} \to Y_i$, and set $U = (MKPX^{i-1}, i)$ and $Y = Y_i$ for $I = i$. Note that Markovity can be verified as before.

Now for achievable pairs (R_{zk}, R_p) we have

$$R_{zk} - \delta \leq \frac{1}{N}\log|\mathcal{K}| \quad \leq \quad \frac{1}{1-\delta}(I(U;Y) + R_p + 2\delta + \frac{1}{N}), \tag{3.107}$$

for some $P(u,x,y) = Q(x,y)P(u|x)$.

For the privacy leakage we can write

$$\begin{aligned}
N\delta \geq I(X^N;M) &= I(K,M,P;X^N) - I(K,P;X^N|M) \\
&\overset{(a)}{=} NI(U;X) - H(K,P|M) + H(K,P|M,X^N) \\
&\geq NI(U;X) - H(P|M) - H(K|P,M) \\
&\geq NI(U;X) - H(P) - H(K,Y^N|P,M) + H(Y^N|P,M,K) \\
&\overset{(b)}{\geq} NI(U;X) - NR_p - N\delta - H(Y^N|P,M) - H(K|P,M,Y^N) + \\
&\quad H(Y^N|P,M,K) \\
&\overset{(c)}{\geq} NI(U;X) - NR_p - N\delta - NH(Y) - H(K|\widehat{K}) + NH(Y|U) \\
&\overset{(d)}{\geq} NI(U;X) - NI(U;Y) - NR_p - N\delta - \delta\log|\mathcal{K}| - 1,
\end{aligned} \tag{3.108}$$

here step (a) holds, since $I(K,M,P;X^N) = NI(U;X)$ holds for an i.i.d. sequence X^N and for U, defined as before, which can be shown in a similar way as (3.97), (b) follows from the definition of achievable pairs (R_{zk}, R_p), (c) holds, since conditioning does not increase entropy, since Y^N is an i.i.d. sequence, since $\widehat{K}$ is a function of P,M and Y^N, since $Y^{i-1} \to MKPX^{i-1} \to Y_i$ holds, and we set $U = (MKPX^{i-1}, i)$ and $Y = Y_i$ for $I = i$, and (d) holds, since for achievable pairs (R_{zk}, R_p) we have $\Pr\{K \neq \widehat{K}\} \leq \delta$, and due to Fano's inequality.

Then from (3.108) and (3.107), letting $\delta \downarrow 0$ and $N \to \infty$, we obtain

$$R_{zk} \leq I(U;Y) + R_p, \tag{3.109}$$

$$R_p \geq I(U;X) - I(U;Y), \tag{3.110}$$

for the same $P(u,x,y) = Q(x,y)P(u|x)$ as before.

Finally, note that $U_i = MKPX^{i-1}$ satisfies Markov condition $U_i \to X_i \to Y_i$, and, consequently, $U \to X \to Y$ holds. This finalizes the converse.

3.5.9 Proof of Thm. 3.8

Achievability Proof for Thm. 3.8

The achievability follows from using the private key P to mask the secret key K in a one-time pad way. Then the helper data become $K \oplus P$, where addition is modulo $|\mathcal{P}|$. Clearly the scheme is secure for $R_{zk} \leq R_p$ and leaks no privacy, as there are no biometric data involved.

Converse for Thm. 3.8

Assume that the secret-key vs. private-key rate pair (R_{zk}, R_p) is achievable. Consider the entropy of the secret. Then we have

$$\begin{aligned}
\log|\mathcal{K}| = H(K) &= I(K;P,M,Y^N) + H(K|P,M,Y^N) \\
&\overset{(a)}{\leq} I(K;Y^N) + I(K;M|Y^N) + I(K;P|Y^N,M) + H(K|\widehat{K}) \\
&\overset{(b)}{\leq} H(M|Y^N) - H(M|Y^N,K) + H(P) + \delta\log|\mathcal{K}| + 1 \\
&\overset{(c)}{\leq} I(M;Y^N,K) + NR_p + N\delta + \delta\log|\mathcal{K}| + 1 \\
&\overset{(d)}{\leq} I(M;X^N,K) + NR_p + N\delta + \delta\log|\mathcal{K}| + 1 \\
&\overset{(e)}{\leq} NR_p + 2N\delta + \delta\log|\mathcal{K}| + 1, \qquad (3.111)
\end{aligned}$$

where step (a) follows from the fact that $\widehat{K}$ is a function of P,M and Y^N, (b) holds, since K is independent of Y^N, since for achievable pairs (R_{zk}, R_p) we have that $\Pr\{\widehat{K} \neq K\} \leq \delta$ and due to Fano's inequality, (c) from the fact that conditioning does not increase entropy, and from the definition of achievable pairs (R_{zk}, R_p), (d) holds due to $M \to KX^N \to Y^N$. Indeed, since M is a function of X^N, K and P only, and K is independent of X^N and Y^N, we have

$$\begin{aligned}
&\Pr\{M=m, K=k, X^N=x^N, Y^N=y^N\} \\
&= \Pr\{Y^N=y^N\}\cdot\Pr\{X^N=x^N|Y^N=y^N\}\cdot\Pr\{K=k\}\cdot \\
&\qquad \Pr\{M=m|K=k, X^N=x^N, Y^N=y^N\} \\
&= \Pr\{Y^N=y^N\}\cdot\Pr\{X^N=x^N, K=k|Y^N=y^N\}\cdot\Pr\{M=m|K=k, X^N=x^N\}.
\end{aligned}$$

Step (e) holds, since for achievable pairs (R_{zk}, R_p) we have that $I(M;X^N,K) \leq N\delta$.

Rearranging and dividing both parts of the above expression by N, we obtain for achievable pairs (R_{zk}, R_p) that

$$R_{zk} - \delta \leq \frac{1}{N}\log|\mathcal{K}| \leq \frac{1}{1-\delta}(R_p + 2\delta + \frac{1}{N}). \qquad (3.112)$$

Finally, letting $\delta \downarrow 0$ and $N \to \infty$, we obtain the converse.

3.6 Relations Between Regions

3.6.1 Overview

In Fig. 3.11 we summarize our results on the achievable regions obtained for all eight considered settings. We cannot compare the regions for models with leakage

with regions for models with zero-leakage. Therefore in the figure we show pairs of achievable regions for models with leakage and models with zero-leakage. The region pairs are given for models with generated keys and models with chosen keys for unconditional and conditional privacy leakage.

	Generated keys	Chosen keys
Unconditional leakage	$\mathcal{R}_1/\mathcal{R}_3$	$\mathcal{R}_1/\mathcal{R}_3$
Conditional leakage	$\mathcal{R}_1/\mathcal{R}_3$	$\mathcal{R}_2/\mathcal{R}_4$

Figure 3.11: *Region overview. By slash (/) we separate the regions for models with leakage and models with zero-leakage.*

Looking at the figure we can see that for all models but one the pairs of achievable regions are the same, i.e. $\mathcal{R}_1/\mathcal{R}_3$. However, when chosen keys are used in the conditional leakage setting, we obtain a different pair of regions. In this case we get regions $\mathcal{R}_2/\mathcal{R}_4$.

Consider first the models with privacy leakage. It is clear that the secret-generation system can be transformed into the chosen-key system (one-time pad makes it possible). Therefore the amount of secret information that can be conveyed with biometric data from one terminal to another should be at least the same as the amount of common secret key that can be extracted from biometric data by two terminals. Our theorems show that they are the same. On the other hand, if we look at the leakage, then in secret-generation models for the conditional case we get that $I(S,X^N;M) = I(X^N;M)$, since S is a function of X^N. Thus the regions for the conditional and unconditional cases for secret-generation models are the same. In chosen-key models, K is independent of X^N, and therefore information that a pair (K,X^N) contains is larger than the information that a pair (S,X^N) does. Moreover, to reliably convey K, M should contain some information about both K and X^N. Now if we consider unconditional privacy leakage $I(X^N;M)$, then, since we convey the same amount of secret information that was extracted in the secret-generation setting, we need at most the same amount of information from biometric data to conceal the key (think about one-time pad again). Hence the helper data of the chosen-key setting should provide at most the same amount of information on the X^N as in the secret-generation setting and, consequently, leaks at most the same amount of information on X^N.

Therefore the achievable region in this case could be again the same as in the secret-generation setting. Our theorems confirm this. However, when conditional notion of privacy leakage is used, then, since we require our model to be secure while $I(X^N;M) \leq I(K,X^N;M) = I(K;M) + I(X^N;M|K)$, all the leakage "load" goes on biometrics. Thus we have larger privacy leakage and smaller achievable region. Now, since models with zero-leakage are the extension of models with privacy leakage when we additionally use private key, also three of four corresponding achievable regions are the same.

Note that the reasoning above shows that the regions for the secret-generation models in both the unconditional and conditional case are smaller than or equal to the region for chosen-key systems in unconditional case. We do not have the intuition why these regions are exactly the same. It remains to be an open question.

3.6.2 Comparison of $\mathcal{R}_1$ and $\mathcal{R}_2$

Comparing $\mathcal{R}_1$ and $\mathcal{R}_2$, we see from (3.18) and (3.19) that for some fixed U with $P(u,x,y) = Q(x,y)P(u|x)$ we have that $\mathcal{R}_2 \subseteq \mathcal{R}_1$.

Observe that for each point $(R,L) \in \mathcal{R}_2$, there exits an auxiliary random variable U with $P(u,x,y) = Q(x,y)P(u|x)$, such that

$$\begin{aligned} R &\leq I(U;Y), \\ L &\geq I(U;X) \end{aligned} \tag{3.113}$$

holds. Then also the following inequalities hold

$$\begin{aligned} R &\leq I(U;Y), \\ R-L &\geq I(U;X) - I(U;Y). \end{aligned} \tag{3.114}$$

Therefore we may conclude that $(R,R-L) \in \mathcal{R}_1$.

Let $\partial\mathcal{R}_1$ denote the boundary of $\mathcal{R}_1$. Then let $(R^*,L^*) \in \partial\mathcal{R}_1$. We look at all auxiliary random variables U such that

$$I(U;Y) = R^*.$$

Moreover, among these random variables U we take the one such that the leakage rate is minimum, i.e.

$$I(U;X) - I(U;Y) = L^*.$$

Note that if this leakage rate $I(U;X) - I(U;Y)$ is minimum, then also $I(U;X)$ is minimum with which R^* is achieved. Therefore $(R^*,R^*+L^*) \in \partial\mathcal{R}_2$. Thus given a boundary of $\mathcal{R}_1$ we can construct the boundary of $\mathcal{R}_2$. Using similar arguments, it can also be shown that boundary of $\mathcal{R}_1$ can be constructed from the boundary of $\mathcal{R}_2$.

3.6.3 $\mathcal{R}_3$. Relation to $\mathcal{R}_1$

Note that $\mathcal{R}_3$ can be constructed as an extension of $\mathcal{R}_1$. Indeed, observe that for each $(R,L) \in \mathcal{R}_1$ there exits an auxiliary random variable U with $P(u,x,y) = Q(x,y)P(u|x)$, such that

$$\begin{aligned} R &\leq I(U;Y), \\ L &\geq I(U;X) - I(U;Y). \end{aligned} \tag{3.115}$$

From these inequalities it also follows that

$$\begin{aligned} R+L &\leq I(U;Y) + L, \\ L &\geq I(U;X) - I(U;Y). \end{aligned} \tag{3.116}$$

Therefore we may conclude that $(R+L,L) \in \mathcal{R}_3$. Similarly, for each $(R,L) \in \mathcal{R}_3$ there exits an auxiliary random variable U with $P(u,x,y) = Q(x,y)P(u|x)$ for which it holds that

$$\begin{aligned} R &\leq I(U;Y) + L, \\ L &\geq I(U;X) - I(U;Y), \end{aligned} \tag{3.117}$$

and then for $R-L \geq 0$ it holds that

$$\begin{aligned} R-L &\leq I(U;Y), \\ L &\geq I(U;X) - I(U;Y). \end{aligned} \tag{3.118}$$

This allows us to conclude that $(R-L,L) \in \mathcal{R}_1$.

Note also that for any $\alpha \geq 0$, if $(R,L) \in \mathcal{R}_1$ and U is same as before, we have that

$$\begin{aligned} L+\alpha &\geq L \geq I(U;X) - I(U;Y), \\ R+L+\alpha &\leq I(U;Y) + L + \alpha, \end{aligned} \tag{3.119}$$

and then also $(R+\alpha, L+\alpha) \in \mathcal{R}_3$, for any $\alpha \geq 0$.

Observe that for $\mathcal{R}_3$ we can rewrite the bound for the secret-key rate as

$$0 \leq R_s \leq I(U;X) + (R_p - (I(U;X) - I(U;Y))). \tag{3.120}$$

In this way secret keys in models with achievable region $\mathcal{R}_3$ can be seen as a combination of common randomness, see Ahlswede and Csiszár [4], and a part of a cryptographic (private) key that remains after masking the leakage. We may also conclude that biometrics can be used to increase cryptographic key size if both cryptographic and biometric keys are used in secrecy systems. Moreover, in this setting a biometric key would guarantee the authenticity of a user, while a cryptographic key would guarantee zero-privacy leakage.

3.6.4 $\mathcal{R}_4$

Note that the form of $\mathcal{R}_4$ implies that biometrics is actually useless in the setting where both a chosen key and a private key are involved in a secrecy system. Note, that just as for $\mathcal{R}_3$, we can see the bound for the secret-key rate as

$$0 \leq R_s \leq I(U;X) + (R_p - I(U;X)). \tag{3.121}$$

Then secret keys in models with achievable region $\mathcal{R}_4$ can be seen again as a combination of common randomness and a part of a cryptographic (private) key that remains after masking the leakage (in $\mathcal{R}_2$). In this case, however, we observe that using biometrics we do not gain anything.

3.7 Conclusions and Remarks

In this chapter we have investigated privacy leakage in biometric systems which are based on i.i.d. discrete biometric sources. We distinguished between secret-generation systems and chosen-secret systems. Moreover, we have focused not only on systems in which we require the privacy leakage to be as small as possible, but also on systems in which a private key is used to remove all privacy leakage. For the resulting four settings we considered both conditional and unconditional leakage. This led to eight fundamental balances and the corresponding secret-key vs. privacy-leakage rate regions and secret-key vs. private-key rate regions.

Summarizing, we conclude that for systems without a private key, the achievable region is equal to $\mathcal{R}_1$, except for the chosen-key case with conditional leakage where the achievable region is in principle smaller and only equal to $\mathcal{R}_2$. When $\mathcal{R}_1$ is the achievable region the rate can be either larger or smaller than the leakage depending on the source quality, however when $\mathcal{R}_2$ is the achievable region the rate cannot be larger than the leakage.

Similarly we may conclude that for zero-leakage systems, the achievable region is equal to $\mathcal{R}_3$, except for the chosen-key case with conditional leakage where the achievable region is only equal to $\mathcal{R}_4$. It is important to observe that in this last case the biometrics are actually useless. In zero-leakage systems the secret-key rate cannot be smaller than the private-key rate.

Regarding the achievable regions, we may finally conclude that the a secret-key vs. privacy-leakage rate region is never larger than the corresponding secret-key vs. private-key rate region. This is intuitively clear if we realize that a model is optimal if the private key is used to mask the helper data (privacy leakage), and remaining private-key bits are transformed into extra secret-key bits.

Recall the rate-leakage ratio, discussed in the example of the introduction to the current chapter. This ratio characterizes the slope of the boundary of the achievable regions found here. The higher the slope is the better the trade-off between

the secret-key rate and the privacy-leakage rate is. It is not difficult to see that the slope corresponding to the Ahlswede-Csiszár [3] result is the smallest slope achievable in secret-generation systems, see also Fig. 3.5. On the other hand, if we look at the slope corresponding to the key-rate vs. the zero privacy-leakage rate we derive a characterization for biometric data quality. Indeed, the higher this slope is, the larger the achievable region is and the better the "channel" between enrollment and authentication biometric sources is.

The achievability proofs that we have presented in this chapter can serve as guidelines for designing codes that achieve near-optimal performance. They suggest that optimal codes should incorporate both vector quantization methods and Slepian-Wolf techniques. In the linear case Slepian-Wolf coding is equivalent to transmitting the syndrome of the quantized sequence.

The fundamental trade-offs found in this chapter can be used to assess the optimality of practical biometric systems. We will see it in the next chapter, when we analyze a particular realization of the biometric model with chosen keys. Moreover, the trade-offs that we have found can be used to determine whether a certain biometric modality satisfies the requirements of an application. Furthermore, as we could see, zero-leakage biometric systems can be used to combine traditional cryptographic secret keys with biometric data. It gives us the opportunity to get the best of the two worlds: the biometric part would guarantee the authenticity of a user and increase the secret key size, while the cryptographic part provides strong secrecy and prevents privacy leakage.

We have only looked at systems here based on a single biometric modality. Further investigations are needed to find how the trade-offs behave in cases with multiple modalities.

In practice, biometric features are often represented by continuous vectors, and therefore the fundamental results for biometric systems based on continuous Gaussian biometric data would be an interesting next step to consider.

At the end of this chapter, we would like to mention that the results that we have proved here were presented at Allerton conference [35]. At the same conference the recent results of Lai et al. also on the privacy-secrecy trade-off in biometric systems were reported [44]. Although there are some overlapping results (the two basic theorems), our investigations expand in the direction of extra private keys and conditional leakage, while Lai et al. extended their basic results by considering side information models.

Chapter 4

Leakage in Fuzzy Commitment Schemes

To live effectively is to live with adequate information (Norbert Wiener).

4.1 Introduction

Fuzzy commitment, introduced by Juels and Wattenberg [41], is a particular realization of a binary biometric secrecy system with chosen secret keys considered in the previous chapter of this thesis. In the fuzzy commitment scheme, the helper data are constructed as a codeword from a selected error-correcting code, used to encode a chosen secret, masked with the biometric sequence that has been observed during enrollment. The scheme is primarily designed for biometric data represented by binary uniform memoryless sequences, and it is provably secure for this case.

The scheme became a popular technique for designing biometric secrecy systems, since it is convenient and easy to implement using standard error-correcting codes. The implementation of fuzzy commitment for different biometric modalities can be found in Kevenaar et al. [42] (faces), Hao et al. [33] (irises), Campisi et al. [11] (signatures), Yang and Verbauwhede [95] (irises), etc. In practice, however, biometric data are rarely uniform. Biometric data used in fuzzy commitment based systems, e.g. in the literature mentioned above, do not satisfy the criteria of being uniform and memoryless. Nevertheless, it is assumed that these systems are secure. Also the privacy properties of these systems are hardly investigated. In Smith [72], though, it was already observed that in fuzzy commitment the helper data leak information on the secret if the biometric data are non-uniform, and that they must also leak some information about the biometric data. The privacy leakage corresponding to the maximum secret-key rate for the original uniform memoryless setting was also determined by Tuyls and Goseling [79].

In this chapter we will investigate the properties of the fuzzy commitment scheme when the biometric data statistic is memoryless and totally-symmetric, memoryless and input-symmetric, memoryless, and stationary ergodic. We will use the fundamental secret-key vs. privacy-leakage rate trade-offs found in Chapter 3 to assess

the optimality of fuzzy commitment. We will show that the fuzzy commitment scheme is only optimal for the totally-symmetric memoryless case and only if the scheme operates at the maximum secret-key rate. Moreover, we will show that for the general memoryless and stationary ergodic cases the scheme reveals information on both the secret and biometric data. We will not be able to determine the achievable rate-leakage regions for these two cases and will only provide outer bounds on the corresponding achievable rate-leakage regions. These bounds will be sharpened for systematic parity-check codes.

4.2 The Fuzzy Commitment Scheme

4.2.1 Description

We start with description of biometric sources. A fuzzy commitment scheme processes a binary biometric enrollment sequence $x^N = \{x_1, x_2, \ldots, x_N\}$ with symbols $x_n \in \{0,1\}$ for $n = 1,2,\ldots,N$ and a binary biometric authentication sequence $y^N = \{y_1, y_2, \ldots, y_N\}$ with symbols $y_n \in \{0,1\}$ for $n = 1,2,\ldots,N$. These sequences are generated by a biometric source according to some distribution $\{Q(x^N, y^N), x^N \in \{0,1\}^N, y^N \in \{0,1\}^N\}$. We distinguish between the following four cases, i.e. the totally-symmetric memoryless case, the input-symmetric memoryless case, the memoryless case, and the stationary ergodic case.

1. The Totally-Symmetric Memoryless Case. We assume that

$$\Pr\{X^N = x^N, Y^N = y^N\} = \prod_{n=1}^{N} Q(x_n, y_n), \tag{4.1}$$

for some joint probability distribution $\{Q(x,y), x \in \{0,1\}, y \in \{0,1\}\}$, satisfying

$$Q(0,0) = Q(1,1) = (1-q)/2, \tag{4.2}$$
$$Q(0,1) = Q(1,0) = q/2, \tag{4.3}$$

where $0 \leq q \leq 1/2$. Here the parameter q is called crossover probability.

2. The Input-Symmetric Memoryless Case. We assume that (4.1) holds for some joint probability distribution $\{Q(x,y), x \in \{0,1\}, y \in \{0,1\}\}$ that satisfies

$$Q(1,0) + Q(1,1) = 1/2. \tag{4.4}$$

The crossover probability is defined as

$$q \stackrel{\Delta}{=} Q(0,1) + Q(1,0). \tag{4.5}$$

3. The Memoryless Case. Now we assume that (4.1) holds for an arbitrary joint probability distribution $\{Q(x,y), x \in \{0,1\}, y \in \{0,1\}\}$. Again, the crossover probability is defined as

$$q \stackrel{\Delta}{=} Q(0,1)+Q(1,0). \tag{4.6}$$

   Now also the probability that X is equal to 1 becomes an important parameter, and we define

$$\rho \stackrel{\Delta}{=} Q(1,0)+Q(1,1). \tag{4.7}$$

4. The Stationary Ergodic Case. We assume that the process $\{\ldots,(X_{-1},Y_{-1}), (X_0,Y_0),(X_1,Y_1),\ldots\}$ is stationary and ergodic. Then the sequences of random variables $X^N = (X_1,X_2,\ldots,X_N)$ and $Y^N = (Y_1,Y_2,\ldots,Y_N)$ correspond to our biometric enrollment and authentication sequences, respectively.

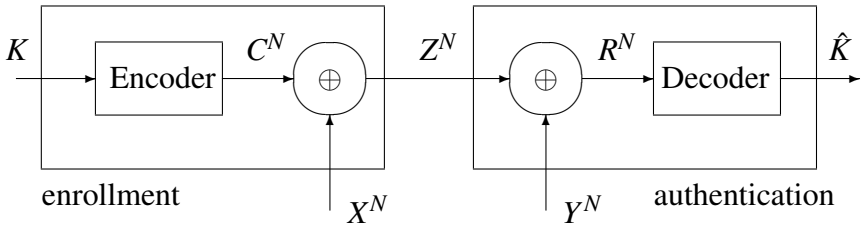


Figure 4.1: *A fuzzy commitment scheme.*

Now consider the fuzzy commitment scheme presented in Fig. 4.1. In this scheme a secret key k from alphabet $\{1,2,\ldots,|\mathcal{K}|\}$ is chosen uniformly at random independently of biometric data, hence

$$\Pr\{K=k\} = 1/|\mathcal{K}| \text{ for all } k \in \{1,2,\ldots,|\mathcal{K}|\}. \tag{4.8}$$

The chosen secret key k is observed at the enrollment side together with a biometric enrollment sequence x^N. The secret key k is encoded into a binary codeword $c^N = (c_1,c_2,\ldots,c_N)$ with $c_n \in \{0,1\}$ for $n = 1,2,\ldots,N$. We write $c^N = e(k)$, where $e(\cdot)$ is the encoding function. Then the biometric enrollment sequence is added modulo 2 to the codeword. This results in the sequence $z^N = (z_1,z_2,\ldots,z_N)$ with $z_n \in \{0,1\}$ for $n = 1,2,\ldots,N$, hence

$$z^N = c^N \oplus x^N = e(k) \oplus x^N. \tag{4.9}$$

This sequence is referred to as helper data and is public. The helper data are released to the authentication side.

During authentication, a biometric authentication sequence y^N is observed and added modulo 2 to the received helper data z^N, resulting in a binary sum

$$r^N = z^N \oplus y^N = e(k) \oplus x^N \oplus y^N. \tag{4.10}$$

This sum $r^N = \{r_1, r_2, \ldots, r_N\}$ with $r_n \in \{0,1\}$ for $n = 1,2,\ldots,N$ can be seen as the codeword c^N to which a noise sequence $x^N \oplus y^N$ is added. This codeword r^N is then decoded, hence the estimate $\widehat{k}$ of the secret key k is determined as

$$\widehat{k} = d(r^N) = d(e(k) \oplus (x^N \oplus y^N)), \tag{4.11}$$

where $d(\cdot)$ is the decoding function.

We are interested in a number of quantities. We require the scheme to be such that the error probability $\Pr\{\widehat{K} \neq K\}$ is as small as possible, while the number of secret keys $|\mathcal{K}|$ should be as large as possible. Moreover, we want the amount of information that the helper data leak about the secret $I(K;Z^N)$ and about the biometric data $I(X^N;Z^N)$ to be as small as possible. Now we give a formal definition of achievable triples.

Definition 4.1 *For a fuzzy commitment scheme a rate - leakage triple (R_k, R_{lk}, R_{lb}) with $R_k \geq 0$ is achievable if for all $\delta > 0$ and for all N large enough, there exist encoders $e(\cdot)$ and decoders $d(\cdot)$ such that*

$$\begin{aligned} & & \Pr\{\widehat{K} \neq K\} &\leq \delta, \\ R_k + \delta &\geq \frac{1}{N}\log|\mathcal{K}| &&\geq R_k - \delta, \\ & & \frac{1}{N} I(K;Z^N) &\leq R_{lk} + \delta, \\ & & \frac{1}{N} I(X^N;Z^N) &\leq R_{lb} + \delta. \end{aligned} \tag{4.12}$$

Moreover, we define $\mathcal{R}_{fc}$ to be the region of all achievable rate - leakage triples for a fuzzy commitment scheme. Furthermore, we define the secret-key vs. privacy-leakage rate region

$$\mathcal{R}_{fc}|R_{lk} = 0 \stackrel{\Delta}{=} \{(R_k, R_{lb}) : (R_k, 0, R_{lb}) \in \mathcal{R}_{fc}\}, \tag{4.13}$$

for the zero secrecy-leakage case.

In the next sections we will investigate the properties of the region of achievable rate-leakage triples for each of the four biometric statistics cases described above. First, however, we start with some general remarks.

4.2.2 Preliminary Analysis of Information Leakage

It is our goal to investigate the information-leakage properties of the fuzzy commitment scheme. Note that in Def. 4.1 we define the privacy leakage as unconditional mutual information between biometric enrollment sequence and helper data $I(X^N;Z^N)$ although a stronger definition of the privacy leakage is possible, i.e. the conditional one $I(X^N;Z^N|K)$, as in Def. 3.2 of Chapter 3. However, for the conditional definition of privacy leakage we obtain

$$\begin{aligned} I(X^N;Z^N|K) &= H(Z^N|K) - H(Z^N|X^N,K) \\ &= H(X^N \oplus C^N|K) - H(X^N \oplus C^N|X^N,K) \\ &= H(X^N|K) \\ &= H(X^N), \end{aligned} \tag{4.14}$$

where the last two equalities follow from the facts that C^N is a function of K and that X^N and K are independent. This demonstrates that the helper data Z^N leak (contain) the entire biometric sequence X^N if the secret key is known. We conclude that the fuzzy commitment scheme is not private in the conditional privacy-leakage sense. Therefore in the rest of the chapter we only concentrate on the unconditional privacy leakage.

The unconditional mutual information for the secrecy and privacy leakage can be rewritten as

$$\begin{aligned} I(K;Z^N) &= H(Z^N) - H(Z^N|K) \\ &= H(Z^N) - H(C^N \oplus X^N|K) \\ &= H(Z^N) - H(X^N), \end{aligned} \tag{4.15}$$

and

$$\begin{aligned} I(X^N;Z^N) &= H(Z^N) - H(Z^N|X^N) \\ &= H(Z^N) - H(X^N \oplus C^N|X^N) \\ &= H(Z^N) - H(C^N). \end{aligned} \tag{4.16}$$

4.3 The Totally-Symmetric Memoryless Case

4.3.1 Statement of Results, Discussion

We have a complete result for the totally-symmetric memoryless case. The result is stated in the following theorem. A special case of this result, when the secret-key rate is maximal, is also presented in Smith [72] and in Tuyls and Goseling [79]. The proof of this theorem will be provided in the next subsection.

Theorem 4.1 *For fuzzy commitment in the totally-symmetric memoryless case with crossover probability q the achievable region $\mathcal{R}_{fc}$ is given by*

$$\begin{aligned}\mathcal{R}_{fc} = \big\{(R_k, R_{lk}, R_{lb}) \quad : \quad & 0 \le R_k \le 1 - h(q), \\ & R_{lk} \ge 0, \\ & R_{lb} \ge 1 - R_k \qquad \big\}. \end{aligned} \tag{4.17}$$

Here $h(a) = -a\log(a) - (1-a)\log(1-a)$ is the binary entropy function.

Moreover, if we restrict ourselves to the secrecy leakage $R_{lk} = 0$ in Thm. 4.1, then the corresponding secret-key vs. privacy-leakage rate region is given by

$$\begin{aligned}\mathcal{R}_{\text{fc}|R_{lk}=0} = \big\{(R_k, R_{lb}) \quad : \quad & 0 \le R_k \le 1 - h(q), \\ & R_{lb} \ge 1 - R_k \qquad \big\}. \end{aligned} \tag{4.18}$$

This result for the totally-symmetric memoryless case can be compared to the corresponding secret-key vs. privacy-leakage rate region $\mathcal{R}^u_{ck}$, for the case of unconditional privacy leakage in a biometric model with chosen keys, where we do not restrict ourselves to fuzzy commitment. Note that although the achievable regions $\mathcal{R}_{\text{fc}|R_{lk}=0}$ and $\mathcal{R}^u_{ck}$ are defined slightly differently, the general region $\mathcal{R}^u_{ck}$ also provides the corresponding minimum privacy leakage for a given secret-key rate. Therefore we can compare regions $\mathcal{R}_{\text{fc}|R_{lk}=0}$ and $\mathcal{R}^u_{ck}$ for given secret-key rates.

Region $\mathcal{R}^u_{ck}$ was determined in Chapter 3 in Thm. 3.3, and can be stated for the totally-symmetric memoryless case as

$$\begin{aligned}\mathcal{R}^u_{ck} = \big\{(R_k, R_l) \quad : \quad & 0 \le R_k \le 1 - h(q * p), \\ & R_l \ge h(q * p) - h(p), \\ & \text{for some } 0 \le p \le 1/2\big\}, \end{aligned} \tag{4.19}$$

where $p * q \stackrel{\Delta}{=} p(1-q) + (1-p)q$.

Now it follows that for the privacy leakage of fuzzy commitment we obtain

$$\begin{aligned} R_{lb} &\ge 1 - R_k \\ &= h(q) \\ &\ge h(q * p) - h(p). \end{aligned} \tag{4.20}$$

The last inequality follows from the observation that $h(q*p) - h(p) = H(U|Y) - H(U|X) = I(U;X|Y) \le H(X|Y) = h(q)$, where Markov condition $U \to X \to Y$ holds and the "channel" between X and U is binary symmetric with crossover probability p. Note that equality in (4.20) can only be established if $R_k = 1 - h(q)$. Therefore for rates strictly smaller than $1 - h(q)$ the privacy leakage of the fuzzy commitment scheme is strictly larger than necessary. The coding methods proposed in Chapter 3 achieve smaller privacy leakage.

Proposition 4.1 *In the totally-symmetric memoryless case fuzzy commitment is only optimal for secret-key rates* $1-h(q)$*. For secret-key rates below* $1-h(q)$ *fuzzy commitment has the privacy leakage strictly larger than necessary.*

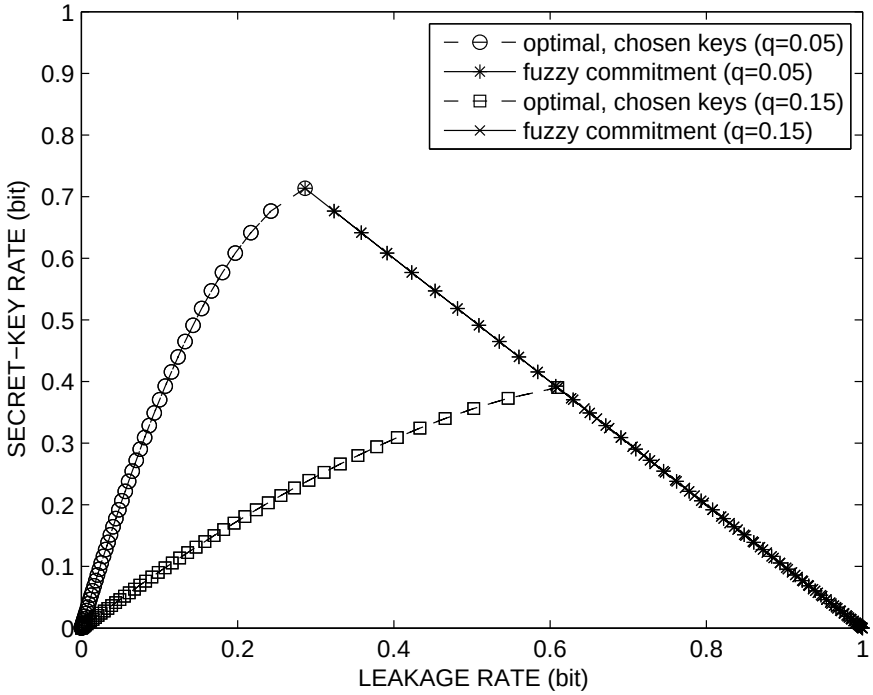


Figure 4.2: *Secret-key vs. privacy-leakage rate regions for two values of the crossover probability q. Marked with "o" and "□" are the boundaries of the optimal region* $\mathcal{R}^{u}_{ck}$*, marked with "*" and "×" are the boundaries of the fuzzy-commitment region* $\mathcal{R}_{fc}|R_{lk}=0$*.*

In Fig. 4.2 we have depicted (marked with "o" and "□") the boundary of the optimal rate-leakage region $\mathcal{R}^{u}_{ck}$ for two values of the crossover probability, i.e. for $q=0.05$ and $q=0.15$. Moreover, we have plotted in both figures the boundary of the fuzzy-commitment region $\mathcal{R}_{\mathrm{fc}}|R_{lk}=0$ (marked with "*" and "×"). From Fig. 4.2 it is clear that the privacy leakage of the fuzzy commitment scheme, even in the totally-symmetric memoryless case, is much larger than necessary for the secret-key rates smaller than the maximum rate $1-h(q)$. This is the main conclusion of this section.

4.3.2 Proof of the Results

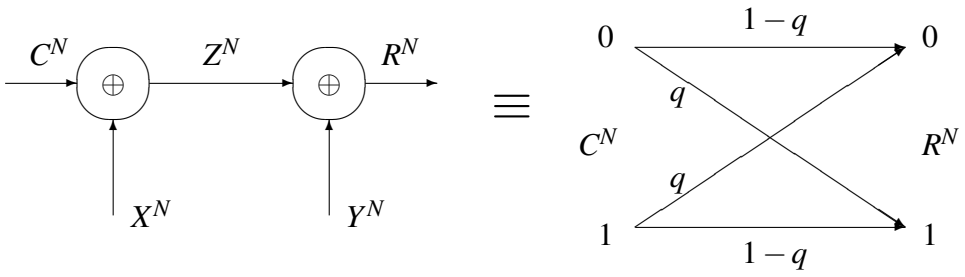


Figure 4.3: *In the memoryless cases the channel between C^N and R^N is a binary symmetric channel with crossover probability $q = Q(0,1)+Q(1,0)$.*

Proof of Thm. 4.1

Achievability proof: In the memoryless case we can write for the transition probabilities of the "channel" from C^N to R^N that

$$\Pr\{R^N = r^N | C^N = c^N\} \quad = \quad \prod_{n=1}^{N} \Pr\{R_n = r_n | C_n = c_n\}, \tag{4.21}$$

where for all $n = 1,2,\ldots,N$

$$\begin{aligned} \Pr\{R_n \neq c_n | C_n = c_n\} = 1 - \Pr\{R_n = c_n | C_n = c_n\} &= \Pr\{X_n \neq Y_n\} \\ &= Q(1,0)+Q(0,1). \end{aligned} \tag{4.22}$$

Therefore, see Fig. 4.3, the channel between C^N and R^N is a binary symmetric channel (BSC) with crossover probability $Q(1,0)+Q(0,1)$. By definition, for all memoryless cases we have for the crossover probability

$$Q(1,0)+Q(0,1) \quad = \quad q. \tag{4.23}$$

It is well-known, see e.g. Gallager [29], p. 146, that the capacity of BSC with crossover probability q is $1-h(q)$. In other words, for $0 \leq R_k \leq 1-h(q)$, for all $\varepsilon > 0$ and all N large enough, there exist encoders $e(\cdot)$ and decoders $d(\cdot)$ such that

$$R_k + \varepsilon \;\geq\; \frac{1}{N}\log|\mathcal{K}| \;\geq\; R_k - \varepsilon, \tag{4.24}$$

$$\Pr\{K \neq \widehat{K}\} \;\leq\; \varepsilon. \tag{4.25}$$

We may assume, for small ε at least, that this code does not contain two identical codewords, since any code with $2M-1$ codewords and average error probability

$\varepsilon/2 < 1/4$ has a subcode of size M and maximum error probability at most $\varepsilon < 1/2$. This follows from an expurgation argument, see e.g. Gallager [29], p. 151. Since the code does not contain two identical codewords, we can assume that $H(C^N) = \log|\mathcal{K}|$.

Now we concentrate on such codes and consider the secrecy leakage first. From (4.15) we obtain that

$$\begin{aligned} I(K;Z^N) &= H(C^N \oplus X^N) - H(X^N) \\ &= 0 \\ &\leq \varepsilon. \end{aligned} \tag{4.26}$$

Next, for the privacy leakage we write

$$\begin{aligned} I(X^N;Z^N) &\overset{(a)}{=} H(C^N \oplus X^N) - H(C^N) \\ &\overset{(b)}{=} N - \log|\mathcal{K}| \\ &\overset{(c)}{\leq} N(1 - R_k + \varepsilon), \end{aligned} \tag{4.27}$$

where step (a) follows from (4.16), step (b) holds, since the code does not contain identical codewords, and (c) follows from (4.24).

Then, dividing both sides of (4.27) by N, and letting $N \to \infty$ and $\varepsilon \downarrow 0$, we conclude from (4.24)-(4.27), that the triple $(R_k, 0, 1 - R_k)$ is achievable for $0 \leq R_k \leq 1 - h(q)$.

Converse: Assume that for the fuzzy commitment scheme the triple (R_k, R_{lk}, R_{lb}) is achievable. Consider first the entropy of the secret,

$$\begin{aligned} \log|\mathcal{K}| = H(K) &= I(K;R^N) + H(K|R^N) \\ &\overset{(a)}{=} I(K;C^N \oplus X^N \oplus Y^N) + H(K|R^N, \widehat{K}) \\ &\leq H(C^N \oplus X^N \oplus Y^N) - H(C^N \oplus X^N \oplus Y^N|K) + H(K|\widehat{K}) \\ &\overset{(b)}{\leq} N - H(X^N \oplus Y^N) + \delta \log|\mathcal{K}| + 1 \\ &\overset{(c)}{\leq} N - Nh(q) + \delta \log|\mathcal{K}| + 1, \end{aligned} \tag{4.28}$$

where step (a) follows from the fact that $\widehat{K}$ is a function of R^N, step (b) holds, since C^N is a function of K, (X^N, Y^N) are independent of K, for achievable triples (R_k, R_{lk}, R_{lb}) we have that $\Pr\{K \neq \widehat{K}\} \leq \delta$, and due to Fano's inequality, and (c) follows from the fact that $X^N \oplus Y^N$ is a sequence of i.i.d. pairs with crossover probability q.

Dividing both parts of the above expression by N and rearranging the terms, we obtain for achievable triples (R_k, R_{lk}, R_{lb}) that

$$R_k - \delta \leq \frac{1}{N} \log|\mathcal{K}| \leq \frac{1}{1-\delta}(1 - h(q) + \frac{1}{N}). \tag{4.29}$$

Next we consider the secrecy leakage and, using (4.15), we get

$$\begin{aligned} R_{lk}+\delta \geq \frac{1}{N} I(K;Z^N) &= \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &= \frac{1}{N}(N-N) \\ &= 0. \end{aligned} \tag{4.30}$$

For the privacy leakage we obtain using (4.16) that

$$\begin{aligned} R_{lb}+\delta \geq \frac{1}{N} I(X^N;Z^N) &= \frac{1}{N}(H(C^N \oplus X^N) - H(C^N)) \\ &\overset{(a)}{\geq} \frac{1}{N}(N - \log|\mathcal{K}|) \\ &\overset{(b)}{\geq} 1 - R_k - \delta, \end{aligned} \tag{4.31}$$

where step (a) follows from the fact that $H(C^N) \leq \log|\mathcal{K}|$, and (b) holds, since for achievable triples (R_k, R_{lk}, R_{lb}) we have that $\log|\mathcal{K}| \leq N(R_k+\delta)$.

Now, letting $N \to \infty$ and $\delta \downarrow 0$, we obtain the converse from (4.29)-(4.31).

■

4.4 The Input-Symmetric Memoryless Case

4.4.1 Statement of Results, Discussion

We start this section with the result that we have obtained for the input-symmetric memoryless case. The proof of this result is identical to the proof of Thm. 4.1 and therefore is omitted.

Theorem 4.2 *For a fuzzy commitment scheme in the input-symmetric memoryless case with crossover probability q the achievable region $\mathcal{R}_{fc}$ is given by*

$$\begin{aligned} \mathcal{R}_{fc} = \big\{(R_k, R_{lk}, R_{lb}) \quad : \quad & 0 \leq R_k \leq 1 - h(q), \\ & R_{lk} \geq 0, \\ & R_{lb} \geq 1 - R_k \qquad \big\}. \end{aligned} \tag{4.32}$$

■

Now if we again restrict the secrecy leakage to be $R_{lk} = 0$ in Thm. 4.2, then the corresponding secret-key vs. privacy-leakage rate region is given by

$$\begin{aligned} \mathcal{R}_{\text{fc}|R_{lk}=0} = \big\{(R_k, R_{lb}) \quad : \quad & 0 \leq R_k \leq 1 - h(q), \\ & R_{lb} \geq 1 - R_k \qquad \big\}. \end{aligned} \tag{4.33}$$

As before, we can compare the resulting zero secrecy-leakage region $\mathcal{R}_{\text{fc}}|R_{lk}=0$ to the region $\mathcal{R}^{u}_{ck}$ for the input-symmetric case when we do not restrict ourselves to fuzzy commitment. In Chapter 3, Thm. 3.3, it was shown that the region of achievable secret-key vs. privacy-leakage rate pairs is given by

$$\begin{aligned}\mathcal{R}^{u}_{ck} = \big\{(R_k,R_l) \quad : \quad & 0 \le R_k \le I(U;Y),\\ & R_l \ge I(U;X) - I(U;Y),\\ & \text{for some } P(u,x,y) = Q(x,y)P(u|x)\big\}. \end{aligned} \tag{4.34}$$

The maximum secret-key rate that is achievable in the optimal case is $I(X;Y)$, if we take $U \equiv X$, see Property 3.1 and also Ahlswede-Csiszár [3]. Note that

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y)\\ &= 1 - H(X\oplus Y|Y)\\ &\ge 1 - H(X\oplus Y)\\ &= 1 - h(q), \end{aligned} \tag{4.35}$$

where $1-h(q)$ is the maximum secret-key rate achievable with fuzzy commitment. Therefore we can conclude that fuzzy commitment is suboptimal if $X\oplus Y$ is not independent of Y.

A simple derivation shows that independence can only occur for $I(X;Y)>0$ if, in addition to being input-symmetric, the source is totally-symmetric.[1] Conclusion is that in the input-symmetric case, when the source is not totally-symmetric, with fuzzy commitment we cannot achieve a positive maximum rate $I(X;Y)$.

---

[1] Indeed, consider a memoryless statistics, which is input-symmetric. Define $\beta \stackrel{\Delta}{=} \Pr\{Y=1\}$ and note that $\Pr\{X\oplus Y=1\} = q$. If we assume that $X\oplus Y$ and Y are independent, then

$$\begin{aligned} Q(1,0) &= \Pr\{X\oplus Y=1, Y=0\} = \Pr\{X\oplus Y=1\}\Pr\{Y=0\} = q(1-\beta),\\ Q(1,1) &= \Pr\{X\oplus Y=0, Y=1\} = \Pr\{X\oplus Y=0\}\Pr\{Y=1\} = (1-q)\beta. \end{aligned} \tag{4.36}$$

Input-symmetry implies that

$$Q(1,0)+Q(1,1) = q(1-\beta)+(1-q)\beta = 1/2. \tag{4.37}$$

For $q \neq 1/2$ equation (4.37) has solution $\beta = 1/2$, and then the statistics is totally-symmetric.

For $q = 1/2$ the independence results in

$$\begin{aligned} Q(0,0) &= \Pr\{X\oplus Y=0\}\Pr\{Y=0\} = (1-\beta)/2,\\ Q(0,1) &= \Pr\{X\oplus Y=1\}\Pr\{Y=1\} = \beta/2,\\ Q(1,0) &= \Pr\{X\oplus Y=1\}\Pr\{Y=0\} = (1-\beta)/2,\\ Q(1,1) &= \Pr\{X\oplus Y=0\}\Pr\{Y=1\} = \beta/2, \end{aligned} \tag{4.38}$$

which implies that $I(X;Y)=0$. Hence we may conclude that in the input-symmetric case, when $I(X;Y)>0$, the independence of $X\oplus Y$ and Y implies total symmetry.

Looking at the privacy leakage of fuzzy commitment we can say that

$$\begin{aligned} R_{lb} &\geq 1 - R_k \\ &\geq h(q) \\ &= H(X \oplus Y) \\ &\geq H(X|Y) \\ &\geq I(U;X) - I(U;Y), \end{aligned} \tag{4.39}$$

for all $U \to X \to Y$. Again for $I(X;Y) > 0$, equality in the above expression is only possible if the biometric source is totally-symmetric and if, in addition, $R_k = 1 - h(q)$. Thus we may conclude that in the input-symmetric case, when $I(X;Y) > 0$ and the source is not totally-symmetric, with fuzzy commitment we cannot achieve privacy leakage, which is optimal in the sense of results presented in Chapter 3.

Proposition 4.2 *In the input-symmetric memoryless case, when the source is not totally-symmetric, fuzzy commitment is suboptimal with respect to both achievable secret-key rate and privacy leakage.*

4.5 The Memoryless Case

4.5.1 Statement of Results, Discussion

We do not have a complete result for the memoryless case in general. What we do have is an outer bound on the achievable region.

First, before stating our results, we define the inverse of the binary entropy function $h(\cdot)$ for $0 \leq \alpha \leq 1$ as

$$h^{-1}(\alpha) \stackrel{\Delta}{=} a, \tag{4.40}$$

if $0 \leq a \leq 1/2$ and $h(a) = \alpha$.

Theorem 4.3 *For fuzzy commitment in the memoryless case with crossover probability q and probability $\Pr\{X = 1\} = \rho$ we obtain for the achievable region $\mathcal{R}_{fc}$*

$$\begin{aligned} \mathcal{R}_{fc} \subseteq \big\{(R_k, R_{lk}, R_{lb}) \quad : \quad & 0 \leq R_k \leq 1 - h(q), \\ & R_{lk} \geq h[\rho * h^{-1}(R_k)] - h(\rho), \\ & R_{lb} \geq h[\rho * h^{-1}(R_k)] - R_k \quad \big\}. \end{aligned} \tag{4.41}$$

Moreover, there exist codes with rates up to $1 - h(q)$.

Note that the maximum achievable rate $1-h(q)$ for fuzzy commitment can be either smaller, equal, or larger than $I(X;Y)$. In the previous section, where we investigated the input-symmetric case, we have observed that for the general input-symmetric case $I(X;Y) > 1-h(q)$, see (4.35). On the other hand, for the general memoryless case for which $X \oplus Y$ is independent of Y, we obtain

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(X) - H(X \oplus Y|Y) \\ &\leq 1 - H(X \oplus Y) \\ &= 1 - h(q), \end{aligned} \tag{4.42}$$

and therefore also $I(X;Y) < 1-h(q)$ is possible. However, Thm. 3.3 and Property 3.1 imply that for rates larger than $I(X;Y)$ it is not possible to achieve non-zero secrecy leakage. More precisely, using the fact that for achievable rates $\Pr\{K \neq \widehat{K}\} \leq \delta$ and Fano's inequality, we obtain

$$\begin{aligned} H(K) &= I(K;R^N) + H(K|R^N) \\ &\leq I(K;Z^N,R^N) + H(K|\widehat{K}) \\ &\leq I(K;Z^N) + I(K;R^N|Z^N) + \delta \log|\mathcal{K}| + 1 \\ &= I(K;Z^N) + H(R^N,Y^N|Z^N) - H(R^N,Y^N|Z^N,K,C^N) + \delta \log|\mathcal{K}| + 1 \\ &= I(K;Z^N) + H(Y^N|Z^N) - H(Y^N|Z^N,K,X^N) + \delta \log|\mathcal{K}| + 1 \\ &\leq I(K;Z^N) + H(Y^N) - H(Y^N|X^N) + \delta \log|\mathcal{K}| + 1 \\ &= I(K;Z^N) + NI(X;Y) + \delta \log|\mathcal{K}| + 1, \end{aligned} \tag{4.43}$$

hence

$$R_k - \delta \leq \frac{1}{N} H(K) \leq \frac{1}{1-\delta}\left(\frac{1}{N} I(K;Z^N) + I(X;Y) + \frac{1}{N}\right). \tag{4.44}$$

This demonstrates that a secret-key rate, which is Δ larger than $I(X;Y)$, results in a secrecy leakage of at least Δ.

Moreover, observe that Thm. 4.3 implies that zero secrecy leakage is only possible if $R_k = 0$ or $\rho = 1/2$, and zero privacy leakage is only possible if $\rho = 0$ or $R_k = 1$. These cases are of no interest, though.

Observe also that for non-trivial cases for $I(X;Y) \geq 1-h(q)$ the privacy leakage in fuzzy commitment is larger than necessary. Indeed, if $R_k > 0$, then

$$\begin{aligned} h[\rho * h^{-1}(R_k)] - R_k &> h(\rho) - R_k \\ &\geq h(\rho) - (1 - h(q)) \\ &\geq H(X) - I(X;Y) \\ &= H(X|Y) \end{aligned}$$

$$\begin{aligned} &\geq I(U;X|Y) \\ &= I(U;X) - I(U;Y), \end{aligned} \tag{4.45}$$

where $I(U;X) - I(U;Y)$ is the privacy leakage achieved in the optimal setting. Note that for the general memoryless case we have strict inequality here.

Proposition 4.3 *In the memoryless case, when the source is not totally-symmetric, fuzzy commitment results in both secrecy and privacy leakage larger than necessary.*

4.5.2 Proof of the Results

We will use Mrs. Gerber's lemma of Wyner and Ziv [93] to investigate the properties of fuzzy commitment. Therefore we restate it here for convenience.

Lemma 4.1 (Mrs. Gerber's Lemma, [93]) *Let C^N be a binary random sequence with entropy $H(C^N) \geq N\nu \geq 0$, and X^N be a binary i.i.d. sequence with entropy $H(X^N) = Nh(\rho)$, then*

$$H(C^N \oplus X^N) \quad \geq \quad Nh[\rho * h^{-1}(\nu)]. \tag{4.46}$$

■

Proof of Thm. 4.3

The statement that there exist codes with rates up to $1 - h(q)$ follows directly from the capacity theorem for the BSC. Therefore we continue with the converse part.

Assume that the rate-leakage triple (R_k, R_{lk}, R_{lb}) is achievable. Then in the same way as (4.29), we obtain for achievable triples (R_k, R_{lk}, R_{lb}) that

$$R_k - \delta \leq \frac{1}{N} \log |\mathcal{K}| \leq \frac{1}{1-\delta}(1 - h(q) + \frac{1}{N}). \tag{4.47}$$

Next we consider the secrecy and privacy leakage. As an intermediate step, we first show that

$$\begin{aligned} \log |\mathcal{K}| = H(K) &= I(K;R^N) + H(K|R^N, \widehat{K}) \\ &\overset{(a)}{\leq} I(C^N;R^N) + \delta \log |\mathcal{K}| + 1 \\ &\leq H(C^N) + \delta \log |\mathcal{K}| + 1, \end{aligned} \tag{4.48}$$

where step (a) follows from the data-processing inequality, see e.g. Cover and Thomas [13], p. 32, from the fact that for achievable triples (R_k, R_{lk}, R_{lb}) we have that $\Pr\{\widehat{K} \neq K\} \leq \delta$ and from Fano's inequality.

Now using (4.48), we may conclude that for achievable triples (R_k, R_{lk}, R_{lb}), it holds that

$$\frac{1}{N}H(C^N) \geq \frac{1}{N}((1-\delta)\log|\mathcal{K}|-1) \geq R_k - \delta - \delta R_k - \frac{1}{N}. \tag{4.49}$$

For the secrecy leakage we can write, using Mrs. Gerber's lemma and (4.15), that

$$\begin{aligned} R_{lk} + \delta \geq \frac{1}{N}I(K;Z^N) &= \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &\geq h[\rho * h^{-1}(R_k - \delta - \delta R_k - \frac{1}{N})] - h(\rho). \end{aligned} \tag{4.50}$$

In a similar manner, we find for the privacy leakage that

$$\begin{aligned} R_{lb} + \delta \geq \frac{1}{N}I(X^N;Z^N) &\overset{(a)}{\geq} \frac{1}{N}(H(C^N \oplus X^N) - \log|\mathcal{K}|) \\ &\geq h[\rho * h^{-1}(R_k - \delta - \delta R_k - \frac{1}{N})] - \frac{1}{N}\log|\mathcal{K}| \\ &\overset{(b)}{\geq} h[\rho * h^{-1}(R_k - \delta - \delta R_k - \frac{1}{N})] - R_k - \delta. \end{aligned} \tag{4.51}$$

where step (a) follows from (4.16) and the fact that $H(C^N) \leq \log|\mathcal{K}|$, and (b) follows from the definition of achievable rates, since then $\log|\mathcal{K}| \leq N(R_k + \delta)$.

Now Thm. 4.3 follows from (4.47), (4.50) and (4.51), if we let $\delta \downarrow 0$ and $N \to \infty$. Note that the continuity of the binary entropy function is essential in this proof.

■

4.6 The Stationary Ergodic Case

4.6.1 Statement of Results, Discussion

Let X^N and Y^N be stationary ergodic sequences. Now we define $H_\infty(X \oplus Y)$ to be

$$H_\infty(X \oplus Y) \overset{\Delta}{=} \lim_{N\to\infty}\frac{1}{N}H(X_1 \oplus Y_1, X_2 \oplus Y_2, \ldots, X_N \oplus Y_N). \tag{4.52}$$

For the stationary ergodic case we have the following result.

Theorem 4.4 *For fuzzy commitment in the stationary ergodic case we obtain for the achievable region $\mathcal{R}_{fc}$ that*

$$\begin{aligned} \mathcal{R}_{fc} \subseteq \big\{(R_k, R_{lk}, R_{lb}) \;:\; & 0 \leq R_k \leq 1 - H_\infty(X \oplus Y), \\ & R_{lk} \geq h[h^{-1}(H_\infty(X)) * h^{-1}(R_k)] - H_\infty(X), \\ & R_{lb} \geq h[h^{-1}(H_\infty(X)) * h^{-1}(R_k)] - R_k \qquad \big\}. \end{aligned} \tag{4.53}$$

Moreover, reliable codes with rates up to $1 - H_\infty(X \oplus Y)$ exist.

The result of Thm. 4.4 demonstrates that zero secrecy leakage is only possible if $H_\infty(X) = 1$, which implies that the X-process is independent and uniformly distributed, or if the secret-key rate $R_k = 0$. Moreover, we may conclude that zero privacy leakage implies that $H_\infty(X) = 0$ or that the secret-key rate $R_k = 1$. These cases are again of no interest.

Note that for the stationary ergodic case we do not have an analog of Thm. 3.3. Nevertheless, we can compare the fuzzy commitment scheme to the two-layer scheme, which is built as a biometric secret generation system, considered in Thm. 2.2, with a masking layer on top of it. In this layer chosen secret key K is masked with generated key S in a one-time pad way.

It can be shown using Thm. 2.2, if the masking layer is used on top of the secret generation model considered there, and using similar reasoning as that used in the achievability proof of Thm. 3.3, that for the two-layer scheme the largest achievable secret-key rate R_k is equal to $I_\infty(X;Y)$. Moreover, that this rate is achievable with privacy leakage $H_\infty(X|Y)$.

Now as in the memoryless case the maximum achievable rate $1 - H_\infty(X \oplus Y)$ for fuzzy commitment can be smaller, equal or larger than $I_\infty(X;Y)$. However, for rates larger than $I_\infty(X;Y)$ it is not possible to achieve zero secrecy leakage. Indeed, we can write for all small $\varepsilon > 0$ and all N large enough, using similar series of steps as those used to derive (4.44), that

$$R_k - \delta \leq \frac{1}{N} H(K) \leq \frac{1}{1-\delta}\left(\frac{1}{N} I(K;Z^N) + I_\infty(X;Y) + \varepsilon + \frac{1}{N}\right). \tag{4.54}$$

Hence, if the maximum secret-key rate in fuzzy commitment is Δ larger than $I_\infty(X;Y)$, then the secrecy leakage of the scheme is at least Δ.

Now consider non-trivial cases when $1 - H_\infty(X \oplus Y) \leq I_\infty(X;Y)$. We obtain for the privacy leakage in the fuzzy commitment scheme when $R_k > 0$ that

$$\begin{aligned} h[h^{-1}(H_\infty(X)) * h^{-1}(R_k)] - R_k &> H_\infty(X) - R_k \\ &\geq H_\infty(X) - (1 - H_\infty(X \oplus Y)) \\ &\geq H_\infty(X) - I_\infty(X;Y) \\ &= H_\infty(X|Y), \end{aligned} \tag{4.55}$$

which demonstrates that with the two-layer scheme we obtain smaller privacy leakage than with fuzzy commitment.

Proposition 4.4 *In the stationary ergodic case fuzzy commitment is not optimal with respect to both secrecy and privacy leakage.*

4.6.2 Proof of the Results

Before proving the results for fuzzy commitment in the stationary ergodic case, we need an auxiliary result.

Binary Analog to the Entropy-Power Inequality

The entropy-power inequality, see Shannon [68], is a useful lower bound for the differential entropy of a sum of two independent real-valued stationary random sequences. We are interested in a similar bound for stationary binary sequences. The binary analog to the entropy-power inequality was derived in Shamai and Wyner [66]. For our purposes, we need an adapted version of this binary analog to the entropy-power inequality.

Assume that a biometric sequence X^N is a stationary binary sequence with entropy

$$H_\infty(X) = \lim_{N\to\infty} \frac{1}{N} H(X_1, X_2, \ldots, X_N) = \lim_{N\to\infty} H(X_N | X_1, X_2, \ldots, X_{N-1}). \tag{4.56}$$

Moreover, now for the binary entropy function $h(\cdot)$ for $0 \le \alpha \le 1$, its inverse $h^{-1}(\alpha) = a$, defined as in the previous section, corresponds to the probability a in a binary i.i.d. sequence with entropy α.

Lemma 4.2 *For the random binary independent sequences X^N and C^N, if X^N is stationary with entropy $H_\infty(X)$ and $H(C^N) \ge N\nu$, the following statement holds*

$$\frac{1}{N} H(Z^N) \quad \ge \quad h[h^{-1}(H_\infty(X)) * h^{-1}(\nu)], \tag{4.57}$$

where $Z^N = (Z_1, Z_2, \ldots, Z_N) = (X_1 \oplus C_1, X_2 \oplus C_2, \ldots, X_N \oplus C_N)$. This is an adapted version of the binary analog to the entropy-power inequality (Shamai and Wyner [66]).

Proof of Lem. 4.2: We denote $X^{n-1} = (X_1, X_2, \ldots, X_{n-1})$ for $n = 1, 2, \ldots, N$, and also C^{n-1} and Z^{n-1} in the same way.

Now, from Shamai and Wyner [66], the last but one equation, and from the facts that $H_\infty(X) \le H(X_n | X^{n-1})$ and $0 \le h^{-1}(\cdot) \le \frac{1}{2}$, it follows that

$$\begin{aligned} H(Z_n | Z^{n-1}) &\ge h[h^{-1}(H(X_n | X^{n-1})) * h^{-1}(H(C_n | C^{n-1}))] \\ &\ge h[h^{-1}(H_\infty(X)) * h^{-1}(H(C_n | C^{n-1}))]. \end{aligned} \tag{4.58}$$

Next we find that

$$\begin{aligned}
\frac{1}{N}H(Z^N) &= \frac{1}{N}\sum_{n=1}^{N} H(Z_n|Z^{n-1}) \\
&\geq \frac{1}{N}\sum_{n=1}^{N} h[h^{-1}(H_\infty(X)) * h^{-1}(H(C_n|C^{n-1}))] \\
&\overset{(a)}{\geq} h[h^{-1}(H_\infty(X)) * h^{-1}(\frac{1}{N}\sum_{n=1}^{N} H(C_n|C^{n-1}))] \\
&= h[h^{-1}(H_\infty(X)) * h^{-1}(\nu)], \qquad (4.59)
\end{aligned}$$

where (a) follows from convexity of $h(\beta * h^{-1}(u))$ in u, since its second derivative is positive, for the details see Wyner and Ziv [93], and Jensen's inequality, see e.g. Cover and Thomas [13], p. 25.

■

Proof of Thm. 4.4

The fact that reliable codes with rates up to $1-H_\infty(X \oplus Y)$ exist for stationary ergodic $X \oplus Y$-processes follows from Verdu and Han [81], p. 1156. It is essential that the noise process is ergodic here.

Next assume that for the fuzzy commitment scheme the triple (R_k, R_{lk}, R_{lb}) is achievable. Then we obtain for the entropy of the secret that

$$\log|\mathcal{K}| = H(K) \leq N - H(X^N \oplus Y^N) + \delta \log|\mathcal{K}| + 1, \qquad (4.60)$$

where the inequality in the above expression holds if we apply the same series of steps as in (4.28) and use the fact that for achievable triples (R_k, R_{lk}, R_{lb}) we have that $\Pr\{\widehat{K} \neq K\} \leq \delta$.

Dividing both parts of the above expression by N and rearranging the terms, we obtain for achievable triples (R_k, R_{lk}, R_{lb}) that

$$R_k - \delta \leq \frac{1}{N}\log|\mathcal{K}| \leq \frac{1}{1-\delta}(1 - \frac{1}{N}H(X^N \oplus Y^N) + \frac{1}{N}). \qquad (4.61)$$

Next, note that $H(C^N) \geq N(R_k - \delta - \delta R_k - 1/N)$, since (4.49) also holds here. Using Lem. 4.2 and (4.15), we obtain that

$$\begin{aligned}
R_{lk} + \delta \geq \frac{1}{N}I(K;Z^N) &= \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\
&\geq h[H_\infty(X) * h^{-1}(R_k - \delta - \delta R_k - \frac{1}{N})] - \frac{1}{N}H(X^N). \qquad (4.62)
\end{aligned}$$

In a similar manner, we find for the privacy leakage that

$$\begin{aligned} R_{lb}+\delta &\geq \frac{1}{N}I(X^N;Z^N) \\ &\overset{(a)}{\geq} \frac{1}{N}(H(X^N\oplus C^N)-\log|\mathcal{K}|) \\ &\geq h[h^{-1}(H_\infty(X))*h^{-1}(R_k-\delta-\delta R_k-\frac{1}{N})]-\frac{1}{N}\log|\mathcal{K}| \\ &\overset{(b)}{\geq} h[h^{-1}(H_\infty(X))*h^{-1}(R_k-\delta-\delta R_k-\frac{1}{N})]-R_k-\delta. \end{aligned} \tag{4.63}$$

where step (a) follows from (4.16) and the fact that $H(C^N)\leq\log|\mathcal{K}|$, and (b) holds, since for achievable triples (R_k,R_{lk},R_{lb}) we have that $\log|\mathcal{K}|\leq N(R_k+\delta)$.

Now Thm. 4.4 follows from (4.60), (4.62) and (4.63) if we let $\delta\downarrow 0$ and $N\to\infty$. ■

4.7 Tighter Bounds with Systematic Parity-Check Codes

4.7.1 Tighter Bounds for the Stationary Ergodic Case

Better lower bounds on the leakages can be obtained if we use binary systematic parity-check codes. We assume that the information symbols are followed by the parity symbols. First, we need the following result, though.

Lemma 4.3 *Let C^N be the sequence of random variables corresponding to a binary linear code where the first $\log|\mathcal{K}|$ information symbols (the systematic part) are followed by $N-\log|\mathcal{K}|$ parity symbols. In this way $H(C_n|C^{n-1})=1$ for $n\leq\log|\mathcal{K}|$ and $H(C_n|C^{n-1})=0$ for $n>\log|\mathcal{K}|$, where we also assume that $|\mathcal{K}|$ is a power of 2, and hence $\log|\mathcal{K}|$ is integer. Then for the independent sequences of binary variables X^N and C^N, if X^N is stationary with entropy $H_\infty(X)$ and $H(C^N)\geq N\nu$, the following statement holds*

$$\frac{1}{N}H(C^N\oplus X^N) \geq H_\infty(X)+\nu(1-H_\infty(X)). \tag{4.64}$$

Proof of Lem. 4.3: Using (4.59) from the proof of Lem. 4.2, we can write

$$\begin{aligned} \frac{1}{N}H(Z^N) &= \frac{1}{N}\sum_{n=1}^{N}H(Z_n|Z^{n-1}) \\ &\geq \frac{1}{N}\Big(\sum_{n=1}^{\log|\mathcal{K}|}h[h^{-1}(H_\infty(X))*h^{-1}(1)]+ \end{aligned}$$

$$\begin{aligned} & \sum_{n=\log|\mathcal{K}|+1}^{N} h[h^{-1}(H_\infty(X)) * h^{-1}(0)]\Big) \\ = \;& \frac{1}{N}(\log|\mathcal{K}| + (N-\log|\mathcal{K}|)H_\infty(X)) \\ \geq \;& H_\infty(X) + \frac{1}{N}\log|\mathcal{K}|(1-H_\infty(X)) \\ \geq \;& H_\infty(X) + \nu(1-H_\infty(X)), \end{aligned} \tag{4.65}$$

where the last inequality follows from $\log|\mathcal{K}| \geq H(C^N) \geq N\nu$.

■

Theorem 4.5 *For fuzzy commitment in the stationary ergodic case, if systematic parity-check codes are applied, we obtain for the achievable region $\mathcal{R}_{fc}$ that*

$$\begin{aligned} \mathcal{R}_{fc} \subseteq \big\{(R_k, R_{lk}, R_{lb}) \quad : \quad & 0 \leq R_k \leq 1 - H_\infty(X \oplus Y), \\ & R_{lk} \geq R_k(1-H_\infty(X)), \\ & R_{lb} \geq H_\infty(X)(1-R_k) \qquad \big\}. \end{aligned} \tag{4.66}$$

From this theorem we may conclude that in the stationary ergodic case, when systematic parity-check codes are used in fuzzy commitment, the secrecy leakage can only be zero if the secret-key rate $R_k = 0$ or if the entropy $H_\infty(X) = 1$. On the other hand, zero privacy leakage implies that either the rate $R_k = 1$ or $H_\infty(X) = 0$. However, these cases are not interesting.

Proof of Thm. 4.5: Assume that the triple (R_k, R_{lk}, R_{lb}) is achievable. Just as in Thm. 4.4 we obtain that

$$R_k - \delta \leq \frac{1}{N}\log|\mathcal{K}| \leq \frac{1}{1-\delta}(1 - \frac{1}{N}H(X^N \oplus Y^N) + \frac{1}{N}). \tag{4.67}$$

Moreover, we have that $H(C^N) \geq N(R_k - \delta - \delta R_k - 1/N)$, since (4.49) also holds here. Then using Lem. 4.3 and (4.15), we can write for the secrecy leakage that

$$\begin{aligned} R_{lk} + \delta \;&\geq\; \frac{1}{N} I(K; Z^N) \\ &=\; \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &\geq\; (1-H_\infty(X))(R_k - \delta - \delta R_k - \frac{1}{N}) + H_\infty(X) - \frac{1}{N}H(X^N). \end{aligned} \tag{4.68}$$

In a similar way, we obtain for the privacy leakage that

$$\begin{aligned} R_{lb}+\delta \geq \frac{1}{N}I(X^N;Z^N) &\overset{(a)}{\geq} \frac{1}{N}(H(X^N\oplus C^N)-\log|\mathcal{K}|) \\ &\geq H_\infty(X)+(R_k-\delta-\delta R_k-\frac{1}{N})(1-H_\infty(X))-\frac{1}{N}\log|\mathcal{K}| \\ &\overset{(b)}{\geq} H_\infty(X)(1-R_k+\delta R_k+\frac{1}{N})-2\delta-\delta R_k-\frac{1}{N}. \end{aligned} \tag{4.69}$$

where step (a) follows from (4.16) and the fact that $H(C^N)\leq \log|\mathcal{K}|$, and (b) holds, since for achievable triples (R_k,R_{lk},R_{lb}) we have that $\log|\mathcal{K}|\leq N(R_k+\delta)$.

Now from (4.67), (4.68) and (4.69), letting $\delta\downarrow 0$ and $N\to\infty$, we obtain the proof. ■

The fact that the leakage bounds in Thm. 4.5 are indeed stronger than the bounds obtained in Thm. 4.4 follows from convexity. Let U be 1 with probability R_k and 0 with probability $1-R_k$. Then from convexity of $h(\beta * h^{-1}(u))$ in u, we obtain

$$\begin{aligned} &h[h^{-1}(H_\infty(X))*h^{-1}(R_k)] \\ &\quad\leq R_k\,h[h^{-1}(H_\infty(X))*h^{-1}(1)]+(1-R_k)h[h^{-1}(H_\infty(X))*h^{-1}(0)] \\ &\quad= R_k+H_\infty(X)-R_kH_\infty(X). \end{aligned} \tag{4.70}$$

Therefore it follows that

$$\begin{aligned} h[h^{-1}(H_\infty(X))*h^{-1}(R_k)]-H_\infty(X) &\leq R_k+H_\infty(X)-R_kH_\infty(X)-H_\infty(X) \\ &= R_k(1-H_\infty(X)) \qquad (4.71) \\ h[h^{-1}(H_\infty(X))*h^{-1}(R_k)]-R_k &\leq R_k+H_\infty(X)-R_kH_\infty(X)-R_k \\ &= H_\infty(X)(1-R_k). \qquad (4.72) \end{aligned}$$

4.7.2 Tighter Bounds for the Memoryless Case

Note that Lem. 4.3 also holds in the memoryless case, when X^N is i.i.d. with $\Pr\{X=1\}=\rho$. Then (4.64) takes the following form

$$\frac{1}{N}H(C^N\oplus X^N) \geq h(\rho)+\nu(1-h(\rho)). \tag{4.73}$$

Now the tighter bounds on the achievable region for the general memoryless case, when systematic parity-check codes are used, are given by the following theorem. The proof of this theorem is identical to the proof of Thm. 4.5 and is therefore omitted.

Theorem 4.6 *For fuzzy commitment in the memoryless case with crossover probability q and probability $\Pr\{X=1\}=\rho$ if systematic parity-check codes are applied, we obtain for the achievable region $\mathcal{R}_{fc}$ that*

$$\begin{aligned}\mathcal{R}_{fc} \subseteq \big\{(R_k, R_{lk}, R_{lb}) \quad : \quad & 0 \le R_k \le 1-h(q), \\ & R_{lk} \ge R_k(1-h(\rho)), \\ & R_{lb} \ge h(\rho)(1-R_k) \,\big\}. \end{aligned} \tag{4.74}$$

■

Remark: It should be noted that for the totally-symmetric memoryless case and input-symmetric memoryless case the bounds given in the above theorem reduces to the regions given in Thm. 4.1 and Thm. 4.2, respectively.

4.8 Conclusions

In this chapter we have considered fuzzy commitment and investigated its secrecy and privacy leakage properties. It turns out that fuzzy commitment is not private in the conditional privacy-leakage sense.

Next we have concentrated on unconditional privacy leakage. Our analysis has shown that fuzzy commitment is only optimal for the totally-symmetric memoryless case if it operates at the maximum secret-key rate. For secret-key rates which are below the capacity, the scheme is not optimal with respect to privacy leakage. However, it is still optimal with respect to secret-key rates and secrecy leakage.

For the input-symmetric memoryless case, we have concluded that fuzzy commitment is suboptimal with respect to both achievable secret-key rate and privacy-leakage rate. However, it still enjoys zero secrecy leakage.

In the general memoryless and stationary ergodic cases we could only determine outer bounds on the achievable regions. Moreover, we could sharpen these bounds for the case when systematic parity-check codes are used in fuzzy-commitment based biometric systems.

The results for the memoryless case have revealed that fuzzy commitment leads to both secrecy and privacy leakage that are larger than necessary. One may argue that for the memoryless case with fuzzy comminute we can achieve larger secret-key rates than with the optimal scheme. However, we have shown that this increase may only come at the expense of secrecy leakage.

The results for the stationary ergodic case have also demonstrated that fuzzy commitment has non-zero secrecy and privacy leakage in non-trivial cases. We cannot assess its optimality, though, as we do not have an analog of Thm. 3.3 for the stationary ergodic case. Therefore we have compared the fuzzy commitment scheme to a two-layer scheme (which is based on a biometric secret generation model with a

masking layer on top of it) for stationary ergodic biometric sources. It turns out that the two-layer scheme enjoys better properties.

Chapter 5

Context Weighting And Maximizing Using Ratio Representation

Everything should be as simple as it is, but not simpler (Albert Einstein).

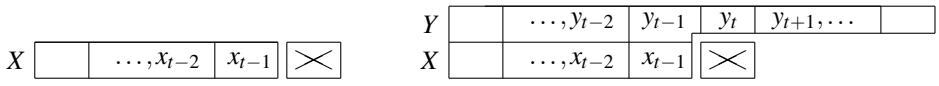
5.1 Introduction

In the next chapter we will study a problem that has to be addressed before any practical biometric secrecy system is built, viz. how much secret information (secret randomness) can be extracted or conveyed with a certain biometric modality. Therefore we will need to estimate the mutual information $I(X;Y)$ between the biometric enrollment and authentication sequences. In principle it is possible to find a model of the source and based on this model to estimate the required mutual information. For instance, in Škorić [71] the secret-key rate for optical PUFs is estimated based on the physical model that is developed there. We will however take a different approach and will estimate this mutual information using observed biometric sequences. We will focus on stationary ergodic biometrics.

The formula for mutual information between two biometric sequences can be expanded in one of three ways, i.e. $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$. Thus we can focus on the estimation of entropies. Our approach is based on the context-tree weighting (CTW) method, which is a universal source coding method introduced by Willems, Shtarkov, and Tjalkens [88]. The CTW method is a sequential procedure that finds a good coding distribution for an observed (biometric) source sequence. This coding distribution can be used to compress the observed sequence, using arithmetic coding techniques. The resulting codeword has a small redundancy and thus its length, divided by the length of the source sequence, gives a good estimate of the entropy.

Now suppose that we use the expression $I(X;Y) = H(X) - H(X|Y)$ to estimate the mutual information. In the CTW method the distribution that a tree source uses to generate the next symbol x_t depends on a finite number of preceding symbols, see

Fig. 5.1(a). These previous symbols are called context. The most recent symbol is assumed to be the most important, the second most recent symbol is the second most important symbol, etc. In this manner the ordering of the context is defined. When we need to estimate the conditional entropy $H(X|Y)$, the context of x_t consists of a finite number of preceding symbols of x_t in the X-sequence, a finite number of preceding and future symbols in the Y-sequence, and the current symbol, see Fig. 5.1(b). In this case the dependencies between x_t and the context symbols are not that obvious, and it is not easy to come up with the same natural context ordering as in the case when the context only consists of X-symbols. Therefore we would like to have more freedom in choosing the context order. This freedom is provided by the so-called class III weighting method, described in Willems, Shtarkov, and Tjalkens [90]. Using the class III weighting method we hope to get better estimates of the entropy and, consequently, better estimates of the mutual information.



(a) for $H(X)$ (b) for $H(X|Y)$

Figure 5.1: *Contexts for x_t. Position of the symbol is denoted by $\times$.*

Another problem that has to be addressed while designing a biometric secrecy system is code construction. In order to design codes for biometric secrecy systems that achieve near-optimal performance, we need to know the statistics of the biometric source. The statistics of the source is determined by the model of the source and the parameters of the model. The model defines the structure of the source and the parameters give the probabilities which the source uses to generates symbols.

Suppose that our source is binary. Given a model of the source and an observed biometric sequence produced by this source, we can partition the observed sequence into subsequences according to the model. For each subsequence the fraction of ones is a good estimate of the probability that corresponds to this subsequence. These probabilities are the parameters of the model. Then the remaining problem is to find the model of the source. Therefore in this chapter we will study the problem of how to efficiently find the best (maximum a posteriori) model for a given biometric sequence.

In order to find the maximum a posteriori model for a given biometric sequence, we could use the context-tree maximizing method proposed by Volf and Willems [84]. Note that in Willems and Tjalkens [91] an efficient implementation of the CTW method based on betas (ratios of block probabilities) was proposed. This implementation results in complexity reduction of the method. Moreover, later, using betas, a simple procedure for determining the a posteriori model probabilities was derived by

Willems at al. [87]. Therefore we are also interested in the procedure for finding the maximum a posteriori model using betas.

In the current chapter in Section 5.2 we will first describe the CTW method introduced in [88]. Then in Section 5.3 we will discuss an efficient implementation of the CTW method proposed in [91], which is based on ratios of block probabilities. Next we will turn to the context-tree maximizing procedure. In Section 5.4 we outline the original procedure proposed by Volf and Willems [84]. Then we will concentrate on context-maximizing using the ratio representation (betas). The beta-based procedure, proposed in Willems et al. [87] and described in Section 5.5.1, determines a posteriori probabilities for a specified model for a given source sequence. Inspired by this idea, in Section 5.5.2 we derive a new method for finding the MAP-model for a given (biometric) sequence using betas. Moreover, in Section 5.6 we will extend these procedures to determine the a posteriori model probabilities and the MAP-model for class III. In these procedures we will again use ratios of block probabilities.[1]

5.2 Context-Tree Weighting Methods

5.2.1 Arithmetic Coding

Denote the binary sequence $(x_1, x_2, \ldots, x_T)$ by x_1^T. Given a coding distribution $P_c(x_1^T)$ over all binary sequences of length T, the Elias algorithm, see e.g. Jelinek [38], generates codewords that satisfy the prefix condition, see e.g. Cover and Thomas [13] pp. 81-82, with lengths

$$L(x_1^T) = \lceil \frac{1}{P_c(x_1^T)} \rceil + 1 < \log \frac{1}{P_c(x_1^T)} + 2. \tag{5.1}$$

Implementations of this method are called arithmetic coding methods, see e.g. Rissanen [61] and Pasco [53]. The codeword length that we obtain in this way is at most two binary digits longer than the length of the ideal codeword, i.e. $-\log P_c(x_1^T)$. We say that the individual *coding redundancy* is smaller than 2. Therefore universal source coding is mainly concerned with finding good coding distributions.

5.2.2 The Krichevski-Trofimov Estimator

The actual probability $\Pr\{X_1^t = x_1^t\}$ of a source sequence x_1^t, for $t = 1, 2, \ldots, T$ is denoted by $P_a(x_1^t)$. For an i.i.d. binary source with an unknown parameter $\theta = P_a(1)$

[1] In this chapter we will use somewhat different notations than in other chapters of this thesis. Here we will denote a sequence $(x_1, x_2, \ldots, x_T)$ by x_1^T instead of by x^T. This definition is stipulated by the fact that sometimes we need to specify the range of symbols in the sequence. Also $s, p, \mathcal{S}$, and $\mathcal{P}$ here have different meaning than in the previous chapters.

we should use

$$P_e(a,b) = \frac{(a-\frac{1}{2})(a-\frac{3}{2})\cdot\ldots\cdot\frac{1}{2}(b-\frac{1}{2})(b-\frac{3}{2})\cdot\ldots\cdot\frac{1}{2}}{(a+b)(a+b-1)\cdot\ldots\cdot 1} \tag{5.2}$$

as coding probability for a sequence containing a zeroes and b ones. This estimate for the actual probability is called the Krichevsky-Trofimov [43] estimate.

Consider a sequence x_1^T with a zeroes and b ones, then from (5.1) we may conclude that

$$L(x_1^T) < \log\frac{1}{P_e(a,b)} + 2. \tag{5.3}$$

Define the individual redundancy for sequence x_1^T as

$$\rho(x_1^T) \stackrel{\Delta}{=} L(x_1^T) - \log\frac{1}{P_a(x_1^T)}, \tag{5.4}$$

then this redundancy for a sequence x_1^T with a zeroes and b ones satisfies

$$\begin{aligned}\rho(x_1^T) &< \log\frac{1}{P_e(a,b)} + 2 - \log\frac{1}{(1-\theta)^a\theta^b} \\ &= \log\frac{(1-\theta)^a\theta^b}{P_e(a,b)} + 2 \\ &\leq \frac{1}{2}\log T + 3,\end{aligned} \tag{5.5}$$

where we applied Lem. 1 of Willems, Shtarkov, and Tjalkens [88] to upper bound the $\log(P_a/P_e)$-term. This term, called the *parameter redundancy*, is never larger than $\frac{1}{2}\log(a+b)+1$. Hence the individual redundancy is not larger than $\frac{1}{2}\log T + 3$ for all x_1^T and all $\theta \in [0,1]$. Therefore this estimator is asymptotically optimal, see Rissanen [60].

5.2.3 Tree Sources

Consider Fig. 5.2. For a *tree source* the probability $P_a(X_t = 1|\ldots,x_{t-2},x_{t-1})$ is determined by starting in the root λ of the tree and moving along the path $x_{t-1},x_{t-2},\ldots$ until a leaf of the tree is reached. In this leaf s we find the desired probability (parameter) θ_s. The suffix set or tree $\mathcal{S}$, containing the paths to all leaves, is called the *model* of the source.

In the example shown in Fig. 5.2 the source has the suffix set $\mathcal{S} = \{00, 10, 1\}$ with parameter vector $\Theta_{\mathcal{S}} = \{\theta_{00}, \theta_{10}, \theta_1\}$. For this source the actual (conditional) probability of the source generating the sequence 01101 given the past symbols $\ldots 010$ is

$$\begin{aligned}P_a(01101|\ldots 010) &= (1-\theta_{10})\theta_{00}\theta_1(1-\theta_1)\theta_{10} \\ &= 0.00945.\end{aligned} \tag{5.6}$$

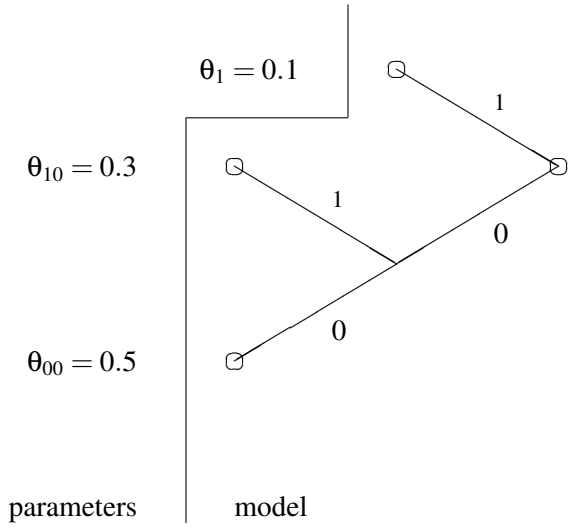


Figure 5.2: *Model (suffix set) and parameters.*

5.2.4 Unknown Parameters, Known Model

The source model (tree) $\mathcal{S}$ partitions the source sequence in i.i.d. subsequences, one for each leaf $s \in \mathcal{S}$. If the parameters of the source are unknown we can use the Krichevski-Trofimov estimator for each of these subsequences. For instance, for $\mathcal{S} = \{00, 10, 1\}$ we get

$$P_e(x_1^T|\mathcal{S}) \quad = \quad P_e(a_{00}, b_{00}) \cdot P_e(a_{10}, b_{10}) \cdot P_e(a_1, b_1), \tag{5.7}$$

where a_s is the number of zeroes in the subsequence of x_1^T corresponding to leaf s, and b_s is the number of ones in this subsequence. In general, we obtain for the estimated probabilities for tree-model $\mathcal{S}$ that

$$P_e(x_1^T|\mathcal{S}) \quad = \quad \prod_{s \in \mathcal{S}} P_e(a_s, b_s). \tag{5.8}$$

If we use this probability estimate as a coding probability, we obtain for the (parameter plus coding) redundancy

$$\begin{aligned} \rho(x_1^T) \quad &< \quad \log \frac{1}{P_e(x_1^T|\mathcal{S})} + 2 - \log \frac{1}{P_a(x_1^T)} \\ &\leq \quad \left(\frac{|\mathcal{S}|}{2} \log \frac{T}{|\mathcal{S}|} + |\mathcal{S}| \right) + 2, \end{aligned} \tag{5.9}$$

for $T \geq |\mathcal{S}|$. Note that the second inequality follows from convexity of the $\log(\cdot)$. Moreover, $\rho(x_1^T) \leq T + 2$, for $T < |\mathcal{S}|$.

5.2.5 Weighting

Consider two sources. For the first source we should use coding distribution $P_c^1(x_1^T)$ to obtain a small redundancy. For the second source we should use distribution $P_c^2(x_1^T)$. If we need a single code that is good for both sources then

$$P_w(x_1^T) = \frac{P_c^1(x_1^T)+P_c^2(x_1^T)}{2} \tag{5.10}$$

would be a good coding distribution. It leads to codeword length

$$\begin{aligned} L_w(x_1^T) &< \log\frac{2}{P_c^1(x_1^T)+P_c^2(x_1^T)}+2 \\ &\leq \log\frac{1}{P_c^i(x_1^T)}+3, \qquad \text{for } i=1,2, \end{aligned} \tag{5.11}$$

and we lose at most one binary digit with this weighting technique!

5.2.6 Unknown Model

Suppose that the actual source model $\mathcal{S}$ is unknown, but its depth is not larger than D. A *context* is a string of binary symbols. Note that to each context s, there corresponds a substring of $(x_1,x_2,\ldots,x_T)$ of symbols that are produced by the source following this context s. Let a_s be the number of zeroes in this subsequence and b_s be the number of ones. The structure containing a node for all contexts s having depth not larger than D is called a *context-tree* $\mathcal{T}_D$. A good estimator for the subsequence corresponding to a context (node) s at depth D is $P_w^s = P_e(a_s,b_s)$. Now let the depth d of some node s be smaller than D and assume that we already have good probability estimates for sequences corresponding to nodes $0s$ and $1s$ at depth $d+1$. Denote these probability estimates by P_w^{0s} and P_w^{1s}, respectively. Then for the subsequence corresponding to s we have two alternatives. We can use the Krichevski-Trofimov estimate $P_e(a_s,b_s)$ for the entire subsequence corresponding to s or we can split up this subsequence into two sub-subsequences and use the product $P_w^{0s}P_w^{1s}$ of the probabilities P_w^{0s} and P_w^{1s} as estimate. If we weight these two alternatives we obtain the weighted probability

$$P_w^s = \begin{cases} \frac{1}{2}P_e(a_s,b_s)+\frac{1}{2}P_w^{0s}P_w^{1s}, & \text{if depth}(s)<D \\ P_e(a_s,b_s), & \text{otherwise} \end{cases}. \tag{5.12}$$

The weighted probability P_w^λ in the root of the context-tree can now be used as coding probability for the entire sequence x_1^T. The method is called the context-tree weighting (CTW) method. What is important is that the weighted probability realized by

CTW satisfies

$$\begin{aligned} P_w^{\lambda} &= \sum_{\mathcal{S}} 2^{-\Gamma_D(\mathcal{S})} \cdot \prod_{s\in\mathcal{S}} P_e(a_s,b_s) \\ &\geq 2^{-\Gamma_D(\mathcal{S}_a)} \cdot \prod_{s\in\mathcal{S}_a} P_e(a_s,b_s), \end{aligned} \tag{5.13}$$

where the summation is over all tree models that fit in the context-tree $\mathcal{T}_D$, see Lem. 2 in Willems, Shtarkov, and Tjalkens [88], the cost of model $\mathcal{S}$ is defined as

$$\Gamma_D(\mathcal{S}) \stackrel{\Delta}{=} 2|\mathcal{S}| - 1 - |\{s \in \mathcal{S}, \text{depth}(s) = D\}|, \tag{5.14}$$

and $\mathcal{S}_a$ is the actual model.

5.2.7 Performance

The individual redundancy $\rho(x_1^T)$ relative to the actual source for sequence x_1^T can be upper bounded by

$$\begin{aligned} \rho(x_1^T) &= L_w(x_1^T) - \log \frac{1}{P_a(x_1^T)} \\ &< \Gamma_D(\mathcal{S}_a) + \frac{|\mathcal{S}_a|}{2} \log \frac{T}{|\mathcal{S}_a|} + |\mathcal{S}_a| + 2, \end{aligned} \tag{5.15}$$

for $T \geq |\mathcal{S}_a|$. Moreover, $\rho(x_1^T) \leq \Gamma_D(\mathcal{S}_a) + T + 2$, for $T < |\mathcal{S}_a|$.

The three terms in bound (5.15) are the cost of specifying the model, i.e. $\Gamma_D(\mathcal{S}_a)$, the cost of specifying the parameters, which is $\frac{|\mathcal{S}_a|}{2} \log \frac{T}{|\mathcal{S}_a|} + |\mathcal{S}_a|$, and the loss of 2 binary digits due to arithmetic coding.

Observe that bound (5.15) holds for the redundancy relative to *any other tree source model* $\mathcal{S}$ with depth $\leq D$.

5.3 Ratios of Probabilities

The CTW method makes use of the context-tree concept, which requires every internal node to store counts a_s, b_s, estimated block probabilities P_e^s and weighted block probabilities P_w^s. In Willems and Tjalkens [91] it was shown that storage complexity reduction can be achieved if the ratio of these probabilities is stored in a node instead of the two probabilities themselves. Storage complexity reduction is also achieved, since ratios of the two block probabilities need not be as accurate as those block probabilities.

Consider an internal node $s \in \mathcal{T}_D$. Suppose that $0s$ (and not $1s$) is a suffix of the context x_{1-D}^0, x_1^{t-1} of x_t. Then we can write for the corresponding conditional weighted probability $P_w^s(X_t = 1|x_{1-D}^0, x_1^{t-1})$ that

$$\begin{aligned}
&P_w^s(X_t = 1|x_1^{t-1}) \\
&\quad = \frac{P_w^s(x_1^{t-1}, X_t = 1)}{P_w^s(x_1^{t-1})} \\
&\quad \stackrel{(a)}{=} \frac{P_e^s(x_1^{t-1}, X_t = 1) + P_w^{0s}(x_1^{t-1}, X_t = 1) P_w^{1s}(x_1^{t-1}, X_t = 1)}{P_e^s(x_1^{t-1}) + P_w^{0s}(x_1^{t-1}) P_w^{1s}(x_1^{t-1})} \\
&\quad \stackrel{(b)}{=} \frac{P_e^s(x_1^{t-1}) P_e^s(X_t = 1|x_1^{t-1}) + P_w^{0s}(x_1^{t-1}) P_w^{0s}(X_t = 1|x_1^{t-1}) P_w^{1s}(x_1^{t-1})}{P_e^s(x_1^{t-1}) + P_w^{0s}(x_1^{t-1}) P_w^{1s}(x_1^{t-1})} \\
&\quad = \frac{\beta_s(x_1^{t-1}) P_e^s(X_t = 1|x_1^{t-1}) + P_w^{0s}(X_t = 1|x_1^{t-1})}{\beta_s(x_1^{t-1}) + 1},
\end{aligned} \tag{5.16}$$

where $\beta_s(x_1^{t-1})$ is the ratio of the block probabilities defined as

$$\beta_s(x_1^{t-1}) \stackrel{\Delta}{=} \frac{P_e^s(x_1^{t-1})}{P_w^{0s}(x_1^{t-1}) P_w^{1s}(x_1^{t-1})}. \tag{5.17}$$

Here step (a) follows from the main CTW definition (5.12), and step (b) follows from the fact that $1s$ is not suffix of x_1^{t-1} and therefore $P_w^{1s}(x_1^{t-1}, X_t = 1) = P_w^{1s}(x_1^{t-1})$. In this expression (and the rest of this section), for simplicity, we omitted x_{1-D}^0 in all conditions.

Assuming that in node s the counts $a_s(x_1^{t-1})$ and $b_s(x_1^{t-1})$ are stored as well as the ratio $\beta_s(x_1^{t-1})$, we have the following sequence of operations:

1. We assume that node $0s$ delivers the conditional weighted probability $P_w^{0s}(X_t = 1|x_1^{t-1})$ to node s.

2. The conditional estimated probability is determined as suggested by Krichevsky and Trofimov [43], i.e.

$$\begin{aligned}
P_e^s(X_t = 0|x_1^{t-1}) &= \frac{a_s(x_1^{t-1}) + \frac{1}{2}}{a_s(x_1^{t-1}) + b_s(x_1^{t-1}) + 1}, \\
P_e^s(X_t = 1|x_1^{t-1}) &= \frac{b_s(x_1^{t-1}) + \frac{1}{2}}{a_s(x_1^{t-1}) + b_s(x_1^{t-1}) + 1}.
\end{aligned} \tag{5.18}$$

3. The outgoing conditional weighted probabilities are determined as

$$\begin{aligned}
P_w^s(X_t = 0|x_1^{t-1}) &= \frac{\beta_s(x_1^{t-1}) P_e^s(X_t = 0|x_1^{t-1}) + P_w^{0s}(X_t = 0|x_1^{t-1})}{\beta_s(x_1^{t-1}) + 1}, \\
P_w^s(X_t = 1|x_1^{t-1}) &= \frac{\beta_s(x_1^{t-1}) P_e^s(X_t = 1|x_1^{t-1}) + P_w^{0s}(X_t = 1|x_1^{t-1})}{\beta_s(x_1^{t-1}) + 1}.
\end{aligned} \tag{5.19}$$

4. The ratio $\beta_s(\cdot)$ is updated with new x_t as

$$\beta_s(x_1^{t-1},x_t) = \begin{cases} \beta_s(x_1^{t-1},x_t)\cdot P_e^s(X_t=0|x_1^{t-1})/P_w^{0s}(X_t=0|x_1^{t-1}), & \text{if } x_t=0 \\ \beta_s(x_1^{t-1},x_t)\cdot P_e^s(X_t=1|x_1^{t-1})/P_w^{0s}(X_t=1|x_1^{t-1}), & \text{if } x_t=1 \end{cases}. \quad (5.20)$$

5. Finally, the counts are incremented

$$\Big(a_s(x_1^{t-1},x_t), b_s(x_1^{t-1},x_t)\Big) \;=\; \begin{cases} (a_s(x_1^{t-1},x_t)+1, b_s(x_1^{t-1},x_t)), & \text{if } x_t=0 \\ (a_s(x_1^{t-1},x_t), b_s(x_1^{t-1},x_t)+1), & \text{if } x_t=1 \end{cases}. \quad (5.21)$$

△

We see that inside the node s there is a *switch* that controls the mixture between the incoming conditional weighted probability $P_w^{0s}(X_t=1|x_1^{t-1})$ and the (internal) one $P_e^s(X_t=1|x_1^{t-1})$. The mixture is determined by $\beta_s(x_1^{t-1})$. For large $\beta_s(x_1^{t-1})$ the outgoing conditional probability is approximately equal to $P_e^s(X_t=1|x_1^{t-1})$, for small $\beta_s(x_1^{t-1})$ it is approximately equal to $P_w^{0s}(X_t=1|x_1^{t-1})$. If s is a leaf of $\mathcal{T}_D$ the outgoing conditional weighted probability is simply $P_e^s(X_t=1|x_1^{t-1})$, i.e. the internal one.

Storage complexity reduction is obtained, since estimated and weighted block probabilities decrease as the sequence length T increases, while the ratio β_s corresponds to two different coding alternatives for the subsequence in the node s and is therefore closer to one. Observe also that (5.19) shows that in practice the performance does not depend on how large and how small β's really can become as long as they are large or small enough.

5.4 Context-Tree Maximizing

5.4.1 Two-Pass Methods

The CTW-method is a *one-pass algorithm*. The source sequence x_1^T is processed in a sequential way, i.e. the first source symbol x_1 is observed, some first code symbols are produced or not, the second symbol x_2 is observed, more code symbols are produced or not, etc. In a *two-pass system* the entire source sequence x_1^T is observed first. Only after that a codeword is constructed. Consider the following *two-pass method.*

1. After observing x_1^T, determine the "best model" $\hat{\mathcal{S}}$ matching to x_1^T.
2. Encode this model $\hat{\mathcal{S}}$.
3. Encode the sequence x_1^T given this model $\hat{\mathcal{S}}$.

To specify such an algorithm we have to specify the parts of which it consists. Some questions that arise now are: What is the best model $\hat{\mathcal{S}}$? How can it be determined efficiently?

5.4.2 The Context-Tree Maximizing Algorithm

When the source produces sequence x_1^T and model $\mathcal{S}$ is chosen as the best model, the resulting coding probability[2] for the two-pass case is

$$2^{-\Gamma_D(\mathcal{S})} \cdot \prod_{s \in \mathcal{S}} P_e(a_s, b_s). \tag{5.22}$$

Here the first factor is the number of bits needed to specify the model $\mathcal{S}$ in a recursive way (i.e. the natural code mentioned in [88]) and the second factor is the coding probability of the sequence x_1^T given the model $\mathcal{S}$, see (5.8).

The context-tree maximizing method, see e.g. Volf and Willems [84] but also Nohre [51], finds the model, maximizing (5.22) recursively, using a context-tree, by taking

$$P_m^s = \begin{cases} \max[\frac{1}{2}P_e(a_s, b_s), \frac{1}{2}P_m^{0s}P_m^{1s}], & \text{if depth}(s) < D \\ P_e(a_s, b_s), & \text{otherwise} \end{cases}. \tag{5.23}$$

It is assumed that the entire sequence x_1^T was processed into the context-tree. Finally, we can find the best model $\mathcal{S}$ by tracking the maximization procedure, starting in the *root* λ of the context-tree. If in a node s in the context-tree $P_e(a_s, b_s) \geq P_m^{0s}P_m^{1s}$ then s is a leaf of the best tree $\hat{\mathcal{S}}$ and we do not have to investigate the sub-tree rooted in s any further. Otherwise s is an internal node of the best model and we have to check the nodes $0s$ and $1s$. Note that

$$P_m^\lambda = \max_{\mathcal{S}} 2^{-\Gamma_D(\mathcal{S})} \cdot \prod_{s \in \mathcal{S}} P_e(a_s, b_s), \tag{5.24}$$

and the model maximizing this expression is our best model, denoted by $\hat{\mathcal{S}}$.

Note that the context-tree maximizing method yields the maximum a posteriori (MAP) tree model given the observed sequence x_1^T. This observation can be found in Willems et al. [87].

5.4.3 Performance

The coding probability for context-tree maximizing satisfies

$$P_m^\lambda = 2^{-\Gamma_D(\hat{\mathcal{S}})} \cdot \prod_{s \in \hat{\mathcal{S}}} P_e(a_s, b_s) \geq 2^{-\Gamma_D(\mathcal{S}_a)} \cdot \prod_{s \in \mathcal{S}_a} P_e(a_s, b_s), \tag{5.25}$$

just like P_w^λ, see (5.13). Therefore maximizing, just like weighting, leads to the redundancy bound (5.15). Observe that this bound holds for any model, not only for $\mathcal{S}_a$.

[2] It satisfies $\sum_{x_1^T} P_m^\lambda(x_1^T) < 1$, however.

5.5 Context-Tree Maximizing Using Ratio Representation

In this section we introduce the procedure for determining the MAP-model for tree sources based on ratios of block probabilities.

5.5.1 Computing A Posteriori Model Probabilities

The procedure for computing a posteriori model probabilities based on ratios was introduced in Willems et al. [87]. Consider a sub-model $\mathcal{S}_s$ (a proper and complete set of strings all having a common suffix s) rooted in the node s of $\mathcal{T}_D$, such that it fits in the context-tree $\mathcal{T}_D$. Then the "conditional" probability of the sub-tree $\mathcal{S}_s$ given x_1^T is defined as

$$Q_w^s(\mathcal{S}_s) \stackrel{\Delta}{=} \frac{2^{-\Gamma_D(\mathcal{S}_s)}\prod_{s'\in\mathcal{S}_s}P_e(a_{s'},b_{s'})}{P_w^s}, \tag{5.26}$$

where the cost of sub-model $\mathcal{S}_s$ is defined as

$$\Gamma_D(\mathcal{S}_s) \stackrel{\Delta}{=} 2|\mathcal{S}_s| - 1 - |\{s' \in \mathcal{S}_s, \mathrm{depth}(s') = D\}|. \tag{5.27}$$

It is reasonable to call this probability a conditional probability, since the denominator in (5.26) can be expressed as

$$P_w^s = \sum_{\mathcal{S}_s} 2^{-\Gamma_D(\mathcal{S}_s)} \prod_{s'\in\mathcal{S}_s} P_e(a_{s'},b_{s'}), \tag{5.28}$$

and

$$\sum_{\mathcal{S}_s} 2^{-\Gamma_D(\mathcal{S}_s)} = 1, \tag{5.29}$$

where the summations are over all sub-models rooted in s having no leaves deeper than $D-\mathrm{depth}(s)$, see Lem. 2 in Willems, Shtarkov, and Tjalkens [88].

Now if $|\mathcal{S}_s| > 1$ and the node is not at level D (since if it is at D, it can not be split), we can split up the sub-model $\mathcal{S}_s$ into sub-models $\mathcal{S}_{0s}$ and $\mathcal{S}_{1s}$ and rewrite the conditional probability as

$$\begin{aligned} Q_w^s(\mathcal{S}_s) &= \frac{2^{-\Gamma_D(\mathcal{S}_{0s})}\prod_{s'\in\mathcal{S}_{0s}}P_e(a_{s'},b_{s'})}{P_w^{0s}} \\ &\quad \cdot\frac{2^{-\Gamma_D(\mathcal{S}_{1s})}\prod_{s'\in\mathcal{S}_{1s}}P_e(a_{s'},b_{s'})}{P_w^{1s}} \\ &\quad \cdot\frac{P_w^{0s}P_w^{1s}}{P_e(a_s,b_s)+P_w^{0s}P_w^{1s}} \\ &= Q_w^{0s}(\mathcal{S}_{0s})Q_w^{1s}(\mathcal{S}_{1s})\frac{1}{\beta_s+1}, \end{aligned} \tag{5.30}$$

for nodes $s \in \mathcal{T}_D$ with depth $< D$, where the ratios are defined as in Section 5.3, i.e.

$$\beta_s \stackrel{\Delta}{=} \frac{P_e(a_s, b_s)}{P_w^{0s} P_w^{1s}}. \tag{5.31}$$

When the sub-model $\mathcal{S}_s$ contains only one leaf s, not at depth D, then

$$Q_w^s(\mathcal{S}_s) = \frac{P_e(a_s, b_s)}{P_e(a_s, b_s) + P_w^{0s} P_w^{1s}} = \frac{\beta_s}{\beta_s + 1}. \tag{5.32}$$

Finally, if the sub-model $\mathcal{S}_s$ consists only of a single leaf-node s at level D, then

$$Q_w^s(\mathcal{S}_s) = 1. \tag{5.33}$$

Summarizing the three considered cases, we can write

$$Q_w^s(\mathcal{S}_s) = \begin{cases} Q_w^{0s}(\mathcal{S}_{0s}) Q_w^{1s}(\mathcal{S}_{1s}) \cdot 1/(\beta_s + 1), & \text{if } |\mathcal{S}_s| > 1 \\ \beta_s/(\beta_s + 1), & \text{if } |\mathcal{S}_s| = 1, \text{depth}(s) < D \\ 1, & \text{if } |\mathcal{S}_s| = 1, \text{depth}(s) = D \end{cases}. \tag{5.34}$$

Now we take

$$P(\mathcal{S}) \stackrel{\Delta}{=} 2^{-\Gamma_D(\mathcal{S})} \tag{5.35}$$

as the *a priori probability* of model $\mathcal{S}$, then we can write for the a posteriori probability of model $\mathcal{S}$, after having observed the source sequence x_1^T, that

$$P_w(\mathcal{S}|x_1^T) = \frac{2^{-\Gamma_D(\mathcal{S})} \prod_{s \in \mathcal{S}} P_e(a_s, b_s)}{P_w^{\lambda}} = Q_w^{\lambda}(\mathcal{S}), \tag{5.36}$$

where the last equality follows from (5.26). Recursive expression (5.34) can now be used to determine the a posteriori probability $Q_w^{\lambda}(\mathcal{S})$ of a model $\mathcal{S}$ from the β's in the context-tree. We just have to form a product which consists of a factor $1/(\beta_{s'} + 1)$ for each internal node s' of the model $\mathcal{S}$ and a factor $\beta_{s''}/(\beta_{s''} + 1)$ for each leaf s'' of the model $\mathcal{S}$ not at level D.

5.5.2 Finding the Maximum A Posteriori Model

In the original paper of Willems et al. [87] for computing a posteriori model probabilities based on ratios of block probabilities, it was observed that context-tree maximizing, i.e. (5.23), yields the MAP tree model given the observed sequence x_1^T. We observe that, on the one hand, a posteriori model probabilities can be computed from the β's in a context-tree, while on the other hand, to determine the MAP-model, we need the context-tree maximizing method. Therefore in this section we develop a method that determines the MAP-model based on the ratios in the context-tree.

First, consider a problem of finding the MAP sub-model corresponding to a node s at depth $< D$. For such a node we can write

$$\max_{\mathcal{S}_s} Q_w^s(\mathcal{S}_s) \quad = \quad \max\left\{\frac{1}{\beta_s+1}\max_{\mathcal{S}_{0s}} Q_w^{0s}(\mathcal{S}_{0s})\max_{\mathcal{S}_{1s}} Q_w^{1s}(\mathcal{S}_{1s}), \frac{\beta_s}{\beta_s+1}\right\}. \quad (5.37)$$

In this expression the last term corresponds to the sub-model that has only a single leaf-node at s. The first term corresponds to all larger sub-models.

For a node at depth D only the one-leaf sub-model plays a role and therefore

$$\max_{\mathcal{S}_s} Q_w^s(\mathcal{S}_s) \quad = \quad 1. \quad (5.38)$$

Now defining for all nodes $s \in \mathcal{T}_D$ the MAP sub-model probability

$$Q_{mw}^s \quad \stackrel{\Delta}{=} \quad \max_{\mathcal{S}_s} Q_w^s(\mathcal{S}_s), \quad (5.39)$$

we can combine the above expressions and define the recursive equation and procedure for finding the MAP-model.

Procedure 5.1 (The Maximum A Posteriori Model Procedure)

1. Compute the MAP model probabilities as

$$Q_{mw}^s \;=\; \begin{cases} \max\left\{Q_{mw}^{0s}Q_{mw}^{1s}\cdot 1/(\beta_s+1), \beta_s/(\beta_s+1)\right\}, & \text{if depth}(s) < D \\ 1, & \text{if depth}(s) = D \end{cases}. \quad (5.40)$$

2. In the root λ of the context-tree find the maximum a posteriori model probability Q_{mw}^{λ}.

3. Track the procedure starting in the root of the context-tree. This yields the MAP-model.

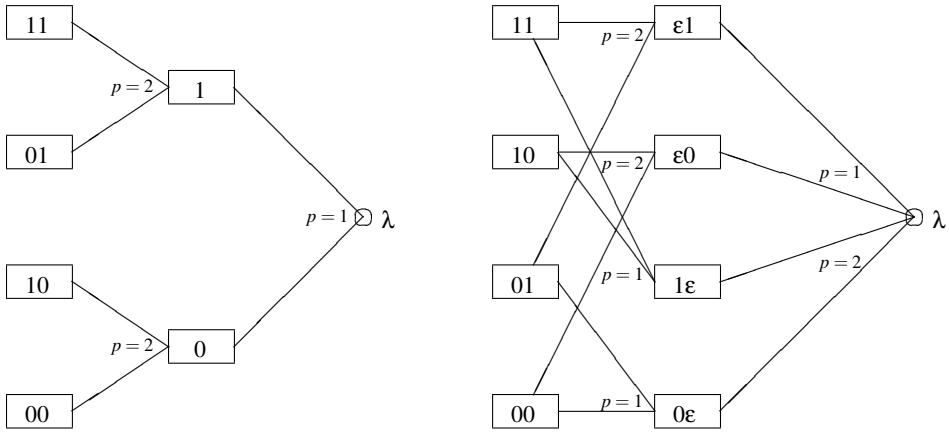
5.6 Context Maximizing Using Ratio Representation: Class III

Now we extend the techniques for computing a posteriori model probabilities and finding the MAP-model described in Section 5.5 to techniques for a more general model class than the tree source class, i.e. for class III of finite context sources. These sources were described in Willems, Shtarkov, and Tjalkens [90].

5.6.1 General Finite Context Sources: Class III

Consider a bounded memory source with memory not larger than D. Hence the distribution that the source uses to generate the next symbol X_t, $t = 1,2,\ldots,T$ is determined by its context $(u_t(1),u_t(2),\ldots,u_t(D))$. In the CTW method, the context of x_t was formed by the most recent symbols, thus $u_t(d) = x_{t-d}$ for $d = 1,2,\ldots,D$. However, more general definitions are possible, the only requirement is that the context should be available to the encoder at encoding time of x_t and to the decoder at decoding time of x_t. In [90] weighting methods were considered for four classes of general finite context sources. In the current section we will concentrate on class III.

Consider first the tree sources. Recall that in the CTW algorithm the context symbols are examined in a fixed order, i.e. from the most recent to the least recent symbol. There the context-tree is a full binary tree with a depth D, and each node splits according to the next context symbol, see Fig. 5.3(a). In every node of the context-tree the algorithm weights two alternatives: the probability that a subsequence associated with the node is memoryless, and the probability that it has to be split further, see (5.12).



(a) Contex-tree (b) Class III

Figure 5.3: *Examples of tree and class III models , for $D = 2$, p indicates a position of the split,* ε *indicates 'don't care' symbol*

In the class III weighting algorithm all possible orders of the context symbols are considered. There a node can be split correspondingly to an arbitrary context position. Therefore the node splits on each context position into two subsets, each corresponding to the value of the context digit on this position. An example of such

a context structure is shown in Fig. 5.3(b). In each node of the context structure the algorithm weights alternatives: the probability that a subsequence associated with the node is memoryless and the probabilities that it has to be split further on some context position.

Let $\mathbf{S}$ be a subset of the set of all contexts $\{0,1\}^D$. In class III model, a subset is determined by the set of context positions $\mathcal{P}$ and the sequence of values at these positions $\prod_{d\in\mathcal{P}} v_d$, hence

$$\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d} \stackrel{\Delta}{=} \{u_1,u_2,\ldots,u_D | u_d = v_d, d\in\mathcal{P}\}. \tag{5.41}$$

The recursive weighting for arbitrary position splitting is defined as

$$P_w(\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}) = \frac{P_e(\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}) + \sum_{p\in\{1,2,\ldots,D\}, p\notin\mathcal{P}} P_w(\mathbf{S}_{\mathcal{P}\cup\{p\},(\prod_{d\in\mathcal{P}} v_d)\times 0}) \cdot P_w(\mathbf{S}_{\mathcal{P}\cup\{p\},(\prod_{d\in\mathcal{P}} v_d)\times 1})}{D-|\mathcal{P}|+1}, \tag{5.42}$$

where $\mathcal{P}\neq\{1,2,\ldots,D\}$. Thus the algorithm weights the following alternatives. The first alternative is that the subset $\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}$ has a single context. And the other alternatives are that the subset has to be split further on some remaining positions p into nodes with contexts that contain 0 and 1 on position p. Note that if the subset has a single context, then the Krichevsky-Trofimov estimator is used, i.e.

$$P_e(\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}) \stackrel{\Delta}{=} P_e(a_{\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}}, b_{\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}}), \tag{5.43}$$

where $a_{\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}}$ and $b_{\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}}$ are the number of instants t for which $(u_t(1),u_t(2),\ldots,u_t(D))\in\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}$ and $x_t=0$ and $x_t=1$, respectively.

For subsets for which all positions are specified (thus they contain a single context) we have that

$$P_w(\mathbf{S}_{\{1,2,\ldots,D\},v_1,v_2,\ldots,v_D}) = P_e(\mathbf{S}_{\{1,2,\ldots,D\},v_1,v_2,\ldots,v_D}) = P_e(\{v_1,v_2,\ldots,v_D\}). \tag{5.44}$$

The weighted probability $P_w(\mathbf{S}_{\{\phi\},\lambda}) = P_w(\{0,1\}^D)$ can be used for sequential encoding and decoding. Here $\{\phi\}$ is an empty set.

The storage complexity of these methods is specified by maximum 3^D number of nodes in the structure. Its computational complexity is proportional to 2^D, since 2^D nodes are to be updated for each symbol x_t. Observe that the class III method has higher complexity than CTW. Indeed, the CTW method needs maximum $2^{D+1}-1$ number of nodes in the structure and only $D+1$ records to update for each symbol x_t.

5.6.2 Computing A Posteriori Model Probabilities

Consider a sub-model $\mathcal{S}_s$, rooted in the node $s = \mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d}$ that corresponds to all splittings with context $\mathbf{S}_{\mathcal{P},\prod_{d\in\mathcal{P}} v_d} = \{u_1, u_2, \ldots, u_D | u_d = v_d, d \in \mathcal{P}\}$. Moreover, let $l(\mathcal{S}_s)$ be a set of leaves of the sub-model $\mathcal{S}_s$. The conditional probability of the sub-model $\mathcal{S}_s$ given x_1^T is defined as

$$Q_w^s(\mathcal{S}_s) \quad \stackrel{\Delta}{=} \quad \frac{P(\mathcal{S}_s)\prod_{s'\in l(\mathcal{S}_s)} P_e(a_{s'}, b_{s'})}{P_w^s}. \tag{5.45}$$

where $P(\mathcal{S}_s)$ is a priori probability of the sub-model $\mathcal{S}_s$ recursively defined as

$$P(\mathcal{S}_s) \quad \stackrel{\Delta}{=} \quad \frac{1}{|\mathcal{P}_s|+1} P(\mathcal{S}_{\{0p\}s}) P(\mathcal{S}_{\{1p\}s}), \tag{5.46}$$

for $|\mathcal{S}_s| > 1$, and $P(\mathcal{S}_s) = 1$, for $|\mathcal{S}_s| = 1$. Here $\mathcal{S}_{\{0p\}s}$ and $\mathcal{S}_{\{1p\}s}$ are the sub-models into which the sub-model $\mathcal{S}_s$ splits. These sub-models correspond to splittings with contexts $\mathbf{S}_{\mathcal{P}\cup\{p\},(\prod_{d\in\mathcal{P}} v_d)\times 0}$ and $\mathbf{S}_{\mathcal{P}\cup\{p\},(\prod_{d\in\mathcal{P}} v_d)\times 1}$, respectively. Position $p \in \mathcal{P}_s$ specifies the context position on which the node s is split further on and $\mathcal{P}_s = \{p : p \in \{1,2,\ldots,D\}, p \notin \mathcal{P}\}$ is the set of all position on which the split is still possible from node s.

Now consider the case when $|\mathcal{S}_s| > 1$ and the node s is not at level D. The sub-model $\mathcal{S}_s$ can be split up into two sub-models $\mathcal{S}_{\{0p\}s}$ and $\mathcal{S}_{\{1p\}s}$ We can rewrite the conditional probability as

$$\begin{aligned} Q_w^s(\mathcal{S}_s) \quad &= \quad \frac{P(\mathcal{S}_{\{0p\}s})\prod_{s'\in l(\mathcal{S}_{\{0p\}s})} P_e(a_{s'}, b_{s'})}{P_w^{\{0p\}s}} \\ &\cdot \quad \frac{P(\mathcal{S}_{\{1p\}s})\prod_{s'\in l(\mathcal{S}_{\{1p\}s})} P_e(a_{s'}, b_{s'})}{P_w^{\{1p\}s}} \\ &\cdot \quad \frac{P_w^{\{0p\}s} P_w^{\{1p\}s}}{P_e(a_s, b_s) + \sum_{p'\in\mathcal{P}_s} P_w^{\{0p'\}s} P_w^{\{1p'\}s}} \\ &= \quad Q_w^{\{0p\}s}(\mathcal{S}_{\{0p\}s}) Q_w^{\{1p\}s}(\mathcal{S}_{\{1p\}s}) \frac{1/\beta_{ps}}{1+\sum_{p'\in\mathcal{P}_s} 1/\beta_{p's}}, \end{aligned} \tag{5.47}$$

where

$$\beta_{ps} \quad \stackrel{\Delta}{=} \quad \frac{P_e(a_s, b_s)}{P_w^{\{0p\}s} P_w^{\{1p\}s}}, \tag{5.48}$$

for nodes s with depth less than D. Note that the ratios $\beta_{sp}(\cdot)$ defined here are analogs of the internal ratios considered in Section 5.3. Observe also that there are $|\mathcal{P}_s|$ of such ratios.

If the sub-model contains only one context s not at depth D, then

$$\begin{aligned} Q_w^s(\mathcal{S}_s) &= \frac{P_e(a_s,b_s)}{P_e(a_s,b_s)+\sum_{p'\in\mathcal{P}_s} P_w^{\{0p'\}s} P_w^{\{1p'\}s}} \\ &= \frac{1}{1+\sum_{p'\in\mathcal{P}_s} 1/\beta_{p's}}. \end{aligned} \tag{5.49}$$

Finally, if the sub-model $\mathcal{S}_s$ consists only of a single context s at level D, then

$$Q_w^s(\mathcal{S}_s) = 1. \tag{5.50}$$

Summarizing the equations above, we can write

$$Q_w^s(\mathcal{S}_s) = \begin{cases} Q_w^{\{0p\}s}(\mathcal{S}_{\{0p\}s}) Q_w^{\{1p\}s}(\mathcal{S}_{\{1p\}s}) \cdot (1/\beta_{ps})/(1+\sum_{p'\in\mathcal{P}_s} 1/\beta_{p's}), & |\mathcal{S}_s|>1 \\ 1/(1+\sum_{p'\in\mathcal{P}_s} 1/\beta_{p's}), & |\mathcal{S}_s|=1, |\mathcal{P}|<D. \\ 1, & |\mathcal{S}_s|=1, |\mathcal{P}|=D \end{cases} \tag{5.51}$$

Now if we define $P(\mathcal{S})$ to be the probability of the complete model $\mathcal{S}$, then using (5.45), we can write for the a posteriori probability of a given model $\mathcal{S}$ after having observed a source sequence x_1^T that

$$P_w(\mathcal{S}|x_1^T) = \frac{P(\mathcal{S})\prod_{s\in l(\mathcal{S})} P_e(a_s,b_s)}{P_w^\lambda} = Q_w^\lambda(\mathcal{S}). \tag{5.52}$$

Therefore, similarly to the procedure for tree sources, in order to compute the a posteriori probability corresponding to a model $\mathcal{S}$ we have to form a product that consists of a factor $(1/\beta_{ps'})/(1+\sum_{p'\in\mathcal{P}_{s'}} 1/\beta_{p's'})$ for each internal node s' of the model $\mathcal{S}$ and a factor $1/(1+\sum_{p'\in\mathcal{P}_{s''}} 1/\beta_{p's''})$ for each leaf s'' of the model $\mathcal{S}$ not at level D.

Remark: Note that for class III it would be more natural to define the betas as

$$\beta_{ps} = \frac{P_w^{\{0p\}s} P_w^{\{1p\}s}}{P_e(a_s,b_s)}. \tag{5.53}$$

However, for consistency with the first part of the chapter, we use the definition as in (5.48).

5.6.3 Finding the Maximum A Posteriori Model

Now we can formulate the method to find the MAP-model based on β's in the context-structure of class III given an observed sequence x_1^T. Again consider, first, the maximum a posteriori probability for a sub-model $\mathcal{S}_s$ at node s at depth $< D$. For such a

node we can write

$$\max_{\mathcal{S}_s} Q_w^s(\mathcal{S}_s)$$
$$= \max\Big\{\max_{p\in\mathcal{P}_s}\{\max_{\mathcal{S}_{\{0p\}s}} Q_w^{\{0p\}s}\max_{\mathcal{S}_{\{1p\}s}} Q_w^{\{1p\}s}\frac{1/\beta_{ps}}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}\},\frac{1}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}\Big\}, \quad (5.54)$$

where the first term corresponds to all larger sub-models resulting from all (possible at this level) context splits, and the last term corresponds to the sub-model that has a single context, i.e. to a leaf-node.

For a note at depth D only one-leaf sub-models play a role and therefore

$$\max_{\mathcal{S}_s} Q_w^s(\mathcal{S}_s) \quad = \quad 1. \quad (5.55)$$

Now we define for all nodes s the MAP sub-model probability

$$Q_{mw}^s \quad \stackrel{\Delta}{=} \quad \max_{\mathcal{S}_s} Q_w^s(\mathcal{S}_s). \quad (5.56)$$

The recursive equation for computing the MAP-model probability is summarized as follows.

Procedure 5.2 (The Maximum A Posteriori Model Procedure for Class III)

1. Compute the MAP model probabilities as

$$Q_{mw}^s = \begin{cases} \max\Big\{\max_{p\in\mathcal{P}_s}\{Q_{mw}^{\{0p\}s}Q_{mw}^{\{1p\}s}\frac{1/\beta_{ps}}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}\},\frac{1}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}\Big\}, & |\mathcal{P}|<D \\ 1, & |\mathcal{P}|=D \end{cases}. \quad (5.57)$$

2. In the root λ of the context-structure find the MAP-model probability Q_{mw}^{λ}.

3. To obtain the MAP-model, track the maximizing procedure starting in the root of the context-structure. More precisely, check whether in the node s of the context-structure

$$\max_{p\in\mathcal{P}_s}\{Q_{mw}^{\{0p\}s}Q_{mw}^{\{1p\}s}\frac{1/\beta_{ps}}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}\} \quad \leq \quad \frac{1}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}, \quad (5.58)$$

if so, then s is the leaf of the best model. Otherwise, s is an internal node and we have to investigate the sub-models with $\{0p\}s$ and $\{1p\}s$, where

$$p \quad = \quad \arg\max_{p\in\mathcal{P}_s}\{Q_{mw}^{\{0p\}s}Q_{mw}^{\{1p\}s}\frac{1/\beta_{ps}}{1+\sum_{p'\in\mathcal{P}_s}1/\beta_{p's}}\}. \quad (5.59)$$

5.7 Conclusions

In this chapter context-weighting methods based on ratios of block probabilities have been considered. Since in Willems et al. [87] a method for computing a posteriori model probabilities based on ratios was proposed, there a posteriori model probabilities can be computed from the ratios in a context-tree, while, on the other hand, to determine the MAP tree-model the context-tree maximizing method of Volf and Willems [84] was needed. Therefore in this chapter we have developed a method that determines the MAP-model based on the ratios in the weighted context-tree.

We have extended the methods for determining the a posteriori probability of a specified model and for finding the MAP-model from basic CTW to class III models. It would be interesting to extend the results that we have obtained in the current chapter to class I and class II methods for general finite context sources described in [90], but we leave it for the future research work.

As a concluding remark, it should be mentioned that, although the methods presented in this chapter are described for binary sources, they can be straightforwardly generalized to larger alphabets.

Chapter 6

Secret-Key Rate Estimation Based on Context Weighting Methods

No amount of experimentation can ever prove me right; a single experiment can prove me wrong (Albert Einstein).

6.1 Introduction

In Chapters 2, 3, and 4 of this thesis we have considered biometric secret generation models and biometric models with chosen secret keys. In these settings one terminal is allowed to transmit a message to a second one. We have required that the message reveals negligible information about the secret key and as little as possible information about the biometric data. It is well-known that the maximum secret-key rate produced by two terminals or conveyed by one terminal to another is equal to the mutual information between the two observed biometric data sequences. These results hold when the biometric sequences are produced by i.i.d. sources. This is the Ahlswede and Csiszár [3] result, see also Thm. 2.1. Moreover, these results are also valid for stationary ergodic sources, as shown by Csiszár and Narayan [17], see also Thm.2.2 and the discussion part of Section 4.6.1.

Before designing any practical biometric secrecy system, it is important to evaluate theoretical limits that can be achieved with biometric data on which the system will operate. Hence, given a biometric modality, first of all it is necessary to estimate the amount of secrecy that can be produced or conveyed with this modality. Note also that biometric data such as iris codes, fingerprint minutiae maps, face patterns, PUFs, etc. are often modeled as realizations of two-dimensional processes, see e.g. Jain et al. [36] and Wayman et al. [85]. Therefore we are particularly interested in estimates of mutual information and, correspondingly, of entropy for two-dimensional sources.

In this chapter we will study the estimation of maximum secret-key rates for biometric sources using the CTW method. This method was introduced by Willems, Shtarkov, and Tjalkens [88] and we discussed it in the previous chapter. First we will show that the entropy of a stationary two-dimensional source is a limit of a series

of conditional entropies. A similar result was obtained by Anastassiou and Sakrison [6]. We will extend this result to the conditional entropy of one two-dimensional source given another one. Furthermore, we will show that the basic CTW method also approaches the source entropy in the two-dimensional stationary ergodic case. This result carries over to conditional entropies and joint entropies in the two-dimensional stationary ergodic case.

Finally, we will use these results to estimate the maximum secret-key rate of speckle patterns from optical Physical Unclonable Functions (PUFs). PUFs are a particular case of biometrics that come from inanimate objects. PUFs were first proposed by Pappu [52] and further studied in Gassend et al. [30], Tuyls and Batina [78], and Škorić et al. [70]. A good overview of PUF related technologies can be found in Tuyls et al. [77].

6.2 On the Entropy of Two-Dimensional Stationary Processes

In this section we discuss the relation between entropies of two-dimensional processes and conditional entropies.

6.2.1 On the Entropy of a Two-Dimensional Stationary Process

Consider the two-dimensional process $\{X_{v,h} : (v,h) \in \mathbb{Z}^2\}$, also called random field, and assume that it is stationary (homogeneous), i.e.

$$\Pr\{X_{\mathcal{T}} = x_{\mathcal{T}}\} \quad = \quad \Pr\{X_{\mathcal{T}+(s_v,s_h)} = x_{\mathcal{T}}\}, \tag{6.1}$$

for any template $\mathcal{T}$, any shift (s_v,s_h), and any observation $x_{\mathcal{T}}$. A template is a set of coordinate pairs, i.e. $\mathcal{T} \subset \mathbb{Z}^2$. Moreover, $\mathcal{T}+(s_v,s_h)$ denotes the set of coordinate pairs resulting from a coordinate pair from $\mathcal{T}$, to which the integer shift pair (s_v,s_h) is added. We assume that all symbols take values from the finite alphabet $\mathcal{X}$.

First, for positive integers L we define

$$H_L(X) \quad \stackrel{\Delta}{=} \quad \frac{1}{L^2} H \begin{pmatrix} X_{1,1} & \dots & X_{1,L} \\ \vdots & \ddots & \vdots \\ X_{L,1} & \dots & X_{L,L} \end{pmatrix}, \tag{6.2}$$

then the entropy of a two-dimensional stationary process can be defined as

$$H_\infty(X) \quad \stackrel{\Delta}{=} \quad \lim_{L\to\infty} H_L(X). \tag{6.3}$$

Now we can formulate the following lemma.

Lemma 6.1 *The limit defined in (6.3) exists.*

Proof: From the stationarity of the stochastic process X, the chain rule for entropies, and the fact that conditioning can only decrease entropy, it follows that

$$\begin{aligned} NH\begin{pmatrix} X_{1,1} & \dots & X_{1,N+1} \\ \vdots & \ddots & \vdots \\ X_{M,1} & \dots & X_{M,N+1} \end{pmatrix} - (N+1)H\begin{pmatrix} X_{1,1} & \dots & X_{1,N} \\ \vdots & \ddots & \vdots \\ X_{M,1} & \dots & X_{M,N} \end{pmatrix} & \\ = \; NH\left(\begin{array}{c|ccc} X_{1,N+1} & X_{1,1} & \dots & X_{1,N} \\ \vdots & \vdots & \ddots & \vdots \\ X_{M,N+1} & X_{M,1} & \dots & X_{M,N} \end{array}\right) - H\begin{pmatrix} X_{1,1} & \dots & X_{1,N} \\ \vdots & \ddots & \vdots \\ X_{M,1} & \dots & X_{M,N} \end{pmatrix} & \\ \leq \; 0. & \end{aligned} \tag{6.4}$$

Using inequality (6.4) for $(M,N) = (L,L)$, we obtain

$$H\begin{pmatrix} X_{1,1} & \dots & X_{1,L+1} \\ \vdots & \ddots & \vdots \\ X_{L,1} & \dots & X_{L,L+1} \end{pmatrix} \leq \frac{L+1}{L} H\begin{pmatrix} X_{1,1} & \dots & X_{1,L} \\ \vdots & \ddots & \vdots \\ X_{L,1} & \dots & X_{L,L} \end{pmatrix}, \tag{6.5}$$

subsequently, using a transposed version of inequality (6.4) for $(M,N) = (L,L+1)$, we get

$$\frac{L}{L+1} H\begin{pmatrix} X_{1,1} & \dots & X_{L+1,1} \\ \vdots & \ddots & \vdots \\ X_{1,L+1} & \dots & X_{L+1,L+1} \end{pmatrix} \leq H\begin{pmatrix} X_{1,1} & \dots & X_{L,1} \\ \vdots & \ddots & \vdots \\ X_{1,L+1} & \dots & X_{L,L+1} \end{pmatrix}. \tag{6.6}$$

Combining (6.5) and (6.6), it follows that

$$H_{L+1}(X) - H_L(X) \leq 0. \tag{6.7}$$

Hence the sequence $H_L(X)$ is a non-increasing non-negative sequence in L. This finalizes the proof.

■

The definition of entropy in (6.3) focuses on block-entropies. We will show next that the entropy of a stationary two-dimensional process can also be expressed as a limit of conditional entropies. To this end we define the conditional entropy

$$G_L(X) \stackrel{\Delta}{=} H(X_{L,L}|X_{1,1},\dots,X_{1,2L-1},\dots,X_{L,1},\dots,X_{L,L-1}). \tag{6.8}$$

A visualization of this definition is presented in Fig. 6.1.

Remark: The choice of the conditioning template here is governed by the nature of the CTW method, see Chapter 5, since the CTW method is a coding algorithm that sequentially encodes symbols generated by a source after observing the past subsequence of symbols.

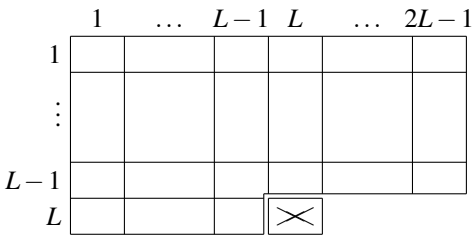


Figure 6.1: *The symbol $X_{L,L}$ and the symbols on which it is conditioned in (6.8).*

Lemma 6.2 *The limit*

$$G_\infty(X) \quad \stackrel{\Delta}{=} \quad \lim_{L\to\infty} G_L(X) \tag{6.9}$$

exists.

Proof: From stationarity and the fact that conditioning never increases entropy, it follows that the sequence $G_L(X)$ is non-increasing in L. Since the entropy is non-negative, so $G_L(X) \geq 0$, and the proof follows.

■

Now we are ready to formulate the main theorem of this section.

Theorem 6.1 *The limits $H_\infty(X)$ and $G_\infty(X)$ are equal, i.e.*

$$G_\infty(X) \quad = \quad H_\infty(X). \tag{6.10}$$

Proof: In order to demonstrate that the limits (6.3) and (6.9) are equal, we first observe, using chain rule, stationarity, and the fact that conditioning never increases entropy, that

$$\begin{aligned} H_L(X) \quad &= \quad \frac{1}{L^2}\sum_{v=1}^{L}\sum_{h=1}^{L} H(X_{v,h}|X_{1,1},\ldots,X_{1,L},\ldots,X_{v,1},\ldots,X_{v,h-1}) \\ &\geq \quad G_L(X). \end{aligned} \tag{6.11}$$

On the other hand, it follows (using similar arguments) that

$$H_{j+2L-2}(X) \quad \leq \quad \frac{H(\sqcap) + j(j+L-1)G_L(X)}{(j+2L-2)^2}, \tag{6.12}$$

where $H(\sqcap)$ corresponds to all symbols in the horseshoe region, see Fig. 6.2.

Applying limit to both sides of the above inequality yields that

$$H_\infty(X) = \lim_{j\to\infty} H_{j+2L-2}(X) \leq G_L(X). \tag{6.13}$$

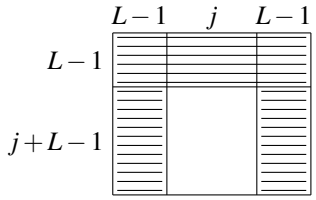


Figure 6.2: *Horseshoe region in a square of size* $(j+2L-2)^2$.

The proof follows from (6.11) and (6.13).

■

Our arguments are a generalization of the arguments for (one-dimensional) stationary sources that can be found in Gallager [29], pp. 56-58. Moreover, they are only slightly different from those given by Anastassiou and Sakrison [6], who first showed that in the two-dimensional case the block-entropy limit equals the conditional-entropy limit.

We conclude that the entropy of a two-dimensional stationary process can be computed by considering the conditional entropy of *a single symbol* given more and more neighboring symbols.

6.2.2 On the Conditional Entropy of a Two-Dimensional Stationary Process Given a Second One

Next we consider the two-dimensional joint process $\{XY_{v,h} : (v,h) \in \mathbb{Z}^2\}$. We assume that it is stationary, i.e.

$$\Pr\{XY_{\mathcal{T}} = xy_{\mathcal{T}}\} \quad = \quad \Pr\{XY_{\mathcal{T}+(s_v,s_h)} = xy_{\mathcal{T}}\}, \tag{6.14}$$

for any template $\mathcal{T}$ any shift (s_v, s_h), and any observation $xy_{\mathcal{T}}$. Again we assume that X-symbols and Y-symbols take values from the finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively.

We may consider the joint entropy $H_\infty(XY)$ of a joint process XY and then obviously Thm. 6.1 holds. Then we can compute conditional entropies by considering this joint entropy and entropies of processes X and Y.

It also makes sense to look at the conditional entropy $H_\infty(X|Y)$ and find out whether a theorem similar in style to Thm. 6.1 can be proved for this situation. This turns out to be possible if we define for positive integers L

$$H_L(X|Y) \quad \triangleq \quad \frac{1}{L^2} H \left(\begin{array}{ccc|ccc} X_{1,1} & \dots & X_{1,L} & Y_{1,1} & \dots & Y_{1,L} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ X_{L,1} & \dots & X_{L,L} & Y_{L,1} & \dots & Y_{L,L} \end{array} \right), \tag{6.15}$$

and define the conditional entropy of a two-dimensional joint stationary process XY as

$$H_\infty(X|Y) \stackrel{\Delta}{=} \lim_{L\to\infty} H_L(X|Y). \tag{6.16}$$

Then the following lemma holds.

Lemma 6.3 *The limit in (6.16) exists.*

Proof: First, we observe that, since conditioning never increases entropy, the following inequality holds

$$\begin{aligned} H\left(\begin{array}{ccc|ccc} X_{1,1} & \dots & X_{1,L} & Y_{1,1} & \dots & Y_{1,L+1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ X_{L,1} & \dots & X_{L,L} & Y_{L+1,1} & \dots & Y_{L+1,L+1} \end{array}\right) & \\ \leq H\left(\begin{array}{ccc|ccc} X_{1,1} & \dots & X_{1,L} & Y_{1,1} & \dots & Y_{1,L} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ X_{L,1} & \dots & X_{L,L} & Y_{L,1} & \dots & Y_{L,L} \end{array}\right). & \end{aligned} \tag{6.17}$$

Then, using the arguments similar to the ones used to show that $H_L(X)$ is non-increasing (see proof of Lem. 6.1) and inequality (6.17), the proof that the sequence $H_L(X|Y)$ is non-increasing in L follows. Finally, since $H_L(X)$ is a positive non-increasing sequence, we conclude that the limit in (6.16) exists.

■

In order to demonstrate that the conditional entropy $H_\infty(X|Y)$ can be expressed as a limit of entropies of a *single symbol* conditioned on surrounding X-symbols and Y-symbols, we define

$$\begin{aligned} G_L(X|Y) \stackrel{\Delta}{=} H(X_{L,L}|X_{1,1},\dots,X_{1,2L-1},\dots,X_{L,1},\dots,X_{L,L-1}, \\ \dots,Y_{1,1},\dots,Y_{2L-1,2L-1}). \end{aligned} \tag{6.18}$$

For a visualization we refer to Fig. 6.3.

Lemma 6.4 *The limit*

$$G_\infty(X|Y) \stackrel{\Delta}{=} \lim_{L\to\infty} G_L(X|Y) \tag{6.19}$$

exists.

Proof: It is easy to see that $G_{L+1}(X|Y) \leq G_L(X|Y)$ using arguments as in the proof of Lem. 6.2, from which and from non-negativity of $G_L(X|Y)$ the proof follows.

■

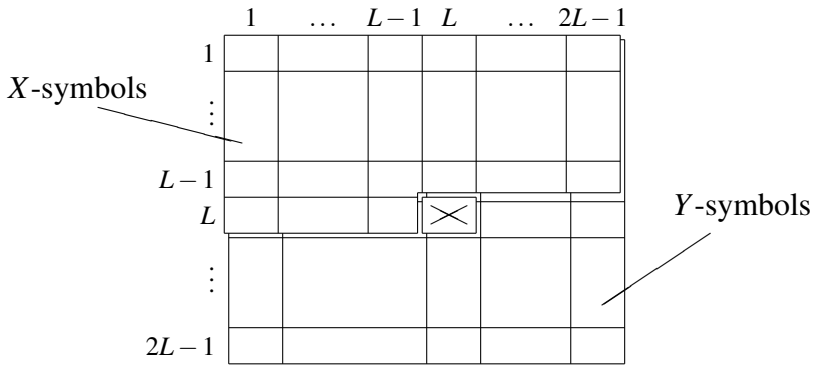


Figure 6.3: *The symbol $X_{L,L}$ and its conditioning symbols. Note that the X-symbols are drawn on top of a square with the Y-symbols.*

Theorem 6.2 *The limits defined in (6.16) and (6.19) are equal, i.e.*

$$G_\infty(X|Y) \quad = \quad H_\infty(X|Y). \tag{6.20}$$

Proof: In order to demonstrate that the limits (6.16) and (6.19) are equal, we observe that (according to the same arguments as used for (6.11) and (6.12))

$$H_L(X|Y) \quad \geq \quad G_L(X|Y), \tag{6.21}$$

$$H_{j+2L-2}(X|Y) \quad \leq \quad \frac{H(\square) + j^2 G_L(X|Y)}{(j+2L-2)^2}, \tag{6.22}$$

where $H(\square)$ corresponds to the X-symbols in the edge region, see Fig. 6.4. Hence we obtain

$$H_\infty(X|Y) \quad = \quad \lim_{j\to\infty} H_{j+2L-2}(X|Y) \quad \leq \quad G_L(X|Y). \tag{6.23}$$

The proof follows from (6.21) and (6.23).

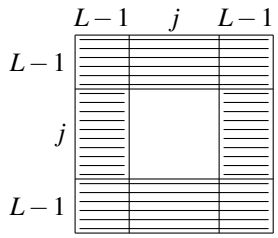


Figure 6.4: *Edge region in a square of size $(j+2L-2)^2$.*

■

We conclude that, in the stationary case, the conditional entropy of a one two-dimensional process X given a second two-dimensional process Y can also be computed by considering the conditional entropy of a single X-symbol given more and more "causal" neighboring X-symbols, and more and more "non-causal"[1] neighboring Y-symbols.

6.3 Mutual Information Estimation

6.3.1 Convergence

Now we turn to the estimation of the mutual information for two-dimensional stationary ergodic sources. We can estimate mutual information $I_\infty(X;Y)$ either by estimating $H_\infty(X)$, $H_\infty(Y)$, and $H_\infty(XY)$, or by estimating $H_\infty(X)$ and $H_\infty(X|Y)$ (or equivalently $H_\infty(Y)$ and $H_\infty(Y|X)$) using the CTW methods discussed in Chapter 5. It was proven in Willems [92] that the CTW method approaches entropy in the one-dimensional ergodic case. The following theorem applies to the two-dimensional case.

Theorem 6.3 *For joint processes XY, the general CTW method achieves entropy $H_\infty(XY)$, as well as $H_\infty(X)$ and $H_\infty(Y)$, and conditional entropies $H_\infty(X|Y)$ and $H_\infty(Y|X)$ in the two-dimensional ergodic case.*

Proof: From Thm. 6.1 and Thm. 6.2 we conclude that we can focus on conditional entropies of a single symbol (or pair of symbols). These are entropies that the CTW method achieves when the observed image gets larger and larger and more and more context symbols become relevant. It is important to use the right ordering of the context symbols though. Therefore the symbols for $L = 2$ should be included first, then those for $L = 3$, etc. The rest of the proof is similar to the proof of Thm. 3 in [92].

■

6.3.2 Using Context Weighting Methods

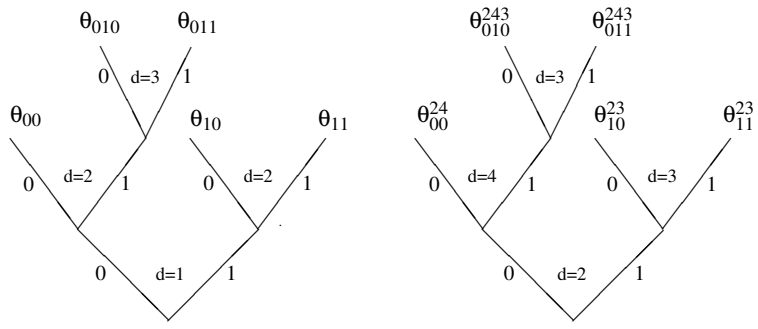
In order to estimate the mutual information between biometric sequences we are going to use context weighting methods. Note that these methods are sequential and at each step they use only the past and the present symbols.

In the basic CTW method for one-dimensional case the context is defined by a set of most recent symbols in a sequence. In a two-dimensional case the probabilities

[1] If we define the order in which symbols are processed in the image (e.g. from left to the right, and from top to bottom), then "causal" symbols are past symbols, while "non-causal" symbols might be both future and past symbols with respect to a certain symbol.

of the next symbol generated by source is determined by the local two-dimensional regions. For our purposes we need more flexibility in choosing the context symbols, however. This flexibility is provided by the weighting methods for general finite context sources that were proposed in Willems, Shtarkov, and Tjalkens [90]. Here we consider the two simplest classes, i.e. class IV and class III. These methods were described in the previous chapter.

Consider a source that has produced a sequence $(\ldots, x_{t-2}, x_{t-1})$ so far. Then, at time t, this source generates a new symbol x_t. The context for this symbol x_t consists of D symbols denoted by $(z_{t1}, z_{t2}, \ldots, z_{tD})$. Observe that each of these symbols could be any symbol available to both the encoder and decoder while encoding/decoding x_t. On the other hand, if there is a "side-information" sequence y^N available, then we could take $z_{td} = y_{t+d-1}$, but combinations of both past x-symbols and past and/or future y-symbols are also possible.



(a) Class IV (b) Class III

Figure 6.5: *Example of class IV and class III models.*

Consider a simple example. In a class IV method it is assumed that the actual probability of the next symbol x_t being 1 is based on the first d context symbols $(z_{t1}, z_{t2}, \ldots z_{td})$, where d depends on the context $(z_{t1}, z_{t2}, \ldots z_{tD})$ that has occurred. For instance, if the source model corresponds to the tree in Fig. 6.5(a), and the context $(z_{t1}, z_{t2}, \ldots z_{tD})$ at time t is $(011\varepsilon\ldots\varepsilon)$, the probability θ_{011} of the next symbol x_t being 1 can be found in the leaf 011. We have denoted a "don't care" context-symbol by ε here. The subscript 011 refers to the values 0, 1, and 1 of the context symbols z_{t1}, z_{t2}, and z_{t3}, respectively.

Class III models can also be described using a tree. However, the ordering of the context symbols is not fixed as in class IV. For a source model corresponding to the tree in Fig. 6.5(b), when the context $(z_{t1}, z_{t2}, \ldots z_{tD})$ at time t is $(\varepsilon 001\varepsilon\ldots\varepsilon)$, the probability θ^{243}_{010} of the next symbol x_t being 1 can be found in leaf 010. Note that the superscript 243 denotes the context ordering, i.e. first z_{t2} is used, then z_{t4}, and, finally, z_{t3}. The subscript 010 now refers to the values 0, 1, and 0 of these context

symbols z_{t2}, z_{t4}, and z_{t3}, respectively.

For both model classes the context weighting encoder (implicitly) specifies the context structure and corresponding parameters to a decoder. This results in the model and parameter redundancies, respectively, and thus in an increased codeword length. It will be evident that the class III methods are more general than the class IV ones. Since they adapt better to the source, the performance of the class III methods should therefore be better. Indeed the so-called parameter redundancy is smaller for class III than for class IV, but since class III is richer than class IV, its model redundancy is also larger. It depends on the length of the source sequence which of the two effects will dominate. For small lengths, the class IV methods will outperform the class III methods. For large lengths the effect of model redundancy becomes negligible and the class III method gives a smaller codeword length.

6.4 Biometric Secrecy Systems in the Stationary Ergodic Case

In Chapter 2 we presented Thm. 2.2. This theorem states that for biometric sequences which are generated by jointly stationary ergodic sources, the maximum secret-key rate that can be produced in the secret generation model is equal to $I_\infty(X;Y)$. Using the techniques described above, we can now estimate the maximum secret-key rates for stationary ergodic sources.

6.5 Experimental Results

In this section we consider a specific example of biometric data from inanimate objects, i.e. optical Physical Unclonable Functions (PUFs). Using the context weighting methods, we estimate the maximum secret-key rate for binary images obtained from optical PUFs speckle patterns.

6.5.1 Physical Unclonable Functions

In the introduction to this thesis we have already discussed PUFs. In this chapter we focus on optical PUFs. These PUFs were originally proposed in Pappu [52] and were further studied by Tuyls and Batina [78] and Škorić et al. [70].

Optical PUFs consist of a transparent optical material (e.g. glass) with randomly distributed light-scattering particles. Different challenges are obtained by directing a laser beam under different angles through a PUF. Shining a laser beam through the optical medium produces speckle patterns (responses) that are picked up by a CCD camera. The response depends on the exact position and direction of the chal-

lenge. The speckle patterns obtained from two measurements at the same challenge are shown in Fig. 6.6. Note that the speckle-images are very similar.

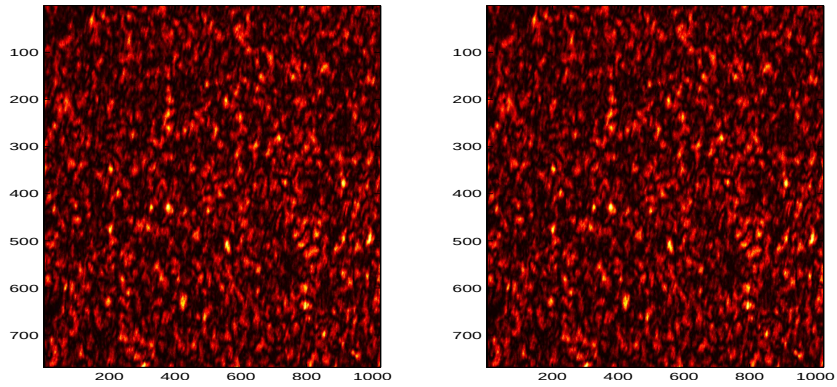


Figure 6.6: *Two speckle patterns resulting from the same challenge.*

A typical PUF-based key generation protocol (see e.g. Tuyls and Batina [78] or Škorić et al. [70]) involves an enrollment measurement of the challenge-response pair (CRP) and an authentication measurement of the same CRP. These measurements (speckle patterns) correspond to the X- and Y- sequences in biometric secret generation model in Fig. 2.1. Gabor-filtering and thresholding as proposed by Pappu [52] transform each speckle pattern into a binary image.

We have investigated five optical PUFs (labeled "A", "B", "C", "D", and "E") and for each of these five PUFs we have considered two challenges (two different laser-angles labeled "0" and "1"). For each of the ten challenges we have measured 25 speckle patterns that were Gabor-transformed and thresholded. Each speckle pattern resulted therefore in one binary 64×64 image. We denote the binary image corresponding to speckle-pattern of the enrollment image by $\mathbf{X}$ and the binary image corresponding to speckle-pattern of the authentication image by $\mathbf{Y}$. Fig. 6.8 shows an example of enrollment and authentication PUF pairs.

In the rest of this chapter we find out how large the mutual information $I_\infty(\mathbf{X};\mathbf{Y})$ is for (our) optical PUFs.

6.5.2 Secret-Key Rate Estimation

We use the methods that were described in the previous sections to estimate the mutual information between enrollment and authentication measurements of optical PUFs. From Feng et al. [26] it is known that the two-point intensity correlations in a speckle pattern are translation invariant. Therefore we may conclude that an optical PUF speckle pattern can be modeled as a stationary process. Moreover, this process is also ergodic due to statistical properties of speckle patterns, viz. the spatial

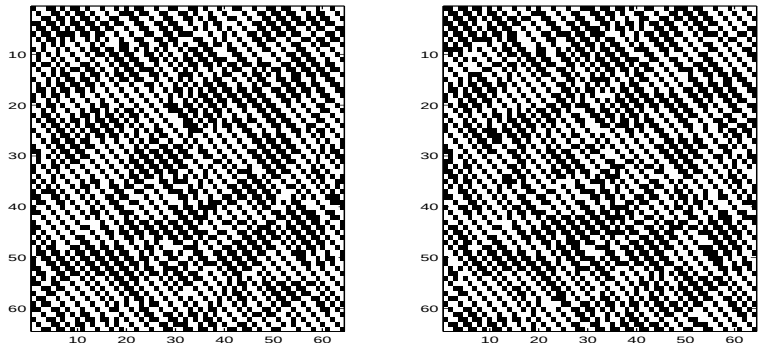


Figure 6.7: *Images* $\mathbf{X}$ *(left) and* $\mathbf{Y}$ *(right) resulting from experiment A0 with Gabor angle* $\varphi = 45^\circ$.

distribution of intensities is the same as the PUF ensemble distribution of intensities, see Goodman [31]. Therefore the methods proposed in the previous sections are applicable.

The secret keys are extracted from the pre-processed measurements of speckle patterns. Preprocessing includes Gabor-filtering (at 45°), thresholding and subsampling, like e.g. in Škorić et al. [70], and results in 64×64 binary images. An example of a pair of enrollment and authentication images $\mathbf{X}, \mathbf{Y}$ is depicted in Fig. 6.7. We observe that the enrollment and authentication images differ slightly due to the measurement noise. Moreover, we see that application of a 45° Gabor filter results in diagonal stripes. These stripes are caused by the high correlation in the direction perpendicular to the direction of the filter, see Škorić et al. [70]. Since correlation is the strongest between points that are in the vicinity of each other, and it decreases with the distance, as noted by Škorić et al. [70], it is natural to consider positions for context candidates as shown in Fig. 6.8. This template appears to have a good balance between performance and complexity. We have also considered a larger template. However, using this larger template did not lead to smaller entropy estimates.

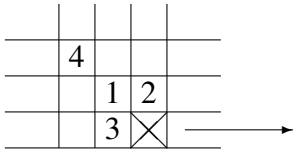


Figure 6.8: *Template showing four context symbols and their ordering. Note that the ordering is only important for class IV. The arrow indicates the direction in which the image is processed.*

We can calculate the mutual information with two alternative formulae, either by estimating it as $I_\infty(X;Y) = H_\infty(X) + H_\infty(Y) - H_\infty(XY)$ or as $I_\infty(X;Y) = H_\infty(X) - H_\infty(X|Y)$. Note that for each entropy involved in the formulae we have to compress

an image (or a pair of images) using the context weighting method.

In what follows we describe, in more details, the analysis that we have conducted.

Class IV Analysis

1. The basic approach that we have used is based on the template shown in Fig. 6.8. This template contains four context positions. Using the class IV method we have determined codeword lengths $\lambda(X)$ and $\lambda(Y)$ and the joint codeword length $\lambda(XY)$. Note that $\lambda(XY)$ results from compressing a quaternary image, since both symbols in a XY-symbol pair are binary. Using the symmetric mutual information formula, we computed a mutual information estimate for each of the ten experiments ("A0", "A1", "B0", etc.). Table 6.2(a) lists these estimates in the column labeled "bas". Table 6.1(a) shows the results for the corresponding entropy estimates $\widehat{H}(X)$, $\widehat{H}(Y)$, and $\widehat{H}(XY)$. The mutual information averaged over the ten experiments turns out to be 0.2911 bit/pixel. Fig. 6.9 shows the codeword lengths for experiment A0.

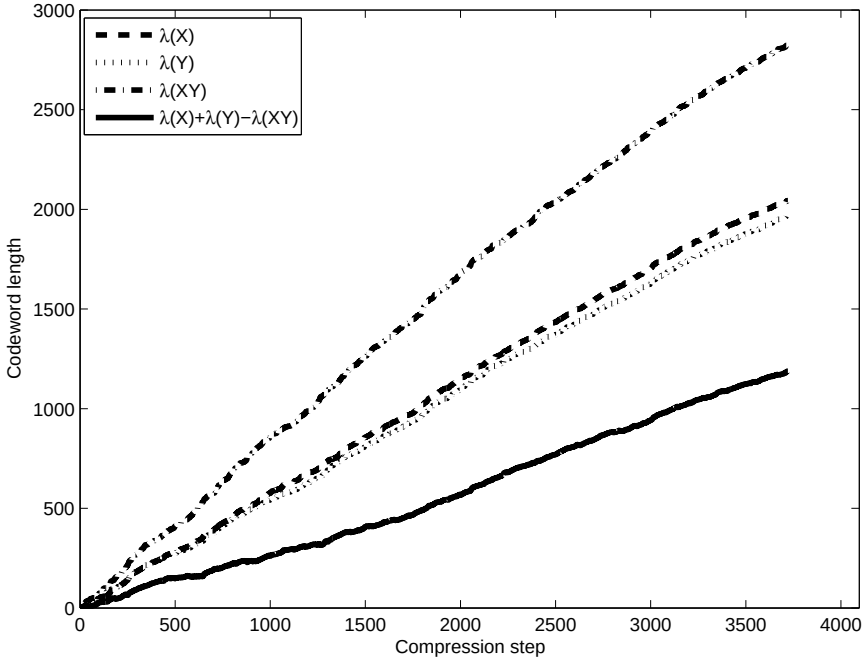


Figure 6.9: *Codeword lengths* $\lambda(X)$, $\lambda(Y)$, $\lambda(XY)$, *and* $\lambda(X)+\lambda(Y)-\lambda(XY)$ *as a function of the number of processed positions.*

2. The second approach is based on the assumption that the statistics of binarized Gabor-filtered speckle patterns are symmetric, i.e. the probability of a binary symbol x given context (c_1, c_2, c_3, c_4) is the same as the probability of $1-x$ given $(1-c_1, 1-c_2, 1-c_3, 1-c_4)$. There are good reasons for this assumption. While the statistics of the original, unfiltered speckle pattern are not symmetric under dark↔bright reversal (due to the exponential intensity distribution, see Goodman [31]), the binarization of the Gabor coefficients discards most of asymmetry-related effects.

   The symmetry assumption reduces the number of parameters that need to be handled by the CTW method and therefore it should result in more reliable estimates of the entropy and, consequently, more reliable estimates of the mutual information. Comparing the columns "sym" and "bas" in Table 6.1(a), we conclude that the symmetry assumption leads to improved (smaller) entropy estimates for all Gabor images. This implies that the symmetry assumption is reasonable. The corresponding estimates of the mutual information are listed in the column "sym" in Table 6.2(a). From this table we see that the average of the ten estimates is larger than the average found using the basic approach. More specifically, nine out of ten estimates are larger than for the basic approach.

3. In the third approach we have increased the template size from four to six context symbols, see Fig. 6.10. Just as in the previous approach we assumed symmetry of the statistics. The resulting entropy estimates (column "sym+lar") show that we do not gain from increasing the template size.

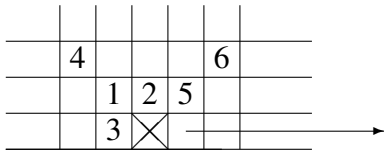


Figure 6.10: *Template showing increased number of context symbols and their ordering.*

4. In the fourth approach we have determined mutual information using the conditional formula $I(X;Y) = H(X) - H(X|Y)$. To determine the codeword length $\lambda(X|Y)$, we selected seven context symbols in total from both **X** and **Y** images. The resulting template is shown in Fig. 6.11. Again we assumed that the statistics are symmetric. This method leads to higher mutual information estimates than the estimates based on $H(X) + H(Y) - H(XY)$, see the column labeled "sym+con".

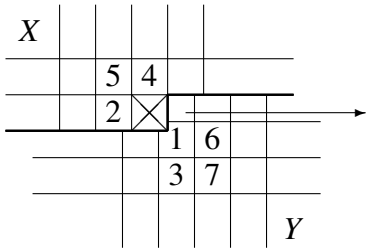


Figure 6.11: *Template showing the context symbols and their ordering for computation of* $\lambda(X|Y)$*. The current position (*$\times$*) in the* **X***-image corresponds to position* 1 *in the* **Y***-image.*

Class III Analysis

The same analysis was performed using the class III context weighting method. We used the same context positions as before, but note that the ordering is irrelevant now. Tables 6.1(b) and 6.2(b) describe the results of the class III analysis. Just as for class IV, the estimates based on the symmetry assumption are more reliable than those obtained from the basic approach. Moreover, for class III a larger template does not improve the estimates and also the conditional formula here leads to the highest mutual information estimates.

From the results of the entropy estimation in Table 6.1, we may conclude that the entropy estimates for class III are smaller and, consequently, more reliable than the estimates for class IV. Therefore we have more confidence in the mutual information estimates obtained from the class III weighting methods than from the class IV methods. The difference between corresponding estimates is always quite small, though. These small differences can be explained by noting that the template ordering was optimized to perform well for the class IV methods. Note that class III model obtained using the procedures described in Chapter 5 can be used to indicate the appropriate context ordering for class IV.

Remark: Looking at the entropy estimates in Table 6.1, we notice that for both class IV and class III models, $\widehat{H}(XY) - \widehat{H}(Y) > \widehat{H}(X|Y)$. From this we conclude that the conditional entropy estimate from $\lambda(X|Y)$ is more reliable than the estimate from $\lambda(XY) - \lambda(Y)$. As a consequence, the conditional formula for mutual information does lead to more accurate estimates than the symmetric formula.

Table 6.1: *Entropy estimates.*

(a) Class IV

	$\widehat{H}(X)$			$\widehat{H}(Y)$			$\widehat{H}(XY)$			$\widehat{H}(X\|Y)$
exp	bas	sym	sym+lar	bas	sym	sym+lar	bas	sym	sym+lar	sym
A0	.5194	.5125	.5135	.5241	.5181	.5193	.8198	.8081	.8097	.2656
A1	.5213	.5142	.5154	.5189	.5119	.5126	.7054	.6868	.6895	.1557
B0	.5289	.5216	.5229	.5284	.5217	.5230	.7791	.7609	.7635	.2141
B1	.5188	.5122	.5126	.5219	.5161	.5170	.7743	.7561	.7565	.2353
C0	.5238	.5173	.5166	.5116	.5056	.5041	.7083	.6822	.6839	.1606
C1	.5404	.5339	.5327	.5384	.5321	.5318	.8053	.7826	.7851	.2420
D0	.5305	.5253	.5246	.5273	.5228	.5236	.7345	.7171	.7190	.1846
D1	.5260	.5192	.5188	.5194	.5126	.5117	.7503	.7241	.7259	.2009
E0	.5291	.5223	.5235	.5346	.5285	.5294	.7938	.7767	.7780	.2355
E1	.5492	.5420	.5423	.5296	.5232	.5234	.7596	.7449	.7465	.2042
ave	.5287	.5221	.5223	.5254	.5193	.5196	.7630	.7439	.7458	.2098
std	.0096	.0096	.0093	.0079	.0080	.0085	.0390	.0412	.0411	.0358

(b) Class III

	$\widehat{H}(X)$			$\widehat{H}(Y)$			$\widehat{H}(XY)$			$\widehat{H}(X\|Y)$
exp	bas	sym	sym+lar	bas	sym	sym+lar	bas	sym	sym+lar	sym
A0	.5177	.5113	.5136	.5219	.5167	.5187	.8108	.8068	.8077	.2591
A1	.5196	.5133	.5157	.5163	.5103	.5116	.6965	.6823	.6857	.1488
B0	.5270	.5207	.5234	.5270	.5208	.5234	.7688	.7516	.7562	.2080
B1	.5171	.5114	.5123	.5208	.5156	.5176	.7713	.7566	.7541	.2276
C0	.5223	.5166	.5174	.5100	.5045	.5040	.6939	.6753	.6811	.1496
C1	.5395	.5332	.5331	.5365	.5310	.5312	.7997	.7826	.7857	.2368
D0	.5289	.5244	.5254	.5265	.5223	.5246	.7301	.7155	.7207	.1796
D1	.5245	.5185	.5185	.5183	.5123	.5122	.7438	.7240	.7264	.1948
E0	.5265	.5209	.5232	.5323	.5274	.5291	.7818	.7705	.7738	.2274
E1	.5478	.5416	.5434	.5270	.5219	.5233	.7463	.7407	.7427	.1952
ave	.5271	.5212	.5226	.5236	.5183	.5196	.7543	.7406	.7434	.2027
std	.0098	.0098	.0096	.0078	.0080	.0085	.0398	.0422	.0410	.0365

Table 6.2: *Mutual information estimates.*

(a) Class IV

exp	bas	sym	sym+lar	sym+con
A0	.2236	.2224	.2231	.2469
A1	.3348	.3393	.3386	.3586
B0	.2782	.2825	.2824	.3075
B1	.2664	.2722	.2731	.2769
C0	.3271	.3408	.3368	.3567
C1	.2735	.2834	.2794	.2919
D0	.3233	.3310	.3293	.3407
D1	.2951	.3078	.3046	.3183
E0	.2699	.2742	.2748	.2869
E1	.3192	.3203	.3193	.3378
ave	.2911	.2974	.2961	.3122
std	.0352	.0374	.0365	.0369

(b) Class III

exp	bas	sym	sym+lar	sym+con
A0	.2288	.2211	.2246	.2522
A1	.3394	.3414	.3416	.3644
B0	.2851	.2899	.2906	.3127
B1	.2666	.2704	.2759	.2837
C0	.3384	.3458	.3403	.3670
C1	.2763	.2816	.2786	.2964
D0	.3252	.3313	.3292	.3447
D1	.2990	.3068	.3043	.3236
E0	.2770	.2778	.2784	.2935
E1	.3285	.3228	.3240	.3463
ave	.2964	.2989	.2987	.3184
std	.0363	.0385	.0366	.0376

6.6 Conclusions

We have used context weighting methods to estimate the secret-key rate of binarized Gabor-filtered speckle patterns obtained from optical PUFs. Several alternative approaches lead to the conclusion that secret-key rates up to 0.3 bit/pixel can be realized.

Class III context weighting methods give more reliable and slightly higher estimates of the secret-key capacity than class IV methods, since class III context weighting methods are based on a richer model class than class IV methods and since the size of PUF-sequences is large enough to compensate for the model redundancy. Inspection shows that entropy estimates based on class III context weighting methods are smaller than entropy estimates based on class IV methods. In theory, our methods only converge to the entropy for asymptotically large images and if there is no bound on the context size. Note that we have definitively not reached this situation here.

In the present chapter we have focused on estimating the secret-key rate for 45° Gabor images. It is obvious that similar estimates can be found for images that result from 135° Gabor filtering. The 45° and 135° Gabor images are very weakly correlated, as was noted by Škorić et al. [70]. These images represent almost independent data, but their statistics are equivalent and therefore it is possible to compress them using the same context-tree, see [34]. The estimates obtained in this way are, in principle, more reliable than the estimates based only on 45° Gabor images.

The estimates that we obtain here can be used to evaluate the performance of existing methods for both secret-key extraction and secret-key binding. It appears that the secret-key rate estimates that were obtained in the current chapter are typically significantly larger than the secret-key rates obtained in most practical systems. As

an example, we first consider the fuzzy commitment scheme performed on optical PUFs, presented in Škorić et al. [70]. Our estimates show that secret keys of size larger than 1200 bits can, in principle, be generated. In [70] only 553 binary digits (per Gabor-filtered image) were extracted, and, moreover, these binary digits were correlated. We see that our estimate of the secret-key size is by at least a factor of 2.1 larger than the size of the extracted keys in [70], since there is correlation present in the secret-key digits extracted in [70]. Moreover, in Chapter 16 of Tuyls et al. [76] a method that extracts secret keys consisting of 95 binary digits per Gabor image was described. These 95 digits are nearly independent and uniform. We observe that the secret-key rate of this system is far below our estimate of the secret-key capacity. These examples suggest that there is still much room for improvement in designing secret-key extraction techniques.

Note that techniques like the ones that we have applied here can be used to estimate the secret-key capacity of other biometric modalities such as irises and fingerprints and to evaluate the corresponding secret-key extraction and secret-key binding methods.

As a final remark we mention that although in this chapter we considered binary sources of data, the CTW method and therefore our proposed techniques carry over to larger alphabets.

6.7 Acknowledgements

We would like to thank Philips Research for providing us with the optical PUFs data that were used in the experiments described in the current chapter.

Chapter 7

Conclusions and Future Directions

Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning (Albert Einstein).

7.1 Conclusions

In this thesis we have studied the problem of generating secret keys from noisy data and binding secret keys to noisy data. For this problem we have focused on minimizing the privacy leakage given the secret-key rate in the case when these noisy data are derived from biometrics.

In the first part of this thesis we addressed the trade-off between secret-key rate and privacy leakage in biometric secrecy systems. Four biometric settings were investigated. The first one is the standard (Ahlswede-Csiszár [3]) secret-generation setting. Two terminals observe two correlated sequences. It is the objective of the terminals to form a common secret by interchanging a public message that contains a negligible amount of information about the secret. Since we consider biometric sequences, it is crucial that the public message leaks as little as possible information on the biometric data. The fundamental trade-off was determined for this case. Also for the second setting, in which the secret is not generated but independently chosen, the fundamental balance was found. In the settings three and four zero-leakage systems were considered, where the public message contains a negligible amount of information on both the secret and biometric sequence. To achieve this, a private-key is needed, which can only be observed by the terminals. Both secret generation and chosen secret models were considered and the regions of achievable secret-key vs. private-key rate pairs were determined. For all settings two notions of privacy leakage were considered, unconditional and conditional leakage.

Next, the fuzzy commitment scheme was studied. It was introduced by Juels and Wattenberg [41]. This scheme is a particular realization of a binary biometric secrecy system with chosen secret keys where the helper data are constructed as a codeword from a selected error-correcting code, used to encode a chosen secret, masked with the biometric sequence that has been observed during enrollment. The privacy- and

secrecy-leakage properties of fuzzy commitment were investigated. The analysis was carried out for four cases of biometric data statistics, i.e. for memoryless and totally-symmetric biometric sources, memoryless and input-symmetric sources, memoryless sources, and stationary ergodic sources. The analysis showed that the fuzzy commitment scheme is only optimal for the memoryless totally-symmetric case if the scheme operates at the maximum secret-key rate. Moreover, it was demonstrated that for the memoryless and stationary ergodic cases the scheme leaks more information than necessary on both the secret and biometric data. For these two cases outer bounds on the corresponding achievable rate-leakage regions were derived. Tighter bounds on the rate-leakage regions for the two latter cases were obtained for fuzzy commitment based on systematic parity-check codes.

The next problem that was studied relates to finding the statistics of an observed biometric source sequence pair. These statistics are needed to design a code that has nearly-optimal performance. We could argue that the main question was to find the model (structure) of the source. The context-tree weighting method (Willems, Shtarkov, and Tjalkens [88]) is a sequential universal source coding method that achieves the Rissanen lower bound [60] on the redundancy for tree sources. The same authors also proposed context-tree maximizing, a two-pass version of the context-tree weighting method [89]. Later Willems and Tjalkens [91] described a method based on ratios (betas) of sequence probabilities that can be used to reduce the storage complexity of the CTW method. These betas can be applied to express a posteriori model probabilities in a recursive way (Willems, Nowbahkt-Irani, Volf [87]). We presented new results related to betas. These results provide a new view on the relation between context (tree) weighting and maximizing. The results that we have obtained can be applied to find the best model matching to an observed biometric sequence pair.

Finally, methods to estimate the maximum secret-key rates of noisy sources (e.g. biometrics and Physical Unclonable Functions (PUFs)) were proposed. These methods are again based on context weighting. PUFs and biometrics are often modeled as two-dimensional processes. Therefore we investigated the entropy of a stationary two-dimensional structure and showed that it is a limit of a series of conditional entropies, a result that was also found by Anastassiou and Sakrison [6]. We extended this result to the conditional entropy of one two-dimensional structure given another one. It was also shown that the general context-tree weighting method also approaches the source entropy in the two-dimensional stationary ergodic case. We further extended this result to the two-dimensional conditional entropy and the two-dimensional joint entropy. Based on the obtained results we performed several experiments on optical PUFs. The estimates of the maximum secret-key rates can be effectively used not only to evaluate the feasibility of a biometric modality to be a secret-key source, but also to evaluate existing algorithms for key extraction and binding.

7.2 Future Directions

Considering the field of biometric secrecy systems, we see that there are still many open questions.

In this thesis we concentrated on i.i.d. biometric sources. It is also interesting to investigate how we can use the fundamental trade-offs obtained here to analyze the models based on non-i.i.d. biometric sources.

Also the results that we have presented in this thesis are asymptotic. Therefore, a question that still remains is how the performance of biometric secrecy systems is influenced when real-life finite biometric sequences are used.

An interesting direction to consider is how multiple secret keys can be created from a single biometric in such a way that these keys can be easily canceled if compromised, or in such a way that they can be used in different databases. It is important to realize that in both cases multiple helper data sequences are needed, and we should assume that all these sequences are public. As before we require that all secrecy leakages from all publicly available data are negligible, and, moreover, we want the total privacy leakage from all publicly available data to be as small as possible. Note that compromised keys can also be assumed to be public. One way to solve the problem of multiple keys is to partition the biometric sequences in as many parts as the number of keys we need to obtain and generate/choose a key for each part. The crucial question is whether we can do better than that.

Another interesting problem relates to the fusion of biometric modalities in secrecy systems. The questions that arise here are (a) how should we distribute the privacy leakage over the biometric modalities given a fixed total secret-key rate such that the total privacy leakage is minimized, and (b) does a combination of modalities result in a smaller total privacy leakage than the sum of the privacy leakages for the individual modalities if we fix the total secret-key rate?

Observe that, in practice, biometric features are often represented by real-valued numbers. Therefore it would be interesting to determine the fundamental trade-off between secret-key and privacy-leakage rates also for continuous biometric sources. In a first study, we could focus on Gaussian sources.

Another natural next problem to look at is actual code construction for biometric secrecy systems. These codes should achieve close-to-optimal secret-key vs. privacy-leakage rate behavior. It would be nice if we could construct these codes from standard building blocks, i.e. convolutional codes (see Johannesson and Zigangirov [39]), TURBO codes (see Berrou et al. [8]), or LDPC codes (see Gallager [28]).

Bibliography

[1] *BIOMETRICS, Journal of the International Biometric Society*.

[2] "http://www.argusensure.com/page7/page7.html."

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, pp. 1121–1132, July 1993.

[4] ——, "Common randomness in information theory and cryptography - part II: CR capacity," *IEEE Transactions on Information Theory*, vol. 44, pp. 225–240, January 1998.

[5] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Transactions on Information Theory*, vol. 21, no. 6, pp. 629–637, Nov 1975.

[6] D. Anastassiou and D. J. Sakrison, "Some results regarding the entropy rate of random fields." *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 340–343, 1982.

[7] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *ACISP*, 2005, pp. 242–252.

[8] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error–correcting coding and decoding: Turbo-codes," vol. 2, May 1993, pp. 1064–1070.

[9] I. Buhan, J. Doumen, and P. Hartel, "Controlling leakage of biometric information using dithering," in *16th European Signal Processing Conference, EUSIPCO*, 2008.

[10] I. Buhan, J. Doumen, P. H. Hartel, Q. Tang, and R. N. J. Veldhuis, "Embedding renewable cryptographic keys into continuous noisy data," in *ICICS*, 2008, pp. 294–310.

[11] P. Campisi, E. Maiorana, M. Prats, and A. Neri, "Adaptive and distributed cryptography for signature biometrics protection," in *SPIE Conf. on Security, Steganography and Watermarking of Multimedia Contents IX*, vol. 6505, 2007.

[12] R. Clarke, "Human identification in information systems: Management challenges and public policy issues," *Information Technology & People*, vol. 7, no. 4, pp. 6–37, 1994.

[13] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley and Sons Inc., 1991.

[14] T. Cover, "A proof of the data compression theorem of Slepain and Wolf for ergodic sources," *IEEE Transactions on Information Theory*, vol. 22, pp. 226–228, March 1975.

[15] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1982.

[16] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, 2000.

[17] ——, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[18] G. Davida, Y. Frankel, and B. Matt, "On the relation of error correction and cryptography to an off-line biometric based identification scheme," in *In Proceedings of WCC99, Workshop on Coding and Cryptography*, 1999.

[19] ——, "On enabling secure applications through off-line biometric identification," in *In Proceedings of the IEEE 1998 Symposium on Security and Privacy*, 1998.

[20] D. Denteneer, J. Linnartz, P. Tuyls, and E. Verbitskiy, "Reliable (robust) biometric authentication with privacy protection," in *Proc. of IEEE Benelux Symp. on Inf Theory, Veldhoven, The Netherlands*, 2003.

[21] D.Maltoni, D.Maio, A.K.Jain, and S.Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer, 2003.

[22] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in cryptology - Eurocrypt 2004*, 2004.

[23] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[24] B. Dorizzi, "Biometrics at the frontiers, assessing the impact on society, technical impact of biometrics," European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), Tech. Rep., 2005.

[25] S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 2, 2007, pp. 129–132.

[26] S. Feng, C. Kane, P. A. Lee, and A. D. Stone, "Correlations and fluctuations of coherent wave transmission through disordered media," *Phys. Rev. Lett.*, vol. 61, no. 7, pp. 834–837, Aug 1988.

[27] N. Frykholm and A. Juels, "Error-tolerant password recovery," in *CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security*. New York, NY, USA: ACM, 2001, pp. 1–9.

[28] R. G. Gallager, "Low density parity check codes," *IRE Transactions on Information Theory*, vol. 8, pp. 21–28, Ja. 1962.

[29] R. Gallager, *Information Theory and Reliable Communcation*. New York: Wiley, 1968.

[30] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled physical random functions," in *In Proceedings of the 18th Annual Computer Security Conference*, December 2002. [Online]. Available: citeseer.ist.psu.edu/article/gassend02controlled.html

[31] J. W. Goodman, *Laser Speckle and Related Phenomena*. Springer-Verlag, Berlin, 1984, ch. Statistical properties of laser speckle patterns, pp. 9–75.

[32] D. Gündüz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *In Proceedings of the IEEE Information Theory Workshop, Porto, Portugal*, 2008.

[33] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[34] T. Ignatenko, G. Schrijen, B. Škorić, P. Tuyls, and F. Willems, "Estimating the secrecy rate of physical unclonable functions with the context-tree weighting method," in *Proc. of 2006 IEEE Int. Symp. Information Theory, July 9-14 2006, Seattle, WA, USA*, 2006, pp. 499–503.

[35] T. Ignatenko and F. Willems, "Privacy leakage in biometric secrecy systems," in *Proc. of Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, September 23-26 2008,Monticello, IL, USA*, 2008.

[36] A. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in a Networked Society*. Kluwer Academic Publishers, 1999.

[37] A. K. Jain, K. N, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, 2008.

[38] F. Jelinek, *Probabilistic Information Theory Discrete and Memoryless Models*. New York: McGraw-Hill Book Company, 1968.

[39] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Wiley-IEEE Press, 1999.

[40] A. Juels and M. Sudan, "A fuzzy vault scheme," in *IEEE International Symposium on Information Theory*, 2002, p. 408.

[41] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *6th ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[42] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in *AutoID*, 2005, pp. 21–26.

[43] R. Krichevsky and V.K.Trofmov, "The performance of universal encoding," *IEEE Transactions on Information Theory*, vol. 27, pp. 199–207, 1981.

[44] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proc. of Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, September 23-26 2008,Monticello, IL, USA*, 2008.

[45] J.-P. M. G. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *AVBPA*, 2003, pp. 393–402.

[46] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri, "Template protection for HMM-based on-line signature authentication," in *Comp. Vision and Pattern Recognition Works., IEEE Comp. Society Conf.*, June 2008, pp. 1–6.

[47] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, May 1993.

[48] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *IEEE Symposium on Security and Privacy*, 2001, pp. 202–213.

[49] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *ACM Conference on Computer and Communications Security*, 1999, pp. 73–82.

[50] K. Nandakumar, A. Nagar, and A. Jain, "Hardening fingerprint fuzzy vault using password," in *ICB07*, 2007, pp. 927–937.

[51] R. Nohre, "Some topics in descriptive complexity," Ph.D. dissertation, Linköping University, 1993.

[52] R. Pappu, "Physical one-way functions," Ph.D. dissertation, M.I.T., 2001.

[53] R. Pasco, "Source coding algorithms for fast data compression," Ph.D. dissertation, Department of Electrical Engineering, Stanford University, CA, 1976.

[54] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: security and privacy concerns," *Security & Privacy, IEEE*, vol. 1, no. 2, pp. 33–42, March-April 2003.

[55] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," *Information Theory Workshop, 2007. ITW '07. IEEE*, pp. 442–447, Sept. 2007.

[56] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[57] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, April 2007.

[58] R. Renner and S. Wolf, "Smooth Renyi entropy and its properties," in *IEEE International Symposium on Information Theory (ISIT)*, 2004.

[59] A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symp. Math. Stat. and Prob.*, vol. 1, 1961, pp. 547–561.

[60] J. Rissanen, "Universal coding, information, prediction, and estimation," *IEEE Transactions on Information Theory*, vol. 30, no. 4, pp. 629–636, July 1984.

[61] J. J. Rissanen, "Generalized Kraft inequality and arithmetic coding," *IBM Journal of Research and Development*, vol. 20, pp. 198–203, 1976.

[62] N. Schmid and F. Nicolo, "On empirical recognition capacity of biometric systems under global PCA and ICA encoding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 512–528, Sept. 2008.

[63] N. A. Schmid and J. A. O'Sullivan, "Performance prediction methodology for biometric systems using a large deviations approach," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 3036–3045, Oct. 2004.

[64] B. Schneier, *Applied cryptography (2nd ed.)*. New York, NY, USA: John Wiley & Sons, Inc., 1996.

[65] ——, "Inside risks: the uses and abuses of biometrics," *Communications of the ACM*, vol. 42, no. 8, p. 136, 1999.

[66] S. Shamai and A. Wyner, "A binary analog to the entropy-power inequality," *IEEE Trans. on Information Theory*, vol. 36, no. 6, pp. 1428–1430, November 1990.

[67] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[68] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 623–656, 1948.

[69] ——, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[70] B. Škorić, P. Tuyls, and W. Ophey, "Robust key extraction from physical unclonable functions," in *ACNS*, 2005, pp. 407–422.

[71] B. Škorić, "On the entropy of keys derived from laser speckle; statistical properties of Gabor-transformed speckle," *Journal of Optics A, Pure and Applied Optics*, vol. 10, no. 5, 2008.

[72] A. Smith, "Maintaining secrecy when information leakage is unavoidable," Ph.D. dissertation, MIT, 2004.

[73] Y. Sutcu, Q. Li, and N. Memon, "How to protect biometric templates," in *SPIE Conf. on Security, Steganography and Watermarking of Multimedia Contents IX*, vol. 6505, 2007.

[74] A. Teoh, A. Goh, and D. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Trans. on Pattern Analysis and Machine Intell.*, vol. 28, no. 12, pp. 1892–1901, 2006.

[75] E. Tuncel, "Capacity/storage tradeoff in high-dimensional identification systems," July 2006, pp. 1929–1933.

[76] P. Tuyls, G. Schrijen, F.Willems, and T.Ignatenko, *In Book Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer, 2007, ch. Secure Key Storage with PUFs, pp. 269–292.

[77] P. Tuyls, B. Škorić, and T. Kevenaar, Eds., *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer, 2007.

[78] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Topics in Cryptology - CT-RSA 2006*, ser. Lecture Notes in Computer Science. Springer-Verlag, 2006.

[79] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *ECCV Workshop BioAW*, 2004, pp. 158–170.

[80] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[81] S. Verdu and T. S. Han, "A general formula for channel capacity," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1147–1157, July 1994.

[82] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal of the IEEE*, vol. 55, pp. 109–115, 1926.

[83] A. Vetro, (moderator), contributors: A. K. Jain, R. Chellappa, S. C. Draper, N. Memon, and P. J. Phillips, "Forum on signal processing for biometric systems," *IEEE Signal Processing Magazine*, vol. 24, no. 6, pp. 146–152, Nov 2007.

[84] P. Volf and F. Willems, "A study of the context tree maximizing method," in *16th Symp. on Information Theory in the Benelux*, 1995, pp. 3–9.

[85] J. Wayman, A. Jain, and D. Maltoni, Eds., *Biometric systems : technology, design and performance evaluation*. London : Springer-Verlag, 2005.

[86] F. Willems, T. Kalker, J. Goseling, and J.-P. Linnartz, "On the capacity of a biometrical identification system," in *Proc. of 2003 IEEE Int. Symp. Information Theory*, 2003.

[87] F. Willems, A. Nowbakht, and P. Volf, "Maximum a posteriori probability tree models," in *4th International ITG Conference on Source and Channel Coding*, 2002, pp. 335–340.

[88] F. Willems, Y. Shtarkov, and T. Tjalkens, "The context tree weighting method: basic properties," *IEEE Transactions on Information Theory*, 1995.

[89] ——, "Context tree maximizing," in *2000 Conference on Information Sciences and Systems*, 2000.

[90] ——, "Context weighting for general finite context sources," *IEEE Trans. on Information Theory*, vol. 42, no. 5, pp. 1514–1520, 1996.

[91] F. Willems and T. Tjalkens, "Complexity reduction of the context-tree weighting method," in *18th Symp. on Information Theory in the Benelux*, F. Willems and T. Tjalkens, Eds. Veldhoven (NL): Werkgemeenschap Informatie- en Communicatietheorie, Enschede (NL), 1997, pp. 123–130.

[92] F. M. Willems, "The context-tree weighting method : extensions," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 792–798, 1998.

[93] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–I," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 769–772, Nov 1973.

[94] ——, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, January 1976.

[95] S. Yang and I. Verbauwhede, "Secure iris verification," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 2, 2007, pp. 133–136.

Glossary

List of abbreviations

BASIS	Biometric Authentication Supporting Invisible Security
BSC	Binary Symmetric Channel
CRP	Challenge-Response Pair
FAR	False Acceptance Rate
FRR	False Rejection Rate
ICA	Independent Component Analysis
ID	Identity
i.i.d.	Independent identically distributed
CTW	Context Tree Weighting
LDA	Linear Discriminant Analysis
MAP	Maximum A Posteriori Model
PCA	Principal Components Analysis
PUF	Physical Unclonable Function
XOR	exclusive or, addition modulo-2

Notations

$\log(\cdot)$	Logarithm to the base 2
$\mathcal{X}$	A set ($\mathcal{A}, \mathcal{B}, \ldots, \mathcal{Z}$ are used to denote sets)
X	A random variable
x	Realization of random variable X
X^N	A sequence of random variables of length N
x^N	Realization of a sequence of random variables X^N
x_a^b	A sequence $(x_a, x_{a+1}, \ldots, x_b)$, a, b integers, $b \geq a$
$\mathbf{x}$	A vector
$\mathbf{X}$	An image
$\mathcal{A}_\varepsilon^{(N)}(X_1, X_2, \ldots, X_K)$	A set of ε-typical N-sequences
$\mathcal{B}_\varepsilon^{(N)}(X_1, X_2, \ldots, X_K)$	A modified set of ε-typical N-sequences
$Q(\cdot)$	Source distribution
$P(\cdot)$	Arbitrary (test) distribution
$\Pr\{\cdot\}$	Probability of an event
$H(X)$	Entropy of a discrete random variable X
$I(X;Y)$	Mutual information between X and Y
$H_\infty(X)$	Entropy rate of a stationary process
$h(\cdot)$	Binary entropy function
$\oplus$	Modulo addition modulo
$\ominus$	Modulo subtraction
$\widehat{S}$	Estimate of S
$\overline{P}$	Average of P
$\lvert\mathcal{S}\rvert$	Size of $\mathcal{S}$
$\subseteq$	Subset
∂	Boundary
$a * b$	$a(1-b) + b(1-a)$
$\lceil a \rceil$	Largest integer not greater than a

Acknowledgment

First and foremost I would like to thank my thesis supervisor dr.ir. Frans Willems for introducing me to the fascinating world of Information Theory. I am grateful to him for guiding me through the Ph.D process, teaching me basic concepts, critical thinking, scientific writing, and conveying to me high standards of research. Although I have to admit that his perfectionism sometimes made my life hard, I still appreciated it a lot. Being strict at times, he is one of the kindest people I have ever known. Without his guidance and support the outcome of this work would have been impossible. I have not only enjoyed working with him, but also discussing different non-work related topics, as he is an amiable person with substantial and interesting opinions. He will always be an example of an excellent researcher and great personality for me.

I would also like to express my sincere gratitude to prof.dr. Ton Kalker for giving me an opportunity to pursue this Ph.D project, for his constant support, advice, and friendship. I also greatly appreciate his valuable critique and scientific discussions that helped improve the draft of this thesis and that always prompt me to look at scientific problems and my research from different perspectives.

I would like to express my gratitude to my promotor, prof.dr.ir. Jan Bergmans, for letting me join his group and his support especially in the final stage of my Ph.D completion.

I am also grateful to the members of the Doctorate Committee: prof.dr. P.Narayan, prof.dr.ir. J.P.M.G.Linnartz, prof.dr. M.C.Gastpar, prof.dr.ir. C.H.Slump, and prof.dr.ir. A.C.P.M.Backx - for their presence in the defence and for devoting their valuable time to reading, criticizing and improving the draft of this thesis.

Many thanks to dr. Pim Tuyls (Philips Labs/intrisic ID) who showed me the opportunity of taking up this Ph.D project. I also would like to thank him as well as dr. Boris Škorić and Geert-Jan Schrijen for fruitful discussions and collaboration that also led to the results presented in the last chapter of this thesis. I would also like to thank dr. Michiel van der Veen (Philips Labs/priv-ID) for guiding me in the first year of my Ph.D when Ton has left for the US.

I would also like to express my gratitude to our BASIS team: dr.ir. Raymond Veldhuis, dr. Ben Schouten, dr.ir. Luuk Spreeuwers, Gert Beumer, Onkar Ambekar, Stefan Bonchev, and dr.ir. Asker Bazen - for fruitful and pleasant collaboration in the course of the project. Special thanks to Raymond for leading the project. Many thanks also to the User Committee of the BASIS project - Huib Pasman, Jan Heim

van Blankenstein, Roel Croes, Max Snijder, Gert Suur, Thijs Veugen, and John de Waal - for their interest and support of this research.

I would like to thank all the colleagues of the SPS group. I owe them pleasant time and atmosphere that they created in our group. It was always fun to participate in the SPS events, especially the one with the theme "boerengolf". Needless to say, our "fake" SPS events were also a success. Special thanks to Harald, Tamara, Andrei, Emmanuel, Chin Keong, Rik, and Arijit for this. It was also nice having Pedro around during his Ph.D visit to our group. It was always enjoyable going to lunch as well as going out with my Italian friends and colleagues: Massimo, Chiara, and Luigi. In the end, these lunches would make something that I, Joep, and Harald have always been trying to achieve though with Dutch, - they would make me fluent in Italian.

It is impossible not to mention my Ph.D colleague and former roommate Joep. It was fun having all these different-topic discussions from elections to intercultural differences, competing on a number of countries and capitals that we visited and his commenting on my conference presentations. It was a great time having him around! I am grateful to him for being my friend. I also would like to devote next lines to my Ph.D colleague and consequent roommate Chiara. I appreciate a lot her constant support and willingness to help as well as lively discussions about shoes and other important matters and her being a nice squash partner, or rather a competitor. Of course, I cannot forget Massimo. I always enjoyed a lot our career and life discussions, his fitness supervision, and his choice of restaurants.

I would also like to mention my friends without whom life is dull and who implicitly and explicitly supported me during this period of my life. I would like to thank Snezhana, Dima, Marjana, Sergey, and Shura as well as Tanya, Olya, Inga, Valera, and Vitya, who are far way but nevertheless close in thoughts.

Я хочу поблагодарить своих родителей за то, что они с детства привили мне осознание важности хорошего образования, за их помощь, любовь и постоянную поддержку. Без них я бы никогда не смогла достичь того, что я достигла. Огромное спасибо Маме за то, что когда-то она разрешила мне уехать в США, без этого шага я бы никогда не очутилась в Голландии и не получила бы данную докторскую степень. Я также хочу поблагодарить Ваню за его поддержку и любовь. Я также хочу сказать большое спасибо д.Валере за его поддержку и помощь. Также спасибо Людмиле Сергеевне и д.Игорю за их интерес и поддержку.

Last but not least I would like to thank my dear husband Sergey. I am grateful to him for all his support, understanding, and love that helped me overcome periods of difficulties and that allowed me to share with him moments of joy. I am happy that he is part of my life.

Curriculum Vitae

Tanya Ignatenko was born on 16th of June, 1978 in Minsk, Belarus.

In 2001 she received the M.Sc. degree (with honors) in applied mathematics from the Belarussian State University, Minsk, Belarus. She wrote a master thesis on autoregressive conditional heteroskedasticity (ARCH) models of time series and their application in econometrical analysis.

In 2002, she joined a two-year Post-Master program in Technological Design at Mathematics for Industry, Stan Akkermans Institute, at Eindhoven University of Technology, the Netherlands. In 2004, she received her PDEng (Professional Doctorate of Engineering) degree. Her final project focused on the evaluation of reliable (robust) biometric authentication schemes with privacy protection and was carried out at the Philips Research Laboratories.

During her final project at Mathematics for Industry, she became interested in biometrics and privacy problems, and in 2004 she joined the Signal Processing Systems group at the Electrical Engineering Department of Eindhoven University of Technology, to do Ph.D research on the topic of privacy and secrecy aspects of biometric systems, which is reported in this thesis.

Tanya Ignatenko is a member of the Institute of Electrical and Electronics Engineers (IEEE). Her research interests include secure private biometrics, information theoretical secret sharing, multiuser information theory, and source coding.