A communication-theoretical view on secret extraction

Linnartz, J.P.M.G.; Skoric, B.; Tuyls, P.T.

Published in:
Security with noisy data: on private biometrics, secure key storage and anti-counterfeiting

DOI:
10.1007/978-1-84628-984-2_4

Published: 01/01/2007

Document Version
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

• A submitted manuscript is the author's version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

Citation for published version (APA):
Linnartz, J. P. M. G., Skoric, B., & Tuyls, P. T. (2007). A communication-theoretical view on secret extraction. In P. Tuyls, B. Skoric, & T. Kevenaar (Eds.), Security with noisy data: on private biometrics, secure key storage and anti-counterfeiting (pp. 57-78). Berlin: Springer. DOI: 10.1007/978-1-84628-984-2_4

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 25. Oct. 2018
For example, suppose that \( \alpha^G = a_1, a_2, \ldots, a_{14} \), but \( a_{15} \not\in A \) and \( a_{15} \in A' \) (\( A' \) comprises "Animal House," "Anna Karenina," "Bonnie and Clyde," "Casablanca," etc.). In this case, the answers are misaligned. In fact, \( x' \) and \( x \) may differ in every single position!

For this example of KBA via lists, a more suitable metric of error is set difference (i.e., \( |A \setminus A'| \)). Viewed another way, we would like a fuzzy-commitment system that is permutation invariant. Juels and Sudan [159, 160] proposed a system (called a "fuzzy vault") that has this property. Subsequent work by Dodis et al., treated in Chapters 5 and 6 of this book, proposes more general and efficient constructions considering another natural metric called edit distance. Chapter 6, in particular, investigates extension into the realm of dynamic adversarial models, in which the adversary is presumed to have more power than the ability simply to compromise \( y \).

Although researchers have offered some initial steps, rigorous matching of fuzzy commitment and similar constructions to real-world systems largely remains a rich, open area of research.

4

A Communication-Theoretical View on Secret Extraction

Jean-Paul Linnartz, Boris Skorić, and Pim Tuyls

4.1 Introduction

The recent achievements in enhanced throughput, efficiency, and reliability of wireless communication systems can largely be attributed to the availability of a versatile mathematical framework for the behavior and performance of digital transmission schemes. The key foundation was Shannon's 1948 paper [251] that introduced the notion of capacity. The term capacity is defined as the maximum achievable rate of information exchange, where the maximization is conducted over all possible choices of transmission and detection techniques. The existence of a fundamental limit has acted as an irresistible target for ambitious engineers. However, it was only until the 1990s that the signal processing capabilities allowed a true exploitation of these insights and the throughput of practical systems closely reached the capacity limits. Another important condition was met earlier: the availability of sufficiently realistic statistical models for signals, the noise, and the channel.

The research area of biometrics is presumably less mature in this respect, but strong progress is being made into the statistical modeling of biometric measurements and of sensor imperfections. Most importantly, the notion of a distance between two biometric measurements appears to exist, where a larger distance indicates a lesser likelihood of a statistical deviation. A further refinement is that errors in measurements can be modeled with well-behaved joint probability functions. Anticipating the further sophistication and verification of such models, this chapter proposes a framework that models the capacity and performance of such systems, initially assuming generic probabilistic models for biometric sources and sensor aberrations.

We argue that the maximum information rate of the biometric measurement channel can be related directly to the identification capacity of the biometric system. The statistical behavior of the biometrics as well as the variability between different (imperfect) measurements are assumed to be known in the form of a statistical model. This reveals a commonality between
communication systems and biometric systems that can be covered by a variation on Shannon’s theory.

In communications, reliable transfer of data can be separated from security functions such as encryption for confidentiality. The usual approach is to start with source coding to compress the input data into an efficient representation, followed by encryption. Third, redundancy is added in the form of channel coding to allow for error correction. In this regard, the biometric system is different. Biometric signals cannot be compressed, encrypted, protected by error correction, or in any other form be pre-conditioned before being offered to a sensor. Nonetheless, one needs to involve non-linear operations during the detection, for instance to prevent impersonation and leakage of confidential personal information. The second part of this chapter shows that security operations can be performed to shield important information from untrusted parties without significantly affecting the user capacity or security of the system.

4.2 Preliminaries

We distinguish between identification and verification. Identification estimates which person is present by searching for a match in a database of reference data for many persons. The decoder a priori does not know whether he sees “Peggy” or “Petra.” The outcome of the identification is either the (most likely) identity of the person present, or an error; that is, the decoder cannot establish who the person is with reasonable accuracy.

When assessing the user capacity of an identification system, we are interested in knowing how many individuals can be identified reliably by a biometrical identification system—i.e., how this is a function of the amount of observed data and the quality of the observations.

On the other hand, verification attempts to establish whether the prover (i.e., the person who is undergoing the verification test) truly is Peggy, which she claims to be. The prover provides not only biometric data but also a message in which she claims to be Peggy. In security language, the decoder is called the verifier and is named Victor. He is assumed to have some a priori knowledge about Peggy—for instance, in the form of certified reference data—but at the start of the protocol he is not yet sure whether Peggy is present or another person performing an impersonation attack. The outcome of the verification is binary: either “the prover is Peggy” or “the prover is not Peggy.”

In identification, the verifier must have access to a database of reference data from all individuals. In verification, this is not necessary and, typically, the reference data of only Peggy suffices. An identification algorithm can, at least in theory, be modified into a verification algorithm by grouping the set of all outputs except “the person is Peggy” into the single outcome “the person is not Peggy.” However, in general, the optimization and decision regions are usually chosen differently for identification and verification. Identification systems make the most likely choice, whereas verification systems are designed around false-positive and false-negative probabilities.

Private verification, which we will address from Section 4.8 onwards, is a special form of verification in which certain security requirements are also met. In particular, the outcome of private verification can be that the person not only shows biometrics that fit with Peggy, but also that she knows a secret that only Peggy is supposed to know. After the private verification session, Victor preferably doesn’t know what the secret is, although Victor can be convinced that the prover knows Peggy’s secret.

4.3 Model: Biometrics as Random Codewords

Biometrical systems in general involve two phases. In an enrollment phase all individuals are observed, and for each individual $p \in \{1, \ldots, M\}$, a record $Y(p)$ is added to a database. This record is called “reference data,” “enrollment data,” or “template” and contains $L$ symbols from the alphabet $\mathcal{Y}$. The enrollment data is a noisy version of the biometrical data $X(p) \in \mathcal{X}$ corresponding to the individual $p$. The set of enrollment data for all users is denoted as the entire $L \times M$ matrix $Y = (Y(1), Y(2), \ldots, Y(M))$.

In the operational phase, an unknown individual is observed again. The resulting identification data $Z$, another noisy version of the biometrical data $X$ of the unknown individual, is compared to (all or a subset of) the enrollment data in the database and the system has to come up with an estimate of the individual. This model is depicted in Fig. 4.1. An essential fact in this procedure is that both in the enrollment phase and in the operational phase, noisy versions of the biometrical data are obtained. The precise biometrical data $X(p)$ remain unknown.

$$x(1) \rightarrow P_x(g|x) \rightarrow y(1)$$
$$x(2) \rightarrow P_x(g|x) \rightarrow y(2)$$
$$\vdots$$
$$x(M) \rightarrow P_x(g|x) \rightarrow y(M)$$

**Fig. 4.1.** Model of a biometrical identification system. Each biometric measurement is represented as a noisy channel.
We use capital notation $X$, $Y$, and $Z$ for random variables and boldface to denote vectors in this section of dimension $L$. Moreover, $x$, $y$, and $z$ denote realizations or the random variables. Each individual has a biometrical data sequence $x = (x_1, x_2, \ldots, x_L)$ with components $x_i \in X$ for $i = 1, \ldots, L$. The sequence $x(p)$ is the sequence for person $p$.

For the development of the theory, preferably we assume that the components of each sequence are independent and identically distributed (IID) and that the biometric source can generate arbitrarily long sequences ($L \to \infty$). In practice, most physical or biological parameters show correlation, but often a set of biometric measurements can be transformed into a sequence of IID random variables. Communication engineers usually consider data to arrive sequentially, and usually speak of a "memoryless source" if $X$ is IID and of a "memoryless time-invariant channel" if for a memoryless source $Y$ (resp. $Z$) is also IID.

The measured output sequence $Z$ is used by a decoder. In identification, the decoder has access to all $M$ enrollment sequences stored in the database $Y$. The decoder produces an estimate $\hat{p}$ of the index of the unknown individual, $\hat{p} = \text{Dec}(z, y)$. An erasure $\perp$ is also a valid decoder output. Hence, $\hat{p} \in \{1, 2, \ldots, M\}$. Two relevant system parameters are the maximal error probability $P_{\text{max}}$ and the rate $R$:

$$P_{\text{max}} = \max_{1 \leq p \leq M} \left[ P[\hat{p} \neq p | P = p] \right] \text{ and } R = \frac{1}{L} \log_2 M. \quad (4.1)$$

For an ideal binary ($X = \{0, 1\}$) biometric system, we have $M = 2^L$, so $R = 1$. The Identification Capacity, to be defined later, describes asymptotic system properties that theoretically apply only for the case of infinitely long sequences $L \to \infty$. In fact, we will argue that there exists a rate $C_{\text{id}}$ such that $P_{\text{max}}$ is arbitrarily small for rates below capacity ($R < C_{\text{id}}$) and that $P_{\text{max}}$ necessarily tends to unity for rates above $C_{\text{id}}$. This $C_{\text{id}}$ will be called the identification capacity.

**Source and Channel Model**

We will denote the probabilities on $X$ as the source model. We define the "enrollment channel" as the probability of $Y(p)$ conditioned on the biometric $X(p)$. Similarly, we define the operational (or identification) channel as the probability of $Z(p)$ conditioned on $X(p)$.

In communication systems, the channel is mostly modeled as a statistical operation that is independent of the source. In our generic biometric framework, that is not necessarily the case, although our examples assume this.
We use the identity $I(A;B) = H(A) + H(B) - H(A,B)$. The entropies $H(Y), H(Z)$, and $H(Y,Z)$ are computed from the probability of the "true" biometric $X$ and the transition properties over the enrollment and identification channel, where

$$
P(Y) = y = \prod_{j=1}^{L} Q(x_j) P_r(y_j|x_j),
$$

$$
P(Z) = z = \prod_{j=1}^{L} Q(x_j) P_r(z_j|x_j),
$$

$$
P(Y, z) = \prod_{j=1}^{L} Q(x_j) P_r(y_j|x_j) P_r(z_j|x_j).
$$

Note that none of these probabilities depend on $p$.

For an IID (memoryless) source, $H(X) = \sum_{i=1}^{L} H(x_i) = L H(x_i)$. Similarly, the entropies of $Y$ and $Z$ can be calculated componentwise.

### 4.5 Proof Outline for Theorem 4.1

As in communication theory, the proof of the capacity theorem consists of a part that there exist rates that achieve capacity and a part that proves the non-existence of rates above $C_{ID}$ with a low average error rate.

Another important step is the random coding argument [66]. This is the observation that we can prove that the average over all randomly chosen sequences achieves an error rate that vanishes. In the development of a theoretical framework for communication systems, this was an innovative step that laid the foundation for several proofs. Here, Shannon's theory apparently fits biometrics naturally, whereas for communication systems, it was a creative, initially believed assumption to support the derivation of bounds. As first exploited in [292], random coding is a very natural and appropriate model for biometric systems, where the source model is one of randomly generated sequences. In communication systems, an engineer can choose an optimum code sequence for every potential message to be transmitted. Shannon postulated that if the engineer just picks random sequences to represent messages on average, he achieves capacity, so there must be codes that do at least as good. Note that the generation of the IID biometrical data yields the randomness that makes it all work. We get the random code $[y(1), y(2), \ldots, y(M)]$ by the very nature of biometrics.

---

1 Yet, the distribution and statistical dependence of biometrics can be questioned.

### 4.5.1 Achievability

In this subsection, we prove that for all $\delta \geq 0$, the rate $R_{ID} \geq I[X, Y] - \delta$ can be achieved.

To prove that there are rates that achieve low error rates, we postulate a decoder that is based on typical sequences for $Y, Z$ and $Y, Z$ jointly. Typical sets are explained in more detail in textbooks such as [66]. The core idea is that a random sequence is with probability 1 a typical sequence. This implies that any typical sequence has a probability that is close to $2^{-L(X)}, 2^{-L(Y)}, 2^{-L(Y,Z)}$, respectively. More precisely, the jointly typical set $A_\epsilon$ is defined as the collection of sequences $(Y, Z)$ such that $P_{Y, Z}(y, z) \leq 2^{-L(X) - \epsilon}$. And similarly for sequences of $Y$ and $Z$ separately. An important property is that a sequence $Y, Z$ chosen randomly according to the underlying biometric statistical model is a typical sequence with probability higher than $1 - \epsilon$.

For our proof, we postulate a decoder that generates as its output the unique index $\hat{y}$ satisfying

$$
y(\hat{y}), x \in A_\epsilon.
$$

(4.8)

If no unique $\hat{y}$ exists, the decoder outputs an erasure.

Two kinds of error can occur. An error of the first kind (cf. a false rejection if we had addressed a verification system) occurs when the enrollment sequence of the tested individual $p$ is not typical with his identification sequence resulting from the test. We define the event that the enrollment $(Y(p)$ and an observed identification $Z$ are jointly typical as

$$
E_0 = \{(Y(p), Z) \in A_\epsilon\}.
$$

Without loss of generality we denote the test sequence as $p = 1$. Thus, a false rejection corresponds to $E_1$. An error of the second kind (cf. a false acceptance) occurs if the enrollment sequence of some other individual $p' \neq p$ is typical with $p'$'s identification sequence. This corresponds to $E_2, E_3, E_4, E_5$.

For errors of the first kind, the probability $P[Y(p), Z(p) \notin A_\epsilon] \leq \epsilon$ for all large enough $L$. For errors of the second kind, we calculate the probability that two randomly chosen sequences $Y$ and $Z$ match, where the sequences are not necessarily taken from a specific realization of a population but produced by a statistical process that randomly generates sequences over $\mathcal{X}$. Let $x$ be the output of the identification channel that is caused by $X(p)$. For all $y \in \mathcal{Y}^L$ and $z \in \mathcal{Z}^L$ and $p' \neq p$, we have

$$
P(Y(p') = y, Z(p) = z) = \prod_{l=1}^{L} Q(x_l) P_r(y_l|x_l) \sum_{l \in \mathcal{X}^L} Q(l) P_r(z_l|x_l).
$$
Using the properties of typical sequences (e.g., Theorem 8.6.1 in [66]), the false-acceptance probability of two randomly chosen sequences satisfies

$$P_p(Y(p'), Z(p)) \in A_\varepsilon \leq 2^{-H(Y(p)|Z(p))+1}.$$  

An error of any kind occurs with probability $P[e] = \mathbb{P}[e = 1] = \mathbb{P}[E_1 \cup E_2 \cup \cdots \cup E_M]$. By applying the union bound, one obtains

$$P[e] \leq \mathbb{P}[E_1] + \sum_{p=2}^{M} \mathbb{P}[E_p].$$

Hence, for sufficiently large $L$, we have

$$P[e] \leq \varepsilon + \sum_{i=1}^{\infty} 2^{-H(Y(p)|Z(p))+1}L \leq \varepsilon + 2^{L-2[H(Y(p)|Z(p))-L\|]} \leq 2\varepsilon.$$  

Thus, $P[\hat{P} \neq P|P = p]$ can be made smaller than $2\varepsilon$ by increasing $L$.

### 4.5.2 Converse

In this subsection we show that there exists no identification scheme that can identify more than $2^{H(Y; Z)}$ persons with negligible error probability:

$$P[\hat{P} \neq P] \leq \max_{p=1,..,M} P[\hat{P} \neq P|P = p],$$  

which we require to remain arbitrarily small. Applying Fano’s inequality, we get for the entropy in $P$, knowing the database $Y$ and observation $Z$,

$$H(P|Y, Z) \leq 1 + P[\hat{P} \neq P] \log_2 M.$$  

Note that we did not assume any a priori distribution over the individuals that are to be identified. Let us see what happens if we assume that $P$ is uniformly distributed over $\{1, 2, \ldots, M\}$. Using inequality (4.11), we obtain

$$\log_2 M = H(P) = H(P|Y) = H(P|Y) - H(P|Z, P, Y) + H(P|Z, Y) \leq I(P; Z|Y) + 1 + P[\hat{P} \neq P] \log_2 M.$$  

Another useful inequality is obtained as follows:

$$I(P; Z|Y) = H(Z|Y) - H(Z|P, Y) \leq H(Z) - H(Z|P, Y) = H(Z) - H(Z|P) + H(Y|P) = I(Z(p); Y(p)) = LI(Y; Z).$$  

Combining (4.13) and (4.14), we get

$$\log_2 M \leq I(Y; Z) + 1 + P[\hat{P} \neq P] \log_2 M$$

or

$$\log_2 M \leq \frac{I(Y; Z) + 1/L}{1 - P[\hat{P} \neq P]}.$$  

When we take the limit $L \to \infty$, we obtain $R_{id} \leq I(Y; Z)(1 + \delta)$. Now as we let $\delta \to 0$ (where $\delta$ is defined in Def. 4.1), which implies $P[\hat{P} \neq P] \to 0$, we have that $R_{id} \leq I(Y; Z)$. By combining with the first part of the proof, it follows that the capacity $C_{id} = I(Y; Z)$.

### 4.5.3 Examples: Bernoulli Variables

Let us consider a hypothetical biometric that gives balanced IID binary values. Let the biometric $X$ form a Bernoulli random variable $\{X = \{0, 1\}\}$ with parameter $p = P[X = 1] = 0.5$. Moreover, let

$$Y = X \oplus N_e, \quad Z = X \oplus N_i,$$  

with Bernoulli noise variables $N_e$ and $N_i$ having parameters $d_e$ and $d_i$, respectively. The addition $\oplus$ is modulo 2. Then

$$P[Y \neq Z] = d = d_e(1 - d_i) + (1 - d_e)d_i.$$  

The mutual information per symbol is given by

$$I(Y; Z) = H(Z) - H(Z|Y).$$  

which yields $I(Y; Z) = \log M - H(Z) - H(Z|Y)$. Note that in this example, we can conceptually think of the enrollment process as error-free and the identification process as distorted by the concatenation of the original channels $X \to Y$ and $X \to Z$, yielding a binary symmetric channel with probability of error $d$.

### 4.5.4 Examples: IID Gaussian Variables

As a second example, we consider the case that $X$ is IID Gaussian, zero mean, with variance $\sigma^2_x$. Moreover, for every dimension $l$, let

$$Y_i = X_i + N_e, \quad Z_i = X_i + N_i,$$  

with zero-mean Gaussian noise variables $N_e$ and $N_i$ having variances $\sigma^2_x$ and $\sigma^2_{N_e}$, respectively. The covariance matrix $\Sigma_{XZ}$ is given by
amplified and the outcome will bear no resemblance to the expected outcome. 

channel the outcome. Minor changes at the input of a cryptographic function are

equivalent. This illustrates how the enrollment output sequences \( Y(1), Y(2) \) 

value close to a quantization threshold, minor amounts of noise can change 

the database. This calculation is of modest complexity. Particularly, if

the observation \( x \) is fixed (i.e., not a function of \( p \)). For the decoder, the relevant probability can be written as

\[
P[Z(p) = x|Y(p) = y(p)] = \prod_{i=1}^{L} \sum_{x_i} Q(x_i) P_i(x_i|p(z_i|x)) P(z_i|x). \tag{4.21}
\]

Here the sum is over all possible \( x \), which is of modest complexity. Particularly If \( X \) contains IID elements and if the channel models \( P_i(x_i|x) \) and \( P(z_i|x) \) are known (e.g., from Sections 4.5.3 and 4.5.4), the complexity of this calculation is small. Yet this decision variable has to be calculated for all \( p \) in the database. This illustrates how the enrollment output sequences \( Y(1), Y(2), \ldots \) 

\( (e.g., from Sections 4.5.3 and 4.5.4). \) The complexity of this calculation is small. Yet this decision variable has to be calculated for all \( p \) in the database. This illustrates how the enrollment output sequences \( Y(1), Y(2), \ldots \)

channel \( \{ Z, P(z|x), Y \} \). These codewords are observed via a memoryless channel \( \{ Z, P(z|x), Y \} \).

Note that decoding according to our achievability proof involves an exhaustive search procedure. It is not known how an identification scheme can be modified in such a way that the decoding complexity is decreased. However, the helper data proposed in the second half of this chapter has the side effect of accelerating the recognition process.

4.7 Private Templates

Identification inherently requires that a verifier searches for matches with the measured \( Z \) in a database \( Y \) that contains data about the entire population. This introduces the security and privacy threat that the verifier who steals biometric templates from some (or even all) persons in the database can perform impersonation attacks. This threat was recognized by several researchers [33, 186, 277]. When a private verification system is used on a large scale, the reference database has to be made available to many different verifiers, who, in general, cannot be trusted. Matsumoto et al. [189] showed that information stolen from a database can be used to construct artificial biometrics to impersonate people. Creation of artificial biometrics is possible even if only part of the template is available. Hill [146] showed that if only minuscule templates of a fingerprint are available, it is still possible to successfully construct artificial biometrics that pass private verification.

To develop an insight in the security aspects of biometrics, we distinguish between verification and private verification. In a typical verification situation, access to the reference template allows an malicious Victor to artificially construct measurement data that will pass the verification test, even if Peggy has never exposed herself to a biometric measurement after the enrollment.

In private verification, the reference data should not leak relevant information to allow Victor to (effectively) construct valid measurement data. Such protection is common practice for storage of computer passwords. When a computer verifies a password, it does not compare the password \( Y \) typed by the user with a stored reference copy. Instead, the password is processed by a cryptographic one-way function \( F \) and the outcome is compared against a locally stored reference string \( F(Y) \). So \( Y \) is only temporarily available on the system hardware, and no stored data allow calculation of \( Y \). This prevents attacks from the inside by stealing unencrypted or decryptable secrets.

The main difference between password checking and biometric private verification is that during biometric measurements, it is unavoidable that noise or other aberrations occur. Noisy measurement data are quantized into discrete values before these can be processed by any cryptographic function. Due to external noise, the outcome of the quantization may differ from experiment to experiment. In particular, if one of Peggy’s biometric parameters has a value close to a quantization threshold, minor amounts of noise can change the outcome. Minor changes at the input of a cryptographic function are amplified and the outcome will bear no resemblance to the expected outcome.
This property, commonly referred to as "confusion" and "diffusion," makes it less trivial to use biometric data as input to a cryptographic function. The notion of near matches or distance between enrollment and operational measurements vanishes after encryption or any other cryptographically strong operation. Hence, the comparison of measured data with reference data cannot be executed in the encrypted domain without prior precautions to contain the effect of noise.

Furthermore, with increasing $M$ and $L$, the probability that a "randomly created" natural biometric vector lies near a decision boundary goes to unity for any a priori defined digitization scheme. Error correction coding does not help, because the biometrics are generated randomly; thus, they do not naturally lie centered inside decision regions, as codewords would do.

A common misperception is that encryption of $Y$ and decryption prior to the verification solve this security threat. This would not prevent a dishonest Victor from stealing the decrypted template $Y$, because Victor knows the decryption key.

The next subsection presents an algorithm to resolve these threats. It is based on a "helper data scheme" that resembles "fuzzy extractors," covered in Chapter 5.

In addition to private verification, a further application can be the generation of a secret key. We illustrate this by the example of access to a database of highly confidential encrypted documents to which only a set of specific users is allowed access. The retrieval system authenticates humans and retrieves a decryption key from their biometric parameters. This system must be protected against a dishonest software programmer Mallory who has access to the biometric reference data from all users. If Mallory downloads the complete reference data file, all encrypted documents, and possibly reads all the software code of the system, she should not be able to decrypt any document.

Meanwhile, it is important to realize that protection of the reference data stored in a database is not a complete solution to the above-mentioned threats. After having had an opportunity to measure operational biometric data, a dishonest Victor uses those measurement data. This can happen without anyone noticing it: Victor grabs the fingerprint image left behind on a sensor. This corresponds to grabbing all keystrokes, including the plain passwords, typed by a user. We do not address this last attack in this chapter.

4.7.1 The Helper Data Architecture

We observe that a biometric private verification system does not need to store the original biometric templates. Examples of systems that use other architectures and achieve protection of templates are private biometrics [81], fuzzy commitment [161], conatable biometrics [231], fuzzy vault [159], quantizing secret extraction [182], and secret extraction from significant components [283]. The systems proposed in [81, 159, 161, 182, 283] are all based on architectures that use helper data.

In order to combine private biometric verification with cryptographic techniques, we derive helper data during the enrollment phase. The helper data $W$ guarantees that a unique string $S$ can be derived from the biometrics of an individual during the private verification as well as during the enrollment phase. The helper data serves two purposes. On the one hand, it is used to reduce the effects of noise in the biometric measurements. More precisely, it ensures that with high probability, the measured noisy biometric always falls within the same decision region taken by the detector. As a result, exactly the same string $S$ is always extracted from the same $p$. Since the string $S$ is not affected by noise anymore, it can be used as input to cryptographic primitives without causing avalanches of errors. Thus, $S$ can be handled in the same secure manner as computer passwords.

However, since random biometrics are usually not uniformly distributed, the extracted string $S$ is not guaranteed to be uniform. Therefore, another part of the helper data is used to extract the randomness of the biometric measurements. Usually, this is done by letting the helper data be a pointer to a randomly chosen function from a universal set of hash functions (see Chapter 5). The left-over hash lemma guarantees that the hashed string is indistinguishable from a uniformly random string. The error-correction phase is usually called information reconciliation and the randomness extraction is called the privacy amplification phase.

Private biometric verification consists of two phases: enrollment and private verification. During the enrollment phase, Peggy visits a Certification Authority (CA) where her biometrics are measured and reference data (including helper data) are generated. For on-line applications, such protected reference data can be stored in a central database (possibly even publicly accessible), or those data can be certified with a digital signature of the CA, and given to Peggy. In the latter case, it is Peggy's responsibility to (securely) give this certified reference data to Victor. Thus, the reference data consists of two parts: the cryptographic key value $V = F(S)$ against which the processed measurement data are compared, and the data $W$ which assist in achieving reliable detection.

Assuming that these data are available as $V(Peggy) = v, W(Peggy) = w$, Peggy authenticates herself as follows:

- When she claims to be Peggy, she sends her identifier message to Victor.
- Victor retrieves the helper data $w$ from an on-line trusted database. Alternatively, in an off-line application, Peggy could provide Victor with reference data $(v, w)$ certified by the CA.
- Peggy allows Victor to take a noisy measurement $s$ of her biometrics.
- Victor calculates $s' = G(w, z)$. Here, $G$ is a "shielding" function, to be discussed later.
- Optional for key establishment: Victor can extract further cryptographic keys from $s'$—for instance, to generate an access key.
• Vector calculates the cryptographic hash function \( v' = F(s') \).

• \( v' \) is compared with the reference data \( v \). If \( v' = v \), the private verification is successful.

Here, we used lowercase \( n, x, y, z, v \), and \( w \) to explicitly denote that the protocol operates on realizations of the random variables \( N \), \( X \), \( Y \), \( Z \), \( W \), and \( V \), respectively. The length of these vectors is denoted as \( L_N \), \( L_X \), \( L_Y \), \( L_Z \), and \( L_V \), respectively. Often, the same type of measurement is done for enrollment and verification; thus, \( L_Y = L_Z \) and \( Y = Z \).

Further, \( S \) and \( F(S) \) are discrete-valued (typically binary) vectors of length \( L_Y \) and \( L_Z \), respectively. Note that here we make an exact match. Checking for imperfect matches would not make sense because of the cryptographic operation \( F \). Measurement imperfections (noise) are eliminated by the use of \( W \) and the so-called \( \delta \)-contracting property of the shielding function \( G \).

4.7.2 Definitions

During enrollment, \( Y(\text{Peggy}) = y \) is measured. Some secret \( S(\text{Peggy}) = s \in S^{1+} \) is determined, and the corresponding \( V = F(s) \in Y^{1+} \) is computed. In later sections, we will address whether \( s \) can be chosen arbitrarily \( (s \in S^{1+}) \) by the CA, or that the enrollment algorithm explicitly outputs one specific value of \( s \) based on \( y \). Also, a value for \( W(\text{Peggy}) = w \) is calculated such that not only \( G(w, y) = s \) but also during private verification \( G(w, z) = s \) for \( z \approx x \), more precisely for distances \( d(z, x) \leq \delta \). We call a function that supports this property \( \delta \)-contracting.

Definition 4.2. Let \( G : W^{1+} \times Y^{1+} \rightarrow S^{1+} \) be a function and \( \delta > 0 \) be a non-negative real number. The function \( G \) is a \( \delta \)-contracting function if and only if for all \( y \in Y^{1+} \), there exists (an efficient algorithm to find) at least one vector \( w \in W^{1+} \) and one \( s \in S^{1+} \) such that \( G(w, y) = G(w, z) = s \) for all \( z \in Y^{1+} \) such that \( d(z, y) \leq \delta \).

We now argue that helper data are an essential attribute to make a secure biometrics system. We show this by contradiction namely by initially assuming that \( W \) does not depend on \( p \).

Theorem 4.2. If \( G(w, z) = f(z) \) for all \( w \), then either the largest contracting range of \( \delta \) is \( 0 \) or \( G(w, z) \) is a constant independent of \( z \).

Proof. Take \( W = w_0 \). Assume \( G \) is \( \delta \)-contracting, with \( \delta > 0 \). Choose two points \( z_1 \) and \( z_2 \) such that \( G(w_0, z_1) = s_1 \) and \( G(w_0, z_2) = s_2 \). Define a vector \( r = x_2 - x_1 \) such that \( 0 < d(0, r) < \delta \). Then \( s_1 = G(w_0, z_1) = G(w_0, x_1 + r) = G(w_0, x_1 + 2r) = \ldots = s_2 \). Thus \( G(w_0, z_2) = G(w_0, z_1) \) is constant.

Corollary. The desirable property that biometric data can be verified in the encrypted domain (in an information-theoretic sense) cannot be achieved unless person-specific data \( W \) is used. Private biometric verification that attempts to process \( Z \) without such helper data is doomed to store decryptable user templates.

Any function is \( \delta \)-contracting. If the radius \( \delta \) is properly chosen as a function of the noise power, the \( \delta \)-contracting property ensures that despite the noise, for a specific Peggy all likely measurements \( Z \) will be mapped to the same value of \( S \). This can particularly be guaranteed if \( L \rightarrow \infty \). For private verification schemes with large \( L_Y = L_Z = L \), \( d(Z, Y) \rightarrow \sigma_N^2/L \), where \( \sigma_N^2 \) is the noise power. So one needs to ensure that \( \delta \) is sufficiently larger than \( \sigma_N \).

Definition 4.3. Let \( G : W^{1+} \times Y^{1+} \rightarrow S^{1+} \) be a \( \delta \)-contracting function with \( \delta > 0 \) and let \( \epsilon > 0 \) be a non-negative real number. The function \( G \) is called \( \epsilon \)-revealing if and only if for all \( y \in Y^{1+} \), there exists (an efficient algorithm to find) a vector \( w \in W^{1+} \) such that \( |w; G(w, y)| < \epsilon \).

Hence, \( W \) conceals \( S \): it reveals only a well-defined, small amount of information about \( S \). Similarly, we require that \( F(S) \) conceals \( S \). However, we do not interpret this in the information-theoretic sense but in the complexity-theoretic sense; that is, the computational effort to obtain a reasonable estimate of \( S \) or \( F(S) \) is prohibitive, even though in the information-theoretic sense, \( F(S) \) may (uniquely) define \( S \).

The above definitions address properties of the shielding function \( G \). Efficient enrollment requires an algorithm \( \Gamma(Y) \rightarrow (W, S) \) to generate the helper data and the secret. The procedure \( \Gamma \) is a randomized procedure and only used during enrollment.

4.7.3 Example: Quantization Indexing for IID Gaussian

Let \( X, Y, Z, N_u \), and \( N \) be Gaussian variables as defined in Section 4.5.4. Moreover, \( L_Y = L_Z = L_N = L \) and \( X' = Y = Z = W = R \). The core idea is that measured data are quantized. The quantization intervals are alternatingly mapped to \( s_0 = 0 \) and \( s_1 = 1 \). The helper data \( v_1 \) acts as a bias in the biometric value to ensure detection of the correct value of \( s_1 \). This example resembles strategies known in the literature on Quantization Index Modulation (QIM) [29], which is a specific form of electronic watermarking, and on writing on dirty paper. QIM was applied to biometrics in [182].

**Enrollment in QIM**

During enrollment, \( s_1 \) is measured and the CA generates \( v_1 \) such that the value of \( y + v_1 \) is pushed to the center of the nearest quantization interval that corresponds to the correct \( s_1 \) value:

\[
v_1 = \begin{cases} 
(2n + \frac{1}{2})y - y & \text{if } s_1 = 1 \\
(2n - \frac{1}{2})y - y & \text{if } s_1 = 0, 
\end{cases}
\]

(4.22)
Communication-Theoretical View

Here, \( I(f) \) is the pdf of \( W \). Information leaks whenever \( f(w_i | S_1 = 1) \neq f(w_i) \). Since the pdf of \( X_1 \) is not flat, some values of \( w_i \) are more likely than others even within \( -q < w_i < q \). This gives an imbalance in the above a posteriori probability.

We now quantify the information leakage given our assumptions on the statistical behavior of the input signal \( X_1 \). The statistics of \( W_1 \) are determined by those of \( X_1 \) and \( S_1 \). We observe that for \( s_j = 1 \), \( w_i = (2n + 1/2)q - w_y \), so

\[
\begin{align*}
I(W_1; S_1) &= 1 - h(P_1) \leq 1 - \frac{1}{2} \log_2 \left( 2 \int_{-q}^{q} |f(w)| \, dw \right). 
\end{align*}
\]

(4.26)

Using Bayes’ rule, the symmetry properties of \( f \), and the uniformity of \( S \), we obtain

\[
\begin{align*}
I(W_1; S_1) &= \int_{-q}^{q} f(w | S_1 = 1) \log_2 f(w | S_1 = 1) \, dw - \int_{-q}^{q} f(w) \log_2 f(w) \, dw. 
\end{align*}
\]

(4.27)

Fig. 4.3 shows that quantization values as crude as \( q/\sigma_w \) are sufficient to ensure small leakage (<10^{-3}). Crude quantization steps are favorable as these allow reliable detection (i.e., a large contracting range).

4.8 Secrecy and Identification Capacity

It is natural to ask what the maximum length of the secret key that can be extracted from a biometric measurement is. The size of the secrets is expressed as the rate \( R_S \), expressed as the effective key size in bits per biometric symbol (entropy bits/symbol). The maximum achievable rate is defined accordingly by the secrecy capacity \( C_s \).

Definition 4.4 (Secrecy capacity). The secrecy capacity \( C_s \) is the maximal rate \( R_s \) such that for all \( \varepsilon > 0 \), there exist encoders and decoders that, for sufficiently large \( L_s \), achieve

\[
\begin{align*}
\mathbb{P}(S' \neq S) &\leq \varepsilon, \\
I(W; S) &\leq \varepsilon, \\
\frac{1}{L_s} I(S) &\geq (R_s - \varepsilon).
\end{align*}
\]

(4.29) (4.30) (4.31)

Here, \( f \) is the pdf of \( W \). Information leaks whenever \( f(w_i | S_1 = 1) \neq f(w_i) \). Since the pdf of \( X_1 \) is not flat, some values of \( w_i \) are more likely than others even within \( -q < w_i < q \). This gives an imbalance in the above a posteriori probability.

We now quantify the information leakage given our assumptions on the statistical behavior of the input signal \( X_1 \). The statistics of \( W_1 \) are determined by those of \( X_1 \) and \( S_1 \). We observe that for \( s_j = 1 \), \( w_i = (2n + 1/2)q - w_y \), so

\[
\begin{align*}
I(W_1; S_1) &= 1 - h(P_1) \leq 1 - \frac{1}{2} \log_2 \left( 2 \int_{-q}^{q} |f(w)| \, dw \right). 
\end{align*}
\]

(4.26)

Using Bayes’ rule, the symmetry properties of \( f \), and the uniformity of \( S \), we obtain

\[
\begin{align*}
I(W_1; S_1) &= \int_{-q}^{q} f(w | S_1 = 1) \log_2 f(w | S_1 = 1) \, dw - \int_{-q}^{q} f(w) \log_2 f(w) \, dw. 
\end{align*}
\]

(4.27)

Fig. 4.3 shows that quantization values as crude as \( q/\sigma_w \) are sufficient to ensure small leakage (<10^{-3}). Crude quantization steps are favorable as these allow reliable detection (i.e., a large contracting range).

4.8 Secrecy and Identification Capacity

It is natural to ask what the maximum length of the secret key that can be extracted from a biometric measurement is. The size of the secrets is expressed as the rate \( R_S \), expressed as the effective key size in bits per biometric symbol (entropy bits/symbol). The maximum achievable rate is defined accordingly by the secrecy capacity \( C_s \).

Definition 4.4 (Secrecy capacity). The secrecy capacity \( C_s \) is the maximal rate \( R_s \) such that for all \( \varepsilon > 0 \), there exist encoders and decoders that, for sufficiently large \( L_s \), achieve

\[
\begin{align*}
\mathbb{P}(S' \neq S) &\leq \varepsilon, \\
I(W; S) &\leq \varepsilon, \\
\frac{1}{L_s} I(S) &\geq (R_s - \varepsilon).
\end{align*}
\]

(4.29) (4.30) (4.31)
Fig. 4.3. Mutual information $I(W_i; S_i)$ as a function of the quantisation step size $q_{1/2}$.

Eq. (4.29) ensures correctness of the secret, (4.30) ensures secrecy with respect to eavesdropping of the communication line, and (4.31) guarantees high entropy in the secret. Eq. (4.31) is a stronger requirement than versatility.

If $I(W; S)$ is small and $H$ is large, an impersonation attack is based on artificial biometrics that pass an private verification. We remark that, in general, $I(V, W; X)$ is large in the strict information-theoretical sense. In the computational sense, however, it is infeasible to derive information about $S$ from $V$. Hence, from a computational point of view, $V$ does not reveal information about $X$.

The uncertainty expressed by $H(S|W) = H(S) - I(W; S)$ defines a security parameter $H$ for impersonation. It gives the number of attempts that have to be performed in order to achieve successful impersonation. In order to compute the secrecy capacity the following lemma is needed, which we present here for the sake of completeness.

**Lemma 4.1.** For continuous random variables $X$, $Y$ and $e > 0$, there exists a sequence of discretized random variables $X_d$ and $Y_d$ that converge pointwise to $X$, $Y$ (when $d \to \infty$) such that for sufficiently large $d$,

$$I(X; Y) \geq I(X_d; Y_d) \geq I(X; Y) - \epsilon. \quad (4.32)$$

With some modifications to the results from [4,194], the following theorem can be proven using Lemma 4.1.

**Theorem 4.3.** The secrecy capacity of a biometric system equals

$$C_s = I(Y(p); Z(p)). \quad (4.33)$$

**Proof.** We start with the achievable argument. The proof that $I(Y; Z)$ can be achieved if $Y$ and $Z$ are discrete variables is analogous to the proof in [4]. In order to prove achievability in the continuous case, we choose $e > 0$ and approximate the random variables $Y$ and $Z$ by discretized (quantized) versions, $Y_d$ and $Z_d$, respectively, such that $I(Y; Z) - I(Y_d, Z_d) \leq \epsilon$. (The fact that such a quantization exists follows from Lemma 4.1.) Then, taking the encoder that achieves the capacity for the discrete case $(Y_d, Z_d)$, it follows that we can achieve $I(Y_d; Z_d)$. Since this can be done for any $\epsilon > 0$, the proof follows.

The fact that $I(Y; Z)$ is an upper bound for $C_s$ for discrete random variables follows from the Fano inequality and some basic entropy inequalities. For the continuous case, this follows again by an approximation argument using Lemma 4.1.

It was proven in [270] that there exists a biometric private verification algorithm that achieves both the secrecy capacity $C_s$ and the identification capacity $C_{id}$ at the same time.

**Identification Capacity, Revisited**

We have derived the secrecy capacity for secure private verification systems with helper data. Yet, the identification capacity was up to this section only established for systems without helper data. In this subsection, we show that the identification capacity is equal to the channel capacity of the biometric sensor if helper data and shielding functions are applied.

**Definition 4.5 (Identification capacity).** The identification capacity $C_{id}$ is the maximal rate $R_{id}$ such that for every $\epsilon > 0$, for sufficiently large $L$, there exists an identification strategy that achieves

$$\Pr[P \neq p] \leq \epsilon \quad \text{and} \quad \frac{1}{L} \log M \geq R_{id} - \epsilon. \quad (4.34)$$

where the average is over all individuals and over all random realizations of all biometrics.

A private verification scheme with helper data can be used for identification: For a biometric measurement $y$, the verifier performs an exhaustive search over the entire population of candidates $p' \in \{1, \ldots, M\}$ by retrieving from a database the values $w$ and $v$ for each candidate and checking if $F(G(w, y)) = v$. In practice, such a system can be computationally more efficient than a straightforward identification scheme mentioned in the first part of this chapter: It does not need to consider near matches, but only exact matches. The exact
matches are performed in the binary domain and therefore are very efficient. The above definition addresses such a system.

For systems without enrollment noise, it can be shown [218, 292] that if the \( \delta \)-contracting range is chosen such that it matches the sphere that verification noise creates around \( X \), the biometric identification systems, including template-protecting systems, satisfy \( C_{id} = I(X; Y) \). This result can be interpreted merely as a statement that helper data do not negatively influence the performance.

\[4.9\] Relation with Fuzzy Extractors

In this book, several chapters deal with key extraction from noisy data, in general, and biometrics, in particular. A well-known technique that is treated in Chapter 5 is called Fuzzy Extractors. Here, we prove that the helper data technique developed in this chapter is equivalent to that of a fuzzy extractor. We need some details of the construction of a fuzzy extractor. For those details, we refer to Chapter 5. We define

\[ \text{Gen}(y) = \Gamma(y) \quad \text{and} \quad \text{Rep}(w, y) = G(w, x). \]

With this definition, the following two theorems have been proven [280].

**Theorem 4.4.** Suppose that there exists a \( (Y, m, l, \delta, \epsilon \leq 1/4) \) fuzzy extractor with generation and reproduction procedures \( \text{Gen} \) and \( \text{Rep} \) constructed by using a secure sketch and with \( K \) uniformly distributed over \( \{0, 1\}^l \) statistically independent from \( (X, Y) \). Then, there exists a \( \delta \)-contracting, \( \eta \)-revealing function \( G \), with counterpart \( \Gamma \), with

\[ \eta = h(2\epsilon) + 2\epsilon(\text{Gen}(y)) + |K| + h(\epsilon) + \epsilon|K|. \]

This theorem proves that a fuzzy extractor implies a helper data algorithm that is \( \eta \)-revealing. Furthermore, we have the following converse.

**Theorem 4.5.** Let \( G \) be a \( \delta \)-contracting, \( \epsilon \)-revealing function creating a uniformly random key \( K \) on \( \{0, 1\}^l \) wrt to a probability distribution \( P_Y \) with \( H_{\infty}(X) > m \). Then there exists a \( (X, m, l, \delta, \sqrt{\epsilon}) \) fuzzy extractor.

For the proofs of Theorems 4.4. and 4.5. we refer the reader to [280].

Theorem 4.5 explains that a helper data algorithm leads to a fuzzy extractor whose key is "only" \( \sqrt{\epsilon} \)-distinguishable from random if the helper data algorithm was \( \epsilon \)-revealing. Theorems 4.4. and 4.5. show that fuzzy extractors and helper data algorithms are equivalent up to parameter values.

\[4.10\] Conclusion

We have developed an information-theoretic framework for biometrics. We described biometric identification in terms of two communication channels both having the same biometric source \( X \), but with the enrollment data \( Y \) and the operational measurement \( Z \) as destinations. We have shown that it is possible to derive bounds on the capacity of biometric identification systems with relatively simple methods. The main result is that capacity can be computed as the mutual information \( I(Y; Z) \) between a input source \( Y \) and an output source \( Z \) that are related by the concatenation of the backward enrollment channel and the forward identification channel. The base-2 logarithm of the number of persons that can be distinguished reliably is expressed as the number of symbols in the observation, multiplied by the rate \( R \). For rates \( R \) smaller than \( I(Y; Z) \), this probability can also be made smaller than any \( \epsilon > 0 \) by increasing \( L \).

We showed that the secrecy capacity measures the entropy available in a key derived from the person. This result has been connected to a protocol that satisfies privacy and security requirements—in particular, the protection of templates to prevent misuse by a dishonest verifier. We have introduced the notions of \( \delta \)-contracting and \( \epsilon \)-revealing shielding functions, where the \( \delta \)-contraction describes the robustness against noise in the biometric sensor. The \( \epsilon \)-revelation describes the absence of any leakage of information via publicly available templates.

The identification capacity appears to be determined by the "channel capacity" of the biometric sensor, also for schemes that involve template protection. Similarly, the entropy of a secret that can be derived from the biometric measurement depends on the channel capacity of the biometric sensor.