Quantization effects in biometric systems

Quantization Effects in Biometric Systems

Frans M.J. Willems
Eindhoven University of Technology
Electrical Engineering Department
Eindhoven, The Netherlands

Tanya Ignatenko
Eindhoven University of Technology
Electrical Engineering Department
Eindhoven, The Netherlands

***Abstract*—The fundamental secret-key rate vs. privacy-leakage rate trade-offs for secret-key generation and transmission for i.i.d. Gaussian biometric sources are determined. These results are the Gaussian equivalents of the results that were obtained for the discrete case by the authors and independently by Lai et al. in 2008. Also the effect that binary quantization of the biometric sequences has on the ratio of the secret-key rate and privacy-leakage rate is considered. It is shown that the squared correlation coefficient must be increased by a factor of $\pi^2/4$ to compensate for such a quantization action, for values of the privacy-leakage rate that approach zero, when the correlation coefficient is close to zero.**

I. Introduction

Maurer [19] and slightly later Ahlswede and Csiszar [1] introduced the concept of secret sharing. In their source model two terminals observe two dependent sequences $\underline{X}$ and $\underline{Y}$. It is the objective of both terminals to generate a common secret key S by interchanging a public message H (helper data), that should only contain a negligible amount of information about the secret key. Ahlswede and Csiszar showed that the maximum secret key rate that can be achieved in this way is equal to the mutual information $I(X;Y)$ between the sequences. Their achievability proofs can be expressed in terms of the Slepian-Wolf methods that were presented by Cover [5] in which binning of typical sequences plays an important role, see also Ye and Narayan [6] and [11].

The concept of secret sharing is closely related to the generation of common randomness. When two terminals try to generate common randomness the issue of secrecy of the helper data is ignored. Common randomness capacity was first studied in a systematic way by Ahlswede and Csiszar [2]. Later helper terminals were introduced by Csiszar and Narayan in their investigations in [6]. Venkatesan and Anantharam [27] studied the idea to use channel noise for generation of common randomness.

In a biometric setting, where the X-sequence corresponds to the enrollment data and the Y-sequence to the authentication data, it is crucial that the public message H leaks as little information as possible about the biometric data. The reason for this is that compromised biometric data cannot be replaced. Smith [23] has investigated this leakage (privacy leakage) and came to the conclusion that it cannot be avoided. A similar conclusion can be found in Linnartz and Tuyls [18]. For key generation the trade-off between secret-key rate and privacy-leakage rate for the i.i.d. discrete case was determined recently by the authors [12], and independently and at the same time, by Lai et al [16]. Our results confirm the statement of Smith for a binary symmetric double source (BSDS). The authors [12] and Lai et al. [16] also consider secret-key transmission. This technique is called key-binding in the review paper by Jain et al. [13]. In this setting a model is studied in which an independently chosen secret key should be transmitted by the first terminal via a public message to the second terminal. The two terminals observe two dependent biometric sequences, and again the first requirement is that the public helper data should be uninformative about the transmitted secret key. The second requirement is that the privacy leakage in the helper data should be as small as possible. Also for key transmission the fundamental secret-key rate vs. privacy-leakage rate balance was determined in [12] and [16].

Where in [12] and [16] the discrete case is considered, we study here the case where the biometric sequences are assumed to be generated by a Gaussian correlated source. For such a Gaussian source we determine the fundamental balance between the secret-key rate and the privacy-leakage rate. Moreover we focus on the fundamental issues that occur when Gaussian biometric sequences are binary (two-level) quantized. Binary quantization of biometric data was first proposed by Daugman [10] for iris recognition. Later Tuyls et al. [21] considered binary quantization in practical secret-key generation systems, with an emphasis on generating reliable components. Kelkboom et al. [15] focussed specifically on binary quantized Gaussian biometrics and found an expression for the corresponding cross-over probability in the binary domain. Quantization in quantum key distribution protocols is discussed by Van Assche et al. [26]. Standard (natural and Gray coded) multi-level quantizers for biometrics combined with LDPC codes were studied by Ye at al. [30]. Sutcu et al. [25] considered biometric-specific quantizers, also focussing on LDPC codes. A multi-level quantizer based on likelihood ratios was proposed by Chen et al. [7]. In Li et al. [17] biometrical quantizers were analysed. It is observed by these authors that the quantizer has a large impact on the so-called entropy loss. Moreover they observe (see also [24]) that the entropy loss serves as an upper bound to the information leakage. As a consequence they state the problem to find a bound on the exact (privacy) information leakage.

It should be noted that the references above did not actually focus on privacy leakage in their research. It is our objective to demonstrate in this paper that quantization not only has a significant effect on the secret-key rate as we know from

classical communication theory, but also on the trade-off between the secret-key rate and the privacy-leakage rate.

Before we start with the presentation of our results we want to make the reservation that we do not discuss the validity of the Gaussian assumption in this paper. It is well-known that most transmission channels can be modeled as additive white Gaussian noise channels, however whether such models can be used for a wide range of biometrics will probably remain a point of discussion for the next years.

The outline of our paper is as follows. In section II we will describe our Gaussian key-generation and key-transmission models. We define the achievability of secret-key vs. privacy-leakage rate-pairs. In section III we state our results, i.e. we give the optimal trade-off between secret-key rate and privacy-leakage rate. The proofs of these results are provided in the appendix. In section IV we will discuss some properties of the rate-leakage region for the Gaussian case and demonstrate them using an example. Then in section V we will briefly summarize the rate-leakage results that were obtained in [12] for a binary symmetric double source. In section VI the effect that binary quantization of the Gaussian biometric sequences has on the rate-leakage trade-off is subject of investigation. Section VII considers the rate-leakage performance of some of the schemes that were proposed in the literature. In section VIII we will make some concluding remarks.

II. Definitions

A. A Gaussian Biometric Source

A Gaussian biometric system is based on a *Gaussian biometric source* $\{G_\rho(x,y), x \in \mathbf{R}, y \in \mathbf{R}\}$ that produces an X-sequence $\underline{x} = (x_1, x_2, \cdots, x_N)$ with N real-valued symbols and a Y-sequence $\underline{y} = (y_1, y_2, \cdots, y_N)$ also having N real-valued components. The density corresponding to sequence pair $(\underline{X}, \underline{Y})$ is given by

$$p_{\underline{X},\underline{Y}}(\underline{x},\underline{y}) = \prod_{n=1}^{N} G_\rho(x_n, y_n), \tag{1}$$

where

$$G_\rho(x,y) = \frac{1}{2\pi\sqrt{1-\rho^2}} \exp\left(-\frac{x^2+y^2-2\rho xy}{2(1-\rho^2)}\right), \tag{2}$$

for $x \in \mathbf{R}, y \in \mathbf{R}$, and correlation coefficient $|\rho| < 1$. Observe that the source pairs $\{(X_n, Y_n), n = 1, \ldots, N\}$ are independent of each other and identically distributed (i.i.d.) according to $G_\rho(\cdot,\cdot)$. Also note that scaling can always be applied to obtain unit X-variance and unit Y-variance.

B. Two Models

The sequences $\underline{x}$ and $\underline{y}$ are observed by an encoder and decoder, respectively. The encoder produces an index $h \in \{1, 2, \cdots, M_H\}$, which is referred to as helper data. These helper data are made public and used by the decoder.

We can subdivide biometric systems into those in which both terminals are supposed to *generate* a secret, and systems in which a uniformly chosen secret is *transmitted* from the encoder to the decoder. The generated or transmitted secret s assumes values in $\{1, 2, \cdots, M_S\}$. The decoders estimate $\widehat{s}$ of the secret s also assumes values from $\{1, 2, \cdots, M_S\}$. In transmission systems the secret S is a uniformly distributed index, hence

$$\Pr\{S = s\} = 1/M_S \text{ for all } s \in \{1, 2, \cdots, M_S\}. \tag{3}$$

In the next subsections we will consider secret generation and secret transmission in full detail.

C. Secret Generation

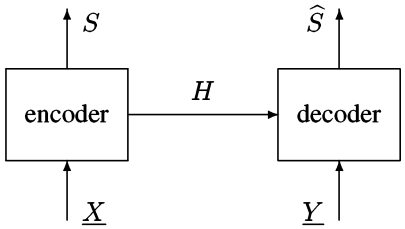

Fig. 1. Model for biometric secret generation.

In a biometric secret-key generation system, see Fig. 1, the encoder observes the biometric source sequence $\underline{X}$ and produces a secret S and helper data H, hence

$$(S, H) = e(\underline{X}), \tag{4}$$

where $e(\cdot)$ is the encoder mapping. The helper data H are sent to the decoder which is also observing the second biometric source sequence $\underline{Y}$. This decoder now forms an estimate $\widehat{S}$ of the secret that was chosen by the encoder, hence

$$\widehat{S} = d(\underline{Y}, H), \tag{5}$$

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

Definition 1: A rate-leakage pair (R, L) with $R \geq 0$ is achievable in a Gaussian biometric secret-key generation setting if for all $\delta > 0$ for all N large enough there exist encoders and decoders such that[1]

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ H(S) + N\delta \geq \log(M_S) &\geq N(R-\delta), \\ I(S;H) &\leq N\delta, \\ I(\underline{X};H) &\leq N(L+\delta). \end{aligned} \tag{6}$$

Moreover, let $\mathcal{G}_\rho^{\text{sg}}$ be the region of all achievable rate-leakage pairs for a secret-key generation system based on Gaussian source density $G_\rho(\cdot,\cdot)$.

D. Secret Transmission

In a biometric secret-key transmission system, see Fig. 2, a secret S, that is to be transmitted from encoder to decoder, is uniformly distributed, see (3). The encoder observes the source sequence $\underline{X}$ and the secret S and produces the integer helper data H, hence

$$H = e(S, \underline{X}), \tag{7}$$

[1]We take 2 as base of the log throughout this paper.

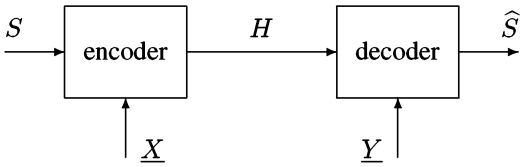

Fig. 2. Model for biometric secret transmission.

where $e(\cdot,\cdot)$ is the encoder mapping. The public helper data H are sent to the decoder that also observes the other source sequence $\underline{Y}$. This decoder forms an estimate $\widehat{S}$ of the secret that was transmitted, hence

$$\widehat{S} = d(H, \underline{Y}), \tag{8}$$

and $d(\cdot,\cdot)$ is the decoder mapping.

Definition 2: In a Gaussian biometric secret-key transmission system, a rate-leakage pair (R, L) with $R \geq 0$ is achievable if for all $\delta > 0$ for all N large enough there exist encoders and decoders such that

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ \log(M_S) &\geq N(R-\delta), \\ I(S;H) &\leq N\delta, \\ I(\underline{X};H) &\leq N(L+\delta). \end{aligned} \tag{9}$$

Moreover, let $\mathcal{G}_\rho^{\text{st}}$ be the region of all achievable rate-leakage pairs for a secret-key transmission system based on Gaussian source density $G_\rho(\cdot,\cdot)$.

III. Statement of Results

In order to state our results we first define the region $\mathcal{R}_\rho$. After that we present two theorems.

$$\begin{aligned} \mathcal{R}_\rho \triangleq \{(R,L) \quad : \quad & 0 \leq R \leq \frac{1}{2}\log\left(\frac{1}{\alpha\rho^2+1-\rho^2}\right), \\ & L \geq \frac{1}{2}\log\left(\frac{\alpha\rho^2+1-\rho^2}{\alpha}\right), \\ & \text{for } 0 < \alpha \leq 1\}. \end{aligned} \tag{10}$$

Theorem 1 (Secret Generation):

$$\mathcal{G}_\rho^{\text{sg}} = \mathcal{R}_\rho. \tag{11}$$

Theorem 2 (Secret Transmission):

$$\mathcal{G}_\rho^{\text{st}} = \mathcal{R}_\rho. \tag{12}$$

IV. Properties of the Region $\mathcal{R}_\rho$, and an Example

A. Convexity

To prove the convexity of $\mathcal{R}_\rho$ we define the rate-leakage function

$$R_\rho(L) \triangleq \max_{(R,L)\in\mathcal{R}_\rho} R, \tag{13}$$

for which we can write

$$R_\rho(L) = \frac{1}{2}\log\left(\frac{1-\rho^2/2^{2L}}{1-\rho^2}\right). \tag{14}$$

Now it can be shown that the second derivative $d^2R_\rho(L)/dL^2 \leq 0$. Therefore $R_\rho(L)$ is convex-$\cap$ in $L \geq 0$ and consequently region $\mathcal{R}_\rho$ is convex.

B. Asymptotic Secret-Key Rate

Note that asymptotically for increasing privacy-leakage rate

$$\begin{aligned} \lim_{L\to\infty} R_\rho(L) &= \lim_{L\to\infty} \frac{1}{2}\log\left(\frac{1-\rho^2/2^{2L}}{1-\rho^2}\right) \\ &= \frac{1}{2}\log\left(\frac{1}{1-\rho^2}\right) = I(X;Y). \end{aligned} \tag{15}$$

It is important to notice that the privacy-leakage rate has to increase to infinity to achieve this limit.

C. Slopes

If one is interested in achieving a small privacy-leakage rate L, the ratio between the secret-key rate and the privacy leakage rate becomes important. For the "rate-zero slope" γ_0 of the tangent to $R_\rho(L)$ at $L = 0$ we find

$$\gamma_0 \triangleq \left.\frac{dR_\rho(L)}{dL}\right|_{L=0} = \frac{\rho^2}{1-\rho^2}. \tag{16}$$

Inspection shows that this slope is equal to the signal-to-noise ratio for the "channel" from X to Y.

Another interesting parameter is the "rate-one slope" defined as

$$\gamma_1 \triangleq \max_{(R,R-1)\in\mathcal{R}_\rho} \frac{R}{1-R}. \tag{17}$$

It is not so difficult to see that in the Gaussian case

$$\gamma_1 = \frac{2-\log(4-3\rho^2)}{\log(4-3\rho^2)}. \tag{18}$$

D. Example

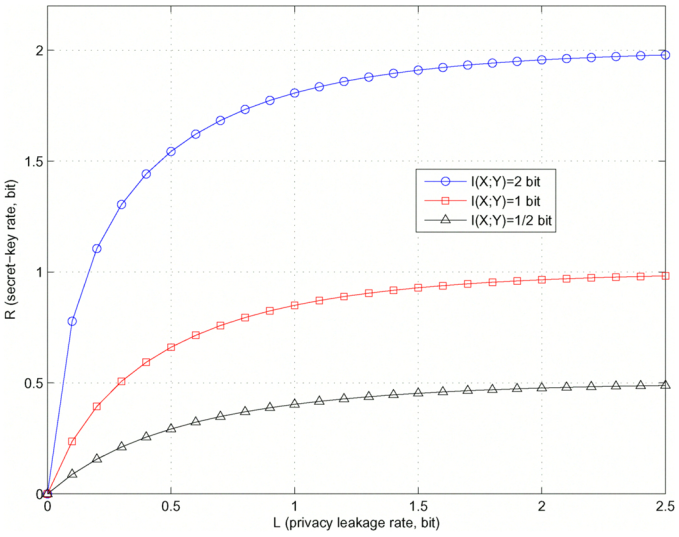

Fig. 3. Boundary of the achievable region $\mathcal{R}_\rho$ for three values of ρ.

In Fig. 3 we have depicted the boundary of the region $\mathcal{R}_\rho$, i.e. $R_\rho(L)$, as a function of the leakage L for three values of the square of the correlation coefficient ρ, i.e. for $\rho^2 = 1/2, 3/4$, and $15/16$. Note that corresponding asymptotic secret-key rates $I(X;Y)$ are $1/2, 1$, and 2 bit respectively. We can also determine the rate-zero slopes for these three values of

ρ^2. It turns out that the slopes are $1, 3$, and 15, respectively. We may conclude from this behavior that better biometrics have a better rate-zero slope. Therefore it is important to put enough effort in pre-processing the biometric data, such that as little extra noise as possible is introduced.

V. Binary Symmetric Biometric Systems

A binary symmetric biometric system is based on a *binary symmetric double source* $\{Q(x,y), x \in \{0,1\}, y \in \{0,1\}\}$. This source produces a sequence $\underline{x} = (x_1, x_2, \cdots, x_N)$ with N symbols from $\{0,1\}$ and a sequence $\underline{y} = (y_1, y_2, \cdots, y_N)$ also having N components in $\{0,1\}$. Sequence pair $(\underline{x}, \underline{y})$ occurs with probability

$$\Pr\{(\underline{X}, \underline{Y}) = (\underline{x}, \underline{y})\} = \prod_{n=1}^{N} Q(x_n, y_n). \tag{19}$$

We consider a binary symmetric source with crossover probability $0 \leq q \leq 1/2$, hence $Q(x,y) = (1-q)/2$ for $y = x$ and $q/2$ for $y \neq x$. For such a source the rate-leakage function, for both key generation and key transmission, is equal to

$$R_q(L) = 1 - h(p * q), \tag{20}$$

for p satisfying $h(p * q) - h(p) = L$. Here $h(\cdot)$ is the binary entropy function in bits. This was proved by the authors in [12].

A first problem is now to find out what the rate-zero slope for a binary system is, as a function of the cross-over probability q of the binary symmetric double source. Therefore we consider the behavior of $1 - h(p)$ for $\epsilon = \frac{1}{2} - p$ close to zero. Note that in this case

$$\begin{aligned} &\frac{1 - h(\frac{1}{2} - \epsilon)}{\log(e)} \\ &= \ln(2) + (\frac{1}{2} - \epsilon)\ln(\frac{1}{2} - \epsilon) + (\frac{1}{2} + \epsilon)\ln(\frac{1}{2} + \epsilon) \\ &= (\frac{1}{2} - \epsilon)\ln(1 - 2\epsilon) + (\frac{1}{2} + \epsilon)\ln(1 + 2\epsilon) \\ &= \frac{1}{2}\ln(1 - 4\epsilon^2) - \epsilon\ln(1 - 2\epsilon) + \epsilon\ln(1 + 2\epsilon) \\ &\approx 2\epsilon^2. \end{aligned} \tag{21}$$

Next observe that

$$p * q = (\frac{1}{2} - \epsilon)(1 - q) + (\frac{1}{2} + \epsilon)q = \frac{1}{2} - \epsilon(1 - 2q). \tag{22}$$

Therefore we can make the following approximations

$$\begin{aligned} 1 - h(p * q) &\approx \log(e) 2\epsilon^2 (1 - 2q)^2 \\ h(p * q) - h(p) &= 1 - h(p) - 1 + h(p * q) \\ &\approx \log(e) 2\epsilon^2 (1 - (1 - 2q)^2), \end{aligned} \tag{23}$$

and we finally may conclude that

$$\gamma_0 \triangleq \frac{dR_q(L)}{dL}\bigg|_{L=0} = \frac{(1-2q)^2}{1 - (1-2q)^2}. \tag{24}$$

For crossover probabilities $q = 0.2500, 0.1667$, and 0.0804 we have computed the rate-leakage function using (20). The resulting curves were plotted in Fig. 4. Check that the rate-zero slopes for L close to 0, are $0.3333, 0.8000$, and 2.3801 respectively.

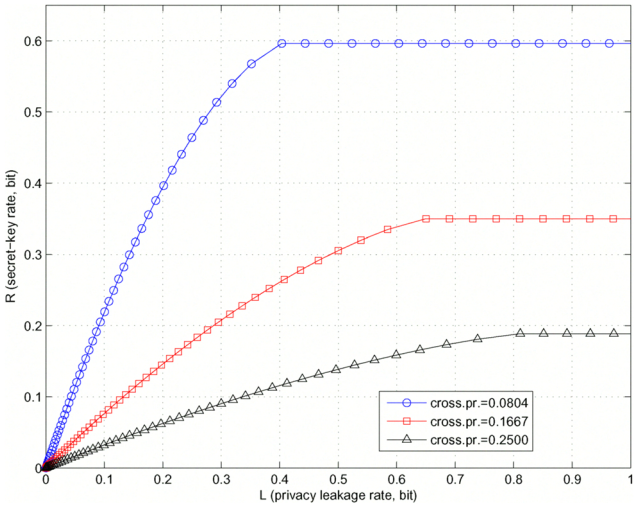

Fig. 4. Secret-key rate versus privacy-leakage rate functions for three values of the cross-over probability q.

VI. Binary Quantization

In this section we will study the effect of binary quantization of the Gaussian biometric sequences. We assume that after quantization processing on the resulting binary sequences is performed. It will be clear that the resulting binary statistic is binary symmetric as in the previous section. The main problem is now to find out how the cross-over probability q relates to the correlation coefficient ρ of the Gaussian statistic.

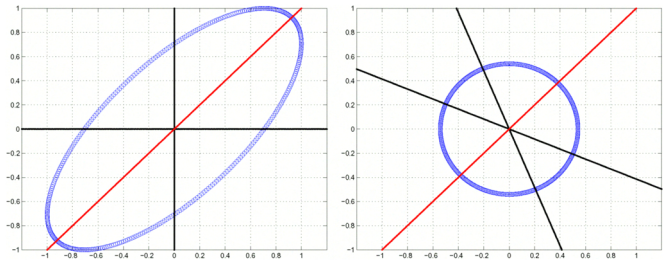

Fig. 5. Compressing a cigar (left) such that it becomes a ball (right).

Suppose that the cigar in Fig. 5, left, corresponds to coordinates (x,y) where the Gaussian density $G_\rho(x,y)$ equals some constant. Now the variance in the $Y = X$ direction is $(1+\rho)/2$ and $(1-\rho)/2$ in the $Y = -X$ direction. Note that the cross-over probability q corresponds to the mass of the cigar in the second or fourth quadrant. Instead of manipulating with the integral, we can compress the cigar in the $Y = X$ direction, by a factor $\sqrt{(1+\rho)/(1-\rho)}$, to transform it into a circle, see Fig. 5, right. Then the cross-over probability is then the angle between the two black lines, divided by π. Compression brings the tangent of half the angle between the black lines

from one down to $\sqrt{(1-\rho)/(1+\rho)}$. Therefore

$$q = \frac{2}{\pi} \arctan\left(\sqrt{\frac{1-\rho}{1+\rho}}\right). \tag{25}$$

This formula, together with (24) allows us to determine the zero-rate slope of a binary quantized system.

In Fig. 4 we have chosen the cross-over probabilities q according to (25) for squared correlation-coefficients $1/2, 3/4$, and $15/16$. It can be checked that the resulting zero-rate slopes ($0.3333, 0.8000$, and 2.3801 respectively) are significantly smaller than the corresponding zero-rate slopes ($1, 3$, and 15) from Fig. 3.

For small values of the squared correlation coefficient ρ^2 we can quantify the loss that is caused by binary quantization. In that case we can approximate q by

$$q \approx \frac{1}{2} - \frac{\rho}{\pi}, \tag{26}$$

and formula (24) results in the rate-zero slope

$$\gamma_0 = \frac{(2\rho/\pi)^2}{1-(2\rho/\pi)^2}. \tag{27}$$

We can conclude from this and (16) that the squared correlation coefficient ρ^2 must be increased by a factor of $\pi^2/4$ to compensate for the binary quantization actions, if we are interested in maintaining the rate-zero slope constant.

Representing this loss in decibels gives 3.92 dB, which is twice the loss in signal-to-noise ratio that we get in transmission over an AWGN channel when we do binary signalling at the transmitter and hard decision at the receiver, and focus on capacity (see Proakis [20], p. 460) at small signal-to-noise ratios. The factor of two could be explained from the fact that in a biometric system we quantize at both sides.

VII. Comparison

In this section we discuss the privacy-leakage properties of some secret-key generation schemes that were described in the literature. It should be noted that here we consider the operational rates.

The (key-generation) scheme presented by Linnartz and Tuyls [18], which is based on quantization index modulation (QIM, see [8]), has a privacy-leakage rate that is infinite. If we focus on $\sigma_x^2/\sigma_n^2 = 3$ (or $\rho^2 = 3/4$) then $I(X;Y) = 1$ bit. Now with quantization interval-size $q = 1.41\sigma_x$ we obtain for the security-leakage rate $I(S;H) = 0.0101$ bit and an error probability $P_e = 0.2218$ and consequently secret-key rate of at most 0.2366 bit. The privacy-leakage that is unavoidable for this key rate, see Fig. 3, is only a few tenths of a bit. Note however that that infinitely large privacy-leakage that comes with the Linnartz-Tuyls scheme, does not imply that we can recover the biometric sequence from the helper data.

In biometric key-transmission systems based on fuzzy commitment (proposed by Juels and Wattenberg [14]), during enrollment a randomly chosen codeword from a binary error-correcting code is added modulo-2 to the binary enrollment sequence. If the rate of this code is R, the secret-key rate is R too, and the privacy-leakage rate is equal to $1-R$ if the enrollment sequence is uniform and identically distributed. If the observed biometric is symmetric with cross-over probability q and $R = 1-h(q)$, the pair $(R, 1-R)$ is optimal, i.e. it satisfies (20), with $p = 0$. When the rate is taken smaller than $1-h(q)$ however, the leakage increases and the resulting pair (R, L) becomes suboptimal. If the binary biometric sequences result from binary quantization of real-valued (Gaussian) sequences, the effect described in the previous section causes an extra loss. As an example of such systems we mention Tuyls et al. [21]. Note that the rate-one slope (18) can be used as a benchmark to evaluate the performance of fuzzy commitment combined with binary quantization.

Ye et al. [30] consider the Gaussian case. They apply scalar multi-level quantization instead of binary quantization at the enrollment side. Moreover at the authentication side soft decision is used. Therefore this scheme certainly improves upon the fuzzy commitment schemes with respect to the secret-key rate. The privacy-leakage rate is not considered but it should be clear that the syndrome rate increases when the quantizer depth grows. Therefore the Ye et al. method in principle incorporates the balance between privacy-leakage and secret-key rate. What is not optimal is that scalar quantization is used. A scheme with similar properties was presented by Bloch et al. [4].

VIII. Concluding Remarks

Kelkboom et al. [15] also investigated how the cross-over probability depends on the statistics of a Gaussian source and came up with expressions similar to (25) for various settings.

We have taken here mutual information as a metric for privacy leakage. This gave us the opportunity to determine the fundamental trade-off. Maybe however other metrics would be more appropriate. We could e.g. try to create helper data such that the estimation error made by an arbitrary reconstruction device having access to the helper data is maximized. Using rate-distortion theory we can lower bound this distortion since we have an upper bound on the privacy-leakage rate (if we fix the secret-key rate), but such a bound may not be tight.

We have determined the trade-off for i.i.d. Gaussian sources here. In practice a biometric however consists of components having correlation values within a smaller or larger range. It should be possible to find the rate-leakage function for such sources based on the basic trade-off for the i.i.d. case that was found here.

A final remark is about coding schemes. Inevitably the first concern is to design codes (preferably based on standard components and methods) that achieve the trade-off that we found here. A second point of attention should be to find out what happens with the leakage if we apply conservative codes. We have already seen that with fuzzy commitment decreasing the rate results in an increased privacy-leakage.

Acknowledgment

The authors would like to thank Ton Akkermans, Emile Kelkboom, Tom Kevenaar, Jean-Paul Linnartz, Boris Skoric, and Raymond Veldhuis for valuable discussions and suggestions.

APPENDIX

A. Proof of Theorem 1

The proof of this theorem consists of two parts. The first part, i.e. the converse will be treated in detail. The second part concerns the achievability of which we will only provide an outline.

1) The Converse: First we consider the entropy of the secret. We use that $\widehat{S} = d(H, \underline{Y})$ and Fano's inequality $H(S|\widehat{S}) \leq F$, where $F \triangleq 1 + \Pr\{\widehat{S} \neq S\} \log(M_S)$.

$$\begin{aligned} H(S) &= I(S; H, Y^N) + H(S|H, Y^N, \widehat{S}) \\ &\leq I(S; H, Y^N) + H(S|\widehat{S}) \\ &\leq I(S; H) + I(S; Y^N|H) + F \\ &= I(S; H) + I(S, H; Y^N) + F \\ &= I(S; H) + h(Y^N) - h(Y^N|S, H) + F. \quad (28) \end{aligned}$$

Now we continue with the leakage.

$$\begin{aligned} I(X^N; H) &\geq H(H, \widehat{S}|Y^N) - H(S, H|X^N) \\ &= H(S, H, \widehat{S}|Y^N) - H(S|H, Y^N, \widehat{S}) \\ &\quad -H(S, H|X^N) \\ &\geq H(S, H|Y^N) - H(S|\widehat{S}) - H(S, H|X^N) \\ &\geq H(S, H|Y^N) - F - H(S, H|X^N) \\ &= I(S, H; X^N) - I(S, H; Y^N) - F \\ &= h(X^N) - h(X^N|S, H) \\ &\quad -h(Y^N) + h(Y^N|S, H) - F. \quad (29) \end{aligned}$$

We are now ready to use Shannon's entropy power inequality [22]. For a simple proof of this inequality see [28]. We use here a conditional version of the entropy power inequality similar to Lemma II in [3]. However first we have to transform the statistical relation between X and Y as described by the density in (2) into an additive version. Note that

$$Y = \rho X + N, \quad (30)$$

where N is Gaussian with mean zero and variance $1-\rho^2$, and independent of X, see Fig. 6.

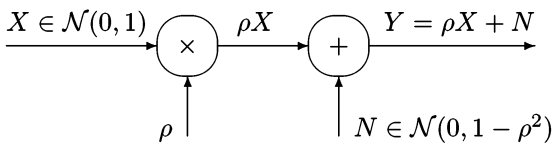

Fig. 6. Additive equivalent relation between two unit variance correlated variables X and Y.

From the (conditional version of the) entropy power inequality we may conclude that if $\frac{1}{N}h(X^N|S,H) = \frac{1}{2}\log_2(2\pi e\alpha)$ then $\frac{1}{N}h(Y^N|S,H) \geq \frac{1}{2}\log_2(2\pi e(\alpha\rho^2 + 1 - \rho^2))$. Note that we may assume that $0 < \alpha \leq 1$ since X has unit variance, and $\alpha = 0$ would imply that $H(S,H) = \infty$ which is impossible for finite ranges M_S and M_H.

For achievable (R, L) for all $\delta > 0$ and N large enough, we first obtain that

$$\begin{aligned} \frac{\log(M_S)}{N} &\leq \frac{H(S)}{N} + \delta \\ &\leq \frac{I(S;H) + h(Y^N) - h(Y^N|S,H) + F}{N} + \delta \\ &\leq \delta + \frac{1}{2}\log\left(\frac{1}{\alpha\rho^2 + 1 - \rho^2}\right) + \frac{1}{N} + \delta\frac{\log(M_S)}{N} + \delta \end{aligned} \quad (31)$$

for some $0 \leq \alpha \leq 1$. In the last inequality the fact that Y has unit variance led to differential entropy $h(Y^N) = \frac{N}{2}\log(2\pi e)$. From (31) we may conclude that

$$R - \delta \leq \frac{\log(M_S)}{N} \leq \frac{2\delta + \frac{1}{2}\log\left(\frac{1}{\alpha\rho^2+1-\rho^2}\right) + \frac{1}{N}}{1-\delta}. \quad (32)$$

Moreover for achievable (R, L) for all $\delta > 0$ and N large enough, we get

$$\begin{aligned} L + \delta &\geq \frac{I(X^N; H)}{N} \\ &\geq \frac{h(X^N) - h(X^N|S,H) - h(Y^N) + h(Y^N|S,H) - F}{N}, \\ &\geq \frac{1}{2}\log\left(\frac{\alpha\rho^2 + 1 - \rho^2}{\alpha}\right) - \frac{1}{N} - \delta\frac{\log(M_S)}{N}, \end{aligned} \quad (33)$$

for some $0 < \alpha \leq 1$. Now, in the last inequality we used that the differential entropies $h(X^N) = h(Y^N)$ since X and Y both have unit variance.

If we let $\delta \downarrow 0$ and $N \to \infty$, then we obtain the converse from both (32) and (33). As an intermediate step it follows from (32) and $|\rho| < 1$ that $\log(M_S)/N$ is finite.

2) Outline of the Achievability Proof: Let $0 < \alpha \leq 1$. We start by fixing the joint density of U, X, and Y such that the Markov condition $U - X - Y$ holds. Let U be Gaussian with mean zero and variance $1 - \alpha$. Moreover assume that

$$X = U + V, \quad (34)$$

where V, independent of U, is Gaussian with mean zero and variance α, see Fig. 7. Finally Y follows from X as in Fig. 6.

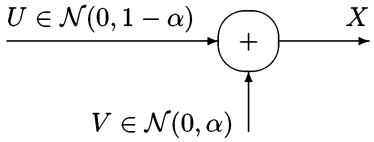

Fig. 7. Additive noise V transforming U into X.

Note that now $I(U;Y) = \frac{1}{2}\log\left(\frac{1}{\alpha\rho^2+1-\rho^2}\right)$ and $I(U;X) = \frac{1}{2}\log\left(\frac{1}{\alpha}\right)$.

Next we randomly generate roughly $2^{NI(U;X)}$ sequences $\underline{u}$, Gaussian, with mean zero and variance $1 - \alpha$. Each of those sequences gets a random s-label and a random h-label. These labels are uniformly chosen. The s-labels can assume roughly $2^{NI(U;Y)}$ values, the h-label roughly

$2^{N(I(U;X)-I(U;Y)}$ values. The encoder, upon observing the source sequence $\underline{x}$, first finds a sequence $\underline{u}$ that is jointly typical with $\underline{x}$. It is understood that we use Gaussian typicality here, see Cover and Thomas [9], Chapter 9, also [29]. Since there are roughly $2^{NI(U;X)}$ such sequences, this is possible with vanishing error probability. Then the encoder outputs the s-label corresponding to this sequence as secret, and sends the h-label corresponding to $\underline{u}$ as helper data to the decoder. The decoder observes the source sequence $\underline{y}$ and determines the source sequence $\widehat{\underline{u}}$ with an h-label matching to the helper data, such that $(\widehat{\underline{u}}, \underline{y})$ is jointly typical. It can be shown that the decoder can reliably recover $\underline{u}$ now, since it has to search among roughly $2^{NI(U;Y)}$ alternatives. It is easy to check that the leakage is not larger than $I(U;X)-I(U;Y)$. An important additional property of the proof is that $\underline{u}$ can be recovered reliably from both the s-label and the h-label. Now, after having proved that $H(\underline{U})$ is roughly equal to $NI(U;X)$ and using that $H(S) \leq NI(U;Y)$ and $H(H) \leq N(I(U;X) - I(U;Y))$ (roughly), it easily follows that $I(S;H)$ is negligible. Uniformity of the secret S also can be demonstrated similarly.

B. Proof of Theorem 2

The converse for this theorem is an adapted version of the converse for secret generation. The achievability proof is also based on the achievability proof for secret generation.

1) Converse: As in the converse for secret generation

$$\log(M_S) = H(S) \leq I(S;H) + h(Y^N) - h(Y^N|S,H) + F, \tag{35}$$

and

$$\begin{aligned} I(X^N;H) &\geq h(X^N) - h(X^N|S,H) \\ &\quad -h(Y^N) + h(Y^N|S,H) - F. \end{aligned} \tag{36}$$

For achievable (R,L) for all $\delta > 0$ and N large enough, we first obtain that

$$\begin{aligned} \frac{\log(M_S)}{N} &\leq \frac{I(S;H) + h(Y^N) - h(Y^N|S,H) + F}{N} \\ &\leq \delta + \frac{1}{2}\log\left(\frac{1}{\alpha\rho^2 + 1 - \rho^2}\right) + \frac{1}{N} + \delta\frac{\log(M_S)}{N} \end{aligned} \tag{37}$$

for some $0 < \alpha \leq 1$. From (37) we may conclude that

$$R - \delta \leq \frac{\log(M_S)}{N} \leq \frac{\delta + \frac{1}{2}\log\left(\frac{1}{\alpha\rho^2+1-\rho^2}\right) + \frac{1}{N}}{1-\delta}. \tag{38}$$

As before for achievable (R,L) for all $\delta > 0$ and N large enough, we get

$$\begin{aligned} L + \delta &\geq \frac{I(X^N;H)}{N} \\ &\geq \frac{1}{2}\log\left(\frac{\alpha\rho^2 + 1 - \rho^2}{\alpha}\right) - \frac{1}{N} - \delta\frac{\log(M_S)}{N}, \end{aligned} \tag{39}$$

for some $0 < \alpha \leq 1$. If we let $\delta \downarrow 0$ and $N \to \infty$, then we obtain the converse from both (38) and (39).

2) Achievability Proof: The achievability proof corresponding to Theorem 2 is based on the proof of Theorem 1. The difference is that we use a so called masking layer, see Figure 8, that uses the generated secret S_g in a one-time pad system to hide the transmitted secret S_t. Such a masking layer was already used by Ahlswede and Csiszar [1]. The operations in the masking layer are simple. Denote by $\oplus$ addition modulo M_S and by $\ominus$ subtraction modulo M_S then

$$\begin{aligned} H_t &= S_t \oplus S_g, \\ \widehat{S}_t &= H_t \ominus \widehat{S}_g = S_t \oplus (S_g \ominus \widehat{S}_g), \end{aligned} \tag{40}$$

where H_t should be considered as additional helper data.

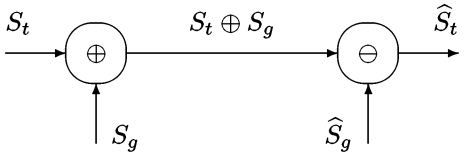

Fig. 8. The masking layer.

Now keeping in mind that S_t is uniform on $\{1,2,\cdots,M_S\}$ and independent of X^N, the generated secret S_g, and corresponding helper data H_g, we obtain

$$\begin{aligned} &I(S_t; H_g, (S_t \oplus S_g)) \\ &\quad = I(S_t;H_g) + I(S_t;(S_t \oplus S_g)|H_g) \\ &\quad \leq H(S_t \oplus S_g) - H(S_t \oplus S_g|H_g, S_t) \\ &\quad \leq \log(M_S) - H(S_g|H_g,S_t) \\ &\quad \leq \log(M_S) - H(S_g|H_g) \\ &\quad \leq \log(M_S) - H(S_g) + I(S_g;H_g) \end{aligned} \tag{41}$$

and

$$\begin{aligned} &I(X^N; H_g, (S_t \oplus S_g)) \\ &\quad = I(X^N;H_g) + I(X^N;(S_t \oplus S_g)|H_g) \\ &\quad \leq I(X^N;H_g) + H(S_t \oplus S_g) - H(S_t \oplus S_g|H_g, X^N, S_g) \\ &\quad \leq I(X^N;H_g) + \log(M_S) - H(S_t|H_g, X^N, S_g) \\ &\quad = I(X^N;H_g) + \log(M_S) - \log(M_S) \\ &\quad = I(X^N;H_g). \end{aligned} \tag{42}$$

Theorem 1 states that there exist (for all $\delta > 0$ and N large enough) encoders and decoders for which $\Pr\{\widehat{S}_g \neq S_g\} \leq \delta$, and

$$\begin{aligned} H(S_g) + N\delta \geq \log(M_S) &\geq N(R-\delta), \\ I(S_g;H_g) &\leq N\delta, \\ I(X^N;H_g) &\leq N(L+\delta). \end{aligned} \tag{43}$$

Therefore, using the masking layer implies that $\widehat{S}_t = S_t$ if $\widehat{S}_g = S_g$, and thus $\Pr\{\widehat{S}_t \neq S_t\} \leq \delta$, and

$$\begin{aligned} \log(M_S) &\geq N(R-\delta), \\ I(S_t; H_g, (S_t \oplus S_g)) &\leq 2N\delta, \\ I(X^N; H_g, (S_t \oplus S_g)) &\leq N(L+\delta), \end{aligned} \tag{44}$$

and consequently rate-leakage pairs that are achievable for secret generation are also achievable for secret transmission.

REFERENCES

[1] R. Ahlswede and I. Csiszar, "Common Randomness in Information Theory and Cryptography - Part I: Secret Sharing," *IEEE Trans. Inform. Theory,* vol. IT-39, pp. 1121-1132, July 1993.

[2] R. Ahlswede and I. Csiszar, "Common Randomness in Information Theory and Cryptography - Part II: CR Capacity," *IEEE Trans. Inform. Theory,* vol. IT-44, pp. 225 - 240, January 1998.

[3] P. Bergmans, "A Simple Converse for Broadcast Channels with Additive White Gaussian Noise," *IEEE Trans. Inform. Th.,* Vol. IT - 20, No. 2, pp. 279 - 280, March 1974.

[4] M. Bloch, A. Thangaraj, and S.W. McLaughlin, "Efficient Reconciliation of Correlation Continuous Random Variables using LDPC Codes," *arXiv,* arXiv:cs/0509041v1.

[5] T.M. Cover, "A Proof of the Data Compression Theorem of Slepain and Wolf for Ergodic Sources," *IEEE Trans. Inform. Theory,* vol. IT-22, pp. 226 - 228, March 1975.

[6] I. Csiszar and P. Narayan, "Common Randomnness and Secret Key Generation with a Helper," *IEEE Trans. Inform. Theory,* vol. IT-46, pp. 344 - 366, March 2000.

[7] C. Chen, R.N.J. Veldhuis, T.A.M. Kevenaar, and A.H.M. Akkermans, "Multi-Bits Biometric String Generation Based on the Likelihood Ratio," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* Workshop on Biometrics, 24-28 Jun 2008, Anchorage, Alaska, US. pp. 1-7.

[8] B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Trans. Inform. Theory,* Vol. 47, pp. 1423 -1443, May 2001.

[9] T.M. Cover and Y. Thomas, *Elements of Information Theory.* Wiley & Sons, New York, 1991. Second edition, 2006.

[10] J.G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. on Pattern Anal. Mach. Intell.,* vol. 15, No. 11, pp. 1148 - 1161, Nov. 1993.

[11] T. Ignatenko and F. Willems, "On the Security of the XOR-Method in Biometric Authentication Systems," *Proc. 27th Symp. Inform. Theory in the Benelux,* Noordwijk, The Netherlands, June 8-9, 2006, pp. 197 - 204.

[12] T. Ignatenko and F.M.J. Willems, "Privacy Leakage in Biometric Secrecy Systems, *Proc. 2008 46th Annual Allerton Conference on Communication, Control and Computing,* September 23 - 26, 2008, Monticello, IL, USA.

[13] A.K. Jain, K. Nandakamur, and A. Nagar, "Biometric Template Security," *EURASIP Journal on Advances of Signal Processing,* Vol. 2008, Article ID 579416, 17 pages.

[14] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme, *Proc. 6th ACM Conf. on Computer and Communications Security,* ACM Press, pp. 26 - 36, 1999.

[15] E.J.C. Kelkboom, G. Garcia Molina, T.A.M. Kevenaar, R.N.J. Veldhuis, and W. Jonker, "Binary Biomterics: An Analytic Framework to Estimate the Bit Error Probability under Gaussian Assumption," *2nd IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2008*, 29 Sep - 1 Oct 2008, Washington, USA. pp. 1-6. IEEE Computer Society Press.

[16] L. Lai, S.-W. Ho, and H.V. Poor, "Privacy-Security Tradeoffs in Biometric Security Systems," *Proc. 2008 46th Annual Allerton Conference on Communication, Control and Computing,* September 23 - 26, 2008, Monticello, IL, USA.

[17] Q. Li, Y. Sutcu, and N. Memon, "Secure Sketch for Biometric Templates," *Asiacrypt,* volume 4284 of LNCS, Shanghai, China, December 2006. [

[18] J.-P. Linnartz and P. Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," *4th Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, 2003, pp. 393- 401.

[19] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Trans. Inform. Theory,* IT-39, pp. 733-742, 1993.

[20] J.G. Proakis, *Digital Communications.* McGraw-Hill, Fourth Ed. (Int.), 2001.

[21] P. Tuyls, A.H.M. Akkermans, T.A.M. Kevenaar, G.-J. Schrijen, A, Bazen, and R.N.J. Veldhuis, "Practical Biometric Authentication with Template Protection," *5th Int. Conf. on Audio- and Video-Based Personal Authentication (AVBPA)*, Rye Brook, New York. pp. 436-446. Springer-Verlag Berlin, 2005.

[22] C.E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.,* vol. 27, pp. 379 - 423 (Part I), 623 - 656 (Part II), July/Oct. 1948.

[23] A.D. Smith, *Maintaining Secrecy when Information Leakage is Unavoidable,* Ph.D. thesis, Massachusetts Institute of Technology, August 2004.

[24] Y. Sutcu, Q. Li, and N. Memon, "Protecting Biometric Templates With Sketch: Theory and Practice," *IEEE Trans. on Inform. Forens. and Security,* Vol. 2, No. 3. Set. 2007, pp. 503 - 512.

[25] Y. Sutcu, S. Rane, J.S. Yedidia, S.C. Draper, and A. Vetro, "Feature Extraction for a Slepian-Wolf Biometric System Using LDPC Codes," *Proc. IEEE Int. Symp. Inform. Theory,* Toronto, July 6-11, 2008, pp. 2297 - 2301.

[26] G. Van Assche, J. Cardinal, a nd N.J. Cerf, "Reconcilliation of a Quantum-Distributed Gaussian Key," *IEEE Trans. Inform. Th.,* Vol. IT - 50, No. 2, pp. 394 - 400, Feb. 2004.

[27] S. Venkatesan and V. Anantharam, "The Common Randomness Capacity of a Pair of Independent Discrete Memoryless Channels," *IEEE Trans. Inform. Theory,* vol. IT-44, pp. 215 - 224, January 1998.

[28] S. Verdu and D. Guo, "A Simple Proof of the Entropy Power Inequality," *IEEE Trans. Inform. Th.,* Vol. IT - 52, No. 5, pp. 2165 - 2166, May 2006.

[29] F.M.J. Willems, "Coding Theorem for the AWGN Channel in Terms of Jointly Typical Sequences," *Proc. 10th Symp. on Inform. Th. in the Benelux,* Houthalen, Belgium, May 25 & 26, 1989, pp. 13 - 18.

[30] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Gaussian Random Variables," *IEEE Int. Symp. Inform. Theory,* Seattle, USA, July 9 - 14, 2006, pp. 2593 - 2597.

[31] Chunxuan Ye and P. Narayan, "Secret and Private Key Constructions for Simple Multiterminal Source Models," *Proc. IEEE Int. Symp. Inform. Theory,* Adelaide, Australia, Sept. 4 - 9, 2005, pp. 2138 - 2141.