# Biometric systems: privacy and secrecy aspects

# Biometric Systems: Privacy and Secrecy Aspects

Tanya Ignatenko, *Member, IEEE*, and Frans M. J. Willems, *Fellow, IEEE*

***Abstract*—This paper addresses privacy leakage in biometric secrecy systems. Four settings are investigated. The first one is the standard Ahlswede–Csiszár secret-generation setting in which two terminals observe two correlated sequences. They form a common secret by interchanging a public message. This message should only contain a negligible amount of information about the secret, but here, in addition, we require it to leak as little information as possible about the biometric data. For this first case, the fundamental tradeoff between secret-key and privacy-leakage rates is determined. Also for the second setting, in which the secret is not generated but independently chosen, the fundamental secret-key versus privacy-leakage rate balance is found. Settings three and four focus on zero-leakage systems. Here the public message should only contain a negligible amount of information on both the secret and the biometric sequence. To achieve this, a private key is needed, which can only be observed by the terminals. For both the generated-secret and the chosen-secret model, the regions of achievable secret-key versus private-key rate pairs are determined. For all four settings, the fundamental balance is determined for both unconditional and conditional privacy leakage.**

***Index Terms*—Biometric secrecy systems, common randomness, privacy, private key, secret key.**

## I. Introduction

### A. State of the Art

With recent advances of biometric recognition technologies, these methods are seen to be elegant and interesting building blocks that can substitute or reinforce traditional cryptographic and personal authentication systems. However, as Schneier [34] pointed out, biometric information, unlike passwords and standard secret keys, if compromised cannot be canceled and easily substituted: people only have limited resources of biometric data. Moreover, stolen biometric data result in a stolen identity. Therefore, use of biometric data rises privacy concerns, as noted by Prabhakar *et al.* [30]. Ratha *et al.* [32] investigated vulnerability points of biometric secrecy systems, and at the DSP forum [40], secrecy- and privacy-related problems of biometric systems were discussed.

Considerable interest in the topic of biometric secrecy systems resulted in the proposal of various techniques over the past decade. Recent developments in this area led to methods grouped around two classes: cancelable biometrics and "fuzzy encryption." Detailed summaries of these two approaches can be found in Uludag *et al.* [39] and in Jain *et al.* [20].

It is the objective of cancelable biometrics, introduced by Ratha *et al.* [32], [33], Ang *et al.* [3], and Maiorana *et al.* [25], to avoid storage of reference biometric data in the clear in biometric authentication systems. These methods are based on non-invertible transformations that preserve the statistical properties of biometric data and rely on the assumption that it is hard to exactly reconstruct biometric data from the transformed data and applied transformation. However, hardness of a problem is difficult to prove; and, in practice, the properties of these schemes are assessed using brute-force attacks. Moreover, visual inspection shows that transformed data, e.g., the distorted faces in Ratha *et al.* [33], still contain a lot of biometric information.

The "fuzzy encryption" approach focuses on generation and binding of secret keys from/to biometric data. These secret keys are used to regulate access to, e.g., sensitive data, services, and environments in key-based cryptographic applications and, in particular, in biometric authentication systems (all referred to as biometric secrecy systems). In biometric secrecy systems, a secret key is generated/chosen during an enrollment procedure in which biometric data are observed for the first time. This key is to be reconstructed after these biometric data are observed again during an attempt to obtain access (authentication). Since biometric measurements are typically noisy, reliable biometric secrecy systems also extract so-called helper data from the biometric observation at the time of enrollment. These helper data facilitate reliable reconstruction of the secret key in the authentication process. The helper data are assumed to be public, and therefore they should not contain information on the secret key. We say that the secrecy leakage should be negligible. Important parameters of a biometric secrecy system include the size of the secret key and the information that the helper data contain (leak) on the biometric observation. This latter parameter is called privacy leakage.[1] Ideally, the privacy leakage should be small, to avoid the biometric data of an individual's becoming compromised. Moreover, the secret-key length (also characterized by the secret-key rate) should be large to minimize the probability that the secret key is guessed and unauthorized access is granted.

Implementations of such biometric secrecy systems include methods based on various forms of Shamir's secret sharing [35]. These methods are used to harden passwords with biometric data; see, e.g., Monrose *et al.* [27], [28]. The methods based on error-correcting codes, which bind uniformly distributed secret keys to biometric data and which tolerate (biometric) errors in

Manuscript received September 19, 2008; revised August 27, 2009. First published September 29, 2009; current version published November 18, 2009. This work was supported in part by SenterNovem under Project IGC03003B. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Klara Nahrstedt.

The authors are with the Department of Electrical Engineering, Eindhoven University of Technology, 5612 AZ Eindhoven, The Netherlands (e-mail: t.ignatenko@tue.nl; f.m.j.willems@tue.nl).

Digital Object Identifier 10.1109/TIFS.2009.2033228

[1]The privacy leakage is only assessed with respect to the helper data. We do not consider the leakage from the secret key, since secret keys are either stored using one-way encryption (in authentication systems) or discarded (in key-based cryptographic applications).

these secret keys, were formally defined by Juels and Wattenberg [22]. Less formal approaches can be found in Davida *et al.* [10], [11]. Later error-correction based methods were extended to the set difference metric developed by Juels and Sudan [21]. Some other approaches focus on continuous biometric data and provide solutions that rest on quantization of biometric data as in Linnartz and Tuyls [24], Denteneer *et al.* [12] (with emphasis on reliable components), Teoh *et al.* [38], and Buhan *et al.* [6]. Finally, a formal approach for designing secure biometric systems for three metric distances (Hamming, edit, and set), called fuzzy extractors, was introduced in Dodis *et al.* [13] and Smith [36] and further elaborated in [14]. Fuzzy extractors were subsequently implemented for different biometric modalities in Sutcu *et al.* [37] and Draper *et al.* [15].

### B. Motivation

A problem of the existing practical systems is that sometimes they lack formal security proofs and rigorous security formulations. On the other hand, the systems that do provide formal proofs actually focus on secrecy only while neglecting privacy. For instance, Frykholm and Juels [16] only provide their analysis for the secrecy of the keys. Similarly, Linnartz and Tuyls [24] offer information-theoretical analysis for the secrecy leakage but no corresponding privacy leakage analysis. Dodis *et al.* [13], [14] and Smith [36] were the first to address the problem of code construction for biometric secret-key generation in a systematic information-theoretical way. Although their works provide results on the maximum secret-key rates in biometric secrecy systems, they also focus on the corresponding privacy leakage. In a biometric setting, however, the goal is to minimize the privacy leakage and, more specifically, to minimize the privacy leakage for a given secret-key rate. The need for quantifying the exact information leakage on biometric data was also stated as an open question in Sutcu *et al.* [37]. In this paper, we study the fundamental tradeoff between the secret-key rate and privacy-leakage rate in biometric secrecy systems. This tradeoff is studied from an information-theoretical prospective.

Our approach to the problem of generating secret keys out of biometric data is closely related to the concept of secret sharing, which was introduced by Maurer [26] and (slightly later) by Ahlswede and Csiszár [1]. In the source model of Ahlswede and Csiszár [1], two terminals observe two correlated sequences $X^N$ and $Y^N$ and aim at producing an as large as possible common secret $S$ by interchanging a public message $M$. This message, which we refer to as helper data, should only provide a negligible amount of information on the secret. It was shown that the maximum secret-key rate in this model is equal to the mutual information $I(X;Y)$ between the observed sequences. The secret sharing concept is also closely related to the concept of common randomness generation that was studied by Ahlswede and Csiszár [2] and later extended with helper terminals by Csiszár and Narayan [9]. In common randomness setting, the requirement that the helper data should provide only a negligible amount of information on the generated randomness is dropped.

Recently, Prabhakaran and Ramchandran [31] and Gündüz *et al.* [19] studied source coding problems where the issue of (biometric) leakage was addressed. In their work, though, it is not the intention of the users to produce a secret but to communicate a (biometric) source sequence in a secure way from the first to the second terminal.

### C. Eight Models

In this paper, we consider four biometric settings. The first one is the standard Ahlswede–Csiszár secret-generation setting. There two terminals observe two correlated biometric sequences. It is their objective to form a common secret by interchanging a public message. This message should contain only a negligible amount of information about the secret, but, in addition, we require here that it should leak as little information as possible about the biometric data. For this first case, the fundamental tradeoff between the secret-key rate and the privacy-leakage rate will be determined. It should be noted that this result is in some way similar to and a special case of the secret-key (SK) part of Csiszár and Narayan [9, Th. 2.4].

The second setting that we consider is a biometric model with chosen keys, where the secret key is not generated by the terminals but chosen independently of biometric data at the encoder side and conveyed to the decoder. This model corresponds to key-binding, described in the overview paper of Jain *et al.* [20]. For the chosen-secret setting, we will also determine the fundamental secret-key versus privacy-leakage rate balance.

The other two biometric settings that we analyze correspond to biometric secrecy systems with zero privacy leakage. Ideally, biometric secrecy systems should leak a negligible amount of information not only on the secret but also on the biometric data. However, in order to be able to generate or convey large secret keys reliably, we have to send some data (helper data) to the second terminal. Without any precautions, the helper data leak a certain amount of information on the biometric data. In this way, biometrics solely may not always satisfy the security and privacy requirements of certain systems. However, the performance of biometric systems can be enhanced using standard cryptographic keys. Although this reduces user convenience since, e.g., extra cryptographic keys need to be stored on external media or memorized, such systems may offer a higher level of secrecy and privacy. Practical methods in this direction include attempts to harden the fuzzy vault scheme of Juels and Sudan [21] with passwords by Nandakumar *et al.* [29] and dithering techniques that were proposed by Buhan *et al.* [5].

In our models, we assume that only the two terminals have access to an extra independent private key, which is observed together with the correlated biometric sequences. The private key is used to achieve a negligible amount of privacy leakage (zero leakage). We investigate both the generated-secret model with zero leakage and the chosen-secret model with zero leakage. For both models, we will determine the tradeoff between the private-key rate and the resulting secret-key rate.

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

leakage are motivated by the fact that the helper data may provide more information on the pair of secret key and biometric data than on each of these entities separately.

### D. Modeling Assumptions on Biometric Data

In this paper, we assume that our biometric sequences (feature vectors) are discrete, independent and identically distributed (i.i.d.). Fingerprints and irises are typical examples of such biometric sources. A discrete representation of other biometric modalities can be obtained using quantization. The independence of biometric features is not unreasonable to assume, since principal components analysis, linear discriminant analysis, and other transformations, which are applied to biometric measurements during feature extraction (see Wayman *et al.* [41]), result in more or less independent features. In general, different components of biometric sequences may have different ranges of correlation. However, for reasons of simplicity, we will only discuss identically distributed biometric sequences here.

### E. Paper Organization

This paper is organized as follows. First, we start with an example demonstrating that time-sharing does not result in an optimal tradeoff between secret-key rate and privacy-leakage rate. In Section III, we continue with the formal definitions of all the eight models discussed above. In Section IV, we state the results that will be derived in this paper. We will determine the achievable regions for all the eight settings. The proofs of our results can be found in the Appendixes. Section V discusses the properties of the achievable regions that play a role here. In Section VI, we discuss the relations between the found achievable regions. In Section VII, we present the conclusions.

## II. An Example

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

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

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

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

$$\frac{I(U^{23};Y^{23})}{H(U^{23}|Y^{23})} = \frac{H(Y^{23}) - H(Y^{23}|U^{23})}{H(U^{23}) + H(Y^{23}|U^{23}) - H(Y^{23})} = \frac{23 - H(Y^{23}|U^{23})}{H(Y^{23}|U^{23}) - 11}. \quad (1)$$

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

$$\begin{aligned} H(Y^{23}|U^{23}) &\leq \sum_{n=1}^{23} H(Y_n|U_n) \\ &= 23h\left(p(1-q) + (1-p)q\right) \\ &= 23h(0.1992) \\ &= 16.5683 \end{aligned} \quad (2)$$

where we used that $p \triangleq \Pr\{X_n \neq U_n\} = 254/2048$, since we apply the Golay code as quantizer. If we substitute this upper bound into (1), we get a lower bound for the key-leakage ratio 1.1550, which improves upon the standard ratio of 1.1322. The exact key-leakage ratio is equal to 1.1925 and improves more upon the standard ratio of 1.1322.

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

## III. Eight Cases, Definitions

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

$$\Pr\left\{(X^N, Y^N) = (x^N, y^N)\right\} = \prod_{n=1}^{N} Q(x_n, y_n) \quad (3)$$

hence the source pairs $\{(X_n, Y_n), n = 1, 2, \ldots, N\}$ are independent of each other and identically distributed according to $Q(\cdot,\cdot)$.

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

We can subdivide systems into those in which both terminals are supposed to *generate* a secret (secret key) and systems in which a uniformly *chosen* secret (secret key) is bound to the biometric enrollment sequence $x^N$; see Jain *et al.* [20]. The generated or chosen secret $s$ assumes values in $\{1, 2, \ldots, |\mathcal{S}|\}$. The decoder's estimate $\widehat{s}$ of the secret $s$ also assumes values from $\{1, 2, \ldots, |\mathcal{S}|\}$. In chosen-secret systems, the secret $S$ is a uniformly distributed index; hence,

$$\Pr\{S = s\} = 1/|\mathcal{S}| \text{ for all } s \in \{1, 2, \ldots, |\mathcal{S}|\}. \tag{4}$$

Moreover, we can subdivide systems, according to the helper data requirements, into systems in which the helper data leak information about the biometric enrollment sequence $X^N$ and systems in which this leakage should be negligible. In the *zero-leakage* systems, both terminals have access to a private random key $p \in \{1, 2, \cdots, |\mathcal{P}|\}$. This key is uniformly distributed; hence,

$$\Pr\{P = p\} = 1/|\mathcal{P}| \text{ for all } p \in \{1, 2, \ldots, |\mathcal{P}|\}. \tag{5}$$

Finally, we consider two types of privacy leakage: a) unconditional leakage and b) conditional leakage. Unconditional leakage corresponds to bounding the mutual information $I(X^N; M)$, whereas conditional leakage corresponds to bounding the conditional mutual information $I(X^N; M|S)$. In general, conditional leakage does not imply unconditional leakage, and vice versa.

Next four systems—1) generated-secret systems, 2) chosen-secret systems, 3) generated-secret systems with zero leakage, and 4) chosen-secret systems with zero leakage—are investigated for both unconditional and conditional leakage. This results in eight biometric models.

### A. Generated-Secret Systems

In a biometric generated-secret system (see Fig. 1), the encoder observes the biometric enrollment sequence $X^N$ and produces a secret $S$ and helper data $M$; hence,

$$(S, M) = e(X^N) \tag{6}$$

where $e(\cdot)$ is the encoder mapping. The helper data $M$ are sent to the decoder, which observes the biometric authentication sequence $Y^N$. This decoder now forms an estimate $\widehat{S}$ of the secret $S$ that was generated by the encoder; hence,

$$\widehat{S} = d(Y^N, M) \tag{7}$$

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

We will now define two types of achievability for biometric generated-secret systems. The first one corresponds to unconditional leakage and the second to conditional leakage. These definitions allow us to find out what secret-key rates and privacy-leakage rates can be jointly realized with negligible error probability $\Pr\{\widehat{S} \neq S\}$ and negligible secrecy-leakage rate. We are interested in secret-key rates as large as possible and privacy-leakage rates as small as possible.

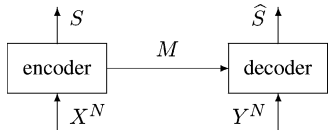



Fig. 1. Model for a biometric generated-secret system.

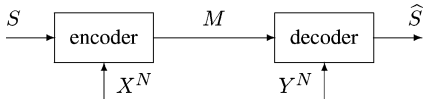



Fig. 2. Model for a biometric chosen-secret system.

*Definition 1:* A secret-key rate versus privacy-leakage rate pair $(R, L)$ with $R \geq 0$ is achievable in a biometric generated-secret setting in the unconditional case if, for all $\delta > 0$ for all $N$ large enough, there exist encoders and decoders such that[2]

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta \\ H(S) + N\delta \geq \log|\mathcal{S}| &\geq N(R - \delta) \\ I(S; M) &\leq N\delta \\ I(X^N; M) &\leq N(L + \delta). \end{aligned} \tag{8}$$

In the conditional case, we replace the last inequality by

$$I(X^N; M|S) \leq N(L + \delta). \tag{9}$$

Moreover, let $\mathcal{R}_{\mathrm{g}}^{\mathrm{u}}$ and $\mathcal{R}_{\mathrm{g}}^{\mathrm{c}}$ be the regions of all achievable secret-key rate versus privacy-leakage rate pairs for generated-secret systems in the unconditional case and conditional case, respectively.

### B. Chosen-Secret Systems

In a biometric chosen-secret (key-binding) system (see Fig. 2), a secret $S$ is chosen uniformly and independently of the biometric sequences; see (4). The encoder observes the biometric enrollment source sequence $X^N$ and the secret $S$ and produces helper data $M$; hence,

$$M = e(S, X^N) \tag{10}$$

where $e(\cdot, \cdot)$ is the encoder mapping. The public helper data $M$ are sent to the decoder that also observes the biometric authentication sequence $Y^N$. This decoder forms an estimate $\widehat{S}$ of the chosen secret; hence,

$$\widehat{S} = d(M, Y^N) \tag{11}$$

and $d(\cdot, \cdot)$ is the decoder mapping. Again we have two types of achievability.

*Definition 2:* In a biometric chosen-secret system, a secret-key rate versus privacy-leakage rate pair $(R, L)$ with $R \geq 0$ is achievable in the unconditional case if, for all $\delta > 0$

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

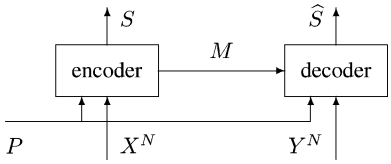



Fig. 3. Model for a biometric generated-secret system with zero-leakage.

for all $N$ large enough, there exist encoders and decoders such that

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta \\ \log|\mathcal{S}| &\geq N(R-\delta) \\ I(S;M) &\leq N\delta \\ I(X^N;M) &\leq N(L+\delta). \end{aligned} \tag{12}$$

In the conditional case, we replace the last inequality by

$$I(X^N;M|S) \leq N(L+\delta). \tag{13}$$

Moreover, let $\mathcal{R}_{\mathrm{c}}^{\mathrm{u}}$ and $\mathcal{R}_{\mathrm{c}}^{\mathrm{c}}$ be the regions of all achievable secret-key rate versus privacy-leakage rate pairs for a chosen-secret system in the unconditional case and conditional case, respectively.

### C. Generated-Secret Systems With Zero Leakage

In a biometric generated-secret system with zero leakage (see Fig. 3), a private random key $P$ that is available to both the encoder and the decoder is uniformly distributed and independent of biometric sequences; see (5). The encoder observes the biometric enrollment sequence $X^N$ and the private key $P$ and produces a secret $S$ and helper data $M$; hence,

$$(S,M) = e(X^N,P) \tag{14}$$

where $e(\cdot,\cdot)$ is the encoder mapping. The helper data $M$ are sent to the decoder that also observes the biometric authentication sequence $Y^N$ and that has access to the private key $P$. This decoder now forms an estimate $\widehat{S}$ of the secret that was generated by the encoder; hence,

$$\widehat{S} = d(Y^N,P,M) \tag{15}$$

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

Next we define achievability for zero-leakage systems. This definition allows us to find out what secret-key rates and private-key rates can be jointly realized with negligible error probability $\Pr\{\widehat{S} \neq S\}$ and negligible secrecy- and privacy-leakage rates. Note that now we are interested in secret-key rates as large as possible and private-key rates as small as possible.

*Definition 3:* In a biometric generated-secret system with zero leakage, a secret-key rate versus private-key rate pair $(R,K)$ with $R \geq 0$ is achievable in the unconditional case if, for all $\delta > 0$ for all $N$ large enough, there exist encoders and decoders such that

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta \\ H(S) + N\delta \geq \log|\mathcal{S}| &\geq N(R-\delta) \\ \log|\mathcal{P}| &\leq N(K+\delta) \\ I(S;M) + I(X^N;M) &\leq N\delta. \end{aligned} \tag{16}$$

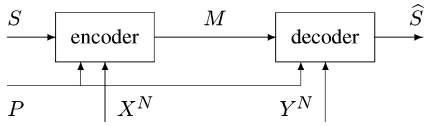



Fig. 4. Model of a chosen-secret system with zero leakage.

In the conditional case, we replace the last inequality by

$$I(S,X^N;M) \leq N\delta. \tag{17}$$

Moreover, let $\mathcal{R}_{\mathrm{zg}}^{\mathrm{u}}$ and $\mathcal{R}_{\mathrm{zg}}^{\mathrm{c}}$ be the regions of all secret-key rate versus private-key rate pairs $(R,K)$ for generated-secret systems with zero leakage in the unconditional case and conditional case, respectively.

### D. Chosen-Secret Systems With Zero Leakage

In a biometric chosen-secret system with zero leakage (see Fig. 4), a private random key $P$ that is available to both the encoder and the decoder is uniformly distributed and independent of biometric sequences; see (5). Moreover, a chosen secret $S$ that is to be conveyed by encoder to the decoder is also uniformly distributed; see (4).

The encoder observes the biometric enrollment sequence $X^N$, the private key $P$, and the secret $S$, and forms helper data $M$. Hence,

$$M = e(S,X^N,P) \tag{18}$$

where $e(\cdot,\cdot,\cdot)$ is the encoder mapping. The helper data $M$ are sent to the decoder that also observes the biometric authentication sequence $Y^N$ and that has access to the private key $P$. This decoder now forms an estimate $\widehat{S}$ of the secret that was chosen by the encoder; hence,

$$\widehat{S} = d(Y^N,P,M) \tag{19}$$

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

*Definition 4:* In a biometric chosen-secret system with zero leakage, a secret-key rate versus private-key rate pair $(R,K)$ with $R \geq 0$ is achievable in the unconditional case if, for all $\delta > 0$ for all $N$ large enough, there exist encoders and decoders such that

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta \\ \log|\mathcal{S}| &\geq N(R-\delta) \\ \log|\mathcal{P}| &\leq N(K+\delta) \\ I(S;M) + I(X^N;M) &\leq N\delta. \end{aligned} \tag{20}$$

In the conditional case, we replace the last inequality by

$$I(S,X^N;M) \leq N\delta. \tag{21}$$

Moreover, let $\mathcal{R}_{\mathrm{zc}}^{\mathrm{u}}$ and $\mathcal{R}_{\mathrm{zc}}^{\mathrm{c}}$ be the regions of all secret-key rate versus private-key rate pairs $(R,K)$ for a chosen-secret system with zero leakage in the unconditional case and conditional case, respectively.

## IV. Statement of Results

In order to state our results, we first define the regions $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and $\mathcal{R}_4$. Then we present the eight theorems.

$$\begin{aligned}\mathcal{R}_1 \triangleq \{(R,L):&0 \le R \le I(U;Y),\\ &L \ge I(U;X) - I(U;Y),\\ &\text{for} \quad P(u,x,y) = Q(x,y)P(u|x)\} \quad (22)\end{aligned}$$

$$\begin{aligned}\mathcal{R}_2 \triangleq \{(R,L):&0 \le R \le I(U;Y),\\ &L \ge I(U;X),\\ &\text{for} \quad P(u,x,y) = Q(x,y)P(u|x)\} \quad (23)\end{aligned}$$

$$\begin{aligned}\mathcal{R}_3 \triangleq \{(R,K):&0 \le R \le I(U;Y) + K\\ &K \ge I(U;X) - I(U;Y),\\ &\text{for} \quad P(u,x,y) = Q(x,y)P(u|x)\}. \quad (24)\end{aligned}$$

Consider, e.g., region $\mathcal{R}_1$. The definition of region $\mathcal{R}_1$ states that it is a union of elementary regions $\{(R,L) : 0 \le R \le I(U;Y), L \ge I(U;X) - I(U;Y)\}$, one for each so-called test channel $\{P(u|x), x \in \mathcal{X}, u \in \mathcal{U}\}$. Note that each test channel specifies the auxiliary alphabet $\mathcal{U}$ and the mutual information $I(U;X)$ and $I(U;Y)$. The union is now over all such test channels. In Appendix A, it is shown that the cardinality of the auxiliary random variable $U$ need not be larger than $|\mathcal{X}|+1$. This result also applies to regions $\mathcal{R}_2$ and $\mathcal{R}_3$.

The definition of the last region does not involve an auxiliary random variable

$$\mathcal{R}_4 \triangleq \{(R,K) : 0 \le R \le K\}. \quad (25)$$

*Theorem 1 (Generated Secret, Unconditional):*

$$\mathcal{R}_{\mathrm{g}}^{\mathrm{u}} = \mathcal{R}_1. \quad (26)$$

*Theorem 2 (Generated Secret, Conditional):*

$$\mathcal{R}_{\mathrm{g}}^{\mathrm{c}} = \mathcal{R}_1. \quad (27)$$

*Theorem 3 (Chosen Secret, Unconditional):*

$$\mathcal{R}_{\mathrm{c}}^{\mathrm{u}} = \mathcal{R}_1. \quad (28)$$

*Theorem 4 (Chosen Secret, Conditional):*

$$\mathcal{R}_{\mathrm{c}}^{\mathrm{c}} = \mathcal{R}_2. \quad (29)$$

*Theorem 5 (Zero-Leakage Generated Secret, Unconditional):*

$$\mathcal{R}_{\mathrm{zg}}^{\mathrm{u}} = \mathcal{R}_3. \quad (30)$$

*Theorem 6 (Zero-Leakage Generated Secret, Conditional):*

$$\mathcal{R}_{\mathrm{zg}}^{\mathrm{c}} = \mathcal{R}_3. \quad (31)$$

*Theorem 7 (Zero-Leakage Chosen Secret, Unconditional):*

$$\mathcal{R}_{\mathrm{zc}}^{\mathrm{u}} = \mathcal{R}_3. \quad (32)$$

*Theorem 8 (Zero-Leakage Chosen Secret, Conditional):*

$$\mathcal{R}_{\mathrm{zc}}^{\mathrm{c}} = \mathcal{R}_4. \quad (33)$$

The proofs of these theorems are given in Appendix B.

## V. Properties of the Regions $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and $\mathcal{R}_4$

### A. Convexity

Note that $\mathcal{R}_1$ is convex. To see this, observe that if $(R_i, L_i) \in \mathcal{R}_1$ for $i = 1, 2$, there exists $U_i$ such that $U_i - X - Y$, and $R_i \le I(U_i;Y)$ and $L_i \ge I(U_i;X) - I(U_i;Y)$. Now let $0 < \alpha < 1$, and define a time-sharing variable $T \in \{1,2\}$, which is one with probability $\alpha$ and two with probability $\overline{\alpha} \triangleq 1-\alpha$. Construct the new auxiliary random variable $U \triangleq (T, U_T)$ and then observe that $U - X - Y$ and

$$\begin{aligned}\alpha R_1 + \overline{\alpha} R_2 &\le \alpha I(U_1;Y) + \overline{\alpha} I(U_2;Y)\\ &= H(Y) - \alpha H(Y|U_1) - \overline{\alpha} H(Y|U_2)\\ &= H(Y) - H\left(Y|(U_T,T)\right) = I(U;Y) \quad (34)\end{aligned}$$

and

$$\begin{aligned}\alpha L_1 + \overline{\alpha} L_2 &\ge \alpha\left[I(U_1;X) - I(U_1;Y)\right]\\ &\quad + \overline{\alpha}\left[I(U_2;X) - I(U_2;Y)\right]\\ &= H(X) - H(Y) - H\left(X|(U_T,T)\right)\\ &\quad + H\left(Y|(U_T,T)\right)\\ &= I(U;X) - I(U;Y). \quad (35)\end{aligned}$$

From the above expressions, we conclude that $\alpha(R_1, L_1) + \overline{\alpha}(R_2, L_2) \in \mathcal{R}_1$, and hence $\mathcal{R}_1$ is convex. In a similar way, we can show that $\mathcal{R}_2$ and $\mathcal{R}_3$ are convex. The proof that $\mathcal{R}_4$ is convex is straightforward.

### B. Achievability of Special Points

By setting $U \equiv X$ in the definitions of the regions $\mathcal{R}_1$, $\mathcal{R}_2$, and $\mathcal{R}_3$, we obtain the achievability of the pairs

$$\begin{aligned}(R,L) &= (I(X;Y), H(X|Y))\\ (R,L) &= (I(X;Y), H(X))\\ (R,K) &= (H(X), H(X|Y)) \quad (36)\end{aligned}$$

in region $\mathcal{R}_1$, region $\mathcal{R}_2$, and region $\mathcal{R}_3$, respectively.

Observe that $I(X;Y)$ is the largest possible secret-key rate for regions $\mathcal{R}_1$ and $\mathcal{R}_2$, which is the Ahlswede–Csiszár secrecy capacity [1], since $I(U;Y) \le I(U,X;Y) = I(X;Y)$. This immediately follows from the Markovity $U - X - Y$.

Observe also that the largest possible secret-key rate for region $\mathcal{R}_3$ is $H(X)$, which is the common randomness capacity studied in Ahlswede and Csiszár [2].

Lastly, note that for $(R,L) \in \mathcal{R}_2$, we may conclude that $R \le L$. This is a consequence of $R \le I(U;Y) \le I(U;X,Y) = I(U;X) \le L$, which follows from $U - X - Y$.

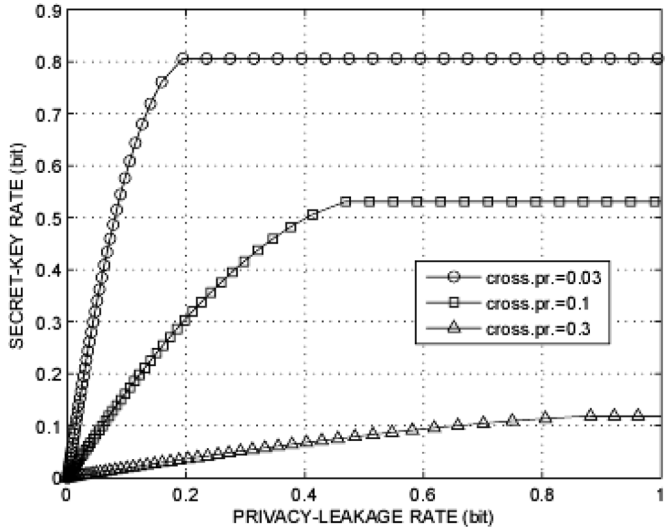



Fig. 5. Secret-key rate versus privacy-leakage rate function $R_1(\cdot)$ for three values of the crossover probability $q$.

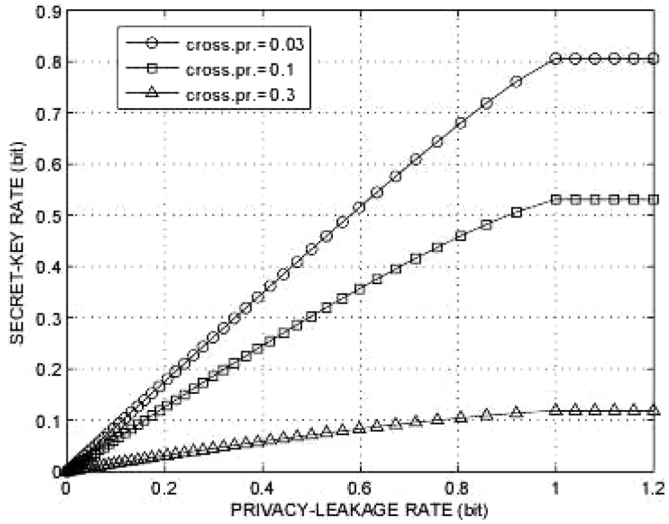



Fig. 6. Secret-key rate versus privacy-leakage rate function $R_2(\cdot)$ for three values of the crossover probability $q$.

### C. Example: Binary Symmetric Double Source

To illustrate the (optimal) tradeoff between the secret-key rate and the privacy-leakage rate, and the secret-key rate and the private-key rate, we consider a binary symmetric double source with crossover probability $0 \leq q \leq 1/2$; hence $Q(x,y) = (1-q)/2$ for $y = x$ and $Q(x,y) = q/2$ for $y \neq x$. For such a source

$$\begin{aligned} I(U;Y) &= 1 - H(Y|U) \\ I(U;X) - I(U;Y) &= H(Y|U) - H(X|U). \end{aligned} \tag{37}$$

Mrs. Gerber's lemma by Wyner and Ziv [43] tells us that if $H(X|U) = v$, then $H(Y|U) \geq h(q * h^{-1}(v))$, where $h(a) \triangleq -a\log(a) - (1-a)\log(1-a)$ is the binary entropy function, $a * b \triangleq a(1-b) + (1-a)b$, and $0 \leq h^{-1}(v) \leq 1/2$. If now $p$ is such that $h(p) = v$, then $H(X|U) = h(p)$ and $H(Y|U) \geq h(q * p)$. For binary symmetric $(U,X)$ with crossover probability $p$, the minimum $H(Y|U)$ is achieved and, consequently, using definition

$$R_j(r) \triangleq \max\{R : (R,r) \in \mathcal{R}_j\} \text{ for } j = 1,2,3,4 \tag{38}$$

we obtain the secret-key versus privacy-leakage rate function

$$R_1(L) = 1 - h(p * q) \tag{39}$$

for $p$ satisfying $h(p * q) - h(p) = L$. We have computed the secret-key rate versus privacy-leakage rate function $R_1(\cdot)$ for crossover probabilities $q = 0.03, 0.1$, and $0.3$ using (39) and plotted the results in Fig. 5. From this figure, we can conclude that for small $q$, the secret-key rate is large compared to the privacy-leakage rate, while for large $q$, the secret-key rate is smaller than the privacy-leakage rate. Note that this function applies to generated-secret systems and to chosen-secret systems in the unconditional case.

For the chosen-secret system in the conditional case, we obtain the corresponding secret-key versus privacy-leakage rate function

$$R_2(L) = 1 - h(p * q) \tag{40}$$

for $p$ satisfying $1 - h(p) = L$. The corresponding results for crossover probabilities $q = 0.03, 0.1$, and $0.3$ are plotted in Fig. 6. Note that now the secret-key rate cannot be larger than the privacy-leakage rate.

For generated-secret systems with zero leakage and for chosen-secret systems with zero leakage in the unconditional case, it follows that the corresponding secret-key versus private-key rate function takes the form

$$R_3(K) = 1 - h(p) \tag{41}$$

for $p$ satisfying $h(p * q) - h(p) = K$. We have computed the secret-key versus private-key rate function for crossover probabilities $q = 0.03, 0.1$, and $0.3$ using (42). The results are plotted in Fig. 7. From this figure, we can observe that the private-key rate $K$ is never larger than the secret-key rate $R$.

Lastly, for chosen-secret systems with zero leakage in the conditional case, we obtain

$$R_4(K) = K. \tag{42}$$

This function indicates that the biometric sequences are useless in this setting.

## VI. Relations Between Regions

### A. Overview

In Fig. 8, we summarize our results on the achievable regions obtained for all eight considered settings. The region pairs are given for models with unconditional and conditional privacy leakage.

Looking at Fig. 8, we can see that for models with generated secret keys, we obtain the same achievable regions in both unconditional and conditional cases. However, when chosen secret

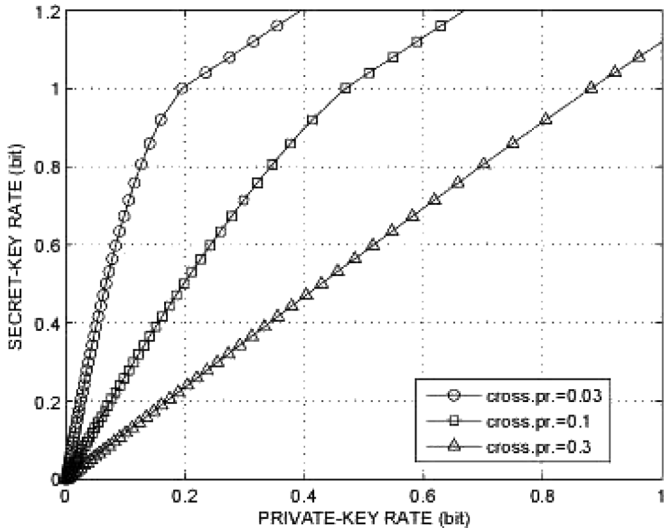



Fig. 7. Secret-key rate versus private-key rate function $\mathcal{R}_3(\cdot)$ for three values of the crossover probability $q$.

| | Generated keys | Chosen keys |
|---|---|---|
| Models with leakage | $\mathcal{R}_1/\mathcal{R}_1$ | $\mathcal{R}_1/\mathcal{R}_2$ |
| Models with zero-leakage | $\mathcal{R}_3/\mathcal{R}_3$ | $\mathcal{R}_2/\mathcal{R}_4$ |

Fig. 8. Region overview. By a slash (/) we separate the regions for models with unconditional and conditional privacy leakage.

keys are used, then, depending on the type of leakage, i.e., unconditional or conditional leakage, we obtain different pair of regions.

Consider first the models with privacy leakage. It is easy to see that, since in a generated-secret model $S$ is a function of $X^N$, we have that $I(X^N;M|S) \approx I(X^N;M)$. Therefore, the achievable regions for generated-secret models in the unconditional and conditional cases are the same.

Now if we look at a chosen-secret model in the unconditional and conditional case, we see that $I(X^N;M) = I(S,X^N;M) - I(S;M|X^N) = I(S;M) + I(X^N;M|S) - I(S;M|X^N)$. Then, since we require $I(S;M) \approx 0$ and since $I(S;M|X^N) \geq 0$, we see that $I(X^N;M|S)$ cannot be significantly smaller than $I(X^N;M)$. This explains that the achievable region in the conditional case cannot be larger than the achievable region in the unconditional case.

It is also intuitively clear why, in the conditional case, privacy leakage for chosen-secret models is larger than privacy leakage for generated-secret models. Note that in chosen-secret models, secret key $S_c$ is independent of $X^N$, and therefore information that a pair $(S_c, X^N)$ contains is larger than the information that a pair $(S_g, X^N)$ corresponding to generated-secret models contains. Next, note that to reliably convey $S_c$, $M_c$ should contain some information about both $S_c$ and $X^N$. Thus, in chosen-secret models, helper data $M_c$ also contain more information than the helper data $M_g$ in generated-secret models, i.e., $I(S_c, X^N; M_c) \geq I(S_g, X^N; M_g)$. Lastly, since in both models we require secrecy leakage to be negligible, we obtain that $I(X^N;M_c|S_c) \geq I(X^N;M_g|S_g)$. This also implies that in chosen-secret models, all the leakage "load" goes on biometrics.

Note that, since models with zero leakage are the extension of models with privacy leakage when we additionally use private key, also three of the four corresponding achievable regions are the same.

### B. Relation Between $\mathcal{R}_1$ and $\mathcal{R}_2$

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

$$\begin{aligned} R &\leq I(U;Y) \\ L &\geq I(U;X). \end{aligned} \tag{43}$$

Then also

$$\begin{aligned} R &\leq I(U;Y) \\ L - R &\geq I(U;X) - I(U;Y) \end{aligned} \tag{44}$$

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

### C. On $\mathcal{R}_3$ and Its Relation to $\mathcal{R}_1$

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

$$\begin{aligned} R &\leq I(U;Y) \\ L &\geq I(U;X) - I(U;Y). \end{aligned} \tag{45}$$

From these inequalities, it also follows that

$$\begin{aligned} R + L &\leq I(U;Y) + L \\ L &\geq I(U;X) - I(U;Y). \end{aligned} \tag{46}$$

Therefore, we may conclude that $(R+L, L) \in \mathcal{R}_3$.

Similarly, for each $(R,L) \in \mathcal{R}_3$, there exists an auxiliary random variable $U$ with $P(u,x,y) = Q(x,y)P(u|x)$ for which

$$\begin{aligned} R &\leq I(U;Y) + L \\ L &\geq I(U;X) - I(U;Y) \end{aligned} \tag{47}$$

and then, for $R - L \geq 0$, we obtain that

$$\begin{aligned} R - L &\leq I(U;Y) \\ L &\geq I(U;X) - I(U;Y) \end{aligned} \tag{48}$$

and consequently $(R-L, L) \in \mathcal{R}_1$.

Lastly, note that if $(R,K) \in \mathcal{R}_3$, there exists a $U$ as before, such that

$$\begin{aligned} R &\leq I(U;Y) + K \\ K &\geq I(U;X) - I(U;Y). \end{aligned} \tag{49}$$

Then for any $\alpha \geq 0$, we have

$$\begin{aligned} R + \alpha &\leq I(U;Y) + K + \alpha \\ K + \alpha &\geq I(U;X) - I(U;Y) \end{aligned} \tag{50}$$

and therefore $(R+\alpha, K+\alpha) \in \mathcal{R}_3$.

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

$$0 \leq R \leq I(U;X) + (K - (I(U;X) - I(U;Y))). \quad (51)$$

In this way, secret keys in models with achievable region $\mathcal{R}_3$ can be seen as a combination of common randomness (see Ahlswede and Csiszár [2]) and a part of a cryptographic (private) key that remains after masking the leakage. We may also conclude that biometrics can be used to increase cryptographic key size if both cryptographic and biometric keys are used in secrecy systems. Moreover, in this setting, a biometric key would guarantee the authenticity of a user, while in addition, a cryptographic key would guarantee zero-privacy leakage.

### D. On $\mathcal{R}_4$

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

$$0 \leq R \leq I(U;X) + (K - I(U;X)). \quad (52)$$

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

## VII. Conclusions and Remarks

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

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

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

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

Recall the key-leakage ratio discussed in the example in the Introduction. This ratio characterizes the slope of the boundary of the achievable regions found here. The higher the slope is, the better the tradeoff between the secret-key rate and the privacy-leakage rate is. It is not difficult to see that the slope corresponding to the Ahlswede–Csiszár [1] result is the smallest slope achievable in generated-secret systems; see also Fig. 5.

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

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

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

In practice, biometric features are often represented by continuous vectors, and therefore the fundamental results for biometric systems based on continuous Gaussian biometric data would be an interesting next step to consider. Note that our proofs make it easy to generalize our results to Gaussian biometric sources.

Lastly, we would like to mention that after writing this paper, the authors learned about recent results of Lai *et al.* [23] also on the privacy-secrecy tradeoff in biometric systems. Although there are some overlapping results (the two basic theorems), our investigations expand in the direction of extra private keys and conditional privacy leakage, while Lai *et al.* extended their basic results by considering side information models.

## Appendix A
## Bound on the Cardinality of $U$

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

$$\begin{aligned} \phi_x(P) &= P(x), \quad \text{for all but one } x \\ \phi_X(P) &= H_P(X) \\ \phi_Y(P) &= H_P(Y) \end{aligned} \quad (53)$$

where, in the last equation, we use $\Pr\{Y = y\} = \sum_x P(x)Q(y|x)$, where $Q(y|x) = Q(x,y)/\sum_y Q(x,y)$. By the Fenchel–Eggleston strengthening of the Caratheodory

lemma (see Wyner and Ziv [44]), there are $|\mathcal{X}|+1$ elements $P_u \in \mathcal{D}$ and $\alpha_u$ that sum to one, such that

$$\begin{aligned} Q(x) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_x(P_u), \quad \text{for all but one } x \\ H(X|U) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_X(P_u) \\ H(Y|U) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_Y(P_u). \end{aligned} \tag{54}$$

The entire probability distribution $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ and, consequently, the entropies $H(X)$ and $H(Y)$ are now specified, and therefore also both $I(U;X)$ and $I(U;Y)$ are. This implies that cardinality $|\mathcal{U}| = |\mathcal{X}|+1$ suffices for all three regions $\mathcal{R}_1$, $\mathcal{R}_2$, and $\mathcal{R}_3$.

## APPENDIX B
## PROOFS OF THEOREMS 1–8

The (basic) achievability proof for Theorem 1 is the most involved proof. Here we only outline its main idea; the complete proof is provided in Appendix C. The achievability proofs for the other seven theorems are based on this basic achievability proof. There this basic achievability proof is further extended by adding an extra layer in which the one-time pad is used to conceal a secret key in chosen-secret settings and helper data in zero-leakage systems. The converses for all theorems are quite standard.

### A. Proof of Theorem 1

It should be noted that Theorem 1 is in some ways similar to and a special case of Theorem 2.4 in Csiszár and Narayan [\cite{Narayan2000}], the SK-part, since for a deterministic encoder $I(X^N;M) = H(M) \leq \log|\mathcal{M}|$. Csiszár and Narayan considered a more general case with three terminals.

*1) Achievability Part of Theorem 1:* Although the complete proof can be found in Appendix C, we will give a short outline here. We start by fixing a conditional distribution $\{P(u|x), x \in \mathcal{X}, u \in \mathcal{U}\}$ that determines the joint distribution $P(u,x,y) = Q(x,y)P(u|x)$, for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $u \in \mathcal{U}$. Then we randomly generate roughly $2^{NI(U;X)}$ auxiliary sequences $u^N$. Each of these sequences gets a random $s$-label and a random $m$-label. These labels are uniformly chosen. The $s$-label can assume roughly $2^{NI(U;Y)}$ values, and the $m$-label roughly $2^{N(I(U;X)-I(U;Y))}$ values. The encoder, upon observing the enrollment sequence $x^N$, finds a sequence $u^N$ that is jointly typical with $x^N$. It outputs the $s$-label corresponding to this sequence as a secret key and sends the $m$-label corresponding to this $u^N$ as helper data to the decoder. The decoder observes the authentication sequence $y^N$ and determines the auxiliary sequence $\widehat{u^N}$ with an $m$-label matching with the helper data, such that $\widehat{u^N}$ and $y^N$ are jointly typical. It can be shown that the decoder can reliably recover $u^N$ and the corresponding secret-key label $s(u^N)$ now. It is easy to check that the unconditional leakage $I(X^N;M)$ is not larger than $I(U;X) - I(U;Y)$. An important additional property of the proof is that the auxiliary sequence $u^N$ can be recovered reliably from both the $s$-label and the $m$-label. Using this property, we can prove that $I(S;M)$ is negligible and that the secret $S$ is close to uniform.

*2) Converse Part of Theorem 1:* First, we consider the entropy of the secret key $S$. We use that $\widehat{S} = d(M, Y^N)$ and Fano's inequality $H(S|\widehat{S}) \leq F$, where $F \triangleq 1 + \Pr\{\widehat{S} \neq S\} \log|\mathcal{S}|$.

$$\begin{aligned} H(S) &= I(S;M,Y^N) + H(S|M,Y^N,\widehat{S}) \\ &\leq I(S;M,Y^N) + H(S|\widehat{S}) \\ &\leq I(S;M,Y^N) + F \\ &\leq I(S;M) + I(S,M;Y^N) + F \\ &= I(S;M) + \sum_{n=1}^{N} I(S,M;Y_n|Y^{n-1}) + F \\ &= I(S;M) + \sum_{n=1}^{N} I(S,M,Y^{n-1};Y_n) + F \\ &\leq I(S;M) + \sum_{n=1}^{N} I(S,M,X^{n-1};Y_n) + F \\ &= I(S;M) + NI(U;Y) + F. \end{aligned} \tag{55}$$

The last two steps require some attention. The last inequality in (55) results from $I(S,M,Y^{n-1};Y_n) \leq I(S,M,X^{n-1},Y^{n-1};Y_n) = I(S,M,X^{n-1};Y_n)$, since $Y^{n-1} - (S,M,X^{n-1}) - Y_n$. This Markovity follows from

$$\begin{aligned} &P(s,m,x^{n-1},y^{n-1},y_n) \\ &\quad = \sum_{x_{n+1}^N} \sum_{x_n} Q(x^{n-1})Q(x_n)Q\left(x_{n+1}^N\right) \\ &\qquad \cdot P(s,m|x^N)Q(y_n|x_n)Q(y^{n-1}|x^{n-1}) \\ &\quad = P(x^{n-1},s,m,y_n)Q(y^{n-1}|x^{n-1}) \\ &\quad = Q(x^{n-1})P(s,m,y_n|x^{n-1})Q(y^{n-1}|x^{n-1}) \end{aligned} \tag{56}$$

i.e., $Y^{n-1} - X^{n-1} - (S,M,Y_n)$. To obtain the last equality in (55), we first define $U_n \triangleq (S,M,X^{n-1})$. Then, if we take a time-sharing variable $T$ uniform over $\{1,2,\ldots,N\}$ and independent of all other variables and set $U \triangleq (U_n,n)$, $X \triangleq X_n$, and $Y \triangleq Y_n$ for $T = n$, we obtain

$$\begin{aligned} \sum_{n=1}^{N} I(S,M,X^{n-1};Y_n) &= \sum_{n=1}^{N} I(U_n;Y_n) \\ &= NI(U_T;Y_T|T) = NI((U_T,T);Y_T) \\ &= NI(U;Y). \end{aligned} \tag{57}$$

Finally, note that

$$\begin{aligned} &P(s,m,x^{n-1},x_n,y_n) \\ &\quad = \sum_{x_{n+1}^N} Q(x^{n-1})Q(x_n)Q\left(x_{n+1}^N\right) P(s,m|x^N)Q(y_n|x_n) \\ &\quad = Q(x_n)Q(y_n|x_n) \sum_{x_{n+1}^N} Q(x^{n-1})Q\left(x_{n+1}^N\right) P(s,m|x^N) \\ &\quad = Q(x_n)Q(y_n|x_n)P(s,m,x^{n-1}|x_n) \end{aligned} \tag{58}$$

and therefore $U_n - X_n - Y_n$ and consequently $U - X - Y$.

If we now assume that $(R, L)$ is achievable, then $F \leq 1 + \delta \log |\mathcal{S}|$, and we obtain that

$$\begin{aligned} R - \delta &\leq \frac{H(S)}{N} + \delta \\ &\leq \delta + I(U;Y) + 1/N + \delta \frac{\log |\mathcal{S}|}{N} + \delta \\ &\leq 2\delta + I(U;Y) + 1/N + \delta \log |\mathcal{X}| \end{aligned} \tag{59}$$

for some $P(u,x,y) = Q(x,y)P(u|x)$, where we have used that, possibly after renumbering, $|\mathcal{S}| \leq |\mathcal{X}|^N$.

Now we continue with the unconditional privacy leakage

$$\begin{aligned} I(X^N;M) &= H(M) - H(M|X^N) \\ &\geq H(M|Y^N) - H(S,M|X^N) \\ &= H(S,M|Y^N) - H(S|M,Y^N,\widehat{S}) \\ &\quad - H(S,M|X^N) \\ &\geq H(S,M|Y^N) - H(S|\widehat{S}) - H(S,M|X^N) \\ &\geq H(S,M|Y^N) - F - H(S,M|X^N) \\ &= I(S,M;X^N) - I(S,M;Y^N) - F \\ &= \sum_{n=1}^{N} I(S,M;X_n|X^{n-1}) \\ &\quad - \sum_{n=1}^{N} I(S,M;Y_n|Y^{n-1}) - F \\ &= \sum_{n=1}^{N} I(S,M,X^{n-1};X_n) \\ &\quad - \sum_{n=1}^{N} I(S,M,Y^{n-1};Y_n) - F \\ &\geq \sum_{n=1}^{N} I(S,M,X^{n-1};X_n) \\ &\quad - \sum_{n=1}^{N} I(S,M,X^{n-1};Y_n) - F \\ &= N\left(I(U;X) - I(U;Y)\right) - F \end{aligned} \tag{60}$$

for the joint distribution $P(u,x,y) = Q(x,y)P(u|x)$ mentioned before. For achievable $(R, L)$, we get, using $|\mathcal{S}| \leq |\mathcal{X}|^N$, that

$$\begin{aligned} L + \delta &\geq \frac{I(X^N;M)}{N} \\ &\geq I(U;X) - I(U;Y) - 1/N - \delta \frac{\log |\mathcal{S}|}{N} \\ &\geq I(U;X) - I(U;Y) - 1/N - \delta \log |\mathcal{X}|. \end{aligned} \tag{61}$$

If we now let $\delta \downarrow 0$ and $N \to \infty$, then we obtain the converse from both (59) and (61).

### B. Proof of Theorem 2

We prove Theorem 2 by showing that $\mathcal{R}_{\mathrm{g}}^{\mathrm{c}} = \mathcal{R}_{\mathrm{g}}^{\mathrm{u}}$. Therefore, first, assume that we have a code for the unconditional case, hence a code satisfying (8). For this code

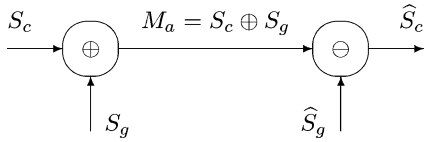



Fig. 9. The masking layer.

$$\begin{aligned} I(X^N;M|S) &= H(M|S) - H(M|S,X^N) \\ &\leq H(M) - H(M|X^N) \\ &= I(X^N;M) \leq N(L+\delta) \end{aligned} \tag{62}$$

hence $\mathcal{R}_{\mathrm{g}}^{\mathrm{c}} \supseteq \mathcal{R}_{\mathrm{g}}^{\mathrm{u}}$. On the other hand, if we have a code for the conditional case, hence a code satisfying (9), then

$$\begin{aligned} I(X^N;M) &= I(X^N,S;M) - I(S;M|X^N) \\ &= I(S;M) + I(X^N;M|S) \\ &\leq N\delta + N(L+\delta) = N(L+2\delta) \end{aligned} \tag{63}$$

which demonstrates that $\mathcal{R}_{\mathrm{g}}^{\mathrm{c}} \subseteq \mathcal{R}_{\mathrm{g}}^{\mathrm{u}}$, and hence $\mathcal{R}_{\mathrm{g}}^{\mathrm{c}} = \mathcal{R}_{\mathrm{g}}^{\mathrm{u}}$.

### C. Proof of Theorem 3

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

*1) Achievability Part of Theorem 3:* The achievability proof corresponding to Theorem 3 is based on the achievability proof of Theorem 1. The difference is that we use a so-called masking layer (see Fig. 9) that uses the generated secret $S_g$ in a one-time pad system to conceal the chosen secret $S_c$. Such a masking layer was also used by Ahlswede and Csiszár [1]. The operations in the masking layer are simple. Denote by $\oplus$ addition modulo $|\mathcal{S}|$ and by $\ominus$ subtraction modulo $|\mathcal{S}|$; then

$$\begin{aligned} M_a &= S_c \oplus S_g \\ \widehat{S}_t &= M_a \ominus \widehat{S}_g = S_c \oplus (S_g \ominus \widehat{S}_g) \end{aligned} \tag{64}$$

where $M_a$ should be considered as *additional* helper data.

Now keeping in mind that $S_c$ is uniform on $\{1, 2, \ldots, |\mathcal{S}|\}$ and independent of $X^N$, the generated secret $S_g$, and corresponding helper data $M_g$, we obtain

$$\begin{aligned} I(S_c;M_g,M_a) &= I(S_c;M_g,S_c \oplus S_g) \\ &= I(S_c;M_g) + I(S_c;S_c \oplus S_g|M_g) \\ &\leq H(S_c \oplus S_g) - H(S_c \oplus S_g|M_g,S_c) \\ &\leq \log |\mathcal{S}| - H(S_g|M_g,S_c) \\ &\leq \log |\mathcal{S}| - H(S_g) + I(S_g;M_g) \end{aligned} \tag{65}$$

and

$$\begin{aligned} I(X^N; M_g, M_a) &= I(X^N; M_g, S_c \oplus S_g) \\ &= I(X^N; M_g) + I(X^N; S_c \oplus S_g | M_g) \\ &\le I(X^N; M_g) + H(S_c \oplus S_g) \\ &\quad - H(S_c \oplus S_g | M_g, X^N, S_g) \\ &\le I(X^N; M_g) + \log|\mathcal{S}| \\ &\quad - H(S_c | M_g, X^N, S_g) \\ &= I(X^N; M_g) + \log|\mathcal{S}| - \log|\mathcal{S}| \\ &= I(X^N; M_g). \end{aligned} \tag{66}$$

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

$$\begin{aligned} H(S_g) + N\delta \ge \log|\mathcal{S}| &\ge N(R - \delta) \\ I(S_g; M_g) &\le N\delta \\ I(X^N; M_g) &\le N(L + \delta). \end{aligned} \tag{67}$$

Therefore, using the masking layer implies that $\widehat{S}_c = S_c$ if $\widehat{S}_g = S_g$, and thus $\Pr\{\widehat{S}_c \neq S_c\} \le \delta$, and

$$\begin{aligned} H(S_c) = \log|\mathcal{S}| &\ge N(R - \delta) \\ I(S_c; M_g, M_a) &\le 2N\delta \\ I(X^N; M_g, M_a) &\le N(L + \delta) \end{aligned} \tag{68}$$

and consequently secret-key rate versus privacy-leakage rate pairs $(R, L)$ that are achievable for generated-secret systems in the unconditional case are also achievable for chosen-secret systems in the unconditional case.

*2) Converse Part of Theorem 3:* As in the converse for generated-secret systems in the unconditional case

$$\log|\mathcal{S}| = H(S) \le I(S; M) + NI(U; Y) + F. \tag{69}$$

We use that $I(S, M, Y^{n-1}; Y_n) \le I(S, M, X^{n-1}; Y_n)$, since also here $Y^{n-1} - (S, M, X^{n-1}) - Y_n$ holds. As before, we define $U_n \triangleq (S, M, X^{n-1})$ and take a time-sharing variable $T$ uniform over $\{1, 2, \ldots, N\}$ and independent of all other variables, and we set $U \triangleq (U_n, n)$, $X \triangleq X_n$, and $Y \triangleq Y_n$ for $T = n$. Now again $U_n - X_n - Y_n$ and consequently $U - X - Y$ hold. Since for achievable $(R, L)$ we have that $F \le 1 + \delta \log|\mathcal{S}|$, we obtain from (69) that

$$R - \delta \le \frac{\log|\mathcal{S}|}{N} \le \frac{1}{1-\delta}\left(\delta + I(U; Y) + 1/N\right) \tag{70}$$

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

For the privacy leakage, we obtain as before

$$I(X^N; M) \ge N\left(I(U; X) - I(U; Y)\right) - F \tag{71}$$

for the joint distribution $P(u, x, y) = Q(x, y)P(u|x)$ mentioned above. For achievable $(R, L)$, we get

$$\begin{aligned} L + \delta &\ge \frac{I(X^N; M)}{N} \\ &\ge I(U; X) - I(U; Y) - 1/N - \delta\frac{\log|\mathcal{S}|}{N} \\ &\ge I(U; X) - I(U; Y) - 1/N \\ &\quad - \frac{\delta}{1-\delta}\left(\delta + I(U; Y) + 1/N\right) \end{aligned} \tag{72}$$

where we used (70) to obtain an upper bound for $(\log|\mathcal{S}|)/N$. If we now let $\delta \downarrow 0$ and $N \to \infty$, then (70) and (72) yield the converse.

### D. Proof of Theorem 4

*1) Achievability Part of Theorem 4:* The achievability part follows again from the basic achievability proof, used in conjunction with a masking layer, as in the achievability proof for Theorem 3. Now we investigate the conditional privacy leakage

$$\begin{aligned} I(X^N; M_g, M_a | S_c) &= I(X^N; M_g, S_c \oplus S_g | S_c) \\ &= I(X^N; M_g, S_g | S_c) = I(X^N; M_g, S_g) \\ &\le H(M_g) + H(S_g). \end{aligned} \tag{73}$$

From (102) of the basic achievability proof in Appendix C, it follows that by construction

$$\begin{aligned} H(M_g) &\le \log|\mathcal{M}| = N\left(I(U; X) - I(U; Y) + 8\epsilon\right) \\ H(S_g) &\le \log|\mathcal{S}| = N\left(I(U; Y) - 3\epsilon\right) \end{aligned} \tag{74}$$

and, therefore,

$$\frac{I(X^N; M_g, M_a | S_c)}{N} \le I(U; Y) + 5\epsilon. \tag{75}$$

This step justifies that $\mathcal{R}_2$ is achievable for chosen-secret systems in the conditional privacy-leakage case.

*2) Converse Part of Theorem 4:* First note that the part related to the secret-key entropy of the converse for Theorem 3 for chosen-secret systems in the unconditional case (70) also applies here.

Now we continue with the conditional privacy leakage

$$\begin{aligned} I(X^N; M | S) &= \sum_{n=1}^{N} I(M; X_n | S, X^{n-1}) \\ &= \sum_{n=1}^{N} I(S, M, X^{n-1}; X_n) \\ &= NI(U; X) \end{aligned} \tag{76}$$

for the joint distribution $P(u, x, y) = Q(x, y)P(u|x)$ that was defined in the secret-key entropy part of the converse for Theorem 3. For achievable $(R, L)$, we get

$$L + \delta \ge \frac{I(X^N; M | S)}{N} = I(U; X). \tag{77}$$

If we now let $\delta \downarrow 0$ and $N \to \infty$, then we obtain the converse from both (70) and (77).

### E. Proof of Theorem 5

*1) Achievability Part of Theorem 5:* We demonstrate achievability here by first showing that $\mathcal{R}_{\text{zg}}^{\text{u}} \supseteq \mathcal{R}_{\text{zg}}^{\text{c}}$. Assume that we have a code for the conditional privacy-leakage case, hence a code satisfying (17); then,

$$\begin{aligned} I(X^N;M)+I(S;M) &\le I(S,X^N;M)+I(S,X^N;M) \\ &\le N\delta + N\delta = 2N\delta \end{aligned} \tag{78}$$

and therefore $\mathcal{R}_{\text{zg}}^{\text{u}} \supseteq \mathcal{R}_{\text{zg}}^{\text{c}}$. In the achievability proof for Theorem 6, we will prove that $\mathcal{R}_{\text{zg}}^{\text{c}} \supseteq \mathcal{R}_3$ and therefore also $\mathcal{R}_{\text{zg}}^{\text{u}} \supseteq \mathcal{R}_3$.

*2) Converse Part of Theorem 5:* We need to prove here that $\mathcal{R}_{\text{zg}}^{\text{u}} \subseteq \mathcal{R}_3$. We start with the entropy of the secret

$$\begin{aligned} H(S) &= I(S;P,M,Y^N)+H(S|P,M,Y^N,\widehat{S}) \\ &\le I(S;P,M,Y^N)+H(S|\widehat{S}) \\ &\le I(S;P,M,Y^N)+F \\ &= I(S;M)+I(S;P|M)+I(S;Y^N|P,M)+F \\ &\le I(S;M)+H(P)+\sum_{n=1}^{N} I(S;Y_n|P,M,Y^{n-1})+F \\ &\le I(S;M)+\log|\mathcal{P}|+\sum_{n=1}^{N} I(S,P,M,X^{n-1};Y_n)+F \\ &= I(S;M)+\log|\mathcal{P}|+NI(U;Y)+F. \end{aligned} \tag{79}$$

We used that $I(S,P,M,Y^{n-1};Y_n) \le I(S,P,M,X^{n-1},Y^{n-1};Y_n) = I(S,P,M,X^{n-1};Y_n)$, since $Y^{n-1} - (S,P,M,X^{n-1}) - Y_n$. Moreover, we created $U = (U_T,T)$ with $U_n \triangleq (S,P,M,X^{n-1})$ and $T$ as before, resulting in $U - X - Y$. Since, possibly after renumbering, $|\mathcal{S}| \le |\mathcal{P}||\mathcal{X}|^N$, we obtain for achievable pairs $(R,K)$ that $F \le 1+\delta\log|\mathcal{S}| \le 1+\delta\log|\mathcal{P}|+\delta N\log|\mathcal{X}|$. Now

$$\begin{aligned} R-\delta &\le \frac{H(S)}{N}+\delta \\ &\le \delta+(1+\delta)(K+\delta)+I(U;Y)+1/N \\ &\quad +\delta\log|\mathcal{X}|+\delta. \end{aligned} \tag{80}$$

In a similar way, we find for the total leakage

$$\begin{aligned} &I(S;M)+I(X^N;M) \\ &\quad \ge I(X^N;M) \\ &\quad \ge H(M)-H(M,P|X^N) \\ &\quad \ge H(M)-H(P) \\ &\quad \ge H(M|Y^N,P)-H(S,M|X^N,P)-\log|\mathcal{P}| \\ &\quad = H(S,M|Y^N,P)-H(S|Y^N,P,M,\widehat{S}) \\ &\qquad -H(S,M|X^N,P)-\log|\mathcal{P}| \\ &\quad \ge H(S,M|Y^N,P)-F-H(S,M|X^N,P)-\log|\mathcal{P}| \\ &\quad = I(S,M;X^N|P)-I(S,M;Y^N|P)-\log|\mathcal{P}|-F \\ &\quad = I(S,P,M;X^N)-I(S,P,M;Y^N)-\log|\mathcal{P}|-F \\ &\quad = \sum_{n=1}^{N} I(S,P,M;X_n|X^{n-1})-\sum_{n=1}^{N} I(S,P,M;Y_n|Y^{n-1}) \\ &\qquad -\log|\mathcal{P}|-F \\ &\quad \ge \sum_{n=1}^{N} I(S,P,M,X^{n-1};X_n)-\sum_{n=1}^{N} I(S,P,M,X^{n-1};Y_n) \\ &\qquad -\log|\mathcal{P}|-F \\ &\quad = NI(U;X)-NI(U;Y)-\log|\mathcal{P}|-F. \end{aligned} \tag{81}$$

Now we get for achievable $(R,K)$, using $|\mathcal{S}| \le |\mathcal{P}||\mathcal{X}|^N$, that

$$\delta \ge I(U;X)-I(U;Y)-(1+\delta)(K+\delta)-1/N-\delta\log|\mathcal{X}| \tag{82}$$

for $P(u,x,y)$ as before.

If we now let $\delta \downarrow 0$ and $N \to \infty$, the converse follows from (80) and (82).

### F. Proof of Theorem 6

In the previous sections, we have seen that $\mathcal{R}_3 \supseteq \mathcal{R}_{\text{zg}}^{\text{u}} \supseteq \mathcal{R}_{\text{zg}}^{\text{c}}$. To prove Theorem 6, we therefore only need to show that $\mathcal{R}_{\text{zg}}^{\text{c}} \supseteq \mathcal{R}_3$. This is done by the following achievability proof.

*1) Achievability Part of Theorem 6:* The achievability proof is an adapted version of the basic achievability proof for generated-secret systems that appears in Appendix C. The first difference is that the secret $S'$ is now the index of $u^N$. This results in a secret-key rate that is $I(U;X)+4\epsilon$ and a helper rate that is equal to $I(U;X)-I(U;Y)+8\epsilon$. Moreover, the helper data $M_g$ are made completely uninformative in a one-time-pad way, using a private key uniform over $|\mathcal{M}|$, the alphabet size of the helper data $M_g$. This results in modified helper data $M_m = M_g \oplus P$, where $\oplus$ denotes addition modulo $|\mathcal{M}|$. Thus, the private-key rate becomes equal to $I(U;X)-I(U;Y)+8\epsilon$.

Now, for the total leakage, we can write

$$\begin{aligned} I(X^N,S';M_m) &= I(X^N,S';M_g\oplus P) \\ &\le \log|\mathcal{M}|-H(M_g\oplus P|X^N,S') \\ &= \log|\mathcal{M}|-H(P|M_g,X^N,S')=0. \end{aligned} \tag{83}$$

The uniformity of the secret $S'$ can be demonstrated using the method described in Appendix C, since $H(I)$ can be lower bounded using (106). This argument demonstrated the achievability of $(R,K)=(I(U;X),I(U;X)-I(U;Y))$.

Achievable regions for generated-secret systems with zero leakage have the property that if an achievable pair $(R,K)$ belongs to it, then also $(R+k,K+k)$ does, for $k \ge 0$. The reason for this is that extra private-key rate $k$ can always be used as extra secret-key rate $k$. This property now demonstrates the achievability of all other pairs of rates in $\mathcal{R}_3$ if we set $k = K-I(U;X)+I(U;Y)$.

Observe that the method proposed here is very similar to the common randomness proof that was given in [2]. The difference is that here, the helper data are masked.

### G. Proof of Theorem 7

*1) Achievability Part of Theorem 7:* We use a masking layer on top of the scheme that demonstrates achievability for Theorem 6. This masking layer combines the chosen secret $S_c$ and

the generated secret $S_g$ into the additional helper $M_a \triangleq S_g \oplus S_c$, where the addition is modulo $|\mathcal{S}|$, the cardinality of the alphabet for the generated secret $S_g$. Now we obtain

$$\begin{aligned} I(X^N; M_m, M_a) &= I(X^N; M_g \oplus P, S_g \oplus S_c) \\ &= I(X^N; M_g \oplus P) \\ &\quad + I(X^N; S_g \oplus S_c | M_g \oplus P) \\ &= 0 \end{aligned} \tag{84}$$

and

$$\begin{aligned} I(S_c; M_m, M_a) &= I(S_c; M_g \oplus P, S_g \oplus S_c) \\ &= I(S_c; S_g \oplus S_c) + I(S_c; M_g \oplus P | S_g \oplus S_c) \\ &= H(S_g \oplus S_c) - H(S_g \oplus S_c | S_c) + 0 \\ &= \log |\mathcal{S}| - H(S_g) \\ &\leq N\delta \end{aligned} \tag{85}$$

where the last step follows from achievability for the case of generated-secret systems with zero leakage.

*2) Converse Part of Theorem 7:* The part of this converse related to the secret-key rate is similar to the secret-key-rate part of the converse given for Theorem 5. It first leads to (79), from which we conclude that, since $H(S) = \log |\mathcal{S}|$, for achievable $(R, K)$ it holds that

$$\frac{\log |\mathcal{S}|}{N} \leq \delta + K + \delta + I(U;Y) + 1/N + \delta \frac{\log |\mathcal{S}|}{N}. \tag{86}$$

Consequently, we obtain

$$R - \delta \leq \frac{\log |\mathcal{S}|}{N} \leq \frac{1}{1-\delta} \left(2\delta + K + I(U;Y) + 1/N\right). \tag{87}$$

Next we concentrate on the privacy-leakage rate part

$$\begin{aligned} & I(S;M) + I(X^N;M) \\ &\quad \geq I(X^N;M) \\ &\quad \geq H(M) - H(S,P,M|X^N) \\ &\quad = I(X^N;S,P,M) - H(S,P|M) \\ &\quad \geq I(X^N;S,P,M) - H(P) - H(S|M,P) \\ &\qquad + H(S|M,P,Y^N,\widehat{S}) - F \\ &\quad = I(X^N;S,P,M) - H(P) - I(Y^N;S|M,P) - F \\ &\quad \geq I(X^N;S,P,M) - \log |\mathcal{P}| - I(Y^N;S,P,M) - F \\ &\quad = NI(U;X) - NI(U;Y) - \log |\mathcal{P}| - F \end{aligned} \tag{88}$$

as before. For achievable $(R, K)$, this results in

$$\delta \geq I(U;X) - I(U;Y) - K - \delta - 1/N - \delta \frac{\log |\mathcal{S}|}{N} \tag{89}$$

for $P(u,x,y) = Q(x,y)P(u|x)$. Here $(\log |\mathcal{S}|)/N$ can be bounded using (87).

Now if we let $\delta \downarrow 0$ and $N \to \infty$, then (80) and (89) yield the converse.

### H. Proof of Theorem 8

*1) Achievability Part of Theorem 8:* The achievability follows immediately if we note that the private key can be used to mask the chosen key in a one-time-pad manner. Observe that we do not use the biometric sequences in any way.

*2) Converse Part of Theorem 8:* We start with the entropy of the secret

$$\begin{aligned} \log |\mathcal{S}| &= H(S) \\ &= I(S;P,M,Y^N) + H(S|P,M,Y^N,\widehat{S}) \\ &\leq I(S;P,M,Y^N) + H(S|\widehat{S}) \\ &\leq I(S;P,M,Y^N) + F \\ &= I(S;Y^N) + I(S;M|Y^N) + I(S;P|Y^N,M) + F \\ &\leq I(S,Y^N;M) + H(P) + F \\ &\leq I(S,X^N;M) + \log |\mathcal{P}| + F. \end{aligned} \tag{90}$$

The fourth inequality is based on $I(S,Y^N;M) \leq I(S,X^N,Y^N;M) = I(S,X^N;M)$ since $Y^N - X^N$, $S - M$. Then for achievable pairs $(R,K)$, since $F \leq 1 + \delta \log |\mathcal{S}|$, we have that

$$R - \delta \leq \frac{\log |\mathcal{S}|}{N} \leq \frac{1}{1-\delta}(\delta + K + \delta + 1/N). \tag{91}$$

If we let $\delta \downarrow 0$ and $N \to \infty$, then we conclude from (91) that $R \leq K$, which finishes the converse.

## APPENDIX C
## BASIC ACHIEVABILITY PROOF

We start our achievability proof by fixing the auxiliary alphabet $\mathcal{U}$ and the conditional probabilities $\{P(u|x), u \in \mathcal{U}, x \in \mathcal{X}\}$ and $0 < \epsilon < 1$. Now $P(u,x,y) = Q(x,y)P(u|x)$, for all $u \in \mathcal{U}, x \in \mathcal{X}, y \in \mathcal{Y}$. Note that $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ is the distribution of the biometric source.

Our achievability proof is based on weak typicality, a concept introduced by Forney [18] and further developed by Cover and Thomas [7]. We will first give a definition of weak typicality. After that, we will define a modified typical set that allows us to obtain a weak-typicality alternative for the so-called Markov lemma that holds for the strong-typicality case; see Berger [4]. Strong typicality was first considered by Wolfowitz [42], but since then, several alternative versions have been proposed; see Berger [4] but also Csiszár and Korner [8] and Cover and Thomas [7]. The main advantage of weak typicality is that the results in principle also hold for nondiscrete random variables. Therefore, our proof generalizes, e.g., to the Gaussian case.

### A. Definition and Properties of $\mathcal{A}_\epsilon^{(N)}$ and $\mathcal{B}_\epsilon^{(N)}$

*Definition 1:* Let $K$ be a positive integer. The set $\mathcal{A}_\epsilon^{(N)}(X_1X_2\cdots X_K)$ of $\epsilon$-typical $N$-sequences[3] $(\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_K)$ with respect to $P(x_1, x_2, \ldots, x_K)$ is, as in Cover and Thomas [7, Sec. 15.2], defined as

$$\begin{aligned} &\mathcal{A}_\epsilon^{(N)}(X_1X_2\cdots X_K) \\ &\quad \triangleq \left\{(\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_K) : \left| \frac{1}{N} \log \frac{1}{P(\underline{v})} - H(V) \right| \leq \epsilon, \right. \\ &\qquad \left. \forall V \subseteq \{X_1, X_2, \ldots, X_K\} \right\} \end{aligned} \tag{92}$$

[3]To get a more compact notation, we use here $\underline{x}$ instead of $x^N$, etc.

where $P(\underline{v}) = \prod_{n=1}^{N} P(v_n)$. Moreover, for given $\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{K-1}$, we define

$$\mathcal{A}_\epsilon^{(N)}(X_K|\underline{x}_1,\ldots,\underline{x}_{K-1}) \triangleq \Big\{\underline{x}_K : (\underline{x}_1,\ldots,\underline{x}_{K-1},\underline{x}_K) \in \mathcal{A}_\epsilon^{(N)}(X_1X_2\cdots X_K)\Big\}. \tag{93}$$

*Definition 2:* Consider typicality with respect to distribution $\{P(u,x,y) = Q(x,y)P(u|x), u \in \mathcal{U}, x \in \mathcal{X}, y \in \mathcal{Y}\}$. Now the set $\mathcal{B}_\epsilon^{(N)}(UX)$ is defined as

$$\mathcal{B}_\epsilon^{(N)}(UX) \triangleq \Big\{(\underline{u},\underline{x}) : \Pr\Big\{\underline{Y} \in \mathcal{A}_\epsilon^{(N)}(Y|\underline{u},\underline{x})| (\underline{U},\underline{X}) = (\underline{u},\underline{x})\Big\} \geq 1-\epsilon\Big\} \tag{94}$$

where $\underline{Y}$ is the output of a "memoryless channel" $Q(y|x) = Q(x,y)/Q(x)$ for $Q(x) = \sum_y Q(x,y)$, whose input is $\underline{x}$. Moreover, $\mathcal{B}_\epsilon^{(N)}(U|\underline{x}) \triangleq \{\underline{u} : (\underline{u},\underline{x}) \in \mathcal{B}_\epsilon^{(N)}(UX)\}$ for all $\underline{x}$.

*Property 1:* If $(\underline{u},\underline{x}) \in \mathcal{B}_\epsilon^{(N)}(UX)$, then also $(\underline{u},\underline{x}) \in \mathcal{A}_\epsilon^{(N)}(UX)$.

This follows from the fact that $(\underline{u},\underline{x}) \in \mathcal{B}_\epsilon^{(N)}(UX)$ implies that there is at least one $\underline{y}$ such that $(\underline{u},\underline{x},\underline{y}) \in \mathcal{A}_\epsilon^{(N)}(UXY)$.

*Property 2:* Let $\underline{U},\underline{X},\underline{Y}$ be i.i.d. with respect to $P(u,x,y) = Q(x,y)P(u|x)$. Then for $N$ large enough

$$\sum_{(\underline{u},\underline{x})\in\mathcal{B}_\epsilon^{(N)}(UX)} P(\underline{u},\underline{x}) \geq 1-\epsilon. \tag{95}$$

The statement follows from observing that

$$\begin{aligned}&\Pr\Big\{(\underline{U},\underline{X},\underline{Y}) \in \mathcal{A}_\epsilon^{(N)}(UXY)\Big\}\\ &\quad\leq \sum_{(\underline{u},\underline{x})\in\mathcal{B}_\epsilon^{(N)}(UX)} P(\underline{u},\underline{x}) + \sum_{(\underline{u},\underline{x})\notin\mathcal{B}_\epsilon^{(N)}(UX)} P(\underline{u},\underline{x})(1-\epsilon)\\ &\quad= 1-\epsilon+\epsilon\Pr\Big\{(\underline{U},\underline{X}) \in \mathcal{B}_\epsilon^{(N)}(UX)\Big\}\end{aligned}$$

or

$$\Pr\Big\{(\underline{U},\underline{X}) \in \mathcal{B}_\epsilon^{(N)}(UX)\Big\} \geq 1 - \frac{1-\Pr\Big\{(\underline{U},\underline{X},\underline{Y}) \in \mathcal{A}_\epsilon^{(N)}(UXY)\Big\}}{\epsilon}. \tag{96}$$

The weak law of large numbers implies that $\Pr\{(\underline{U},\underline{X},\underline{Y}) \in \mathcal{A}_\epsilon^{(N)}(UXY)\} \geq 1-\epsilon^2$ for $N$ large enough. Then (95) follows from (96).

### B. Random Code Construction, Encoding, and Decoding

*Random Coding:* For each index $i \in \{1,2,\ldots,|\mathcal{I}|\}$, generate an auxiliary sequence $\underline{u}(i)$ at random according to $P(u) = \sum_{x,y} Q(x,y)P(u|x)$. Moreover, for each such index $i$ (and the corresponding sequence $\underline{u}(i)$), generate a secret-key label $s(i) \in \{1,2,\ldots,|\mathcal{S}|\}$ and a helper-data label $m(i) \in \{1,2,\ldots,|\mathcal{M}|\}$ uniformly at random.

*Encoding:* The encoder observes the biometric source sequence $\underline{x}$ and then finds the index $i$ such that $(\underline{u}(i),\underline{x}) \in \mathcal{B}_\epsilon^{(N)}(UX)$. If such an index cannot be found, the encoder declares an error and $i$ gets an arbitrary value from $\{1,2,\ldots,|\mathcal{I}|\}$. Using index $i$, the encoder produces a secret key $s(i)$ and helper data $m(i)$. Next the encoder checks whether there is another index $i' \neq i$ such that $s(i') = s(i)$ and $m(i') = m(i)$. If so, the encoder declares an error. If no error was declared by the encoder, then $e = 0$; otherwise $e = 1$. The helper data are sent to the decoder.

*Decoding:* The decoder upon observing the biometric source sequence $\underline{y}$ and receiving the helper data $m$ looks for the unique index $\widehat{i}$ such that both $(\underline{u}(\widehat{i}),\underline{y}) \in \mathcal{A}_\epsilon^{(N)}(UY)$ and $m(\widehat{i}) = m$. If such a unique index exists, the decoder produces a secret-key estimate $s(\widehat{i})$. If not, an error is declared.

### C. Events, Error Probability

*Events:* Let $\underline{X}$ and $\underline{Y}$ be the observed biometric source sequences, $I$ the index determined by the encoder, $S(i)$ and $M(i)$ the random labels assigned to $i \in \{1,2,\ldots,|\mathcal{I}|\}$, and $S$ and $M$ the actual labels. Then define the events

$$\begin{aligned}A_i &\triangleq \Big\{(\underline{U}(i),\underline{X}) \in \mathcal{B}_\epsilon^{(N)}(UX)\Big\}\\ B_i &\triangleq \{S(i) = S \wedge M(i) = M\}\\ C_i &\triangleq \Big\{(\underline{U}(i),\underline{Y}) \in \mathcal{A}_\epsilon^{(N)}(UY)\Big\}\\ D_i &\triangleq \{M(i) = M\}\\ E_i &\triangleq \Big\{(\underline{U}(i),\underline{X},\underline{Y}) \in \mathcal{A}_\epsilon^{(N)}(UXY)\Big\}.\end{aligned}$$

*Error Probability:* For the resulting error probability $\overline{P_E}$ averaged over the ensemble of codes, we have the following upper bound. We assume that $i$ runs over $\{1,2,\ldots,|\mathcal{I}|\}$

$$\begin{aligned}&\Pr\left\{\left(\bigcap_i A_i^c\right) \cup \left(\bigcup_{i\neq I} B_i\right) \cup C_I^c \cup \left(\bigcup_{i\neq I}(C_i\cap D_i)\right)\right\}\\ &\quad\leq \Pr\left\{\bigcap_i A_i^c\right\} + \Pr\left\{\bigcup_{i\neq I} B_i\right\} + \Pr\left\{\left(\bigcup_i A_i\right)\cap C_I^c\right\}\\ &\qquad+\Pr\left\{\bigcup_{i\neq I}(C_i\cap D_i)\right\}\\ &\quad\leq \Pr\left\{\bigcap_i A_i^c\right\} + \sum_{i\neq I}\Pr\{B_i\} + \Pr\left\{\left(\bigcup_i A_i\right)\cap E_I^c\right\}\\ &\qquad+\sum_{i\neq I}\Pr\{C_i\cap D_i\}\end{aligned} \tag{97}$$

where in the last step, we used the fact that $E_I \Rightarrow C_I$.

*First Term:* As in Gallager [17, p. 454], we write

$$\begin{aligned}\Pr\left\{\bigcap_i A_i^c\right\} &= \sum_{\underline{x}\in\mathcal{X}^N} Q(\underline{x}) \prod_i \left(1 - \sum_{\underline{u}\in\mathcal{B}_\epsilon^{(N)}(U|\underline{x})} P(\underline{u})\right)\\ &\overset{(a)}{\leq} \sum_{\underline{x}\in\mathcal{X}^N} Q(\underline{x})\Bigg(1 - 2^{-N(I(U;X)+3\epsilon)}\\ &\qquad\cdot \sum_{\underline{u}\in\mathcal{B}_\epsilon^{(N)}(U|\underline{x})} P(\underline{u}|\underline{x})\Bigg)^{|\mathcal{I}|}\end{aligned}$$

$$\begin{aligned}
&\overset{(b)}{\leq} \sum_{\underline{x}\in\mathcal{X}^N} Q(\underline{x})\Bigg(1-\sum_{\underline{u}\in\mathcal{B}_\epsilon^{(N)}(U|\underline{x})} P(\underline{u}|\underline{x}) \\
&\qquad\qquad + \exp\left(-|\mathcal{I}|2^{-N(I(U;X)+3\epsilon)}\right)\Bigg) \\
&\leq \sum_{(\underline{u},\underline{x})\notin\mathcal{B}_\epsilon^{(N)}(UX)} P(\underline{u},\underline{x}) \\
&\qquad + \sum_{\underline{x}\in\mathcal{X}^N} Q(\underline{x})\exp(-2^{N\epsilon}) \\
&\overset{(c)}{\leq} 2\epsilon
\end{aligned} \tag{98}$$

for $N$ large enough, if $|\mathcal{I}| \geq 2^{N(I(U;X)+4\epsilon)}$. Here (a) follows from the fact that for $(\underline{u},\underline{x}) \in \mathcal{B}_\epsilon^{(N)}(UX)$, using Property 1, we get

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

(b) from the inequality $(1-\alpha\beta)^K \leq 1-\alpha+\exp(-K\beta)$, which holds for $0 \leq \alpha,\beta \leq 1$ and $K > 0$; and (c) from Property 2.

*Second Term:* If $|\mathcal{I}| \leq |\mathcal{S}||\mathcal{M}|2^{-N\epsilon}$, then for all large enough $N$

$$\sum_{i\neq I}\Pr\{B_i\} \leq \frac{|\mathcal{I}|}{|\mathcal{S}||\mathcal{M}|} \leq 2^{-N\epsilon} \leq \epsilon. \tag{99}$$

*Third Term:* For this term, we get

$$\begin{aligned}
&\Pr\left\{\left(\bigcup_i A_i\right)\cap E_I^c\right\} \\
&\leq \max_{(\underline{u},\underline{x})\in\mathcal{B}_\epsilon^{(N)}(UX)} \Pr\left\{\underline{Y}\notin\mathcal{A}_\epsilon^{(N)}(Y|\underline{u},\underline{x})|(\underline{U},\underline{X})=(\underline{u},\underline{x})\right\} \\
&\leq \epsilon
\end{aligned} \tag{100}$$

where the last step follows directly from the definition of $\mathcal{B}_\epsilon^{(N)}(UX)$.

*Fourth Term:* For a fixed $\underline{y}$

$$\begin{aligned}
&\Pr\left\{\underline{U}\in\mathcal{A}_\epsilon^{(N)}(U|\underline{y})\right\} \\
&= \sum_{\underline{u}\in\mathcal{A}_\epsilon^{(N)}(U|\underline{y})} P(\underline{u}) \\
&\leq \sum_{\underline{u}\in\mathcal{A}_\epsilon^{(N)}(U|\underline{y})} P(\underline{u}|\underline{y})\frac{P(\underline{u})Q(\underline{y})}{P(\underline{u},\underline{y})} \\
&\leq 2^{-N(I(U;Y)-3\epsilon)}\cdot\sum_{\underline{u}\in\mathcal{A}_\epsilon^{(N)}(U|\underline{y})} P(\underline{u}|\underline{y}) \leq 2^{-N(I(U;Y)-3\epsilon)}.
\end{aligned}$$

Now, if $|\mathcal{I}| \leq |\mathcal{M}|2^{N(I(U;Y)-4\epsilon)}$, for $N$ large enough

$$\begin{aligned}
\sum_{i\neq I}\Pr\{C_i\cap D_i\} &\leq \sum_{i\neq I}\frac{1}{|\mathcal{M}|}\max_{\underline{y}}\Pr\left\{\underline{U}\in\mathcal{A}_\epsilon^{(N)}(U|\underline{y})\right\} \\
&\leq \frac{|\mathcal{I}|}{|\mathcal{M}|}2^{-N(I(U;Y)-3\epsilon)} \\
&\leq 2^{-N\epsilon} \leq \epsilon.
\end{aligned} \tag{101}$$

*Solution of the Inequalities:* The three inequalities $|\mathcal{I}| \geq 2^{N(I(U;X)+4\epsilon)}$, $|\mathcal{I}| \leq |\mathcal{S}||\mathcal{M}|2^{-N\epsilon}$, and $|\mathcal{I}| \leq |\mathcal{M}|2^{N(I(U;Y)-4\epsilon)}$ are satisfied by

$$\begin{aligned}
|\mathcal{I}| &= 2^{N(I(U;X)+4\epsilon)} \\
|\mathcal{S}| &= 2^{N(I(U;Y)-3\epsilon)} \\
|\mathcal{M}| &= 2^{N(I(U;X)-I(U;Y)+8\epsilon)}.
\end{aligned} \tag{102}$$

### D. Wrap-up

*Secret-Key Rate and Error Probability:* For all $N$ large enough, *there exist codes* in the ensemble of codes ($\underline{u}$ sequences and $s(\cdot)$ and $h(\cdot)$ labels) having error probability $P_E \leq \overline{P_E}$. Here $P_E$ denotes the error probability in the sense of (97). For such a code

$$\Pr\{\widehat{S}\neq S\} \leq P_E \leq \overline{P_E} \leq 2\epsilon+\epsilon+\epsilon+\epsilon = 5\epsilon \tag{103}$$

$$\log|\mathcal{S}| = N\left(I(U;Y)-3\epsilon\right) \tag{104}$$

for our fixed $0 < \epsilon < 1$. This follows from combining (98)–(102).

*Secrecy Leakage:* First, observe that for any sequence $\underline{u}$

$$\begin{aligned}
\sum_{\underline{x}\in\mathcal{A}_\epsilon^{(N)}(X|\underline{u})} P(\underline{x}) &\leq \sum_{\underline{x}\in\mathcal{A}_\epsilon^{(N)}(X|\underline{u})} 2^{-N(I(U;X)-3\epsilon)}P(\underline{x}|\underline{u}) \\
&\leq 2^{-N(I(U;X)-3\epsilon)}\sum_{\underline{x}\in\mathcal{X}^N} P(\underline{x}|\underline{u}) \\
&= 2^{-N(I(U;X)-3\epsilon)}.
\end{aligned} \tag{105}$$

Then note that $(\underline{u}(i),\underline{x}) \in \mathcal{A}_\epsilon^{(N)}(UX)$ if no error was declared by the encoder, and this happens with probability at least 1–2$\epsilon$. For the probability $P(i,e)$ that index $I = i$ occurs together with $E = e$, we can therefore write that $P(i,0) \leq \sum_{\underline{x}\in\mathcal{A}_\epsilon^{(N)}(X|\underline{u}(i))} P(\underline{x})$ and, consequently,

$$\begin{aligned}
H(I,E) &\geq -\sum_{i=1}^{|\mathcal{I}|} P(i,0)\log\left(\sum_{\underline{x}\in\mathcal{A}_\epsilon^{(N)}(X|\underline{u}(i))} P(\underline{x})\right) \\
&\geq N(1-2\epsilon)\left(I(U;X)-3\epsilon\right) \\
&= N\left(I(U;X)-3\epsilon-2\epsilon I(U;X)+6\epsilon^2\right).
\end{aligned} \tag{106}$$

Next observe that the label pair $(S,M)$ uniquely determines $I$ when $E = 0$ and that $I \in \{1,2,\ldots,|\mathcal{I}|\}$ when $E = 1$. Then, using (102) and (106), we get

$$\begin{aligned}
H(S,M,E) &= H(I,S,M,E) - H(I|S,M,E) \\
&\geq H(I,E) - 2\epsilon N\left(I(U;X)+4\epsilon\right) \\
&\geq N\left(I(U;X)-3\epsilon-4\epsilon I(U;X)-2\epsilon^2\right).
\end{aligned} \tag{107}$$

Finally, we obtain for the secrecy leakage

$$\begin{aligned} I(S;M) &\le I(S;M,E) = H(S) + H(M,E) - H(S,M,E) \\ &\le N\left(I(U;Y) - 3\epsilon\right) + N\left(I(U;X) - I(U;Y) + 8\epsilon\right) \\ &\quad + 1 - N\left(I(U;X) - 3\epsilon - 4\epsilon I(U;X) - 2\epsilon^2\right) \\ &= N\left(8\epsilon + 4\epsilon I(U;X) + 2\epsilon^2\right) + 1. \end{aligned} \tag{108}$$

*Uniformity:* The uniformity of the secret key $S$ follows from

$$\begin{aligned} H(S) &= H(S,M,E) - H(M,E|S) \\ &\ge H(S,M,E) - H(M) - H(E) \\ &\ge N\left(I(U;X) - 3\epsilon - 4\epsilon I(U;X) - 2\epsilon^2\right) \\ &\quad - N\left(I(U;X) - I(U;Y) + 8\epsilon\right) - 1 \\ &= N\left(I(U;Y) - 11\epsilon - 4\epsilon I(U;X) - 2\epsilon^2\right) - 1 \\ &= \log|\mathcal{S}| - N\left(8\epsilon - 4\epsilon I(U;X) - 2\epsilon^2\right) - 1 \end{aligned} \tag{109}$$

where the last step follows from (104).

*Privacy Leakage:* Note that from (102), it immediately follows that

$$\begin{aligned} I(X^N;M) &\le H(M) \\ &\le N\left(I(U;X) - I(U;Y) + 8\epsilon\right). \end{aligned} \tag{110}$$

*Conclusion:* We now conclude the proof by letting $\epsilon \downarrow 0$ and $N \to \infty$ and observing that the achievability follows from (103), (104), (108), (109), and (110).

## REFERENCES


[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—Part II: CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[3] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *Proc. ACISP*, 2005, pp. 242–252.

[4] T. Berger, "Multiterminal source coding, the information theory approach to communications," in *CISM Courses and Lectures*, G. Longo, Ed. Berlin, Germany: Springer-Verlag, 1978, vol. 229, pp. 171–231.

[5] I. Buhan, J. Doumen, and P. Hartel, "Controlling leakage of biometric information using dithering," in *Proc. EUSIPCO*, Lausanne, Switzerland, Aug. 25–29, 2008.

[6] I. Buhan, J. Doumen, P. H. Hartel, Q. Tang, and R. N. J. Veldhuis, "Embedding renewable cryptographic keys into continuous noisy data," in *Proc. ICICS*, 2008, pp. 294–310.

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[8] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1982.

[9] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[10] G. Davida, Y. Frankel, and B. Matt, "On the relation of error correction and cryptography to an off-line biometric based identification scheme," in *Proc. Workshop Coding Crypto. (WCC'99)*, 1999, pp. 129–138.

[11] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE 1998 Symp. Security Privacy*, 1998, pp. 148–157.

[12] D. Denteneer, J. Linnartz, P. Tuyls, and E. Verbitskiy, "Reliable (robust) biometric authentication with privacy protection," in *Proc. IEEE Benelux Symp. Inf Theory*, Veldhoven, The Netherlands, 2003.

[13] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Adv. Cryptol. Eurocrypt 2004*, 2004, pp. 523–540.

[14] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[15] S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2007, vol. 2, pp. 129–132.

[16] N. Frykholm and A. Juels, "Error-tolerant password recovery," in *Proc. 8th ACM Conf. Comput. Commun. Security (CCS '01)*, New York, 2001, pp. 1–9.

[17] R. Gallager, *Information Theory and Reliable Communcation*. New York: Wiley, 1968.

[18] J. G. D. Forney, Information theory 1972, course notes , Stanford Univ..

[19] D. Gündüz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proc. IEEE Inf. Theory Workshop*, Porto, Portugal, 2008.

[20] A. K. Jain, K. N, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, pp. 1–7, 2008.

[21] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, 2002, p. 408.

[22] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Security*, 1999, pp. 28–36.

[23] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proc. 46th Ann. Allerton Conf. Commun., Contr., Comput.*, Monticello, IL, Sep. 23–26, 2008.

[24] J.-P. M. G. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proc. AVBPA*, 2003, pp. 393–402.

[25] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri, "Template protection for HMM-based on-line signature authentication," in *Proc. IEEE Conf. Comput. Vision Pattern Recognit. Works*, Jun. 2008, pp. 1–6.

[26] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[27] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Proc. IEEE Symp. Security Privacy*, 2001, pp. 202–213.

[28] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *Proc. ACM Conf. Comput. Commun. Security*, 1999, pp. 73–82.

[29] K. Nandakumar, A. Nagar, and A. Jain, "Hardening fingerprint fuzzy vault using password," in *Proc. ICB07*, 2007, pp. 927–937.

[30] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[31] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. IEEE Inf. Theory Workshop 2007*, Sep. 2007, pp. 442–447.

[32] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[33] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 29, pp. 561–572, Apr. 2007.

[34] B. Schneier, "Inside risks: The uses and abuses of biometrics," *Commun. ACM*, vol. 42, no. 8, p. 136, 1999.

[35] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, 1979.

[36] A. Smith, "Maintaining secrecy when information leakage is unavoidable," Ph.D. dissertation, Massachusetts Inst. of Technology, Cambridge, 2004.

[37] Y. Sutcu, Q. Li, and N. Memon, "How to protect biometric templates," in *Proc. SPIE Conf. Security, Steganogr., Watermark. Multimedia Contents IX*, San Jose, CA, Jan. 2007, vol. 6505.

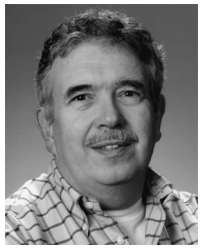
[38] A. Teoh, A. Goh, and D. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[39] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[40] "Forum on signal processing for biometric systems," *IEEE Signal Process. Mag.*, vol. 24, no. 6, pp. 146–152, Nov. 2007.
[41] , J. Wayman, A. Jain, and D. Maltoni, Eds., *Biometric Systems: Technology, Design and Performance Evaluation*. London, U.K.: Springer-Verlag, 2005.
[42] J. Wolfowitz, *Coding Theorems of Information Theory*. Berlin, Germany: Springer-Verlag, 1961.
[43] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications—I," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 6, pp. 769–772, Nov. 1973.
[44] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 1, pp. 1–10, Jan. 1976.

**Tanya Ignatenko** (S'06–M'08) was born in Minks, Belarus, in 1978. She received the M.Sc. degree in applied mathematics from Belarussian State University, Minsk, in 2001. She received the P.D.Eng. and Ph.D. degrees from Eindhoven University of Technology, Eindhoven, The Netherlands, in 2004 and 2009, respectively.

She is a Postdoctoral Researcher with the Electrical Engineering Department, Eindhoven University of Technology. Her research interests include secure private biometrics, multiuser information theory, and information-theoretical secret sharing.



**Frans M. J. Willems** (S'80–M'82–SM'05–F'05) was born in Stein, The Netherlands, in 1954. He received the M.Sc. degree in electrical engineering from Technische Universiteit Eindhoven, Eindhoven, The Netherlands, and the Ph.D. degree from Katholiek Universiteit Leuven, Leuven, Belgium, in 1979 and 1982, respectively.

From 1979 to 1982, he was a Research Assistant with Katholieke Universiteit Leuven. Since 1982, he has been a Staff Member with the Electrical Engineering Department, Technische Universiteit Eindhoven. His research contributions are in the areas of multiuser information theory and noiseless source coding. From 1999 to 2008, he was an Advisor for Philips Research Laboratories for subjects related to information theory. From 2002 to 2006, he was an Associate Editor for Information Theory for the *European Transactions on Telecommunications*.

Dr. Willems received the Marconi Young Scientist Award in 1982. From 1988 to 1990, he was Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY. He was a corecipient of the 1996 IEEE Information Theory Society Paper Award. From 1998 to 2000, he was a member of the Board of Governors of the IEEE Information Theory Society.