Privacy leakage in biometric secrecy systems

DOI:
10.1109/ALLERTON.2008.4797646

Document status and date:
Published: 01/01/2008

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

Forty-Sixth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 23-26, 2008

Privacy Leakage in Biometric Secrecy Systems

Tanya Ignatenko and Frans M.J. Willems
Eindhoven University of Technology,
Electrical Engineering Department,
Eindhoven, The Netherlands,
Email: {t.ignatenko,f.m.j.willems}@tue.nl

***Abstract*— Motivated by Maurer [1993], Ahlswede and Csiszar [1993] introduced the concept of secret sharing. In their source model two terminals observe two correlated sequences. It is the objective of both terminals to form a common secret by interchanging a public message (helper data), that should contain only a negligible amount of information about the secret. Ahlswede and Csiszar showed that the maximum secret key rate that can be achieved in this way is equal to the mutual information between the two source outputs. In a biometric setting, where the sequences correspond to the enrollment and authentication data, it is crucial that the public message leaks as little information as possible about the biometric data, since compromised biometric data cannot be replaced. We investigate the fundamental trade-offs for four biometric settings. The first one is the standard (Ahlswede-Csiszar) secret generation setting, for which we determine the secret key rate - privacy leakage region. Here leakage corresponds to the mutual information between helper data and biometric enrollment sequence conditional on the secret. In the second setting the secret is not generated by the terminals but independently chosen, and transmitted using a public message. Again we determine the region of achievable rate - leakage pairs. In setting three and four we consider zero-leakage, i.e. the public message contains only a negligible amount of information about the secret and the biometric enrollment sequence. To achieve this a private key is needed which can be observed only by the terminals. We consider again both secret generation and secret transmission and determine for both cases the region of achievable secret key rate - private key rate pairs.**

I. Introduction

First, Maurer, [9], and slightly later Ahlswede and Csiszar, [1], introduced the concept of secret sharing. In their source model two terminals observe two correlated sequences $\underline{X}$ and $\underline{Y}$. It is the objective of both terminals to form a common secret S by interchanging a public message H (helper data), that should only contain a negligible amount of information about the secret. Ahlswede and Csiszar showed that the maximum secret key rate that can be achieved in this way is equal to the mutual information $I(X;Y)$ between the correlated source outputs. Their achievability proofs can be expressed in terms of Slepian-Wolf techniques presented by Cover [3], in which binning of typical sequences plays an important role, see e.g. Ye and Narayan, [15], and [7]. The concept of secret sharing is closely related to the generation of common randomness. Common randomness capacity was first studied in a systematic way by Ahlswede and Csiszar, [2], later helper terminals were included by Csiszar and Narayan in their investigations in [5]. Venkatesan and Anantharam [12] studied the idea to use channel noise for generation of common randomness.

When two terminals try to generate common randomness the issue of pricavy of the helper data is ignored. In a biometric setting, where the X-sequence corresponds to the enrollment data and the Y-sequence to the authentication data, it is crucial that the public message H leaks as little information as possible about the biometric data. The reason for this is that compromised biometric data cannot be replaced. Smith [11] has investigated this privacy leakage and came to the conclusion that it cannot be avoided. We have determined the trade-off between secret-key rate and privacy leakage for the i.i.d. case here, and our results confirm this statement for a binary symmetric double source (BSDS).

We will also consider secret transmission. We study a model in which a uniformly chosen secret key is transmitted by the first terminal via a public message to the second terminal. The terminals observe two correlated biometric sequences, and the public helper data should be uninformative about the secret. Again we determine the rate-leakage balance for this setting.

The third topic that we study here is a zero-leakage secret generation protocol. In this protocol an additional random key is made available only to the two terminals. We now focus on helper data that contain only a negligible amount of information about the secret and the biometric sequence. Also for this case we could determine the trade-off between private key rate and the resulting secret key rate.

The last topic that we address is zero-leakage secret transmission. Here again both terminals have access to a private key, but now it is their intention to transmit an independently chosen uniform secret form the first terminal to the second by means of public helper data, that is practically not leaking. The trade-off for this setting will be presented here, i.e. we show how the secret key rate depends on the private key rate.

Recently Prabhakaran and Ramchandran [10] and Gunduz et al. [6] studied source coding problems where also the issue of (biometric) leakage is addressed. In their work it is not the intention of the users to produce a secret but to communicate a (biometric) source sequence in a secure way from a first terminal to a second terminal.

978-1-4244-2926-4/08/$25.00 ©2008 IEEE

II. Four Cases, Definitions

A. Basic Definitions

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

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

hence the source pairs $\{(X_n, Y_n), n = 1, \ldots, N\}$ are independent of each other and identically distributed according to $Q(\cdot,\cdot)$. The biometric source sequences $\underline{x}$ and $\underline{y}$ are in general not independent of each other.

The sequences $\underline{x}$ and $\underline{y}$ are observed by an encoder and decoder, respectively. One of the outputs that the encoder produces is an index $h \in \{1, 2, \cdots, M_H\}$, 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, and systems in which a uniformly chosen secret is *transmitted* from the encoder to the decoder. The generated or transmitted secret s assumes values in $\{1, 2, \cdots, M_S\}$. The decoders estimate $\widehat{s}$ of the secret s also assumes values from $\{1, 2, \cdots, M_S\}$. In transmission systems the secret s is a uniformly distributed index, hence

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

Moreover, we can subdivide systems into systems in which the helper data are allowed to leak some information about the biometric sequence $\underline{X}$, and systems in which this leakage should be negligible. In the so-called *zero-leakage* systems both users have access to a private random key p. This key is uniformly distributed, hence

$$\Pr\{P = p\} = 1/M_P \text{ for all } p \in \{1, 2, \cdots, M_P\}. \tag{3}$$

In the next subsections the four resulting combinations (1) secret generation, (2) secret transmission, (3) zero-leakage secret generation, and (4) zero-leakage secret transmission, will be proposed in detail.

There are two types of privacy leakage, (a) unconditional leakage and (b) conditional leakage. Unconditional leakage corresponds to bounding the mutual information $I(\underline{X}; H)$, whereas conditional leakage corresponds to bounding the conditional mutual information $I(\underline{X}; H|S)$. We will focus in the (stronger[1] restriction) conditional leakage here.

B. Secret Generation

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

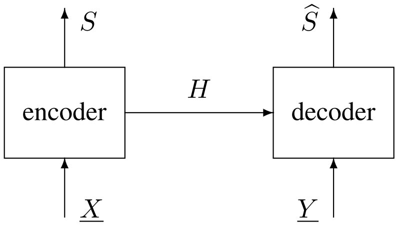

Fig. 1. Model for biometric secret generation.

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

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

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

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

For biometric secret generation we now give the definition of achievability corresponding to conditional privacy leakage.

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

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

Now $\mathcal{R}_{\text{sg}}^{\text{c}}$ is the region of all achievable rate-leakage pairs for a secret generation system in the conditional case. The corresponding rate-leakage function $R_{\text{sg}}^{\text{c}}(L)$ is defined as

$$R_{\text{sg}}^{\text{c}}(L) \overset{\Delta}{=} \max\{R : (R, L) \in \mathcal{R}_{\text{sg}}^{\text{c}}\}. \tag{7}$$

C. Secret Transmission

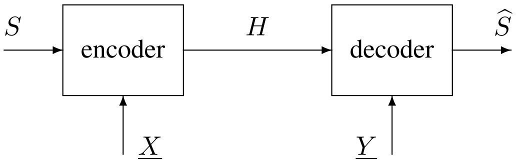

Fig. 2. Model for biometric secret transmission.

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

$$H = e(S, \underline{X}), \tag{8}$$

[1] From $I(\underline{X}; H|S) = I(\underline{X}, S; H) - I(S; H) \geq I(\underline{X}; H) - I(S; H)$ we can conclude that for negligible $I(S; H)$, the conditional leakage $I(\underline{X}; H|S)$ cannot be significantly smaller than the unconditional leakage $I(\underline{X}; H)$.

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

$$\widehat{S} = d(H, \underline{Y}), \tag{9}$$

and $d(\cdot,\cdot)$ is the decoder mapping. Again we consider conditional privacy leakage.

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

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ \log(M_S) &\geq N(R-\delta), \\ I(S;H) &\leq N\delta, \\ I(\underline{X};H|S) &\leq N(L+\delta). \end{aligned} \tag{10}$$

Now $\mathcal{R}^{\text{c}}_{\text{st}}$ is the region of all achievable rate-leakage pairs for a secret generation system in the conditional case. The corresponding rate-leakage function $R^{\text{c}}_{\text{st}}(L)$ is defined as

$$R^{\text{c}}_{\text{st}}(L) \stackrel{\Delta}{=} \max\{R : (R, L) \in \mathcal{R}^{\text{c}}_{\text{st}}\}. \tag{11}$$

D. Zero-Leakage Secret Generation

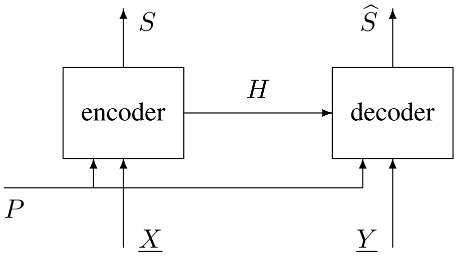

Fig. 3. Model for zero-leakage biometric secret generation.

In a zero-leakage biometric secret generation system, see Fig. 3, a private random key P that is available to both the encoder and the decoder, is uniformly distributed, see (3). An encoder observes the first biometric source sequence $\underline{X}$ and the private key P and produces a secret S and the helper data H, hence

$$(S, H) = e(\underline{X}, P), \tag{12}$$

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

$$\widehat{S} = d(H, \underline{Y}, P), \tag{13}$$

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

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

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ H(S) + N\delta \geq \log(M_S) &\geq N(R-\delta), \\ \log(M_P) &\leq N(K+\delta), \\ I(S,\underline{X};H) &\leq N\delta. \end{aligned} \tag{14}$$

Moreover, let $\mathcal{R}^{\text{c}}_{\text{zsg}}$ be the region of all secret rate-private rate pairs (R, K) for a zero-leakage secret generation system in the conditional case. The corresponding secret rate - private rate function $R^{\text{c}}_{\text{zsg}}(K)$ is defined as

$$R^{\text{c}}_{\text{zsg}}(K) \stackrel{\Delta}{=} \max\{R : (R, K) \in \mathcal{R}^{\text{c}}_{\text{zsg}}\}. \tag{15}$$

Note that the last constraint in (14) is actually a combination of the constraint on $I(S;H)$ and the (conditional) constraint on $I(\underline{X};H|S)$. The same holds for the last constraint in (18).

E. Zero-Leakage Secret Transmission

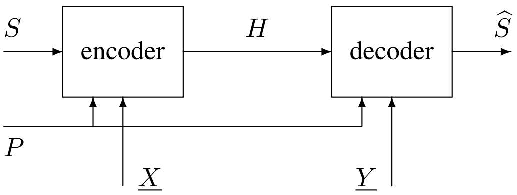

Fig. 4. Model for zero-leakage biometric secret transmission.

In a zero-leakage biometric secret transmission system, see Fig. 4, a private random key P that is available to both the encoder and the decoder, is uniformly distributed, see (3). Moreover, a secret S, that is to be transmitted from encoder to decoder, is also uniformly distributed, see (2).

An encoder observes the first biometric source sequence $\underline{X}$, the private key P and the secret S and forms the helper data, hence

$$H = e(S, \underline{X}, P), \tag{16}$$

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

$$\widehat{S} = d(H, \underline{Y}, P), \tag{17}$$

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

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

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta, \\ \log(M_S) &\geq N(R-\delta), \\ \log(M_P) &\leq N(K+\delta), \\ I(S,\underline{X};H) &\leq N\delta. \end{aligned} \tag{18}$$

Moreover, let $\mathcal{R}^{\mathrm{c}}_{\mathrm{zst}}$ be the region of all secret rate-private rate pairs (R, K) for a zero-leakage secret transmission system in the conditional case. The corresponding secret rate-private rate function $R^{\mathrm{c}}_{\mathrm{zst}}(K)$ is defined as

$$R^{\mathrm{c}}_{\mathrm{zst}}(K) \stackrel{\Delta}{=} \max\{R : (R, K) \in \mathcal{R}^{\mathrm{c}}_{\mathrm{zst}}\}. \tag{19}$$

III. Properties of the achievable regions

A. Convexity

Consider a certain achievable region, e.g. $\mathcal{R}^{\mathrm{c}}_{\mathrm{sg}}$. This region is convex. To see this take two achievable pairs. For each such pair there exists a sequence of codes satisfying (6). By combining the codes corresponding to the first achievable pair with the codes corresponding to the second achievable pair we obtain codes that demonstrate the achievability of a convex combination of the two achievable pairs. This procedure can be followed also for showing that the other regions are convex.

B. Another property

The zero-leakage achievable regions all have the property that if an achievable pair (R, K) belongs to it, also $(R + \alpha, K + \alpha)$ for positive α does. Just use the extra private-key rate α for masking extra secret symbols that can now be transmitted.

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 will present four theorems.

$$\begin{aligned}\mathcal{R}_1 \stackrel{\Delta}{=} \{(R, L) \;\; : \;\; & 0 \le R \le I(U;Y), \\ & L \ge I(U;X) - I(U;Y), \\ & \text{for } P(u,x,y) = Q(x,y)P(u|x)\}. \end{aligned} \tag{20}$$

$$\begin{aligned}\mathcal{R}_2 \stackrel{\Delta}{=} \{(R, L) \;\; : \;\; & 0 \le R \le I(U;Y), \\ & L \ge I(U;X), \\ & \text{for } P(u,x,y) = Q(x,y)P(u|x)\}. \end{aligned} \tag{21}$$

$$\begin{aligned}\mathcal{R}_3 \stackrel{\Delta}{=} \{(R, K) \;\; : \;\; & 0 \le R \le I(U;Y) + K, \\ & K \ge I(U;X) - I(U;Y), \\ & \text{for } P(u,x,y) = Q(x,y)P(u|x)\}. \end{aligned} \tag{22}$$

$$\mathcal{R}_4 \stackrel{\Delta}{=} \{(R, K) : 0 \le R \le K\}. \tag{23}$$

Theorem 1 (Secret Generation, Cond.):

$$\mathcal{R}^{\mathrm{c}}_{\mathrm{sg}} = \mathcal{R}_1. \tag{24}$$

Theorem 2 (Secret Transmission, Cond.):

$$\mathcal{R}^{\mathrm{c}}_{\mathrm{st}} = \mathcal{R}_2. \tag{25}$$

Theorem 3 (Zero-Leakage Secret Generation, Cond.):

$$\mathcal{R}^{\mathrm{c}}_{\mathrm{zsg}} = \mathcal{R}_3. \tag{26}$$

Theorem 4 (Zero-Leakage Secret Transmission, Cond.):

$$\mathcal{R}^{\mathrm{c}}_{\mathrm{zst}} = \mathcal{R}_4. \tag{27}$$

V. The Regions $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and $\mathcal{R}_4$

A. Bound on the Cardinality of Auxiliary Random Variable 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

$$\begin{aligned}\phi_x(P) &= P(x) \text{ for all but one } x, \\ \phi_X(P) &= H_P(X), \\ \phi_Y(P) &= H_P(Y), \end{aligned} \tag{28}$$

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

$$\begin{aligned}Q(x) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_x(P_u) \text{ for all but one } x, \\ H(X|U) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_X(P_u), \\ H(Y|U) &= \sum_{u=1}^{|\mathcal{X}|+1} \alpha_u \phi_Y(P_u). \end{aligned} \tag{29}$$

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 $I(U;Y)$. This implies that cardinality $|\mathcal{U}| = |\mathcal{X}| + 1$ suffices for auxiliary variable U in the regions $\mathcal{R}_1$, $\mathcal{R}_2$, and $\mathcal{R}_3$.

B. Example: Binary Symmetric Double Source

Consider a binary symmetric double source (BSDS) with crossover probability $0 \le q \le 1/2$, hence $Q(x,y) = (1-q)/2$ for $y = x$ and $q/2$ for $y \ne x$. For such a source

$$\begin{aligned}I(U;Y) &= 1 - H(Y|U), \\ I(U;X) - I(U;Y) &= H(Y|U) - H(X|U). \end{aligned} \tag{30}$$

Mrs. Gerber's Lemma [13] tells us that if $H(X|U) = v$ then $H(Y|U) \ge h(q * h^{-1}(v))$, where $h(a) \stackrel{\Delta}{=} -a\log(a) - (1-a)\log(1-a)$ is the binary entropy function. If now $0 \le p \le 1/2$ is such that $h(p) = v$ then $H(X|U) = h(p)$ and $H(Y|U) \ge h(q * p)$. For binary symmetric (U, X) with crossover probability p the minimum $H(Y|U)$ is achieved, and consequently

$$R^{\mathrm{c}}_{\mathrm{sg}}(L) = 1 - h(q * p) \text{ for } p \text{ such that } h(q * p) - h(p) = L. \tag{31}$$

For crossover probabilities $q = 0.03$, 0.1, and 0.3 we have plotted the resulting rate-leakage functions in Fig. 5. We can conclude from this figure that the secret key rate R can be larger but also smaller than the conditional privacy leakage L.

In a similar way it follows that

$$R^{\mathrm{c}}_{\mathrm{st}}(L) = 1 - h(q * p) \text{ for } p \text{ such that } 1 - h(p) = L, \tag{32}$$

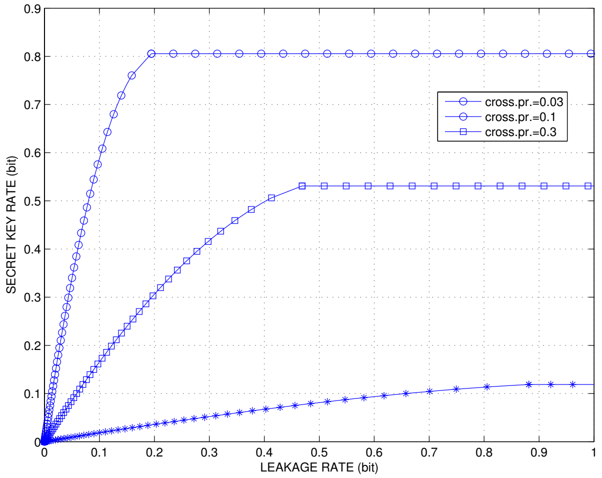

Fig. 5. Rate-leakage function $R^{\mathrm{c}}_{\mathrm{sg}}(\cdot)$ for three values of q.

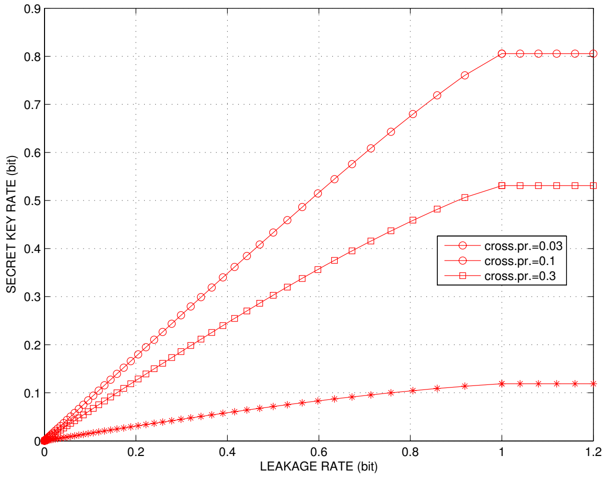

Fig. 6. Rate-leakage function $R^{\mathrm{c}}_{\mathrm{st}}(\cdot)$ for three values of q.

and the resulting functions are plotted in Fig. 6. This figure demonstrates that the secret key rate R in this case never is larger than the conditional privacy leakage L.

Finally it can be shown that

$$R^{\mathrm{c}}_{\mathrm{zsg}}(K) = 1 - h(p) \text{ for } p \text{ such that } h(q * p) - h(p) = K. \tag{33}$$

The resulting plots can be found in Fig. 7. From this figure we can observe that the private key rate K need not be larger than the secret key rate R, we can speak of boosting.

It will be clear that

$$R^{\mathrm{c}}_{\mathrm{zst}}(K) = K. \tag{34}$$

VI. Proof of Thm. 1

The proof of this theorem consists of two parts. The first part, i.e. the converse will be treated in detail. The achievability in the second part will only be outlined.

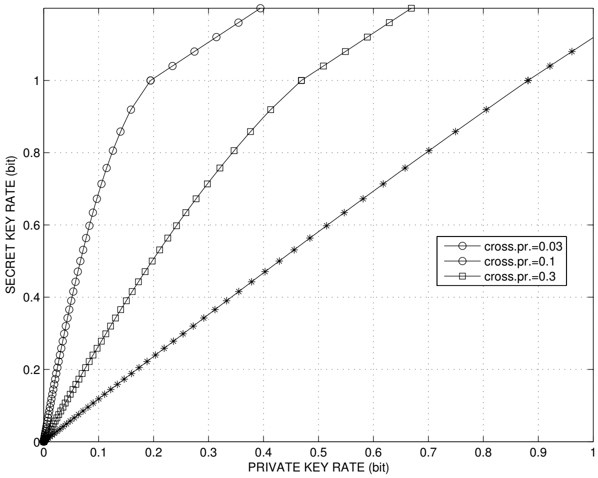

Fig. 7. Secret-Rate - Private-Rate function $R^{\mathrm{c}}_{\mathrm{zsg}}(\cdot)$ for three values of q.

A. Converse

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

$$\begin{aligned}
H(S) &= I(S; H, Y^N) + H(S|H, Y^N, \widehat{S}) \\
&\leq I(S; H, Y^N) + H(S|\widehat{S}) \\
&\leq I(S; H, Y^N) + F \\
&= I(S; H) + \sum_{n=1}^{N} I(S; Y_n | H, Y^{n-1}) + F \\
&\leq I(S; H) + \sum_{n=1}^{N} I(S, H, Y^{n-1}; Y_n) + F \\
&\leq I(S; H) + \sum_{n=1}^{N} I(S, H, X^{n-1}; Y_n) + F \\
&= I(S; H) + NI(U; Y) + F. \qquad (35)
\end{aligned}$$

The last two steps require some attention. The last inequality results from $I(S, H, Y^{n-1}; Y_n) \leq I(S, H, X^{n-1}, Y^{n-1}; Y_n) = I(S, H, X^{n-1}; Y_n)$, since $Y^{n-1} - (S, H, X^{n-1}) - Y_n$. To obtain the last equality, we, first define $U_n \triangleq (S, H, X^{n-1})$. Then if we take a time-sharing variable T uniform over $\{1, 2, \cdots, N\}$ 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

$$\begin{aligned}
&\sum_{n=1}^{N} I(S, H, X^{n-1}; Y_n) \\
&= \sum_{n=1}^{N} I(U_n; Y_n) = NI(U_T; Y_T|T) \\
&= NI((U_T, T); Y_T) = NI(U; Y). \qquad (36)
\end{aligned}$$

Finally, note that $U_n - X_n - Y_n$ and, consequently, $U - X - Y$. For achievable (R, L) we obtain that

$$N(R - \delta) \leq H(S) + N\delta$$

$$\begin{aligned} &\leq \quad N\delta + NI(U;Y) + 1 + \delta\log(M_S) + N\delta \\ &\leq \quad N(I(U;Y) + 2\delta + 1/N + \delta\log|\mathcal{X}|), \quad (37) \end{aligned}$$

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

Now we continue with the conditional leakage.

$$\begin{aligned} &I(S;H) + I(X^N;H|S) \\ &\quad = \quad I(X^N,S;H) = H(H) - H(H|X^N,S) \\ &\quad \geq \quad H(H,\widehat{S}|Y^N) - H(S,H|X^N) \\ &\quad = \quad H(S,H,\widehat{S}|Y^N) - H(S|H,Y^N,\widehat{S}) - H(S,H|X^N) \\ &\quad \geq \quad H(S,H|Y^N) - H(S|\widehat{S}) - H(S,H|X^N) \\ &\quad \geq \quad H(S,H|Y^N) - H(S,H|X^N) - F \\ &\quad = \quad \sum_{n=1}^{N} I(S,H;X_n|X^{n-1}) - \sum_{n=1}^{N} I(S,H;Y_n|Y^{n-1}) - F \\ &\quad = \quad \sum_{n=1}^{N} I(S,H,X^{n-1};X_n) - \sum_{n=1}^{N} I(S,H,Y^{n-1};Y_n) - F \\ &\quad \geq \quad \sum_{n=1}^{N} I(S,H,X^{n-1};X_n) - \sum_{n=1}^{N} I(S,H,X^{n-1};Y_n) - F \\ &\quad = \quad NI(U;X) - NI(U;Y) - F, \qquad (38) \end{aligned}$$

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

$$\begin{aligned} &N(L+\delta) \geq I(X^N;H|S) \\ &\quad \geq \quad NI(U;X) - NI(U;Y) - 1 - \delta\log(M_S) - I(S;H), \\ &\quad \geq \quad N(I(U;X) - I(U;Y) - 1/N - \delta\log|\mathcal{X}| - \delta). \quad (39) \end{aligned}$$

If we now let $\delta \downarrow 0$ and $N \to \infty$, then we obtain from (37) that $R \leq I(U;Y)$ and from (39) that $L \geq I(U;X) - I(U;Y)$. This finishes the converse.

B. Outline of the Achievability Proof

We start by fixing a conditional distribution $\{P(u|x), x \in \mathcal{X}, u \in \mathcal{U}\}$. This 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 $2^{NI(U;X)}$ sequences $\underline{u}$. Each of those sequences gets a random s-label and a random h-label. These labels are uniformly chosen. The s-label can assume roughly $2^{NI(U;Y)}$ values, the h-label roughly $2^{N(I(U;X)-I(U;Y))}$ values. The encoder, upon observing the source sequence $\underline{x}$, outputs the s-label corresponding to this sequence as secret, and sends the h-label corresponding to $\underline{x}$ as helper data to the decoder. The decoder observes the source sequence $\underline{y}$ and determines the source sequence $\widehat{\underline{u}}$ with an h-label matching the helper data, such that $(\widehat{\underline{u}},\underline{y}) \in \mathcal{A}_\epsilon^{(N)}(UY)$. It can be shown that the decoder can reliably recover $\underline{u}$ now. It is easy to check that the conditional leakage $I(\underline{X};H|S) \leq I(\underline{X},S;H) \leq H(H)$ is not larger than $N(I(U;X) - I(U;Y))$. An important additional property of the proof is that $\underline{u}$ can be recovered reliably from both the s-label and the h-label. Now, after having proved that $H(\underline{U})$ is roughly equal to $NI(U;X)$ and using that $H(S) \leq NI(U;Y)$ and $H(H) \leq N(I(U;X) - I(U;Y))$, it easily follows that $I(S;H)$ is negligible. Uniformity of the secret S can be demonstrated similarly.

C. Remark

It should be noted that this result is in some way similar to Thm. 2.4 in Csiszar and Narayan [5], the SK-part.

VII. Proof of Thm. 2

A. Converse

As in the converse for secret generation

$$\log(M_S) = H(S) \leq I(S;H) + NI(U;Y) + F. \qquad (40)$$

We used that $I(S,H,Y^{n-1};Y_n) \leq I(S,H,X^{n-1};Y_n)$ since also here $Y^{n-1} - (S,H,X^{n-1}) - Y_n$. As before we defined $U_n \triangleq (S,H,X^{n-1})$ and took a time-sharing variable T uniform over $\{1,2,\cdots,N\}$ and independent of all other variables and set $U \triangleq (U_n,n)$, $X \triangleq X_n$, and $Y \triangleq Y_n$ for $T = n$. Now again $U_n - X_n - Y_n$ and consequently $U - X - Y$. For achievable (R,L) we obtain

$$N(R-\delta) \leq \log(M_S) \leq \frac{1}{1-\delta}\left(N\delta + NI(U;Y) + 1\right), \qquad (41)$$

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

Now we continue with the conditional leakage. Using that X_n is independent of S and X^{n-1} we get

$$\begin{aligned} I(X^N;H|S) &= \sum_{n=1}^{N} I(X_n;H|S,X^{n-1}) \\ &= \sum_{n=1}^{N} I(S,H,X^{n-1};X_n) \\ &= NI(U;X), \qquad (42) \end{aligned}$$

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

$$N(L+\delta) \geq I(X^N;H|S) \geq NI(U;X). \qquad (43)$$

If we now let $\delta \downarrow 0$ and $N \to \infty$, then we find that $R \leq I(U;Y)$ from (41) and that $L \geq I(U;X)$ from (43). The converse is now complete.

B. Outline of the Achievability Proof

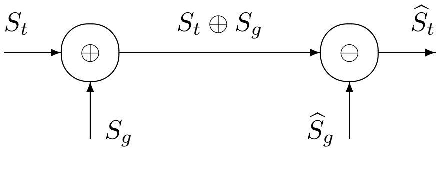

Fig. 8. The masking layer.

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

$$\begin{aligned} H_t &= S_t \oplus S_g, \\ \widehat{S}_t &= H_t \ominus \widehat{S}_g = S_t \oplus (S_g \ominus \widehat{S}_g), \end{aligned} \tag{44}$$

where H_t should be considered as additional helper data.

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

$$\begin{aligned} &I(S_t; H_g, (S_t \oplus S_g)) \\ &\quad= I(S_t; H_g) + I(S_t; (S_t \oplus S_g)|H_g) \\ &\quad\le H(S_t \oplus S_g) - H(S_t \oplus S_g|H_g, S_t) \\ &\quad\le \log(M_S) - H(S_g|H_g, S_t) \\ &\quad= \log(M_S) - H(S_g|H_g) \\ &\quad\le \log(M_S) - H(S_g) + I(S_g; H_g) \end{aligned} \tag{45}$$

and

$$\begin{aligned} I(X^N; H_g, (S_t \oplus S_g)|S_t) &= I(X^N; H_g, S_g|S_t) \\ &\le H(H_g) + H(S_g). \end{aligned} \tag{46}$$

From the basic achievability proof we now obtain that the generated secret is nearly uniform, hence $\log(M_S) - H(S_g)$ is negligible. Moreover we have seen before that $I(S_g; H_g)$ is negligible. Since there are roughly $2^{NI(U;Y)}$ s-labels and roughly $2^{N(I(U;X)-I(U;Y))}$ h-labels, the conditional privacy leakage cannot exceed $NI(U;X)$ significantly, and achievability of Thm. 2 is demonstrated.

VIII. Proof of Thm. 3

A. Converse

We prove here that $\mathcal{R}^{\mathrm{c}}_{\mathrm{zsg}} \subseteq \mathcal{R}_3$. We start with the entropy of the secret.

$$\begin{aligned} &H(S) \\ &\quad= I(S; H, Y^N, P) + H(S|H, Y^N, P, \widehat{S}) \\ &\quad\le I(S; H, Y^N, P) + H(S|\widehat{S}) \\ &\quad\le I(S; H, Y^N, P) + F \\ &\quad= I(S; H) + I(S; P|H) + \sum_{n=1}^{N} I(S; Y_n|H, Y^{n-1}, P) + F \\ &\quad\le I(S; H) + \log(M_P) + \sum_{n=1}^{N} I(S, H, X^{n-1}, P; Y_n) + F \\ &\quad\le I(S; H) + \log(M_P) + NI(U; Y) + F. \end{aligned} \tag{47}$$

We used that $I(S, H, Y^{n-1}, P; Y_n) \le I(S, H, X^{n-1}, Y^{n-1}, P; Y_n) = I(S, H, X^{n-1}, P; Y_n)$ since $Y^{n-1} - (S, H, X^{n-1}, P) - Y_n$. Moreover we created $U = (U_T, T)$ with $U_n \triangleq (S, H, X^{n-1}, P)$ and T as before, resulting in $U - X - Y$. For achievable pairs (R, K) we have that

$$\begin{aligned} &N(R - \delta) \le \log(M_S) \le H(S) + N\delta \\ &\quad\le N\delta + N(K + \delta) + NI(U; Y) + 1 + \delta \log(M_S) \\ &\quad\le N(I(U; Y) + K + 2\delta + 1/N + \delta \log |\mathcal{X}|). \end{aligned} \tag{48}$$

In a similar manner we find for the leakage

$$\begin{aligned} &I(X^N, S; H) \\ &\quad= I(X^N, S, P; H) - I(P; H|X^N, S) \\ &\quad= H(H) - H(P|X^N, S) + H(P|X^N, H, S) \\ &\quad\ge H(H) - H(P) \\ &\quad\ge H(H, \widehat{S}|Y^N, P) - H(S, H|X^N, P) - \log(M_P) \\ &\quad= H(S, H, \widehat{S}|Y^N, P) - H(S|Y^N, P, \widehat{S}, H) \\ &\qquad -H(S, H|X^N, P) - \log(M_P) \\ &\quad\ge H(S, H|Y^N, P) - F - H(S, H|X^N, P) - \log(M_P) \\ &\quad= I(S, H; X^N|P) - I(S, H; Y^N|P) - \log(M_P) - F \\ &\quad= \sum_{n=1}^{N} I(S, H; X_n|P, X^{n-1}) - \sum_{n=1}^{N} I(S, H; Y_n|P, Y^{n-1}) \\ &\qquad - \log(M_P) - F \\ &\quad\ge \sum_{n=1}^{N} I(S, H, X^{n-1}, P; X_n) - \sum_{n=1}^{N} I(S, H, X^{n-1}, P; Y_n) \\ &\qquad - \log(M_P) - F \\ &\quad= NI(U; X) - NI(U; Y) - \log(M_P) - F. \end{aligned} \tag{49}$$

Now we get for achievable (R, K) that

$$\begin{aligned} N\delta &\ge I(X^N, S; H) \\ &\ge N(I(U; X) - I(U; Y)) \\ &\qquad -N(K + \delta) - 1 - \delta N \log |\mathcal{X}|, \end{aligned} \tag{50}$$

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

If we now let $\delta \downarrow 0$ and $N \to \infty$ we first may conclude from (48) that $R \le I(U; Y) + K$. Then (50) yields $K \ge I(U; X) - I(U; Y)$ and hence the converse.

B. Outline of the Achievability Proof

The achievability proof for Thm. 3 is an adapted version of the basic achievability proof for secret generation. The first difference is that the secret is now the index of $\underline{u}$, resulting in a secret rate which is roughly $I(U; X)$. The helper rate is as before roughly $I(U; X) - I(U; Y)$. Moreover, the helper data is made completely uninformative in a one-time-pad way, using the private key resulting in helper data $H \oplus P$ where $\oplus$ denotes addition modulo M_H. Private key rate $I(U; X) - I(U; Y)$ suffices since $I(X^N, S; (H \oplus P)) \le \log(M_H) - H(H \oplus P|X^N, S) = \log(M_H) - H(P|H, X^N, S) = 0$. Using the last property in Sect. III with $\alpha = K - I(U; X) + I(U; Y)$ results in the achievability.

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 is masked.

IX. Proof of Thm. 4

Again we give the converse to this theorem. The achievability proof is only outlined.

A. Converse

We start with the entropy of the secret.

$$
\begin{aligned}
\log(M_S) &= H(S) \\
&= I(S;H,Y^N,P) + H(S|H,Y^N,P,\widehat{S}) \\
&\leq I(S;H,Y^N,P) + H(S|\widehat{S}) \\
&\leq I(S;H,Y^N,P) + F \\
&= I(S;Y^N) + I(S;H|Y^N) + I(S;P|Y^N,H) + F \\
&\leq I(S,Y^N;H) + H(P) + F \\
&\leq I(S,X^N;H) + \log(M_P) + F. \qquad (51)
\end{aligned}
$$

We used that $I(S,Y^N;H) \leq I(S,X^N,Y^N;H) = I(S,X^N;H)$ since $Y^N - X^N, S - H$. For achievable pairs (R,K) we have that

$$N(R-\delta) \leq \log(M_S) \leq \frac{1}{1-\delta}(N\delta + N(K+\delta)+1). \qquad (52)$$

If we let $\delta \downarrow 0$ and $N \to \infty$ we may conclude from (52) that $R \leq K$ which finishes the converse.

B. Outline of the Achievability Proof

The achievability proof follows from using a masking layer in which the secret key is masked by the private key. It is obvious now that there is no privacy leakage. Observe that the biometric sequences are not used!

X. Concluding Remarks

In this paper we have considered privacy leakage in biometric systems. We have investigated systems without an extra private key, and for these systems we have determined how the generated secret key rate relates to the privacy leakage. We have also considered a version of this setup in which the secret key was chosen uniformly and is transmitted.

For the setting in which an extra private key is used by both terminals, we have focussed on the private key rate needed to guarantee negligible privacy leakage for a certain secret key rate. We first considered the case where the key is generated. The case where the secret key is arbitrarily chosen and then transmitted was also investigated. For all cases we could determine the fundamental limits.

The converses that we have constructed are all quite standard, we do not need the "summation by parts" Lemma 7 in of Csiszar and Korner [4].

So far we have only considered conditional privacy leakage, but we will conclude with a few remarks on the unconditional case (where $I(\underline{X};H|S)$ is replaced by $I(\underline{X};H)$ in the definitions of achievability).

Note that achievability in the conditional case implies achievability in the unconditional case since $I(X^N;H) \leq I(S;H) + I(X^N;H|S) = I(X^N,S;H)$ and $I(S;H) \leq I(X^N,S;H)$. (i) Now for secret generation in the unconditional case $\mathcal{R}^{\text{u}}_{\text{sg}} = \mathcal{R}_1$ since the converse in the unconditional case is identical to the converse for the conditional case since $I(X^N;H) = I(X^N,S;H)$ there. (iii) For zero-leakage secret generation in the unconditional case it follows that $\mathcal{R}^{\text{u}}_{\text{zsg}} = \mathcal{R}_3$ if we replace the first steps in the converse for the unconditional case by $I(S;H) + I(X^N;H) \geq I(X^N;H) = H(H) - H(H|X^N) \geq H(H) - H(H,P|X^N) = H(H) - H(P|X^N) \geq H(H) - H(P)$.

(ii) For secret transmission in the unconditional case we get $\mathcal{R}^{\text{u}}_{\text{st}} = \mathcal{R}_1$. The converse is roughly identical to the converse for unconditional secret generation. Achievability follows from the masking layer argument but now we use $I(X^N;H_g,(S_t \oplus S_g)) = I(X^N;H_g) + I(X^N;(S_t \oplus S_g)|H_g) = I(X^N;H_g)$. (iv) For zero-leakage secret transmission in the unconditional case it can be shown that $\mathcal{R}^{\text{u}}_{\text{zst}} = \mathcal{R}_3$. The converse is new. The achievability proof follows from adding two layers to the basic proof, one layer that masks the secret that is to be transmitted by the generated secret (index of $\underline{u}$), and a second layer that masks the generated helper data with the private key. Now $I(X^N;(H_g \oplus P),(S_g \oplus S_t)) = I(X^N;(H_g \oplus P)) + I(X^N;(S_g \oplus S_t)|(H_g \oplus P)) = 0$ and $I(S_t;(H_g \oplus P),(S_g \oplus S_t)) = I(S_t;(S_g \oplus S_t)) + I(S_t;(H_g \oplus P)|(S_g \oplus S_t))) = \log(M_S) - H(S_g)$.

Detailed proofs can be found in [8].

References

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

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

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

[4] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inform. Th.,* Vol. IT - 24, pp. 339 - 348, May 1978.

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

[6] D. Gundüz, E. Erkip, and H.V. Poor, "Secure Lossless Compression with Side Information," *Proc. IEEE Inform. Theory Workshop,* Porto, Portugal, May 5 - 9, 2008.

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

[8] T. Ignatenko and F. Willems, "Biometric Systems: Privacy and Secrecy Aspects," subm. to *IEEE Trans. Inform. Forens. & Secur.,* Sept. 19, 2008.

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

[10] V. Prabhakaran and K. Ramchandran, "On Secure Distributed Source Coding," *Proc. IEEE Inform. Theory Workshop,* Lake Tahoe, California, Sept. 2 - 6, 2007, pp. 442 - 447.

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

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

[13] A.D. Wyner and J. Ziv, "A Theorem on the Entropy of Certain Binary Sequences and Application: Part I," *IEEE Trans. Inform. Th.,* Vol. IT - 19, No. 6, pp. 769 - 773, November 1973.

[14] A.D. Wyner and J. Ziv, "The Rate-Distortion Function for Source Coding with Side Information at the Decoder," *IEEE Trans. Inform. Th.,* Vol. IT - 22, No. 1, pp. 1 - 10, January 1976.

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