Information leakage in fuzzy commitment schemes

Information Leakage in Fuzzy Commitment Schemes

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

***Abstract*—In 1999, Juels and Wattenberg introduced the fuzzy commitment scheme. This scheme is a particular realization of a binary biometric secrecy system with chosen secret keys. It became a popular technique for designing biometric secrecy systems, since it is convenient and easy to implement using standard error-correcting codes. This paper investigates privacy- and secrecy-leakage in fuzzy commitment schemes. The analysis is carried out for four cases of biometric data statistics, i.e., memoryless totally symmetric, memoryless input-symmetric, memoryless, and stationary ergodic. First, the achievable regions are determined for the cases when data statistics are memoryless totally symmetric and memoryless input-symmetric. For the general memoryless and stationary ergodic cases, only outer bounds for the achievable rate-leakage regions are provided. These bounds, however, are sharpened for systematic parity-check codes. Given the achievable regions (bounds), the optimality of fuzzy commitment is assessed. The analysis shows that fuzzy commitment is only optimal for the memoryless totally symmetric case if the scheme operates at the maximum secret-key rate. Moreover, it is demonstrated that for the general memoryless and stationary ergodic cases, the scheme leaks information on both the secret and biometric data.**

***Index Terms*—Biometric secrecy systems, privacy, secret key, security.**

I. Introduction

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, unlike passwords and traditional cryptographic secret keys, biometric information if compromised cannot be canceled and easily substituted: people only have limited resources of biometric data. The latter point combined with the fact that stolen biometric data result in a stolen identity rises privacy concerns associated with the use of biometrics. Indeed, Schneier [1] pointed out that biometric data are not standard secret keys that can be easily canceled. Also Ratha *et al.* [2] investigated the vulnerability points of biometric secrecy systems. In Prabhakar *et al.* [3] security and privacy concerns were raised. Finally, at the DSP forum [4] secrecy and privacy problems and the corresponding protecting technologies were discussed. Thus, deployment of biometrics also requires secure storage and communication of biometric information.

Manuscript received May 20, 2009; revised November 30, 2009; accepted March 10, 2010. Date of publication March 29, 2010; date of current version May 14, 2010. This work was supported in part by SenterNovem, project number IGC03003B. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Hesham El-Gamal.

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.2010.2046984

One of the methods that appeared as a result of recent developments in the area of biometric secrecy systems is fuzzy commitment. The fuzzy commitment scheme, introduced by Juels and Wattenberg [5], is a particular realization of a binary biometric secrecy system with chosen secret keys. In biometric secrecy systems with chosen keys, secret keys are bound 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. A secret key is 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, hence secrecy leakage should be negligible. Important parameters of a biometric system include the size of the secret key and the information that the helper data contain (leak) about the biometric observation. This latter parameter is called privacy leakage. Ideally, privacy leakage should be small, to avoid biometric data of an individual to become 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. In [6], [7], and [8], the fundamental tradeoffs between secret-key and privacy-leakage rates in biometric systems with chosen keys were studied from the information-theoretical point of view. There the achievable secret-key versus privacy-leakage rate regions were determined.

In the fuzzy commitment scheme, the helper data are constructed as a codeword from a selected error-correcting code, used to encode a chosen secret, masked with the biometric sequence that has been observed during enrollment. The scheme is primarily designed for biometric data that are represented by binary uniform memoryless sequences. It is provably secure for this case. The scheme became a popular technique for designing biometric secrecy systems, since it is convenient and easy to implement using standard error-correcting codes. The implementation of fuzzy commitment for different biometric modalities can be found in Kevenaar *et al.* [9] (faces), Hao *et al.* [10] (irises), Campisi *et al.* [11] (signatures), Yang and Verbauwhede [12] (irises), etc. In practice, however, biometric data are rarely uniform. Biometric data used in fuzzy-commitment-based systems, e.g., in the literature mentioned above, do not satisfy the criteria of being uniform and memoryless. Nevertheless, it is assumed that these systems are secure. Also privacy preserving properties of these systems are hardly investigated.

In Smith [13], though, it was already observed that in fuzzy commitment the helper data leak information on the secret if the biometric data are nonuniform, and that they must also leak some information about the biometric data. The privacy leakage corresponding to the maximum secret-key rate for the original uniform memoryless setting was also determined by Tuyls and Goseling [14].

In this paper, we investigate the properties of the fuzzy commitment scheme when the biometric data statistic is memoryless and totally symmetric, memoryless and input-symmetric, memoryless, and stationary ergodic. We use the fundamental secret-key versus privacy-leakage rate tradeoffs found in [6], [7], and [8] to assess the optimality of fuzzy commitment. We show that the fuzzy commitment scheme is only optimal for the totally symmetric memoryless case and only if the scheme operates at the maximum secret-key rate. Moreover, we show that for both the general memoryless and stationary ergodic cases the scheme reveals information on both the secret and biometric data. We are not able to determine the achievable rate-leakage regions for these two cases and only provide outer bounds on the corresponding achievable rate-leakage regions. These bounds are sharpened for systematic parity-check codes.

II. Fuzzy Commitment Scheme

A. Description

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

1) The Totally Symmetric Memoryless Case. We assume that

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

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

$$Q(0,0) = Q(1,1) = (1-q)/2 \tag{2}$$
$$Q(0,1) = Q(1,0) = q/2 \tag{3}$$

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

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

$$Q(1,0) + Q(1,1) = 1/2. \tag{4}$$

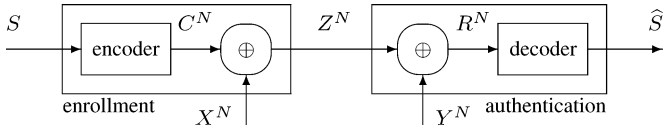


Fig. 1. Fuzzy commitment scheme.

The crossover probability is defined as

$$q \triangleq Q(0,1) + Q(1,0). \tag{5}$$

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

$$q \triangleq Q(0,1) + Q(1,0). \tag{6}$$

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

$$\rho \triangleq Q(1,0) + Q(1,1). \tag{7}$$

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

Now consider the fuzzy commitment scheme (see Fig. 1). In this scheme, a secret key s from alphabet $\{1, 2, \ldots, |\mathcal{S}|\}$ is chosen uniformly at random independently of biometric data, hence

$$\Pr\{S = s\} = 1/|\mathcal{S}| \quad \text{for all} \quad s \in \{1, 2, \ldots, |\mathcal{S}|\}. \tag{8}$$

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

$$z^N = c^N \oplus x^N = e(s) \oplus x^N. \tag{9}$$

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

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

$$r^N = z^N \oplus y^N = e(s) \oplus x^N \oplus y^N. \tag{10}$$

This sum $r^N = \{r_1, r_2, \ldots, r_N\}$ with $r_n \in \{0,1\}$ for $n = 1, 2, \ldots, N$ can be seen as the codeword c^N to which a noise sequence $x^N \oplus y^N$ is added. The received sequence r^N is then

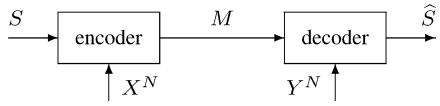


Fig. 2. Model for a biometric system with chosen keys.

decoded, hence the estimate $\widehat{s}$ of the secret key s is determined as

$$\widehat{s} = d(r^N) = d(e(s) \oplus (x^N \oplus y^N)) \tag{11}$$

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

B. Fundamental Regions for Biometric Systems With Chosen Keys

We would like to analyze the fuzzy commitment scheme and assess its optimality. In order to do this, we first give the fundamental tradeoff between secret-key and privacy-leakage rates for a biometric system with chosen secret keys in the memoryless case. These results can be found in [6]–[8].

Consider a generic biometric system with chosen keys (see Fig. 2). This system is based on a biometric source $\{Q(x,y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ that produces an enrollment biometric sequence $x^N = (x_1, x_2, \ldots, x_N)$ with N symbols from the finite alphabet $\mathcal{X}$ and an authentication biometric sequence $y^N = (y_1, y_2, \ldots, y_N)$ having N symbols from the finite alphabet $\mathcal{Y}$. The sequence pair (x^N, y^N) occurs with probability

$$\Pr\{(X^N, Y^N) = (x^N, y^N)\} = \prod_{n=1}^{N} Q(x_n, y_n) \tag{12}$$

hence biometric data statistics is memoryless.

In this system, a secret key S is chosen uniformly and independently of the biometric sequences from alphabet $\{1, 2, \ldots, |\mathcal{S}|\}$. The encoder observes the biometric enrollment source sequence X^N and the secret S and produces helper data M, hence $M = e(S, X^N)$, 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 $\hat{S}$ of the chosen secret, hence $\hat{S} = d(M, Y^N)$, where $d(\cdot,\cdot)$ is the decoder mapping.

In this system, we needed to find out what secret-key rates and privacy-leakage rates could be jointly realized with negligible error probability $\Pr\{\hat{S} \neq S\}$ and negligible secrecy-leakage rate. Here secret-key rates have to be as large as possible and privacy-leakage rates have to be as small as possible.

Definition 1: In a biometric system with chosen keys, a secret-key rate versus privacy-leakage rate pair (R, L_x) with $R \geq 0$ is achievable if for all $\delta > 0$ for all N large enough there exist encoders and decoders such that[1]

$$\begin{aligned} \Pr\{\hat{S} \neq S\} &\leq \delta \\ \frac{1}{N}\log|\mathcal{S}| &\geq R - \delta \\ \frac{1}{N} I(S; M) &\leq \delta \\ \frac{1}{N} I(X^N; M) &\leq L_x + \delta. \end{aligned} \tag{13}$$

[1]Throughout this paper, we take 2 as base of the $\log$.

Moreover, $\mathcal{R}_c^u$ is defined to be the region of all achievable secret-key rate versus privacy-leakage rate pairs for a biometric system with chosen keys.

Using this definition of achievability, in [7], the fundamental region stated in the following theorem was determined.

Theorem 1:

$$\begin{aligned} \mathcal{R}_c^u = \Big\{(R, L_x) : 0 \leq R \leq I(U;Y) \\ L_x \geq I(U;X) - I(U;Y) \\ \text{for } P(u,x,y) = Q(x,y)P(u|x)\Big\}. \end{aligned} \tag{14}$$

C. Definition of Achievable Region for Fuzzy Commitment

It should be noted that fuzzy commitment is a particular realization of a biometric system with chosen keys. It might not be optimal in the information-theoretical sense. Indeed, we will see in the next sections, that it does not always achieve negligible secrecy leakage. Therefore, to analyze fuzzy commitment, we need an extra parameter, secrecy-leakage rate L_s, in the corresponding achievability definition.

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

Definition 2: For a fuzzy commitment scheme, a rate-leakage triple (R, L_s, L_x) with $R \geq 0$ is achievable if for all $\delta > 0$ and for all N large enough, there exist encoders $e(\cdot)$ and decoders $d(\cdot)$ such that

$$\begin{aligned} \Pr\{\widehat{S} \neq S\} &\leq \delta \\ R + \delta \geq \frac{1}{N}\log|\mathcal{S}| &\geq R - \delta \\ \frac{1}{N} I(S; Z^N) &\leq L_s + \delta \\ \frac{1}{N} I(X^N; Z^N) &\leq L_x + \delta. \end{aligned} \tag{15}$$

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

$$\mathcal{R}_{\text{fc}|\text{L}_s=0} \triangleq \{(R, L_x) : (R, 0, L_x) \in \mathcal{R}_{\text{fc}}\} \tag{16}$$

for the zero secrecy-leakage case.

Remark: Here we define the secret-key rate in a slightly different way. This is a technicality needed for our proofs.

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

D. Conditional Versus Unconditional Information Leakage

It is our goal to investigate the information-leakage properties of the fuzzy commitment scheme. Note that in Definition 2 we define the privacy leakage as unconditional mutual

information between biometric enrollment sequence and helper data $I(X^N;Z^N)$, although a stronger definition of the privacy leakage is possible, i.e., the conditional one $I(X^N;Z^N|S)$, as in [6] and [7]. The conditional definition is stronger, since in biometric systems with chosen keys the helper data provide more information on the pair of secret key and biometric data than on each of these entities separately (see [7]). For the conditional definition of privacy leakage, however, we obtain for fuzzy commitment that

$$\begin{aligned} I(X^N;Z^N|S) &= H(Z^N|S) - H(Z^N|X^N,S) \\ &= H(X^N \oplus C^N|S) \\ &\quad - H(X^N \oplus C^N|X^N,S) \\ &= H(X^N|S) = H(X^N) \end{aligned} \tag{17}$$

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

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

$$\begin{aligned} I(S;Z^N) &= H(Z^N) - H(Z^N|S) \\ &= H(Z^N) - H(C^N \oplus X^N|S) \\ &= H(Z^N) - H(X^N) \end{aligned} \tag{18}$$

and

$$\begin{aligned} I(X^N;Z^N) &= H(Z^N) - H(Z^N|X^N) \\ &= H(Z^N) - H(X^N \oplus C^N|X^N) \\ &= H(Z^N) - H(C^N). \end{aligned} \tag{19}$$

III. Totally Symmetric Memoryless Case

A. Statement of Result, Comparison

We have a complete result for the totally symmetric memoryless case. The result is stated in the following theorem. A special case of this result, when the secret-key rate is maximal, is also presented in Smith [13] and in Tuyls and Goseling [14]. The proof of this theorem will be provided in Section III-B.

Theorem 2: For fuzzy commitment in the totally symmetric memoryless case with crossover probability q, the achievable region $\mathcal{R}_{\text{fc}}$ is given by

$$\begin{aligned} \mathcal{R}_{\text{fc}} = \Big\{ (R, L_s, L_x) : 0 \le R \le 1 - h(q) \\ L_s \ge 0 \\ L_x \ge 1 - R \Big\}. \end{aligned} \tag{20}$$

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

Moreover, if we restrict ourselves to the secrecy leakage $L_s = 0$ in Theorem 2, then the corresponding secret-key versus privacy-leakage rate region is given by

$$\begin{aligned} \mathcal{R}_{\text{fc}|\text{L}_s=0} = \Big\{ (R, L_x) : 0 \le R \le 1 - h(q) \\ L_x \ge 1 - R \Big\}. \end{aligned} \tag{21}$$

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

Region $\mathcal{R}_c^u$ given in Theorem 1 (see also [7]) can be stated for the totally symmetric memoryless case as

$$\begin{aligned} \mathcal{R}_c^u = \Big\{ (R, L_x) : 0 \le R \le 1 - h(q * p) \\ L_x \ge h(q * p) - h(p) \\ \text{for some } 0 \le p \le 1/2 \Big\} \end{aligned} \tag{22}$$

where $p * q \triangleq p(1-q) + (1-p)q$.

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

$$L_x \ge 1 - R \ge h(q) \ge h(q * p) - h(p). \tag{23}$$

The last inequality follows from the observation that $h(q*p) - h(p) = H(U|Y) - H(U|X) = I(U;X|Y) \le H(X|Y) = h(q)$, where the Markov condition $U \to X \to Y$ holds and the "channel" between X and U is binary symmetric with crossover probability p. Note that equality in (23) can only be established if $R = 1 - h(q)$ and $p = 0$. Therefore, for rates strictly smaller than $1 - h(q)$, the privacy leakage in the fuzzy commitment scheme is strictly larger than necessary. The coding methods proposed in [7] achieve a strictly smaller privacy leakage.

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

In Fig. 3, we have depicted (marked with "o") the boundary of the optimal rate-leakage region $\mathcal{R}_c^u$ for two values of the crossover probability, i.e., for $q = 0.05$ and $q = 0.15$. Moreover, we have plotted in both figures the boundary of the fuzzy-commitment region $\mathcal{R}_{\text{fc}|\text{L}_s=0}$ (marked with "*"). From Fig. 3, it is clear that the privacy leakage in the fuzzy commitment scheme, even in the totally symmetric memoryless case, is much larger than necessary for the secret-key rates smaller than the maximum rate $1 - h(q)$. This is the main conclusion of this section. In Section IV, we will address fuzzy commitment for the input-symmetric memoryless case. First, however, we will prove Theorem 2.

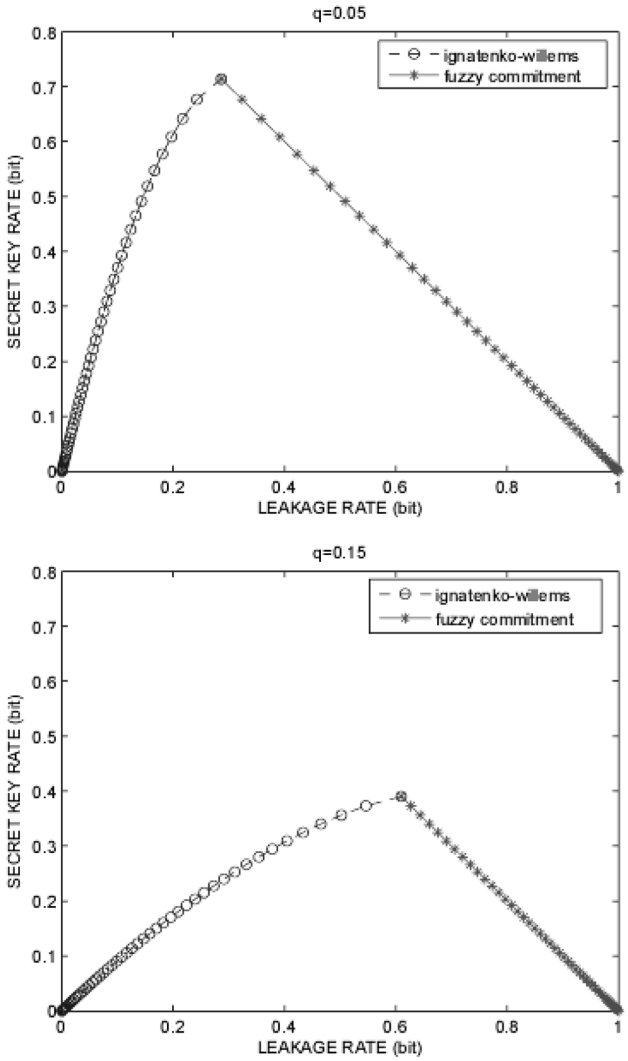


Fig. 3. Secret-key versus privacy-leakage rate regions for two values of the crossover probability q. Marked with "o" is the boundary of the optimal region $\mathcal{R}_c^u$; marked with "*" is the boundary of the fuzzy-commitment region $\mathcal{R}_{\mathrm{fc}|\mathrm{L}_s=0}$.

B. Proof of Theorem 2: Achievability Part

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

$$\Pr\{R^N = r^N | C^N = c^N\} = \prod_{n=1}^{N} \Pr\{R_n = r_n | C_n = c_n\} \tag{24}$$

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

$$\begin{aligned}\Pr\{R_n \neq c_n | C_n = c_n\} &= 1 - \Pr\{R_n = c_n | C_n = c_n\} \\ &= \Pr\{X_n \neq Y_n\} \\ &= Q(1,0) + Q(0,1). \end{aligned} \tag{25}$$

Therefore (see Fig. 4), the channel between C^N and R^N is a binary symmetric channel (BSC) with crossover probability $Q(1,0) + Q(0,1)$. By definition, for all memoryless cases, we have for the crossover probability

$$Q(1,0) + Q(0,1) = q. \tag{26}$$

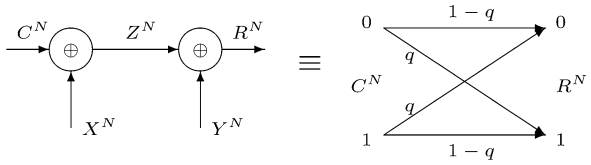


Fig. 4. In the memoryless cases, the channel between C^N and R^N is a BSC with crossover probability $q = Q(0,1) + Q(1,0)$.

It is well-known (see, e.g., Gallager [15, p. 146]) that the capacity of BSC with crossover probability q is $1 - h(q)$. In other words, for $0 \leq R \leq 1 - h(q)$, for all $\varepsilon > 0$ and all N large enough, there exist encoders $e(\cdot)$ and decoders $d(\cdot)$ such that

$$R + \varepsilon \geq \frac{1}{N} \log |\mathcal{S}| \geq R - \varepsilon \tag{27}$$

$$\Pr\{S \neq \widehat{S}\} \leq \varepsilon. \tag{28}$$

We may assume, for small ε at least, that this code does not contain two identical codewords, since any code with $2M-1$ codewords and average error probability $\varepsilon/2 < 1/4$ has a subcode of size M and maximum error probability at most $\varepsilon < 1/2$. This follows from an expurgation argument (see, e.g., Gallager [15, p. 151]). Since the code does not contain two identical codewords, we can assume that $H(C^N) = \log |\mathcal{S}|$. Now we concentrate on such codes and consider the secrecy leakage first. From (18), we obtain that

$$I(S; Z^N) = H(C^N \oplus X^N) - H(X^N) = 0 \leq \varepsilon. \tag{29}$$

Next, for the privacy leakage, we write

$$\begin{aligned} I(X^N; Z^N) &\overset{(a)}{=} H(C^N \oplus X^N) - H(C^N) \\ &\overset{(b)}{=} N - \log |\mathcal{S}| \overset{(c)}{\leq} N(1 - R + \varepsilon) \end{aligned} \tag{30}$$

where step (a) follows from (19), step (b) holds, since the code does not contain identical codewords, and (c) follows from (27).

Then, dividing both sides of (30) by N, and letting $N \to \infty$ and $\varepsilon \downarrow 0$, we conclude from (27)–(30), that the triple $(R, 0, 1 - R)$ is achievable for $0 \leq R \leq 1 - h(q)$.

C. Proof of Theorem 2: Converse Part

Assume that for the fuzzy commitment scheme the triple (R, L_s, L_x) is achievable. Consider first the entropy of the secret

$$\begin{aligned} \log |\mathcal{S}| &= H(S) = I(S; R^N) + H(S|R^N) \\ &\overset{(a)}{=} I(S; C^N \oplus X^N \oplus Y^N) + H(S|R^N, \widehat{S}) \\ &\leq H(C^N \oplus X^N \oplus Y^N) \\ &\quad - H(C^N \oplus X^N \oplus Y^N | S) + H(S|\widehat{S}) \\ &\overset{(b)}{\leq} N - H(X^N \oplus Y^N) + \delta \log |\mathcal{S}| + 1 \\ &\overset{(c)}{=} N - Nh(q) + \delta \log |\mathcal{S}| + 1 \end{aligned} \tag{31}$$

where step (a) follows from the fact that $\widehat{S}$ is a function of R^N, step (b) holds, since C^N is a function of S, (X^N, Y^N) is independent of S, for achievable triples (R, L_s, L_x) we have that

$\Pr\{S \neq \widehat{S}\} \leq \delta$, and due to Fano's inequality, and (c) follows from the fact that $X^N \oplus Y^N$ is a sequence of i.i.d. pairs with crossover probability q.

Dividing both parts of the above expression by N and rearranging the terms, we obtain for achievable triples (R, L_s, L_x) that

$$R - \delta \leq \frac{1}{N}\log|\mathcal{S}| \leq \frac{1}{1-\delta}\left(1 - h(q) + \frac{1}{N}\right). \tag{32}$$

Next we consider the secrecy leakage. Using (18), we get

$$\begin{aligned} L_s + \delta \geq \frac{1}{N} I(S; Z^N) &= \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &= \frac{1}{N}(N - N) = 0. \end{aligned} \tag{33}$$

For the privacy leakage we obtain, using (19), that

$$\begin{aligned} L_x + \delta &\geq \frac{1}{N} I(X^N; Z^N) \\ &= \frac{1}{N}(H(C^N \oplus X^N) - H(C^N)) \\ &\overset{(a)}{\geq} \frac{1}{N}(N - \log|\mathcal{S}|) \overset{(b)}{\geq} 1 - R - \delta \end{aligned} \tag{34}$$

where step (a) follows from the fact that $H(C^N) \leq \log|\mathcal{S}|$, and (b) holds, since for achievable triples (R, L_s, L_x) we have that $\log|\mathcal{S}| \leq N(R + \delta)$.

Now, letting $\delta \downarrow 0$ and $N \to \infty$, and we obtain the converse from (32)–(34).

IV. Input-Symmetric Memoryless Case

A. Statement of Result, Comparison

We start this section with the result that we have obtained for the input-symmetric memoryless case. The proof of this result is identical to the proof of Theorem 2 and therefore is omitted.

Theorem 3: For fuzzy commitment in the input-symmetric memoryless case with crossover probability q the achievable region $\mathcal{R}_{\text{fc}}$ is given by

$$\begin{aligned} \mathcal{R}_{\text{fc}} = \Big\{(R, L_s, L_x) : 0 \leq R \leq 1 - h(q) \\ L_s \geq 0 \\ L_x \geq 1 - R\Big\}. \end{aligned} \tag{35}$$

Now if we again restrict the secrecy leakage to be $L_s = 0$ in Theorem 3, then the corresponding secret-key versus privacy-leakage rate region is given by

$$\begin{aligned} \mathcal{R}_{\text{fc}|L_s=0} = \Big\{(R, L_x) : 0 \leq R \leq 1 - h(q) \\ L_x \geq 1 - R\Big\}. \end{aligned} \tag{36}$$

As before, we can compare the resulting zero secrecy-leakage region $\mathcal{R}_{\text{fc}|L_s=0}$ to the region $\mathcal{R}_c^u$ for the input-symmetric memoryless case when we do not restrict ourselves to fuzzy commitment. This region $\mathcal{R}_c^u$ is given in Theorem 1 (see also [7]).

The maximum secret-key rate that is achievable in the optimal case is $I(X;Y)$, if we take $U \equiv X$ (see also Ahlswede-Csiszár [16]). Note that

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= 1 - H(X \oplus Y|Y) \\ &\geq 1 - H(X \oplus Y) \\ &= 1 - h(q) \end{aligned} \tag{37}$$

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

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

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

$$\begin{aligned} L_x \geq 1 - R \geq h(q) = H(X \oplus Y) \geq H(X|Y) \\ \geq I(X;U|Y) = I(U;X) - I(U;Y) \end{aligned} \tag{38}$$

for all $U \to X \to Y$. Again, for $I(X;Y) > 0$, equality in the above expression is only possible if the biometric source is totally symmetric and if, in addition, $R = 1 - h(q)$. Thus we may conclude that in the input-symmetric case, when $I(X;Y) > 0$ and the source is not totally symmetric, with fuzzy commitment we cannot achieve the privacy leakage, which is optimal in the sense of results presented in [7].

Proposition 2: In the input-symmetric memoryless case, when the source is not totally symmetric, fuzzy commitment is suboptimal with respect to both the achievable secret-key rate and privacy-leakage rate.

V. Memoryless Case

A. Statement of Result, Comparison

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

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

$$h^{-1}(\alpha) \triangleq a \tag{39}$$

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

Theorem 4: For fuzzy commitment in the memoryless case with crossover probability q and probability $\Pr\{X = 1\} = \rho$, we obtain for the achievable region $\mathcal{R}_{\text{fc}}$

$$\begin{aligned} \mathcal{R}_{\text{fc}} \subseteq \Big\{(R, L_s, L_x) : 0 \leq R \leq 1 - h(q) \\ L_s \geq h[\rho * h^{-1}(R)] - h(\rho) \\ L_x \geq h[\rho * h^{-1}(R)] - R\Big\}. \end{aligned} \tag{40}$$

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

Note that the maximum achievable rate $1-h(q)$ for fuzzy commitment can be either smaller, equal, or larger than $I(X;Y)$. In Section IV, where we investigated the input-symmetric case, we have observed that for the general input-symmetric case $I(X;Y) > 1-h(q)$ [see (37)]. On the other hand, for the general memoryless case for which $X \oplus Y$ is independent of Y, we obtain

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(X) - H(X \oplus Y|Y) \\ &\leq 1 - H(X \oplus Y) = 1 - h(q) \end{aligned} \tag{41}$$

and, therefore, also $I(X;Y) < 1-h(q)$ is possible. Thus the rates achievable with fuzzy commitment can also be larger than $I(X;Y)$. However, the Ahlswede-Csiszár result [16] implies that for rates larger than $I(X;Y)$ it is not possible to achieve nonzero secrecy leakage. More precisely, using the fact that for achievable rates $\Pr\{S \neq \widehat{S}\} \leq \delta$ and Fano's inequality, we obtain

$$\begin{aligned} \log|\mathcal{S}| = H(S) &= I(S;R^N) + H(S|R^N) \\ &\leq I(S;Z^N,R^N) + H(S|\widehat{S}) \\ &\leq I(S;Z^N) + I(S;R^N|Z^N) + \delta\log|\mathcal{S}| + 1 \\ &= I(S;Z^N) + H(R^N,Y^N|Z^N) \\ &\quad - H(R^N,Y^N|Z^N,S,C^N) + \delta\log|\mathcal{S}| + 1 \\ &= I(S;Z^N) + H(Y^N|Z^N) \\ &\quad - H(Y^N|Z^N,S,X^N) + \delta\log|\mathcal{S}| + 1 \\ &\leq I(S;Z^N) + H(Y^N) - H(Y^N|X^N) \\ &\quad + \delta\log|\mathcal{S}| + 1 \\ &= I(S;Z^N) + NI(X;Y) + \delta\log|\mathcal{S}| + 1 \end{aligned} \tag{42}$$

hence

$$\begin{aligned} R - \delta &\leq \frac{1}{N}\log|\mathcal{S}| \\ &\leq \frac{1}{1-\delta}\left(\frac{1}{N}I(S;Z^N) + I(X;Y) + \frac{1}{N}\right). \end{aligned} \tag{43}$$

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

Moreover, observe that Theorem 4 implies that zero secrecy leakage is only possible if $R=0$ or $\rho = 1/2$, and zero privacy leakage is only possible if $\rho = 0$ or $R = 1$. The only case of interest, viz. $\rho = 1/2$, though, corresponds to one of the cases considered before.

Observe also that for nontrivial cases for which $I(X;Y) \geq 1-h(q)$ or, in other words, for which the rate is smaller or equal to $I(X;Y)$, the privacy leakage in fuzzy commitment is larger than necessary. Indeed, if $R > 0$, then

$$\begin{aligned} h[\rho * h^{-1}(R)] - R > h(\rho) - R &\geq h(\rho) - (1-h(q)) \\ &\geq H(X) - I(X;Y) \\ &= H(X|Y) \geq I(U;X|Y) \\ &= I(U;X) - I(U;Y) \end{aligned} \tag{44}$$

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

Proposition 3: In the memoryless case, when the source is not totally symmetric, fuzzy commitment results in both secrecy and privacy leakage larger than necessary if $0 < R < 1$ and $\rho \neq 0$.

B. Proof of Theorem 4

We will use Gerber's lemma of Wyner and Ziv [17] to investigate the properties of fuzzy commitment. Therefore, we restate it here for convenience.

Lemma 1 (Gerber's Lemma, [17]): Let C^N be a binary random sequence with entropy $H(C^N) \geq N\nu \geq 0$, and X^N be a binary i.i.d. sequence with entropy $H(X^N) = Nh(\rho)$, then

$$H(C^N \oplus X^N) \geq Nh[\rho * h^{-1}(\nu)]. \tag{45}$$

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

Assume that the rate-leakage triple (R, L_s, L_x) is achievable. Then in the same way as (32), we obtain for achievable triples (R, L_s, L_x) that

$$R - \delta \leq \frac{1}{N}\log|\mathcal{S}| \leq \frac{1}{1-\delta}\left(1 - h(q) + \frac{1}{N}\right). \tag{46}$$

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

$$\begin{aligned} \log|\mathcal{S}| = H(S) &= I(S;R^N) + H(S|R^N,\widehat{S}) \\ &\overset{\text{(a)}}{\leq} I(C^N;R^N) + \delta\log|\mathcal{S}| + 1 \\ &\leq H(C^N) + \delta\log|\mathcal{S}| + 1 \end{aligned} \tag{47}$$

where step (a) follows from the data-processing inequality (see, e.g., Cover and Thomas [18, p. 32]), from the fact that for achievable triples (R, L_s, L_x) we have that $\Pr\{\widehat{S} \neq S\} \leq \delta$ and from Fano's inequality.

Now, using (47), we may conclude that for achievable triples (R, L_s, L_x), it holds that

$$\begin{aligned} \frac{1}{N}H(C^N) &\geq \frac{1}{N}((1-\delta)\log|\mathcal{S}| - 1) \\ &\geq (1-\delta)R - \delta - \frac{1}{N}. \end{aligned} \tag{48}$$

For the secrecy leakage we can write, using Gerber's lemma and (18), that

$$\begin{aligned} L_s + \delta \geq \frac{1}{N}I(S;Z^N) &= \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &\geq h\left[\rho * h^{-1}\left((1-\delta)R - \delta - \frac{1}{N}\right)\right] - h(\rho). \end{aligned} \tag{49}$$

In a similar manner, we find for the privacy leakage that

$$\begin{aligned} L_x + \delta &\geq \frac{1}{N} I(X^N; Z^N) \overset{(a)}{\geq} \frac{1}{N}(H(C^N \oplus X^N) - \log|\mathcal{S}|) \\ &\geq h\left[\rho * h^{-1}\left((1-\delta)R - \delta - \frac{1}{N}\right)\right] - \frac{1}{N}\log|\mathcal{S}| \\ &\overset{(b)}{\geq} h\left[\rho * h^{-1}\left((1-\delta)R - \delta - \frac{1}{N}\right)\right] - R - \delta \end{aligned} \tag{50}$$

where step (a) follows from (19) and the fact that $H(C^N) \leq \log|\mathcal{S}|$, and (b) follows from the definition of achievable rates, since then $\log|\mathcal{S}| \leq N(R+\delta)$.

Now Theorem 4 follows from (46), (49), and (50), if we let $\delta \downarrow 0$ and $N \to \infty$. Note that the continuity of the binary entropy function is essential in this proof.

VI. Stationary Ergodic Case

A. Statement of Result, Comparison

Let X^N and Y^N be stationary ergodic sequences. Now we define $H_\infty(X \oplus Y)$ to be

$$H_\infty(X \oplus Y) \triangleq \lim_{N\to\infty} \frac{1}{N} H(X_1 \oplus Y_1, X_2 \oplus Y_2, \ldots, X_N \oplus Y_N). \tag{51}$$

As in the general memoryless case, we only have an outer bound on the achievable region for the stationary ergodic case. This result is stated in the following theorem.

Theorem 5: For fuzzy commitment in the stationary ergodic case, we obtain for the achievable region $\mathcal{R}_{\text{fc}}$ that

$$\begin{aligned} \mathcal{R}_{\text{fc}} \subseteq \Big\{ &(R, L_s, L_x): \\ &0 \leq R \leq 1 - H_\infty(X \oplus Y) \\ &L_s \geq h[h^{-1}(H_\infty(X)) * h^{-1}(R)] - H_\infty(X) \\ &L_x \geq h[h^{-1}(H_\infty(X)) * h^{-1}(R)] - R \Big\}. \end{aligned} \tag{52}$$

Moreover, reliable codes with rates up to $1 - H_\infty(X \oplus Y)$ exist.

The result of Theorem 5 demonstrates that zero secrecy leakage is only possible if $H_\infty(X) = 1$, which implies that the X-process is independent and uniformly distributed, or if the secret-key rate $R = 0$. Moreover, we may conclude that zero privacy leakage implies that $H_\infty(X) = 0$ or that the secret-key rate $R = 1$. These cases are again of no interest here.

Note that for the stationary ergodic case we do not have an analog of results presented in [7]. Nevertheless, we can compare the fuzzy commitment scheme to the two-layer scheme, which is built as a biometric secret generation system (see Ahlswede-Csiszár [16]) with a masking layer on top of it. In this layer, chosen secret key S is masked with generated key S_g in a one-time pad way (see Vernam [19]).

It is easy to see that the Ahlswede-Csiszár result [16] for the secret generation model also holds in the stationary ergodic case if we use the proof of [20] and the definitions of typical sets as in Cover [21]. Then it can be shown that if the masking layer is used on top of the secret generation model, then for the two-layer scheme, the largest achievable secret-key rate R is equal to $I_\infty(X;Y)$, and, moreover, that this rate is achievable with privacy leakage $H_\infty(X|Y)$.

Now, as in the memoryless case, the maximum achievable rate $1 - H_\infty(X \oplus Y)$ for fuzzy commitment can be smaller than, equal to, or larger than $I_\infty(X;Y)$. However, for rates larger than $I_\infty(X;Y)$, it is not possible to achieve zero secrecy leakage. Indeed, we can write for all small $\epsilon > 0$ and all N large enough, using a similar series of steps as those used to derive (43), that

$$\begin{aligned} R - \delta &\leq \frac{1}{N} H(S) \\ &\leq \frac{1}{1-\delta}\left(\frac{1}{N} I(S; Z^N) + I_\infty(X;Y) \right. \\ &\qquad \left. + \epsilon + \frac{1}{N}\right). \end{aligned} \tag{53}$$

Hence, if the secret-key rate in fuzzy commitment is Δ larger than $I_\infty(X;Y)$, then the secrecy leakage of the scheme is at least Δ.

Now consider nontrivial cases when $1 - H_\infty(X \oplus Y) \leq I_\infty(X;Y)$ and thus $R \leq I_\infty(X;Y)$. We obtain for the privacy leakage in the fuzzy commitment scheme when $R > 0$ that

$$\begin{aligned} &h[h^{-1}(H_\infty(X)) * h^{-1}(R)] - R \\ &\quad > H_\infty(X) - R \\ &\quad \geq H_\infty(X) - (1 - H_\infty(X \oplus Y)) \\ &\quad \geq H_\infty(X) - I_\infty(X;Y) \\ &\quad = H_\infty(X|Y) \end{aligned} \tag{54}$$

which demonstrates that with the two-layer scheme we can obtain smaller privacy leakage than with fuzzy commitment.

Proposition 4: In the stationary ergodic case, fuzzy commitment is not optimal with respect to both secrecy and privacy leakage if $0 < H_\infty(X) < 1$ and $0 < R < 1$.

B. Proof of Theorem 5

1) Binary Analog to the Entropy-Power Inequality: Before proving the results for fuzzy commitment in the stationary ergodic case, we need an auxiliary result. The entropy-power inequality (see Shannon [22]) is a useful lower bound for the differential entropy of a sum of two independent real-valued stationary random sequences. We are interested in a similar bound for stationary binary sequences. The binary analog to the entropy-power inequality was derived by Shamai and Wyner [23]. For our purposes, we need an adapted version of this binary analog to the entropy-power inequality.

Assume that a biometric sequence X^N is a stationary binary sequence with entropy

$$\begin{aligned} H_\infty(X) &= \lim_{N\to\infty} \frac{1}{N} H(X_1, X_2, \ldots, X_N) \\ &= \lim_{N\to\infty} H(X_N | X_1, X_2, \ldots, X_{N-1}). \end{aligned} \tag{55}$$

Moreover, now for the binary entropy function $h(\cdot)$ for $0 \leq \alpha \leq 1$, its inverse $h^{-1}(\alpha) = a$, defined as in the previous section, corresponds to the probability a in a binary i.i.d. sequence with entropy α.

Lemma 2: For the binary mutually independent sequences X^N and C^N, if X^N is stationary with entropy $H_\infty(X)$ and $H(C^N) \geq N\nu$, the following statement holds:

$$\frac{1}{N}H(Z^N) \geq h[h^{-1}(H_\infty(X)) * h^{-1}(\nu)] \tag{56}$$

where $Z^N = (Z_1, Z_2, \ldots, Z_N) = (X_1 \oplus C_1, X_2 \oplus C_2, \ldots, X_N \oplus C_N)$. This is an adapted version of the binary analog to the entropy-power inequality (Shamai and Wyner [23]).

Proof of Lemma 2: We denote $X^{n-1} = (X_1, X_2, \ldots, X_{n-1})$ for $n = 1, 2, \ldots, N$, and also C^{n-1} and Z^{n-1} in the same way.

Now from Shamai and Wyner [23] the second to last equation, from the facts that $H_\infty(X) \leq H(X_n|X^{n-1})$ and $0 \leq h^{-1}(\cdot) \leq 1/2$, it follows that

$$\begin{aligned} H(Z_n|Z^{n-1}) &\geq h[h^{-1}(H(X_n|X^{n-1})) \\ &\quad * h^{-1}(H(C_n|C^{n-1}))] \\ &\geq h[h^{-1}(H_\infty(X)) * h^{-1}(H(C_n|C^{n-1}))]. \end{aligned} \tag{57}$$

Next, we find that

$$\begin{aligned} &\frac{1}{N}H(Z^N) \\ &\quad = \frac{1}{N}\sum_{n=1}^{N} H(Z_n|Z^{n-1}) \\ &\quad \geq \frac{1}{N}\sum_{n=1}^{N} h[h^{-1}(H_\infty(X)) * h^{-1}(H(C_n|C^{n-1}))] \\ &\quad \overset{(a)}{\geq} h\left[h^{-1}(H_\infty(X)) * h^{-1}\left(\frac{1}{N}\sum_{n=1}^{N} H(C_n|C^{n-1})\right)\right] \\ &\quad = h[h^{-1}(H_\infty(X)) * h^{-1}(\nu)] \end{aligned} \tag{58}$$

where (a) follows from convexity of $h(\beta * h^{-1}(u))$ in u, since its second derivative is positive (for the details, see Wyner and Ziv [17]), and from Jensen's inequality (see, e.g., Cover and Thomas [18, p. 25]).

2) Proof of Theorem 5: The fact that reliable codes with rates up to $1 - H_\infty(X \oplus Y)$ exist for stationary ergodic $X \oplus Y$-processes follows from Verdu and Han [24, p. 1156]. It is essential that the noise process is ergodic here.

Next assume that for the fuzzy commitment scheme, the triple (R, L_s, L_x) is achievable. Then we obtain for the entropy of the secret that

$$\log|\mathcal{S}| = H(S) \leq N - H(X^N \oplus Y^N) + \delta \log|\mathcal{S}| + 1 \tag{59}$$

where the inequality in the above expression holds if we apply the same series of steps as in (31) and use the fact that for achievable triples (R, L_s, L_x) we have that $\Pr\{\widehat{S} \neq S\} \leq \delta$. Dividing both parts of the above expression by N and rearranging the terms, we obtain for achievable triples (R, L_s, L_x) that

$$\begin{aligned} R - \delta \leq \frac{1}{N}\log|\mathcal{S}| &\leq \frac{1}{1-\delta} \\ &\quad \times \left(1 - \frac{1}{N}H(X^N \oplus Y^N) + \frac{1}{N}\right). \end{aligned} \tag{60}$$

Next, note that $H(C^N) \geq N((1-\delta)R - \delta - 1/N)$, since (48) also holds here. Using Lemma 2 and (18), we obtain that

$$\begin{aligned} L_s + \delta &\geq \frac{1}{N}I(S; Z^N) = \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &\geq h\left[H_\infty(X) * h^{-1}\left((1-\delta)R - \delta - \frac{1}{N}\right)\right] \\ &\quad - \frac{1}{N}H(X^N). \end{aligned} \tag{61}$$

In a similar manner, we find for the privacy leakage that

$$\begin{aligned} &L_x + \delta \\ &\quad \geq \frac{1}{N}I(X^N; Z^N) \overset{(a)}{\geq} \frac{1}{N}(H(X^N \oplus C^N) - \log|\mathcal{S}|) \\ &\quad \geq h\left[h^{-1}(H_\infty(X)) * h^{-1}\left((1-\delta)R - \delta - \frac{1}{N}\right)\right] \\ &\quad\quad - \frac{1}{N}\log|\mathcal{S}| \\ &\quad \overset{(b)}{\geq} h\left[h^{-1}(H_\infty(X)) * h^{-1}\left((1-\delta)R - \delta - \frac{1}{N}\right)\right] \\ &\quad\quad - R - \delta \end{aligned} \tag{62}$$

where step (a) follows from (19) and the fact that $H(C^N) \leq \log|\mathcal{S}|$, and (b) holds, since for achievable triples (R, L_s, L_x) we have that $\log|\mathcal{S}| \leq N(R + \delta)$.

Now Theorem 5 follows from (60), (61), and (62) if we let $\delta \downarrow 0$ and $N \to \infty$.

VII. Tighter Bounds With Systematic Parity-Check Codes

A. Tighter Bounds for the Stationary Ergodic Case

Better lower bounds on the leakages can be obtained if we use binary systematic parity-check codes. We assume that the information symbols are followed by the parity symbols. First, we need the following result, though.

Lemma 3: Let C^N be the sequence of random variables corresponding to a binary linear code where the first $\log|\mathcal{S}|$ information symbols (the systematic part) are followed by $N - \log|\mathcal{S}|$ parity symbols. In this way, $H(C_n|C^{n-1}) = 1$ for $n \leq \log|\mathcal{S}|$ and $H(C_n|C^{n-1}) = 0$ for $n > \log|\mathcal{S}|$, where we also assume that $|\mathcal{S}|$ is a power of 2, and hence $\log|\mathcal{S}|$ is integer. Then for the mutually independent sequences of binary variables X^N and C^N, if X^N is stationary with entropy $H_\infty(X)$ and $H(C^N) \geq N\nu$, the following statement holds:

$$\frac{1}{N}H(C^N \oplus X^N) \geq H_\infty(X) + \nu(1 - H_\infty(X)). \tag{63}$$

Proof of Lemma 3: Using (58) from the proof of Lemma 2, we can write

$$\begin{aligned}\frac{1}{N}H(Z^N) &= \frac{1}{N}\sum_{n=1}^{N} H(Z_n|Z^{n-1}) \\ &\geq \frac{1}{N}\left(\sum_{n=1}^{\log|\mathcal{S}|} h[h^{-1}(H_\infty(X)) * h^{-1}(1)] \right. \\ &\qquad \left. + \sum_{n=\log|\mathcal{S}|+1}^{N} h[h^{-1}(H_\infty(X)) * h^{-1}(0)]\right) \\ &= \frac{1}{N}(\log|\mathcal{S}| + (N - \log|\mathcal{S}|)H_\infty(X)) \\ &\geq H_\infty(X) + \frac{1}{N}\log|\mathcal{S}|(1 - H_\infty(X)) \\ &\geq H_\infty(X) + \nu(1 - H_\infty(X)) \end{aligned} \tag{64}$$

where the last inequality follows from $\log|\mathcal{S}| \geq H(C^N) \geq N\nu$. This concludes the proof.

Theorem 6: For fuzzy commitment in the stationary ergodic case, if systematic parity-check codes are applied, we obtain for the achievable region $\mathcal{R}_{\text{fc}}$ that

$$\begin{aligned}\mathcal{R}_{\text{fc}} \subseteq \Big\{(R, L_s, L_x) : 0 \leq R \leq 1 - H_\infty(X \oplus Y) \\ L_s \geq R(1 - H_\infty(X)) \\ L_x \geq H_\infty(X)(1 - R)\Big\}. \end{aligned} \tag{65}$$

From this theorem, we may conclude that in the stationary ergodic case, when systematic parity-check codes are used in fuzzy commitment, the secrecy leakage can only be zero if the secret-key rate $R = 0$ or if the entropy $H_\infty(X) = 1$. On the other hand, zero privacy leakage implies that either the secret-key rate $R = 1$ or the entropy $H_\infty(X) = 0$. However, these cases are not interesting, apart from $H_\infty(X) = 1$, which, on the other hand, corresponds to the one of the cases considered in Sections III and IV.

Proof of Theorem 6: Assume that the triple (R, L_s, L_x) is achievable. Just as in Theorem 5 we obtain that

$$R - \delta \leq \frac{1}{N}\log|\mathcal{S}| \leq \frac{1}{1-\delta}\left(1 - \frac{1}{N}H(X^N \oplus Y^N) + \frac{1}{N}\right). \tag{66}$$

Moreover, we have that $H(C^N) \geq N((1-\delta)R - \delta - 1/N)$, since (48) also holds here. Then, using Lemma 3 and (18), we can write for the secrecy leakage that

$$\begin{aligned} L_s + \delta &\geq \frac{1}{N}I(S; Z^N) = \frac{1}{N}(H(C^N \oplus X^N) - H(X^N)) \\ &\geq (1 - H_\infty(X))\left(R - \delta - \delta R - \frac{1}{N}\right) \\ &\quad + H_\infty(X) - \frac{1}{N}H(X^N). \end{aligned} \tag{67}$$

In a similar way, we obtain for the privacy leakage that

$$\begin{aligned} L_x + \delta &\geq \frac{1}{N}I(X^N; Z^N) \\ &\overset{(a)}{\geq} \frac{1}{N}(H(X^N \oplus C^N) - \log|\mathcal{S}|) \\ &\geq \left((1-\delta)R - \delta - \frac{1}{N}\right)(1 - H_\infty(X)) \\ &\quad + H_\infty(X) - \frac{1}{N}\log|\mathcal{S}| \\ &\overset{(b)}{\geq} H_\infty(X)\left(1 - (1-\delta)R + \frac{1}{N}\right) \\ &\quad - 2\delta - \delta R - \frac{1}{N} \end{aligned} \tag{68}$$

where step (a) follows from (19) and the fact that $H(C^N) \leq \log|\mathcal{S}|$, and (b) holds, since for achievable triples (R, L_s, L_x) we have that $\log|\mathcal{S}| \leq N(R + \delta)$. Now from (66), (67), and (68), letting $\delta \downarrow 0$ and $N \to \infty$, we obtain the proof.

The fact that the leakage bounds in Theorem 6 are indeed stronger than the bounds obtained in Theorem 5 follows from convexity. Let U be 1 with probability R and 0 with probability $1 - R$. Then from convexity of $h(\beta * h^{-1}(u))$ in u, we obtain

$$\begin{aligned} &h[h^{-1}(H_\infty(X)) * h^{-1}(R)] \\ &\quad \leq R\,h[h^{-1}(H_\infty(X)) * h^{-1}(1)] \\ &\qquad + (1-R)h[h^{-1}(H_\infty(X)) * h^{-1}(0)] \\ &\quad = R + H_\infty(X) - RH_\infty(X). \end{aligned} \tag{69}$$

Therefore, it follows that

$$\begin{aligned} &h[h^{-1}(H_\infty(X)) * h^{-1}(R)] - H_\infty(X) \\ &\quad \leq R + H_\infty(X) - RH_\infty(X) - H_\infty(X) \\ &\quad = R(1 - H_\infty(X)) \end{aligned} \tag{70}$$

$$\begin{aligned} &h[h^{-1}(H_\infty(X)) * h^{-1}(R)] - R \\ &\quad \leq R + H_\infty(X) - RH_\infty(X) - R \\ &\quad = H_\infty(X)(1 - R). \end{aligned} \tag{71}$$

B. Tighter Bounds for the Memoryless Case

Note that Lemma 3 also holds in the memoryless case, when X^N is i.i.d. with $\Pr\{X{=}1\} = \rho$. Then (63) takes the following form

$$\frac{1}{N}H(C^N \oplus X^N) \geq h(\rho) + \nu(1 - h(\rho)). \tag{72}$$

Now the tighter bounds on the achievable region for the general memoryless case, when systematic parity-check codes are used, are given by the following theorem. The proof of this theorem is identical to the proof of Theorem 6 and is, therefore, omitted.

Theorem 7: For fuzzy commitment in the memoryless case with crossover probability q and probability $\Pr\{X = 1\} = \rho$

if systematic parity-check codes are applied, we obtain for the achievable region $\mathcal{R}_{\text{fc}}$ that

$$\mathcal{R}_{\text{fc}} \subseteq \Big\{(R, L_s, L_x) : 0 \le R \le 1 - h(q) \\ L_s \ge R(1 - h(\rho)) \\ L_x \ge h(\rho)(1 - R)\Big\}. \quad (73)$$

Remark: It should be noted that for the totally symmetric memoryless case and input-symmetric memoryless case, the bounds given in the above theorem reduces to the regions given in Theorem 2 and Theorem 3, respectively.

VIII. Conclusion

In this paper, we have considered fuzzy commitment and investigated its secrecy and privacy leakage properties. It turns out that fuzzy commitment is not privacy preserving in the conditional privacy-leakage sense.

Next we have concentrated on unconditional privacy leakage. Our analysis has shown that fuzzy commitment is only optimal for the totally symmetric memoryless case if it operates at the maximum secret-key rate. For secret-key rates which are below the capacity, the scheme is not optimal with respect to privacy leakage. However, it is still optimal with respect to secret-key rates and secrecy leakage.

For the input-symmetric memoryless case, we have concluded that fuzzy commitment is suboptimal with respect to both the achievable secret-key rate and privacy-leakage rate. It still enjoys zero secrecy leakage, though.

In the general memoryless and stationary ergodic cases, we could only determine outer bounds on the achievable regions. Moreover, we could sharpen these bounds for the case when systematic parity-check codes are used in fuzzy-commitment-based biometric systems.

The results for the memoryless case have revealed that fuzzy commitment leads to both secrecy and privacy leakage that are larger than necessary. One may argue that for the memoryless case with fuzzy commitment, we can achieve larger secret-key rates than with the optimal scheme. However, we have shown that this increase may only come at the expense of secrecy leakage.

The results for the stationary ergodic case have also demonstrated that fuzzy commitment has nonzero secrecy and privacy leakage in nontrivial cases. We cannot assess its optimality, though, as we do not have an analog of results presented in [7] for the stationary ergodic case. Therefore, we have compared the fuzzy commitment scheme to a two-layer scheme (which is based on a biometric secret generation model with a masking layer on top of it) for stationary ergodic biometric sources at maximum secret-key rate. It turns out that the two-layer scheme enjoys better properties.

Finally, we would like to note that in order to achieve secure fuzzy commitment either privacy amplification techniques additionally have to be used (see, e.g., [25]) or an extra step in which uniform memoryless bits are extracted out of biometric sequences has to be performed (see [26]). In general, for the memoryless case, an optimal biometric system with chosen keys should be realized according to the coding principles suggested in [7].

Appendix A
Independence Implies Total Symmetry

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

$$\begin{aligned} Q(1,0) &= \Pr\{X \oplus Y = 1, Y = 0\} \\ &= \Pr\{X \oplus Y = 1\} \Pr\{Y = 0\} = q(1 - \beta) \\ Q(1,1) &= \Pr\{X \oplus Y = 0, Y = 1\} \\ &= \Pr\{X \oplus Y = 0\} \Pr\{Y = 1\} = (1 - q)\beta. \end{aligned} \quad (74)$$

Input-symmetry implies that

$$Q(1,0) + Q(1,1) = q(1 - \beta) + (1 - q)\beta = 1/2. \quad (75)$$

For $q \neq 1/2$, (75) has solution $\beta = 1/2$, and then the statistics is totally symmetric.

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

$$\begin{aligned} Q(0,0) &= \Pr\{X \oplus Y = 0\} \Pr\{Y = 0\} = (1 - \beta)/2 \\ Q(0,1) &= \Pr\{X \oplus Y = 1\} \Pr\{Y = 1\} = \beta/2 \\ Q(1,0) &= \Pr\{X \oplus Y = 1\} \Pr\{Y = 0\} = (1 - \beta)/2 \\ Q(1,1) &= \Pr\{X \oplus Y = 0\} \Pr\{Y = 1\} = \beta/2 \end{aligned} \quad (76)$$

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

References

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

[2] 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.

[3] 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.

[4] A. Vetro, A. K. Jain, R. Chellappa, S. C. Draper, N. Memon, and P. J. Phillips, "Forum on signal processing for biometric systems," *IEEE Signal Process. Mag.*, vol. 24, no. 6, pp. 146–152, Nov. 2007.

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

[6] T. Ignatenko and F. Willems, "Privacy leakage in biometric secrecy systems," in *Proc. 46th Annu. Allerton Conf. Communication, Control, and Computing 2008*, Monticello, IL, Sep. 23–26, 2008, pp. 850–857.

[7] T. Ignatenko and F. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pt. 2, pp. 956–973, Dec. 2009.

[8] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proc. 46th Annu. Allerton Conf. Comm., Control, and Computing*, Monticello, IL, Sep. 23–26, 2008.

[9] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in *Proc. AutoID*, 2005, pp. 21–26.

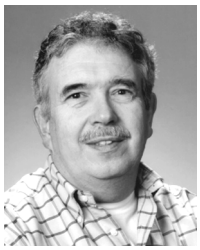
[10] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[11] P. Campisi, E. Maiorana, M. Prats, and A. Neri, "Adaptive and distributed cryptography for signature biometrics protection," in *Proc. SPIE Conf. Sec., Steg. and Water. of Multim. Contents IX*, San Jose, CA, 2007, vol. 6505.

[12] S. Yang and I. Verbauwhede, "Secure iris verification," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, 2007, vol. 2, pp. 133–136.
[13] A. Smith, "Maintaining Secrecy When Information Leakage is Unavoidable," Ph.D. dissertation, MIT, Cambridge, MA, 2004.
[14] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *Proc. ECCV Workshop BioAW*, 2004, pp. 158–170.
[15] R. Gallager, *Information Theory and Reliable Communcation*. New York: Wiley, 1968.
[16] 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.
[17] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications—I," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, Nov. 1973.
[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
[19] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Trans. Amer. Inst. Elect. Eng.*, vol. XLV, pp. 295–301, Jan. 1926.
[20] T. Ignatenko and F. Willems, "On the security of the xor-method in biometric authentication systems," in *Proc. 27th Symp. Inf. Theory in the Benelux 2006*, Noordwijk, The Netherlands, Jun. 8–9, 2006, pp. 197–204.
[21] T. Cover, "A proof of the data compression theorem of Slepain and Wolf for ergodic sources," *IEEE Trans. Inf. Theory*, vol. 22, no. 2, pp. 226–228, Mar. 1975.
[22] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 623–656, 1948.
[23] S. Shamai and A. Wyner, "A binary analog to the entropy-power inequality," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1428–1430, Nov. 1990.
[24] S. Verdu and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1147–1157, Jul. 1994.
[25] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," in *Proc. ISIT: Proc. IEEE Int. Symp. Inf. Theory, Sponsored by The Information Theory Society of The Institute of Electrical and Electronic Engineers*, Trondeheim, Norway, 1994.
[26] T. Ignatenko and F. Willems, "Achieving secure fuzzy commitment scheme for optical pufs," in *Proc. 5th Int. Conf. Intelligent Inf. Hiding and Multimedia Signal Processing 2009*, Kyoto, Japan, Sep. 12–14, 2009, pp. 1185–1188.

Tanya Ignatenko (S'06–M'08) was born in Minsk, 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.

Since 2008, 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.