Privacy leakage in fuzzy commitment schemes

Privacy Leakage in Fuzzy Commitment Schemes

Tanya Ignatenko
Eindhoven University of Technology
Dept. EE, Signal Processing Systems Group
P.O.Box 513, 5600 MB Eindhoven, The Netherlands
t.ignatenko@tue.nl

Abstract

In 1999 Juels and Wattenberg introduced the fuzzy commitment scheme. Fuzzy commitment is a particular realization of a binary biometric secrecy system with a chosen secret key. Three cases of biometric sources are considered, i.e. memoryless and totally-symmetric biometric sources, memoryless and input-symmetric biometric sources, and memoryless biometric sources. It is shown that fuzzy commitment is only optimal for memoryless totally-symmetric biometric sources and only at the maximum secret-key rate. Moreover, it is demonstrated that for memoryless biometric sources, which are not input-symmetric, the fuzzy commitment scheme leaks information on both the secret key and the biometric data.

1 Introduction

Fuzzy commitment, introduced by Juels and Wattenberg [1], is a particular realization of a binary biometric secrecy system with chosen secret keys. In fuzzy commitment the helper data are constructed as a codeword from an error-correcting code, used to encode a chosen secret, masked with the biometric sequence observed during enrollment. The scheme is primarily designed for binary uniform memoryless biometric sequences.

The scheme became a popular technique for designing biometric secrecy systems, since it is convenient and easy to implement using standard error-correcting codes. Its implementation for different biometric modalities can be found in Kevenaar et al. [2] (faces), Hao et al. [3] (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 the privacy properties of these systems are hardly investigated. In Smith [4], though, it was observed that in fuzzy commitment the helper data leak information on the secret if the biometric data are non-uniform, 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 [5].

In this paper we investigate the properties of fuzzy commitment when the biometric data statistic is memoryless and totally-symmetric, memoryless and input-symmetric, and memoryless. 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 the general memoryless case the scheme reveals information on both the secret and biometric data.

2 The Fuzzy Commitment Scheme

2.1 Description

We start with description of 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 $n = 1, 2, \ldots, N$. The 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 cases, i.e. the totally-symme-tric memoryless case, the input-symmetric memoryless case, and the memory-less 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 $Q(0,0) = Q(1,1) = (1-q)/2$, and $Q(0,1) = Q(1,0) = q/2$, 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 $Q(1,0) + Q(1,1) = 1/2$. The crossover probability is defined as $q \triangleq Q(0,1) + Q(1,0)$.

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 $q \triangleq Q(0,1) + Q(1,0)$. Now also the probability that X is equal to 1 becomes an important parameter, and we define $\rho \triangleq Q(1,0) + Q(1,1)$.

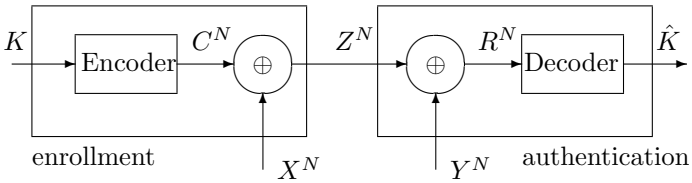

Figure 1: A fuzzy commitment scheme.

Now consider the fuzzy commitment scheme, presented in Fig. 1. In this scheme a secret key k from alphabet $\{1, 2, \ldots, |\mathcal{K}|\}$ is chosen uniformly at random independently of biometric data, hence $\Pr\{K = k\} = 1/|\mathcal{K}|$ for all $k \in \{1, 2, \ldots, |\mathcal{K}|\}$. The chosen secret key k is observed at the enrollment side together with a biometric enrollment sequence x^N. The secret key k 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 $c^N = e(k)$, where $e(\cdot)$ is the encoding function. Then the biometric enrollment sequence is added modulo 2 to the 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 $z^N = c^N \oplus x^N = e(k) \oplus x^N$. 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 $r^N = z^N \oplus y^N = e(k) \oplus x^N \oplus y^N$. 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. This codeword r^N is then decoded, hence the estimate $\widehat{k}$ of the secret key k is determined as $\widehat{k} = d(r^N) = d(e(k) \oplus (x^N \oplus y^N))$, where $d(\cdot)$ is the decoding function.

Now we require the scheme to be such that the error probability $\Pr\{\widehat{K} \neq K\}$ is as small as possible, while the number of secret keys $|\mathcal{K}|$ should be as large as possible. Moreover, we want the amount of information that the helper data leak about the secret $I(K; Z^N)$ and about the biometric data $I(X^N; Z^N)$ to be as small as possible.

Definition 2.1 *For fuzzy commitment a rate - leakage triple (R, L_k, 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*

$$\begin{aligned} \Pr\{\widehat{K} \neq K\} &\leq \delta, \\ R + \delta \geq \log|\mathcal{K}|/N &\geq R - \delta, \\ I(K; Z^N)/N &\leq L_k + \delta, \\ I(X^N; Z^N)/N &\leq L_x + \delta. \end{aligned} \tag{2}$$

Moreover, we define $\mathcal{R}_{fc}$ to be the region of all achievable rate - leakage triples for a fuzzy commitment scheme. We also define the secret-key vs. privacy-leakage rate region $\mathcal{R}_{fc|L_k=0} \triangleq \{(R, L_x) : (R, 0, L_x) \in \mathcal{R}_{fc}\}$, for the zero secrecy-leakage case.

In the next sections we will investigate the properties of the region of achievable rate-leakage triples for each of the three biometric statistics cases described before.

First, however, note that the secrecy and privacy leakage can be rewritten as

$$I(K; Z^N) = H(Z^N) - H(C^N \oplus X^N | K) = H(Z^N) - H(X^N), \tag{3}$$

$$I(X^N; Z^N) = H(Z^N) - H(X^N \oplus C^N | X^N) = H(Z^N) - H(C^N). \tag{4}$$

3 The Totally-Symmetric Memoryless Case

3.1 Statement of Results, Discussion

We have a complete result for the totally-symmetric memoryless case.

Theorem 3.1 *For fuzzy commitment in the totally-symmetric memoryless case with crossover probability q, the achievable region $\mathcal{R}_{fc}$ is given by*

$$\begin{aligned} \mathcal{R}_{fc} = \big\{(R, L_k, L_x) \;:\; & 0 \leq R \leq 1 - h(q), \\ & L_k \geq 0, \\ & L_x \geq 1 - R \qquad \big\}. \end{aligned} \tag{5}$$

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

Moreover, if we restrict ourselves to the secrecy leakage $L_k = 0$ in Thm. 3.1, then

$$\begin{aligned} \mathcal{R}_{\mathrm{fc}|L_k=0} = \big\{(R, L_x) \;:\; & 0 \leq R \leq 1 - h(q), \\ & L_x \geq 1 - R \qquad \big\}. \end{aligned} \tag{6}$$

This result can be compared to the corresponding secret-key vs. privacy-leakage rate region $\mathcal{R}^u_{ck}$ in a biometric model with a transmitted (chosen) key, where we do not restrict ourselves to fuzzy commitment. This region was determined in [6]. Although the achievable regions $\mathcal{R}_{\mathrm{fc}|L_k=0}$ and $\mathcal{R}^u_{ck}$ are defined slightly different, the general region $\mathcal{R}^u_{ck}$ also provides for a given secret-key rate the corresponding minimum privacy leakage. Thus we can compare regions $\mathcal{R}_{\mathrm{fc}|L_k=0}$ and $\mathcal{R}^u_{ck}$ for given secret-key rates.

Region $\mathcal{R}^u_{ck}$ can be stated for the totally-symmetric memoryless case as

$$\begin{aligned} \mathcal{R}^u_{ck} = \big\{(R, L_x) \;:\; & 0 \leq R \leq 1 - h(q * p), \\ & L_x \geq h(q * p) - h(p), \\ & \text{for some } 0 \leq p \leq 1/2 \big\}, \end{aligned} \tag{7}$$

where $p * q \stackrel{\Delta}{=} p(1-q) + (1-p)q$. Now it follows that for the privacy leakage for fuzzy commitment we obtain

$$L_x \;\geq\; 1 - R = h(q) \geq h(q * p) - h(p). \tag{8}$$

The last inequality follows from the observation that $h(q * p) - h(p) = H(U|Y) - H(U|X) = I(U; X|Y) \leq H(X|Y) = h(q)$, where Markov condition $U \to X \to Y$ holds and the "channel" between X and U is binary symmetric with crossover probability p. Equality in (8) can only be established if $R = 1 - h(q)$. Hence for rates strictly smaller than $1 - h(q)$ the privacy leakage of fuzzy commitment is strictly larger than necessary. The coding methods proposed in [6] achieve smaller privacy leakage.

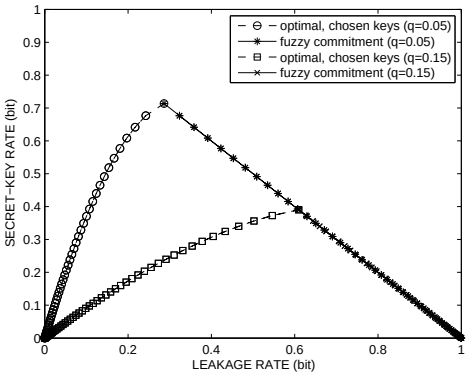

Figure 2: Secret-key vs. privacy-leakage rate regions for two values of q.

In Fig. 2 we have depicted (marked with "o" and "□") the boundary of the optimal rate-leakage region $\mathcal{R}^u_{ck}$ 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 $\mathcal{R}_{\text{fc}}|L_k = 0$ (marked with "*" and "×"). From Fig. 2 it is clear that the privacy leakage of the fuzzy commitment scheme, even in the totally-symmetric memoryless case, is much larger than necessary for secret-key rates smaller than the maximum rate $1 - h(q)$. This is the main conclusion of this section.

3.2 Proof of Thm. 3.1

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

$$\Pr\{R^N = r^N | C^N = c^N\} \;=\; \prod_{n=1}^{N} \Pr\{R_n = r_n | C_n = c_n\}, \tag{9}$$

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

$$\Pr\{R_n \neq c_n | C_n = c_n\} = 1 - \Pr\{R_n = c_n | C_n = c_n\} = \Pr\{X_n \neq Y_n\} = Q(1,0) + Q(0,1).$$

Therefore, see Fig. 3, 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 $Q(1,0) + Q(0,1) = q$.

The capacity of BSC with crossover probability q is $1 - h(q)$ (see e.g. Gallager [7], p. 146). 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

$$R + \varepsilon \;\geq\; \log|\mathcal{K}|/N \;\geq\; R - \varepsilon, \tag{10}$$

$$\Pr\{K \neq \widehat{K}\} \;\leq\; \varepsilon. \tag{11}$$

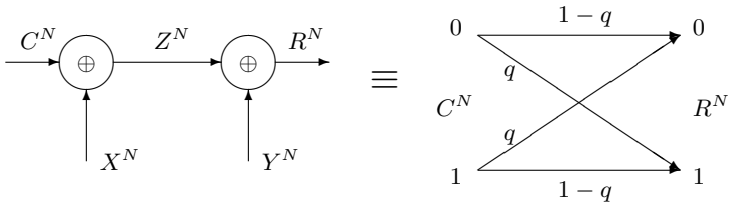

Figure 3: In the memoryless cases the channel between C^N and R^N is a binary symmetric channel with crossover probability $q = Q(0,1) + Q(1,0)$.

Using an expurgation argument, see e.g. Gallager [7], p. 151, we may assume that this code does not contain two identical codewords, and then $H(C^N) = \log|\mathcal{K}|$.

We concentrate on such codes. Consider the secrecy leakage first. From (3) we get

$$I(K; Z^N) = H(C^N \oplus X^N) - H(X^N) = 0 \leq \varepsilon. \tag{12}$$

Next for the privacy leakage we write

$$I(X^N; Z^N) \overset{(a)}{=} H(C^N \oplus X^N) - H(C^N) \overset{(b)}{=} N - \log|\mathcal{K}| \overset{(c)}{\leq} N(1 - R + \varepsilon), \tag{13}$$

where step (a) follows from (4), step (b) holds, since the code does not contain identical codewords, and (c) follows form (10). Then letting $N \to \infty$ and $\varepsilon \downarrow 0$, we conclude from (11)-(13), that the triple $(R, 0, 1-R)$ is achievable for $0 \leq R \leq 1 - h(q)$.

Converse: Assume that for the fuzzy commitment scheme the triple (R, L_k, L_x) is achievable. Consider first the entropy of the secret, note that $H(K) = \log|\mathcal{K}|$, then

$$\begin{aligned}\log|\mathcal{K}| = I(K; R^N) + H(K|R^N) \leq H(C^N \oplus X^N \oplus Y^N) - H(C^N \oplus X^N \oplus Y^N|K) \\ + H(K|\widehat{K}) \overset{(a)}{\leq} N - H(X^N \oplus Y^N) + \delta \log|\mathcal{K}| + 1 \overset{(b)}{\leq} N - Nh(q) + \delta \log|\mathcal{K}| + 1,\end{aligned} \tag{14}$$

here (a) holds, since C^N is a function of K, (X^N, Y^N) are independent of K, since for achievable triples (R, L_k, L_x) we have $\Pr\{K \neq \widehat{K}\} \leq \delta$ and due to Fano's inequality, and (b) holds, since $X^N \oplus Y^N$ is a sequence of i.i.d. pairs with crossover probability q.

From the above expression we obtain for achievable triples (R, L_k, L_x) that

$$R - \delta \leq \log|\mathcal{K}|/N \leq 1/(1-\delta)(1 - h(q) + 1/N). \tag{15}$$

Next we consider the secrecy leakage and, using (3), we get

$$L_k + \delta \geq I(K; Z^N)/N = (H(C^N \oplus X^N) - H(X^N))/N = (N - N)/N = 0. \tag{16}$$

For the privacy leakage we obtain using (4) that

$$L_x + \delta \geq I(X^N; Z^N)/N \overset{(a)}{\geq} (N - \log|\mathcal{K}|)/N \overset{(b)}{=} 1 - R - \delta, \tag{17}$$

here (a) holds, since $H(C^N) \leq \log|\mathcal{K}|$, and (b) since for achievable triples (R, L_k, L_x) : $\log|\mathcal{K}| \leq N(R + \delta)$. Letting $N \to \infty$ and $\delta \downarrow 0$, the converse follows from (15)-(17).

4 The Input-Symmetric Memoryless Case

4.1 Statement of Results, Discussion

In this section we present the result obtained for the input-symmetric memoryless case. The proof of this result is identical to the proof of Thm. 3.1, and therefore is omitted.

Theorem 4.1 *For a fuzzy commitment scheme in the input-symmetric memoryless case with crossover probability q, the achievable region $\mathcal{R}_{fc}$ is given by*

$$\mathcal{R}_{fc} = \big\{(R, L_k, L_x) \;:\; 0 \le R \le 1 - h(q), \; L_k \ge 0, \; L_x \ge 1 - R \big\}. \tag{18}$$

Now if we again restrict the secrecy leakage to be $L_k = 0$ in Thm. 4.1, then

$$\mathcal{R}_{\text{fc}|L_k\,=\,0} = \big\{(R, L_x) \;:\; 0 \le R \le 1 - h(q), \; L_x \ge 1 - R \big\}. \tag{19}$$

As before, we can compare the resulting zero secrecy-leakage region $\mathcal{R}_{\text{fc}|L_k\,=\,0}$ to the region $\mathcal{R}^u_{ck}$ for the input-symmetric case when we do not restrict ourselves to fuzzy commitment. In [6] it was shown that

$$\mathcal{R}^u_{ck} = \big\{(R, L_x) \;:\; 0 \le R \le I(U;Y), \; L_x \ge I(U;X) - I(U;Y), \; \text{for some } P(u,x,y) = Q(x,y)P(u|x) \big\}. \tag{20}$$

The maximum secret-key rate that is achievable in the optimal case is $I(X;Y)$, if we take $U \equiv X$, see Ahlswede-Csiszár [8]. Note that

$$I(X;Y) = H(X) - H(X|Y) = 1 - H(X \oplus Y|Y) \ge 1 - H(X \oplus Y) = 1 - h(q), \tag{21}$$

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

It is easy to see that independence can only occur for $I(X;Y) > 0$, if in addition to input-symmetric the source is totally-symmetric. 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

$$L_x \ge 1 - R \ge h(q) = H(X \oplus Y) \ge H(X|Y) \ge I(U;X) - I(U;Y), \tag{22}$$

for all $U \to X \to Y$. 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 a privacy leakage which is optimal in the sense of results in [6].

5 The Memoryless Case

5.1 Statement of Results, Discussion

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.

First we define the inverse of the binary entropy function $h(\cdot)$ for $0 \le \alpha \le 1$ as $h^{-1}(\alpha) \stackrel{\Delta}{=} a$, if $0 \le a \le 1/2$ and $h(a) = \alpha$.

Theorem 5.1 *For fuzzy commitment in the memoryless case with crossover probability q and probability $\Pr\{X=1\}=\rho$, we obtain for the achievable region $\mathcal{R}_{fc}$*

$$\begin{aligned}\mathcal{R}_{fc} \subseteq \big\{(R, L_k, L_x) \quad : \quad & 0 \le R \le 1-h(q), \\ & L_k \ge h[\rho * h^{-1}(R)] - h(\rho), \\ & L_x \ge h[\rho * h^{-1}(R)] - R \quad \big\}. \end{aligned} \tag{23}$$

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 4 we have seen that for the general input-symmetric case $I(X;Y) > 1-h(q)$, see (21). On the other hand, for the general memoryless case for which $X \oplus Y$ is independent of Y we obtain

$$I(X;Y) = H(X) - H(X|Y) = H(X) - H(X \oplus Y|Y) \le 1 - H(X \oplus Y) = 1 - h(q), \tag{24}$$

hence also $I(X;Y) < 1-h(q)$ is possible. Ahlswede-Csiszár [8] result implies that for rates larger than $I(X;Y)$ it is not possible to achieve non-zero secrecy leakage. Indeed,

$$\begin{aligned} H(K) &= I(K;R^N) + H(K|R^N) \le I(K;Z^N,R^N) + H(K|\widehat{K}) \\ &= I(K;Z^N) + H(Y^N|Z^N) - H(Y^N|Z^N,K,X^N) + H(K|\widehat{K}) \\ &\le I(K;Z^N) + H(Y^N) - H(Y^N|X^N) + \delta \log|\mathcal{K}| + 1 \\ &= I(K;Z^N) + NI(X;Y) + \delta \log|\mathcal{K}| + 1, \end{aligned} \tag{25}$$

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

Observe also that Thm. 5.1 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 $R = 1$. These cases are of no interest, though.

Moreover, observe that for non-trivial cases for $I(X;Y) \ge 1-h(q)$ the privacy leakage in fuzzy commitment is larger than necessary. Indeed, if $R > 0$, then

$$h[\rho * h^{-1}(R)] - R \;>\; h(\rho) - (1-h(q)) \ge H(X|Y) \ge I(U;X|Y) = I(U;X) - I(U;Y),$$

where $I(U;X) - I(U;Y)$ is the privacy leakage that is achieved in the optimal setting.

5.2 Proof of Thm. 5.1

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.

We will use Mrs. Gerber's lemma of Wyner and Ziv [9] to proof our results.

Assume that the rate-leakage triple (R, L_k, L_x) is achievable. Then in the same way as (15), we obtain for achievable triples (R, L_k, L_x) that

$$R - \delta \le \log|\mathcal{K}|/N \le 1/(1-\delta)(1-h(q)+1/N). \tag{26}$$

Next we consider the secrecy and privacy leakage. First we show that

$$\log|\mathcal{K}| = I(K;R^N) + H(K|R^N) \overset{(a)}{\le} I(C^N;R^N) + H(K|\widehat{K}) \overset{(b)}{\le} H(C^N) + \delta \log|\mathcal{K}| + 1, \tag{27}$$

where (a) follows from the data-processing inequality, from the fact that for achievable triples (R, L_k, L_x) we have that $\Pr\{\widehat{K} \ne K\} \le \delta$, and (b) from Fano's inequality.

Using (27), we may conclude that for achievable triples (R, L_k, L_x) it holds that

$$H(C^N)/N \geq ((1-\delta)\log|\mathcal{K}| - 1)/N \geq R - \delta - \delta R - 1/N. \tag{28}$$

For the secrecy leakage we can write, using Mrs. Gerber's lemma and (3), that

$$L_k + \delta \;\; \geq \;\; I(K; Z^N)/N \geq h[\rho * h^{-1}(R - \delta - \delta R - 1/N)] - h(\rho). \tag{29}$$

In a similar manner we find for the privacy leakage that

$$L_x + \delta \stackrel{(a)}{\geq} (H(C^N \oplus X^N) - \log|\mathcal{K}|)/N \stackrel{(b)}{\geq} h[\rho * h^{-1}(R - \delta - \delta R - 1/N)] - R - \delta. \tag{30}$$

where step (a) follows from (4) and the fact that $H(C^N) \leq \log|\mathcal{K}|$, and (b) follows from the definition of achievable rates, since then $\log|\mathcal{K}| \leq N(R+\delta)$.

Now Thm. 5.1 follows from (26), (29) and (30), if we let $\delta \downarrow 0$, and $N \to \infty$.

6 Conclusions

In this paper we have investigated secrecy and privacy leakage properties of fuzzy commitment. 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. For the input-symmetric memoryless case, fuzzy commitment is suboptimal with respect to both achievable secret-key rate and privacy-leakage rate. However, it still enjoys zero secrecy leakage. In the general memoryless case we could only determine outer bounds on the achievable regions. The results for the memoryless case have shown that fuzzy commitment results in both secrecy and privacy leakage larger than necessary.

References

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

[2] 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 *AutoID*, 2005, pp. 21–26.

[3] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[4] A. Smith, "Maintaining secrecy when information leakage is unavoidable," Ph.D. dissertation, MIT, 2004.

[5] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *ECCV Workshop BioAW*, 2004, pp. 158–170.

[6] T. Ignatenko and F. Willems, "Secret rate - privacy leakage in biometric systems," in *to appear in Proc. of 2009 IEEE ISIT, June 28-July 3, 2009, Seoul, Korea*, 2009.

[7] R. Gallager, *Information Theory and Reliable Communcation.* Wiley, 1968.

[8] R. Ahlswede and I. Csiszar, "CR in information theory and cryptography - part I: Secret sharing," *IEEE Trans. on Inf. Th.*, vol. 39, pp. 1121–1132, 1993.

[9] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–i," *IEEE Trans. on Inf. Th.*, vol. 19, 1973.