ON PRIVACY IN SECURE BIOMETRIC AUTHENTICATION SYSTEMS

Tanya Ignatenko, Frans Willems

Eindhoven University of Technology
Fac. ELE, MBS-SPS Group
Den Dolech 2, 5600 MB Eindhoven, The Netherlands

ABSTRACT

We focus here on two secure biometric systems (a common randomness based scheme [1], [2], [3] and a fuzzy commitment scheme [4]) and discuss their privacy preserving properties. We derive bounds on the privacy leakage in these schemes. We also show the relation between employed error-correction and leakage on biometric information, and between privacy and security for the fuzzy commitment scheme.

Index Terms— Biometric authentication, privacy, security

1. INTRODUCTION

Nowadays with the introduction of biometric technologies in daily life the importance of secure storage and communication of data in biometric systems increased. Unlike usual secret keys, which can be canceled and changed if compromised, biometric data is not revokable. Therefore, secure storage of biometric data implies protection of biometric templates in such a way that data which is communicated and/or stored in the database provides no or limited negligible information on the actual biometric data.

Biometric authentication is the process of verifying the identity of an individual using measurements of his/her biological characteristics. The attempts to create secure authentication schemes led to the fuzzy commitment scheme [4]. In this work the idea of the one-time pad principle is used to create a secure authentication scheme. A secret (codeword) associated with a person to be authenticated is hashed using a one-way function and stored in the database. Further, this key is concealed using biometric data, which are assumed to be independent uniformly distributed, and stored in the database as well. During the authentication process, the concealed key is sent via public channel to facilitate reliable verification. A positive authentication decision is only taken if biometric data presented during authentication is close to the enrollment data. In [4], however, no rigorous results were presented on the security of the scheme in case the data is not independent uniformly distributed, as well as on the privacy properties of the scheme.

Thanks to SenterNovem for funding. Project number IGC03003B.

In general, the assumption on the data to be independent uniformly distributed is hardly realistic and, therefore, later in [3] a secure authentication scheme was specified by introducing a common randomness extraction layer combined with one-time pad. It was also proven there that the fuzzy commitment scheme is only secure if it operates on independent uniformly distributed data.

In both schemes in order to perform reliable authentication, some data has to be publicly communicated. In this paper we analyze privacy preserving properties of these schemes, with respect to the publicly communicated data, as well as the relation between privacy and secrecy.

2. FUZZY COMMITMENT SCHEME

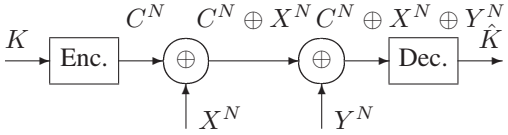

Fig. 1. Fuzzy commitment scheme.

Let us consider the fuzzy commitment scheme (Figure 1). In this scheme an encoder uniformly chooses a binary secret key K for biometric data X^N, and encodes this secret key into a binary codeword C^N, from a selected error-correcting code. The offset $Z^N = C^N \oplus X^N$ is released to the decoder for the authentication.

In the authentication phase the offset Z^N is added modulo-2 to the biometric sequence Y^N, observed by the decoder $\hat{C}^N = Z^N \oplus Y^N = C^N \oplus X^N \oplus Y^N$. The decoder finds the closest codeword in the corresponding error-correcting code and decodes this codeword to a secret key $\widehat{K}$. If $\widehat{K} = K$, the authentication decision is positive.

In the described fuzzy commitment scheme a binary error-correcting code is assumed to be is one-to-one. Since the secret key sequence K is encoded into a binary codeword C^N, this implies that $H(K) = H(C^N) = NR_c$, where R_c is the rate of the chosen code.

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

$$\begin{aligned} H_\infty(X) &= \lim_{N\to\infty} H(X_1, X_2, \cdots, X_N)/N \\ &= \lim_{N\to\infty} H(X_N|X_1^{N-1}). \end{aligned} \quad (1)$$

The binary entropy function $h(\cdot)$ is defined as $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ for $0 \le p \le 1$. And for $0 \le \alpha \le 1$ we define the inverse of the binary entropy function $h^{-1}(\alpha) = q$ if $0 \le q \le 1/2$ and $h(q) = \alpha$. Moreover, for $0 \le p_1, p_2 \le 1$ let $p_1 * p_2 = p_1(1-p_2) + (1-p_1)p_2$.

Theorem 1 *For random binary independent sequences X^N and C^N, if X^N is stationary, the following statement holds:*

$$H(Z^N)/N \ge h[h^{-1}(H_\infty(X)) * h^{-1}(R_c)], \quad (2)$$

where $Z^N = (Z_1, \cdots, Z_N) = (X_1 \oplus C_1, \cdots, X_N \oplus C_N)$. This is an adapted version of the binary analog to the entropy-power inequality (Shamai and Wyner [5]).

In the fuzzy commitment scheme the side information Z^N is publicly communicated to the decoder. Thus, we are interested in the amount of information that can be obtained by an eavesdropper from Z^N about the biometric data X^N. Therefore, to characterize the information leakage, we would like to evaluate the mutual information $I(X^N; Z^N)/N$. This mutual information can now be rewritten as

$$\begin{aligned} I(X^N; Z^N) &= H(Z^N) - H(Z^N|X^N) \\ &= H(X^N \oplus C^N) - H(X^N \oplus C^N|X^N) \\ &= H(X^N \oplus C^N) - H(C^N). \end{aligned} \quad (3)$$

where the last equality holds since C^N is determined by K and X^N and K are independent.

Theorem 2 *In the secure fuzzy commitment scheme, information leakage on X^N is unavoidable, more precisely,*

$$I(X^N; X^N \oplus C^N)/N \ge 1 - R_c.$$

Moreover, for any code rate $R_c < 1$ the privacy leakage decreases if H_∞ decreases, which leads to secrecy leakage.

Proof. Consider a secure fuzzy commitment scheme, viz. a scheme operated on uniform i.i.d. biometric sequences X^N ($H_\infty(X) = 1$). Then substituting $H_\infty(X)$ and R_c into binary analog to entropy-power inequality (2), we obtain the following bound on the biometric information leakage

$$\begin{aligned} I(X^N; Z^N)/N &= H(Z^N)/N - H(C^N)/N \\ &\ge h[h^{-1}(H_\infty(X)) * h^{-1}(R_c)] - R_c \\ &= h[1/2 * h^{-1}(R_c)] - R_c \\ &= h(1/2) - R_c \\ &= 1 - R_c. \end{aligned} \quad (4)$$

Perfect privacy, i.e.

$$I(X^N, Z^N)/N = 0,$$

can be only achieved if $R_c = 1$, but then the error-correcting capability of the code disappears. This solution is not feasible. Thus, we conclude that fuzzy commitment scheme on noisy data does not possess privacy preserving properties and the amount of the information that is leaked by the scheme is lower bounded by $1 - R_c$.

The same bound also follows from the fact that for a simple code with NR_c information symbols, followed by $N - NR_c$ parity symbols, it holds that $H(C_n|C_1^{n-1}) = 1$ for $n \le NR_c$ and $H(C_n|C_1^{n-1}) = 0$ for $n > NR_c$, where we also assume that NR_c is integer. Therefore, from (2)

$$\begin{aligned} H(Z^N)/N &= \frac{1}{N}\sum_{n=1}^{N} H(Z_n|Z_1^{n-1}) \\ &\ge \frac{1}{N}\sum_{n=1}^{NR_c} h[h^{-1}(H_\infty(X)) * h^{-1}(1)] \\ &+ \frac{1}{N}\sum_{n=NR_c+1}^{N} h[h^{-1}(H_\infty(X)) * h^{-1}(0)] \\ &= \frac{1}{N}[NR_c + (N - NR_c)H_\infty(X)] \\ &= R_c + (1 - R_c)H_\infty(X) \\ &= H_\infty(X) + R_c(1 - H_\infty(X)). \end{aligned} \quad (5)$$

Again, for uniform i.i.d. X^N we obtain that

$$I(X^N; Z^N)/N \ge 1 - R_c, \quad (6)$$

and using the same reasoning as before, we conclude that a privacy preserving fuzzy commitment scheme is only obtained if $R_c = 1$, i.e. when no error-correcting code is employed.

If we next consider the case where $H_\infty < 1$, we see that the lower bound on the privacy leakage is reduced to

$$I(X^N; Z^N)/N \ge h[h^{-1}(H_\infty(X)) * h^{-1}(R_c)] - R_c. \quad (7)$$

If $H_\infty = 0$, there is no privacy leakage, however, biometric data are not deterministic, and hence $H_\infty(X) > 0$.
If we additionally know that we apply a simple code with NR_c information symbols, followed by $N - NR_c$ parity symbols, the lower bound becomes better (follows from Jensen's inequality):

$$I(X^N; Z^N)/N \ge H_\infty(X)(1 - R_c). \quad (8)$$

This relaxation, however, will result in information leakage on the secret (see [3]) expressed by the following inequalities:

$$\begin{aligned} \lim_{N\to\infty} I(K; Z^N)/N &\ge h[h^{-1}(H_\infty(X)) * h^{-1}(R_c)] \\ &\quad - H_\infty(X) > 0, \end{aligned} \quad (9)$$

$$\lim_{N\to\infty} I(K; Z^N)/N \ge R_c(1 - H_\infty(X)) > 0, \quad (10)$$

for $0 < H_\infty(X) < 1$. Note, that the last inequality corresponds to the case where we have a simple code with NR_c information symbols, followed by $N - NR_c$ parity symbols. □

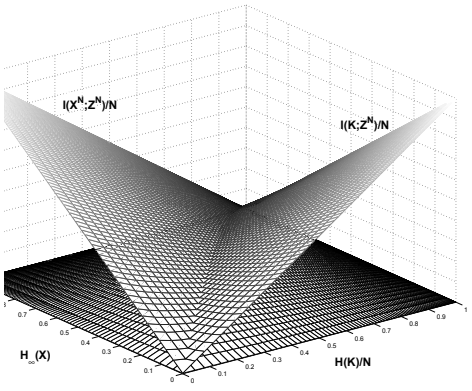

Fig. 2. Lower bound plots on information leakage.

Figure 2 illustrates lower bounds on the amount of the information that the system leaks on a secret and biometric data for different values of $H_\infty(X)$ and R_c, and demonstrates the relations between them. In this figure the general case is considered, i.e the privacy bound (7) and secrecy bound (9) as a function of R_c $(= H(K)/N)$, and $H_\infty(X)$.

3. COMMON RANDOMNESS BASED SCHEME

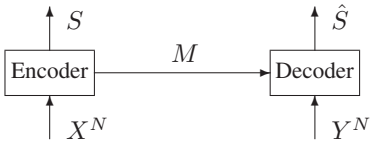

Fig. 3. Randomness extraction.

Biometric authentication system can be viewed as communication system in which an encoder and a decoder have to extract common information (common randomness) S out of two dependent biometric measurements X^N and Y^N. The terminals in the system want to extract as much key information as possible. To ensure reliable reconstruction of the common randomness at the decoder, the encoder sends helper information M to the decoder. The communication of the helper is performed via a public channel, see Figure 3. This model is also referred to as a source-type model and was first considered in [1], [2]. To address the problem of biometric cancelable keys, viz., to bind more than one secret with biometric data, a masking layer is introduced on top of the common randomness layer (see Figure 4). In this layer an independent uniformly distributed secret key K is randomly selected for a biometric data sequence X^N and extra helper information, the secret key added modulo-2 to the common randomness extracted at the first layer, is sent to the decoder. Again, this helper data is publicly communicated.

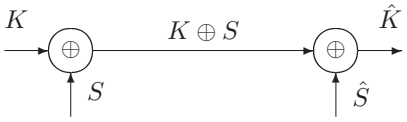

Fig. 4. Masking layer.

The following two theorems (for detailed proofs see [1], [3]) summarize the properties of the secure authentication scheme constructed as above.

Theorem 3 *For the common randomness extraction scheme, processing i.i.d. sequences, for each $\delta > 0$, for all N large enough, there exists a sequence of codes satisfying*

$$\begin{aligned} \Pr\{\hat{S} \neq S\} &\leq \delta, \\ H(S)/N &\geq I(X;Y) - \delta, \\ I(S;M)/N &\leq \delta. \end{aligned}$$

Conversely, there exists no secure ($I(S;M)/N \approx 0$) and reliable ($\Pr\{\hat{S} \neq S\} \approx 0$) scheme if $H(S)/N > I(X;Y)$.

Proof sketch: The achievability proof of the theorem relies on the random binning argument. The set of typical X-sequences is partitioned in codes for the channel from X to Y, there are roughly $2^{NH(X|Y)}$ of such codes and all of these codes contain approximately $2^{NI(X;Y)}$ codewords. The index of the code is sent as helper data to the decoder. The decoder then, knowing the code, uses y^N to recover x^N, and if the secret is the index of x^N within the code, the code-index reveals practically no information about this index. The converse follows applying Fano's inequality. □

Theorem 4 *If we use a masking procedure, based on a uniform binary key sequence, the system preserves its property of being secure, i.e.*

$$I(K; M, K \oplus S)/N \approx 0$$

if $H(K)/N \approx I(X;Y)$.

Proof sketch: Mutual information can be upper bounded as $I(K; M, K \oplus S) \leq NR_s - H(S) + I(S;M)$ and applying Fano's inequality the result of the theorem follows. □

Now we investigate how much information about biometric data is eavesdropped by communication helper data over a public channel.

Theorem 5 *Consider an i.i.d. pair (X,Y) of correlated sources. For all $\epsilon > 0$, N large enough and secrecy rate $R_s = I(X;Y) - \varepsilon$, the mutual information between biometric data and publicly communicated data is upper-bounded by following expression*

$$I(X^N; K \oplus S, M)/N \leq H(X|Y) + 3\varepsilon.$$

Proof. First observe that

$$\begin{aligned} 0 &\leq I(X^N; K \oplus S|M) \\ &= H(K \oplus S|M) - H(K \oplus S|X^N, M) \\ &\leq H(K) - H(K \oplus S|X^N, M, S) \\ &= H(K) - H(K|X^N, M, S) \\ &= H(K) - H(K) = 0 \end{aligned} \tag{11}$$

We use this in

$$\begin{aligned} &I(X^N; K \oplus S, M) \\ &\quad = I(X^N; M) + I(X^N; K \oplus S|M) \\ &\quad = I(X^N; M) \\ &\quad = H(M) - H(M|X^N) = H(M). \end{aligned} \tag{12}$$

Now consider the encoder. We are going to use a random binning argument to prove the result of the theorem. We fix $\varepsilon > 0$ and define two sets $\mathcal{A}_\varepsilon(X)$ and $\mathcal{A}_\varepsilon(X, Y)$ to be typical and jointly typical sequences as in Cover and Thomas [6], based on the joint distribution of the XY-source. To each biometric sequence x^N a helper-label $m \in \{1, 2, \cdots, 2^{NR_h}\}$ is assigned by an encoder with probability $\Pr\{M(x^N) = m\} = 2^{-NR_h}$. Thus,

$$H(M) \leq NR_h. \tag{13}$$

Moreover, a randomness-label $s \in \{1, 2, \cdots, 2^{NR_s}\}$ is assigned to each sequence x^N with probability $\Pr\{S(x^N) = s\} = 2^{-NR_s}$.

The encoder has to make x^N reconstructible from both the helper label m and the randomness label s. Therefore, it has to find a unique sequence x^N with labels m and s such that

$$x^N \in \mathcal{A}_\varepsilon(X). \tag{14}$$

The error probability averaged over the ensemble of random binnings satisfies

$$\begin{aligned} P_\varepsilon &\leq \Pr\{X^N \notin \mathcal{A}_\varepsilon \cup \bigcup_{\substack{x^N \neq X^N: \\ x^N \in \mathcal{A}_\varepsilon}} M(x^N) = M(X^N) \wedge S(x^N) = S(X^N)\} \\ &\leq \Pr\{X^N \notin \mathcal{A}_\varepsilon\} + \sum_{\substack{x^N \neq X^N: \\ x^N \in \mathcal{A}_\varepsilon}} \Pr\{M(x^N) = M(X^N), S(x^N) = S(X^N)\} \\ &\leq \Pr\{X^N \notin \mathcal{A}_\varepsilon\} + |\{x^N : x^N \in \mathcal{A}_\varepsilon\}| 2^{-N(R_h + R_s)} \\ &\leq \varepsilon + 2^{N(H(X)+\varepsilon)} \cdot 2^{-N(R_h+R_s)} \leq 2\varepsilon. \end{aligned} \tag{15}$$

which is satisfied if $R_h + R_s - H(X) - \varepsilon = \varepsilon$. Since the secrecy rate of our system is $R_s = I(X; Y) - \varepsilon$, we conclude

$$R_h = H(X|Y) + 3\varepsilon. \tag{16}$$

Combining (12), (13) and (16), we finalize the proof. □

4. CONCLUSIONS

We have considered two types of secure biometric authentication schemes and investigated their properties of being privacy preserving. The privacy of the system has been analyzed from the publicly communicated data point of view. In general given the secret key and the helper data it is always possible to reconstruct biometric data. Therefore, it is assumed that the secret key is protected by a one-way hash function [4]. Although in this setup secret keys are not private in information theoretical sense, a hash function guarantees computational security (privacy in our case). By analyzing the publicly communicated helper data, it has been shown that none of these schemes is perfectly private and bounds on the privacy loss have been provided. Analysis shows that biometric privacy depends on error-correction method used in the scheme, and the higher the noise in biometric measurements is the more information about the data has to be communicated and, thus, the more biometric information is leaked to an eavesdropper. Moreover, it has been shown that in a fuzzy commitment scheme the effect of increasing privacy will have a negative effect on the secrecy of the system and the other way around. Furthermore, since in general biometric data do not have full entropy and always require an error-correcting code to be used for reliable authentication, the fuzzy commitment scheme will have a decrease in both security and privacy. We conclude that to achieve a secure system with fixed privacy properties, it is better to use a scheme based on a randomness-extraction layer followed by a masking layer.

5. REFERENCES

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - part I: Secret sharing," *IEEE Trans. on Information Theory*, vol. 39, pp. 1121–1132, July 1993.

[2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, pp. 733–742, May 1993.

[3] T. Ignatenko and F. Willems, "On the security of the xor-method in biometric authentication systems," in *Proc. of 27th Symp. on Information Theory in the Benelux*, 2006.

[4] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. of the 6th ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[5] S. Shamai and A.D. Wyner, "A binary analog to the entropy-power inequality," *IEEE Trans. on Information Theory*, vol. 36, no. 6, pp. 1428–1430, November 1990.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons Inc., New York, 1991.