RELIABLE BIOMETRIC AUTHENTICATION WITH PRIVACY PROTECTION

E. VERBITSKIY, P. TUYLS, D. DENTENEER, J.P. LINNARTZ
PHILIPS RESEARCH LABORATORIES
PROF. HOLSTLAAN 4, AA 5656 EINDHOVEN, THE NETHERLANDS
{EVGENY.VERBITSKIY,PIM.TUYLS,DEE.DENTENEER,J.P.LINNARTZ@PHILIPS.COM}

Abstract. We propose a new scheme for reliable authentication of physical objects. The scheme allows not only the combination of noisy data with cryptographic functions but has the additional property that the stored reference information is non-revealing. By breaking into the database and retrieving the stored data, the attacker will not be able to obtain any realistic approximation of the original physical object. This technique has applications in secure storage of biometric templates in databases and in authentication of PUFs (Physical Uncloneable Functions).

1. Introduction

Many cryptographic protocols are based on encryption algorithms and one-way functions. One of the fundamental properties of those functions is that they are very sensitive to small perturbations in their inputs. Therefore, those cryptographic primitives can not be applied straightforwardly when the input data are noisy. This is typically the case when the input data is obtained from the measurement of physical objects such as biometrics [10], PUFs (Physical Uncloneable Functions) [5], [12] etc. Consequently, some additional processing has to be performed in order to remove the noise, while not compromising security.

It is clear that in order to perform the verification procedure of biometric templates, some reference information has to be stored at a central server at work, in the bank, or in the supermarket. However as biometrics are unique identifiers of human beings, a privacy problem arises. People feel uncomfortable with supplying their biometric information to a large number of seemingly secure databases for various reasons. The above arguments imply that a successful protocol has to satisfy the following requirements i) Robustness to noise, ii) Security and iii) Privacy protection.

More specifically, by privacy we mean, that by breaking into a database, an attacker will not learn anything about the biometric template (or the physical structure of the PUF).

We prove that a universal authentication scheme satisfying the above-mentioned requirements i), ii) and iii) does not exist. Hence, the authentication scheme has to be based on features which are selected individually, i.e. on side-information. In this paper, we propose such an authentication method, based on statistical selection of robust features adapted to the given template while preserving privacy. We evaluate the performance of our scheme with respect to requirements i), ii) and iii) in case of Gaussian data with Gaussian noise.

There is a large body of literature on the various aspects of biometric identification, and corresponding cryptographic problems [1, 3, 4, 8, 9]. Those papers propose a scheme based on error-correcting codes and one-way functions. We emphasise that our proposal does not rely on error-correcting codes but is based on a robust way of feature extraction. The method is set-up in such a way that an honest user is correctly authenticated with high probability. Furthermore, given the public information in the database, it is very hard to derive any information about the biometric template.

This paper is organised as follows. In Section 2, we describe the model on which the remaining part of the paper is based. A general capacity bound for this problem setting is derived in Section 3. Finally, we give a detailed description of our solution in the case of Gaussian data with Gaussian noise, in Section 4.

2. The Model

In this section, we describe the model that we have in mind. We distinguish two phases: An Enrolment phase and an Authentication/ Verification phase which are described in detail below.

First, Alice goes with her biometric through an enrolment phase at a certification authority (CA). During this procedure the properties of her biometric are measured with specialised equipment. From the measurement data a secret S is derived. The reference data stored in the database is obtained by applying a (possibly) one-way function h to S. When Alice wants to authenticate herself to Bob at a later point in time, a measurement that extracts analog data Y of her biometric is taken. She asks Bob for the corresponding helper data W which is communicated to her by Bob. These measurement data are then processed together with the helper data W by means of a signal processing function G to construct a secret S'. Finally, $h(S')$ is computed and compared to the stored data $h(S)$ in the database. In order to set up a secure system, the function G has to be robust to noise, versatile and information hiding. The precise meaning of these notions is defined below.

Definition 2.1. *Let $G : \mathbb{R}^{n+m} \to \{0,1\}^k$ be a function and $\epsilon \geq 0$. The function G is called* ϵ-robust to noise *if and only if for all $X \in \mathbb{R}^n$ there exists a vector $W \in \mathbb{R}^m$ such that $\mathbb{P}(G(X+N, W) \neq G(X, W)) \leq \epsilon$, where $\mathbb{P}$ denotes the probability according to the distribution of the noise N.*

Definition 2.2. *Let $G : \mathbb{R}^{n+m} \to \{0,1\}^k$ be a function. The function G is called* versatile *if and only if for all $S \in \{0,1\}^k$ and all $X \in \mathbb{R}^n$, there exists a vector $W \in \mathbb{R}^m$ such that $G(X, W) = S$.*

Definition 2.3. *A two-party protocol generating a secret S is called ϵ-revealing if and only if the communicated helper data W satisfies $\mathbf{I}(W; S) \leq \epsilon$.*

We stress that in order to have a robust, versatile signal processing function $G = G(X, W)$, W must depend on X, i.e. each participant gets its own specific helper data. This was first observed in [10] under stronger robustness conditions. Here, we state a more general version of this theorem.

Theorem 2.1. *Assume that the noise has a continuous density on $\mathbb{R}^n$. Then every ϵ-robust function $G = G(X)$, with $\epsilon < 1/2$, is constant.*

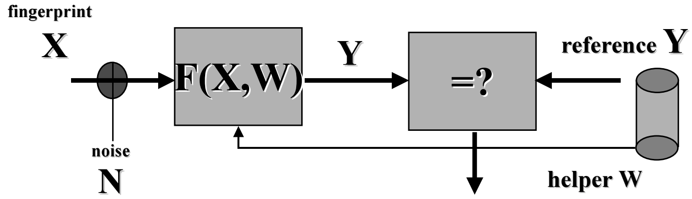

Figure 1. Schematic presentation of an authentication protocol

3. Capacity

In this Section, we derive a bound on the entropy of a secret S generated from noisy data X (taken during enrolment) and Y (taken during measurement) when additional side information W is communicated between both parties. It follows from the model in Section 2, that the constraints of the system are given by:

$$\mathsf{H}(S|X,W)=0,\quad \mathsf{H}(S'|Y,W)=0,\quad \mathbf{I}(S;W)\le\delta,\quad \mathbb{P}(S\neq S')\le\epsilon, \tag{1}$$

where $S=G(X,W)$ and $S'=G(Y,W)$. Using standard entropy arguments, and Fano's inequality we obtain the following result [1].

Theorem 3.1. *Let S be a binary string derived from X and Y by communicating W as described in Eq. 1 then,*

$$\mathsf{H}(S)\le\mathbf{I}(S;W)+\mathbf{I}(X;Y|W)+\mathsf{H}(S|S')\le\delta+\mathbf{I}(X;Y|W)+h(\epsilon)+\epsilon(\log_2(|S|)-1) \tag{2}$$

where h is the binary entropy function.

It is clear that the requirement that W gives little information about S, also implies that W gives little information about X.

The previous theorem implies that when $\mathbf{I}(S;W)\le\delta$, one can only get sufficient entropy in S if $\mathbf{I}(X;Y|W)$ is large, i.e. if given the helper data W, Y gives much information about X.

By taking the supremum over all input probability distributions for X, the bound becomes,

$$\mathsf{H}(S)\le\mathbf{I}(S;W)+C_{XY}+\mathsf{H}(S|S'). \tag{3}$$

where C_{XY} is the capacity of the "channel" between X and Y. For a Gaussian channel, C_{XY} is given by $\log(1+\frac{\sigma_X}{\sigma_N})$ [2].

4. Gaussian data and Gaussian Channels

In this section, we first give a general description of our scheme and then focus on the special case where the physical data X and the noise N are Gaussian distributed.

4.1. Fisher's Transformation.

We assume that the measured physical data consists of enrolment data corrupted by noise. More precisely, assume that $Y=X+N$, where $Y=(Y_1,\dots,Y_n)$ represents the measured physical data, $X=(X_1,\dots,X_n)$ stands for the true signal and $N=(N_1,\dots,N_n)$ represents the noise. Suppose that X has mean m and covariance matrix Σ_X, and that N has mean 0 and covariance matrix Σ_N, which we assume to be positive definite. Let Γ^* be a matrix, consisting of the eigenvectors of $\Sigma_N^{-1/2}\Sigma_X\Sigma_N^{-1/2}$, i.e. $\Sigma_N^{-1/2}\Sigma_X\Sigma_N^{-1/2}\Gamma^*=\Gamma^*\Lambda=$

[1] This theorem is related to the common randomness bounds of [11], though with much less communication.

$\Gamma^*\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Hence, $\lambda_i \geq 0$ for all $i = 1, \ldots, n$ and we may assume without loss of generality that $\lambda_1 \geq \ldots \geq \lambda_n \geq 0$. Next define $\Gamma = \Sigma_N^{-1/2}\Gamma^*$. Using Γ, we define a new vector $\alpha = (\alpha_1, \ldots, \alpha_n)$ by $\alpha_i = \langle Y - m, \gamma_i \rangle$ where γ_i represents the i-th column of Γ.

Assume that X and N have a Gaussian distribution. Then, the following is true[2].

Theorem 4.1 ([7]). *If $X \sim \mathcal{N}(m, \Sigma_X)$, $N \sim \mathcal{N}(0, \Sigma_N)$, $\Sigma_N > 0$; X and N are independent, and α is as defined above, then $\alpha \sim \mathcal{N}(0, \Lambda + I)$.*

4.2. **The Scheme.** Our proposal for a secure authentication of physical objects consists of a selection a k-bit secret based on the signs of several components with large absolute values[3]. The idea is that the noise is not sufficiently large to corrupt the signs of those significant components. This will lead to the reliability of our approach.

Let δ be a small positive number. We will choose δ appropriately depending on the noise level. For each i denote by $p_i = \mathbb{P}(|\alpha_i| > \delta)$, $q_i = 1 - p_i = \mathbb{P}(|\alpha_i| \leq \delta) = \frac{1}{\sqrt{2\pi\lambda_i}}\int_{-\delta}^{\delta} e^{-\frac{t^2}{2\lambda_i}}dt$. Note that we have the following trivial estimate of q_i, $q_i \leq \sqrt{\frac{2}{\pi\lambda_i}}\delta$.

Define the random variables z_i, $i = 1, \ldots, n$, as follows $z_i = 0$ if $|\alpha_i| \leq \delta$ and $z_i = 1$ if $|\alpha_i| > \delta$. Note that z_i, $i = 1, \ldots, n$, are independent Bernoulli random variables, with $\mathbb{P}(z_i = 1) = p_i, \quad \mathbb{P}(z_i = 0) = 1 - p_i = q_i$.

In order for the authentication scheme to be versatile, one has to ensure a large number of significant components, or in other words, the sum $\sum_{i=1}^n z_i$, must be large with a large probability. Note that its expected value is given by $\mathbb{E}(\sum_{i=1}^n z_i) = n - \sum_{i=1}^n q_i$. It is natural to assume that there is a substantial number of components with variance larger than $c\delta^2$, $c > 1$. Suppose that the fraction of such components is at least ρ. Note that if the number of components with variance substantially larger than δ^2 is small, then the whole problem of authentication of physical objects with such properties becomes infeasible, as the data X and Y become then decorrelated. There should be a sufficient amount of "energy" to distinguish various measurements. If there is not enough energy in the signal, the noise will dominate. This will make robust authentication impossible.

Using the estimate on q_i's obtained above, we conclude that

$$\mathbb{E}\Big(\sum_{i=1}^{n} z_i\Big) \geq n - \sum_{i=1}^{[\rho n]} q_i - \sum_{i=[\rho n]+1}^{n} q_i \geq [\rho n]\Big(1 - \sqrt{\frac{2}{\pi c}}\Big).$$

Hence we can conclude that if we have a substantial fraction of components with large variance, then the expected value of the sum we are interested in, will be at

[2] Fisher's Discriminant Transformation is very similar in spirit to the Principal Component Transformation. However, in the case the noise is coloured, i.e., the covariance matrix of the noise is not a multiple of the identity, the Fisher discriminant transformation can provide superior performance.

[3] We note here that two effects are happening: i) we take care of the error correction properties by constructing a binary symmetric channel with low error probability, ii) we generate a secret about which an attacker has no information. This second step can be compared with a privacy amplification step. Extensions of the construction mentioned here are investigated in a forthcoming paper [6].

least a large fraction of the number of such components. In other words, we do not lose many components.

We estimate the probability of the event that the sum $\sum_i z_i$ is small, i.e. that it is substantially smaller then the expected value. Using a classical Bernstein inequality, one easily obtains the following result.

Theorem 4.2. *Let $\{z_i\}_{i=1}^n$ be independent Bernoulli random variables. Let $p_i = \mathbb{E}(z_i)$, $\kappa_1 = \sum_{i=1}^n p_i/n$, $\tau = \sum_{i=1}^n p_i(1-p_i)/n$. Then for any κ_2, $\kappa_2 < \kappa_1$, one has*

$$\mathbb{P}\Big(\sum_{i=1}^n z_i \leq \kappa_2 n\Big) \leq 2\exp\left(-\frac{3(\kappa_1-\kappa_2)^2}{6\tau+2(\kappa_1-\kappa_2)}n\right). \tag{4}$$

Hence, we conclude that the probability of a substantial deviation of $\sum_i z_i$ from its mean value, is exponentially small.

In the case, the noise has a Normal distribution $\mathcal{N}(0, \sigma_N^2 Id)$, where Id is the identity matrix, δ has to be chosen depending on σ_N. For instance, for the Fisher discriminant Transformation, $\delta = 3\sigma_N$ or $\delta = 5\sigma_N$ will be sufficient to ensure correct identification of one bit with probability 99.87% and 99.99997% respectively.

4.3. **Versatility.** Estimates of the previous subsection imply that with a large probability the transformation will give a sufficient number of significant components. We define the set $I_\delta(\alpha) = \{i = 1, \dots, n : |\alpha_i| > \delta\}$. Our main goal is to create a certain k-bit binary secret $S = (s_1, \dots, s_k) \in \{0,1\}^k$ based on α. We say that a secret $S = (s_1, \dots, s_k)$ is **feasible** for α if there exist distinct indexes $i_1, \dots, i_k$ such that $i_j \in I_\delta(\alpha)$, for every $j = 1, \dots, k$, and $s_j = H(\alpha_{i_j})$ for every $j = 1, \dots, k$ (H denotes the Heaviside function). Denote by $\mathcal{S}_\delta(\alpha) \subset \{0,1\}^k$ the set of all feasible secrets for α: $\mathcal{S}_\delta(\alpha) = \{S \in \{0,1\}^k : S \text{ is feasible for } \alpha\}$. One would like $\mathcal{S}_\delta(\alpha)$ to be a large as possible. Under normality assumptions, α_i has a symmetric distribution. Hence if $s_i = H(\alpha_i)$, then $\mathbb{P}\Big(s_i = 1 \Big| |\alpha_i| > \delta\Big) = \mathbb{P}\Big(s_i = 0 \Big| |\alpha_i| > \delta\Big) = \frac{1}{2}$. In the previous section we showed that the expected number of significant components is equal to a certain fraction of n, say γn. Moreover, the probability of a large deviation from the expected number is exponentially small. Since s_i for each i such that $\alpha_i > \delta$ is a symmetrically distributed Bernoulli random variable, it follows from the theory of typical sequences that approximately one-half of s_i's is equal to one, and approximately one-half s is equal to zero. Hence, if we let k (the length of our secret) to be a certain fraction of the expected number of significant components, i.e. $k = \eta_1 n$, say $\eta_1 = \gamma/10$. Then with a large probability, a large portion of all 2^k secrets is feasible for α.

Once we have chosen a feasible secret S, we create the helper data $W = W(X)$ by taking rows of Γ, with indexes $i_j, j = 1, \dots, k$, i.e. W is a $k \times n$ matrix. There is a close relation between the proposed scheme and universal hash functions used for Privacy Amplification [11]. A more general theoretical framework for this and other schemes [3, 4, 8, 9] will be presented in [6].

4.4. **Information revealing.** The transformation $g(X, W)$ is defined as $g(X, W) = WX$ where W is a $k \times n$ matrix that filters out the significant components.

Theorem 4.3. *The proposed scheme is 0-revealing, i.e., $\mathbf{I}(W; S) = 0$.*

References

[1] L. Csirmaz, G.O.H. Katona, *Geometrical Cryptography*, Proceedings of the International Workshop on Coding and Cryptography, Versailles (France), 2003.

[2] T.M. Cover, J.A. Thomas,*Information Theory*, Wiley, New York, 1991.

[3] G.I. Davida, Y. Frankel and B.J. Matt, *On enabling secure applications through off-line biometric identification*, in IEEE Symposium on Privacy and Security, 1998.

[4] G.I. Davida, Y. Frankel and B.J. Matt, *On the relation of error-correction and cryptography to an off-line biometric based identification scheme*, in Proceedings WCC99, Workshop on Coding and Cryptography, 1999.

[5] Blaise Gassend, Dwaine Clarke, Marten van Dijk and Srinivas Devadas, *Controlled Physical Random Functions*, Proceedings of the 18th Annual Computer Security Applications Conference, December, 2002.

[6] J. Goseling, T. Kalker, P. Tuyls, *Secure Authentication Using Physical Random Functions*, in preparation.

[7] K.V. Marda, J.T. Kent, and J.M. Bibby, *Multivariate Analysis*, 1995.

[8] A. Juels and M. Wattenberg, *A Fuzzy Commitment Scheme*, in G. Tsudik ed, Sixth ACM Conference on Computer and Information Security, 28-36, ACM Press 1999.

[9] A. Juels and M. Sudan, *A Fuzzy Vault Scheme*, in ISIT proceedings, Int. Symp. on Inf. Theory, 408, 30 June- 5 July, 2002, Lausanne.

[10] J.P. Linnartz, P. Tuyls, *New shielding functions to enhance privacy and prevent misuse of biometric templates*, accepted at AVBPA 2003 conference on biometrics.

[11] U.M. Maurer, *The Strong Secret Key Rate of Discrete Random Triples*, Communication and Cryptography – Two Sides of One Tapestry, 1994.

[12] P. S. Ravikanth, *Physical One-Way Functions*, ,Massachusetts Institute of Technology, 2001.