# Random projections based item authentication

Sviatoslav Voloshynovskiy*, Oleksiy Koval, Fokko Beekhof and Thierry Pun
University of Geneva, Department of Computer Science,
7 route de Drize, CH 1227, Geneva, Switzerland

## ABSTRACT

In this paper, we consider an item authentication using unclonable forensic features of item surface microstructure images (a.k.a. fingerprints). The advocated authentication approach is based on the source coding jointly with the random projections. The source coding ensures the source reconstruction at the decoder based on the authentication data. The random projections are used to cope with the security, privacy, robustness and complexity issues. Finally, the authentication is accomplished as a binary hypothesis testing for both direct and random projections domains. The asymptotic performance approximation is derived and compared with the exact solutions.

## 1. INTRODUCTION

In the last years, digital reproduction tools have performed an impressive evolution, providing professional solutions to various groups of users. Besides the obvious advantages, these tools offer at the same time unprecedent possibilities for the counterfeiters that can virtually reproduce authentic items, i.e., objects, documents, IDs, packaging or even biometrics. Thus, the item authentication becomes a critical issue demanding an urgent solution for various applications. This urgency is also caused by the fundamental inability to satisfy the security requirements by the currently used proprietary (mostly material-science based) technologies and classical crypto-based techniques. Moreover, the particularities of modern markets, characterized by distributed manufacturing and distribution, require new authentication technologies oriented on the end-users. A practically attractive protocol of item authentication is based on the mobile phones of end-users. This protocol is schematically shown in Figure 1. As secure forensic features that can not be copied or cloned we will consider here a random surface microstructure image known to be a powerful discriminative and difficult to duplicate structure.[3] The user acquires the random surface microstructure image and sends it to the server with the accompanying authentication data. The server, possibly connected to the database of enrolled images, makes the binary decision about requested item authenticity and communicates the decision back to the end-user portable device.

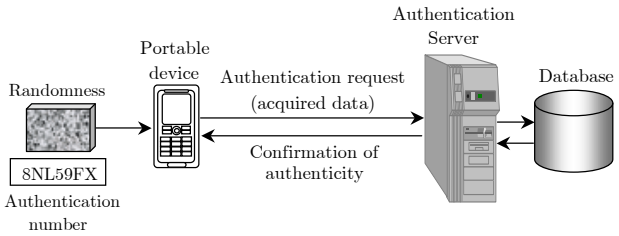



**Figure 1.** Authentication architecture based on portable devices.

The main challenge is to provide reliable authentication based on noisy observation that is different from those acquired at the enrollment stage. Obviously, the traditional cryptography-based authentication will produce a negative result even if a single bit is altered that is not suitable for this protocol. Additionally, the security leakages about the authentication protocol might cause an appearance of a number of attacks targeting to trick the authentication (including impersonation and physical attacks).

To resolve these robustness-security requirements, we propose to use the hypothesis testing framework for the evaluation of item authenticity.[11] The general block-diagram of the considered authentication is shown in

*The contact author is S. Voloshynovskiy (email: svolos@cui.unige.ch). http://sip.unige.ch

Figure 2. Here, we will use the following notations: we use capital letters to denote scalar random variables $X$ and $\mathbf{X}$ to denote vector random variables, corresponding small letters $x$ and $\mathbf{x}$ to denote the realizations of scalar and vector random variables, respectively; we use $\mathbf{X} \sim p_{\mathbf{X}}(\mathbf{x})$ or simply $\mathbf{X} \sim p(\mathbf{x})$ to indicate that a random variable $\mathbf{X}$ is distributed according to $p_{\mathbf{X}}(\mathbf{x})$; all vectors without sign tilde are assumed to be of the length $N$ and with the sign tilde of length $L$.

In the scope of the considered framework, the item index is deduced at the enrollment stage based on the observed data $\mathbf{x}$. We assume here that the *lossless coding* is used, where all sequences $\mathbf{x}$ of length $N$ are generated from some distribution $p_{\mathbf{X}}(\mathbf{x})$. The encoder assigns the index $m$ to each sequence and sends it to the decoder with the rate $R_X \geq H(X)$, where $H(X)$ is the entropy of $X$. The channel includes both the attacker, who can replace the sequence $\mathbf{x}(m)$ on $\mathbf{x}'$ and use index $m$ for $\mathbf{x}'$, and the acquisition channel supposed to be a discrete memoryless channel (DMC) $p_{Y|X}(y|x)$. At the authentication stage, one should make a decision about the item authenticity based on the observed vector $\mathbf{y}$ and the index $m$. For this purpose, the decoder retrieves the sequence $\hat{\mathbf{x}}(m)$ based on $m$, and the binary test produces the final decision by generating the hypothesis $H_0$, i.e., fake, or $H_1$, i.e., genuine. To reduce the rate for $m$, one can further apply *lossy source coding*. In this case, $m$ can be considered as a hash obtained with the corresponding randomized codebook generation. However, this will cause well-known collisions. To avoid this undesirable effect and exploit the fact of $\mathbf{y}$ presence at the decoder that is correlated with the genuine $\mathbf{x}(m)$, one can use *distributed source coding* based on Slepian-Wolf framework.[13] This coding is based on binning, where $m$ is considered as a bin index. In this case the rate can be reduced to $R_X^{SW} \geq H(X|Y)$. Similar in spirit approaches were firstly introduced by Maurer[10] and Ahlswede and Csiszar,[2] where the index $m$ was considered as a helper data for *common randomness* extraction considered to be $\mathbf{x}$.

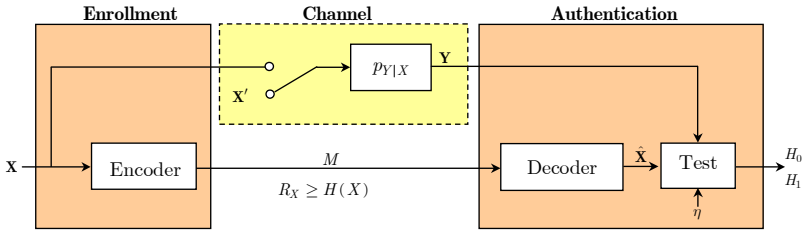



**Figure 2.** Authentication setup based on lossless coding.

Nevertheless, the above result applies to the discrete-value vectors. In the case of continuous-value vectors, one should apply first the quantization that will lead to the distortions at the reconstruction of $\hat{\mathbf{x}}$ and the corresponding collisions depending on the quantizer rate. More generally, the lossy distributed source coding can be considered based on Wyner-Ziv framework[15] using the binning similar to those used in the Slepian-Wolf coding with an auxiliary random vectors $\mathbf{U}$ constructed from $\mathbf{X}$ according to the mapping $p_{\mathbf{U}|\mathbf{X}}$. In this case, the rate-distortion function $R_X^{WZ}(D)$ is defined as:

$$R_X^{WZ}(D) = \min_{p_{U|X}: E[d^N(\mathbf{X},\hat{\mathbf{X}})] \leq D} I(X;U) - I(Y;U), \tag{1}$$

where $d^N(.,.)$ is the distortion measure between two vectors and $D$ is the distortion. For the Gaussian setup considered in this paper, $\mathbf{X} \sim (\mathbf{0}, \sigma_X^2 \mathbf{I}_N)$ and $\mathbf{Y} \sim (\mathbf{0}, \sigma_Y^2 \mathbf{I}_N)$ the rate (1) turns out to be:

$$R_X^{WZ}(D) = \begin{cases} \frac{1}{2}\log_2\left(\frac{\sigma_X^2(1-\rho_{XY}^2)}{D}\right), & \text{for } D < \sigma_X^2(1-\rho_{XY}^2), \\ 0, & otherwise, \end{cases} \tag{2}$$

where $\rho_{XY}^2 = \frac{E[XY]}{\sigma_X \sigma_Y}$ is the correlation coefficient. However, to avoid the collisions and to simplify the consideration, one can suppose that the rate $R_X^{WZ}(D)$ is chosen to be sufficiently high to guarantee the low distortion $D$ that allows to assume that the distortions under both hypothesis $H_0$ and $H_1$ are the same.

The above framework was theoretically considered by Tyuls *et. al.*[14] and Ignatenko and Willems[6] and practically implemented by Martinian *et. al.*[9] and Lin *et. al.*[8] using low-density parity check codes (LDPC) for the distributed coding.

The main idea behind this design was to avoid soft hypothesis testing by replacing it by the direct matching of hashes extracted from the reconstructed data based on noisy measurements using common randomness extraction framework. Two possible schemes were considered.[8,9,14] The first scheme uses the index $s$, $s = \{1, 2, \cdots, 2^{NI(X;Y)}\}$, where $I(X;Y)$ denotes the mutual information between $X$ and $Y$, of the sequence $\mathbf{x}$ in the bin $m$ for the hashing (Figure 3) and the second one is based on the hash computed from the original $\mathbf{x}$ and reconstructed $\hat{\mathbf{x}}$ sequences (Figure 4). The necessity to introduce extra side information is dictated by the need to distinguish the sequences within the same bin $m$ in the case when the informed attacker might produce a fake that will be jointly typical with $\mathbf{y}$. This will lead to the false acceptance. Thus, the hashed values of $s$ or $\mathbf{x}$ aim protecting against such kind of attack. Obviously, the rate of the hash in the second case is higher. A common drawback of these schemes is unavoidable presence of collisions due to the hashing. Therefore, to avoid it Ignatenko and Willems[6] suggested the scheme based on XORring of index $s$ with the secret key $k$ and its validation at the authentication stage based on the decoded version $\hat{s}$ (Figure 5).

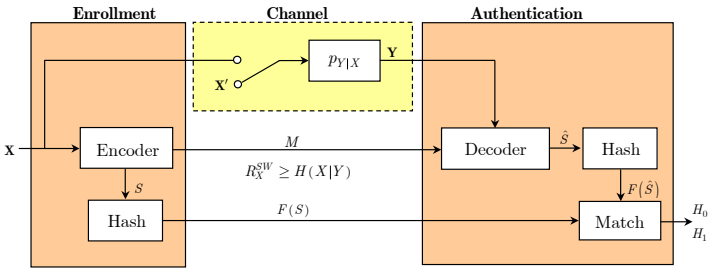



**Figure 3.** Authentication setup based on distributed coding and hashing of sequence index $s$ within the bin $m$.

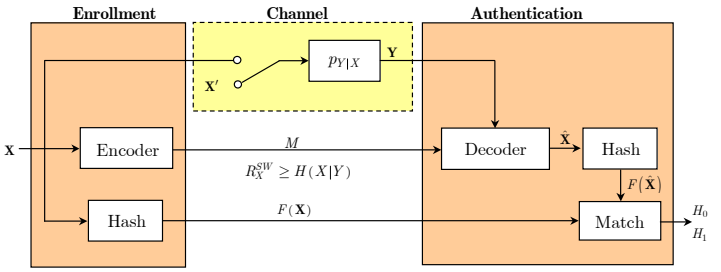



**Figure 4.** Authentication setup based on distributed coding and hashing of original sequence $\mathbf{x}$.

At the same time, the practical implementation of the above schemes was envisioned by the conversion of the continuous vectors to the discrete representations, e.g., extraction of minutia features,[9] quantization of randomly projected data from non-overlapping blocks of size $16 \times 16$,[8] binarization of speckle images based on Gabor transform subbands thresholding[6] and similar transformations predicted for optical and coated physical unclonable functions.[14] All these transformations are not invertible and obviously lead to the information loss due to data processing inequality.[4] The quantitative estimation of such a loss was not reported besides the results of computer modeling. Moreover, the definition of security has also different notion for the considered biometrics authentication systems[6,9,14] and physical item protection. In the biometric context, it is assumed that both $\mathbf{x}$ and $\mathbf{y}$ can be only obtained from the physical person and thus are unknown for the attacker. Therefore, the security leakage sources were considered with respect to the indexes $m$ and $s$ and the corresponding efforts have been dedicated to protect the scheme from the direct disclosure of biometric data $\mathbf{x}$ that can be exploited by the attacker for impersonation. In the item authentication application, the data $\mathbf{x}$ is inherently present for

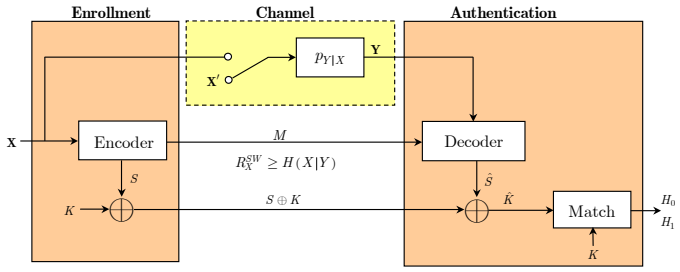



**Figure 5.** Authentication setup based on distributed coding and sequence index $s$ XORing, which identify the sequence $\mathbf{x}$ within the bin $m$.

the counterfeiter and the the security relies on the physical impossibility to reproduce the duplicate or clone that altogether with the index $m$ and any assisting data might be accepted as the authentic item. Nevertheless, there are a number of crypto-based attacks that can benefit from the disclosure of the coding-authentication scheme to present a fake $\mathbf{x}'$ with the index $m$ that can be falsely accepted.

Therefore, as the first step on the way toward the theoretical quantification of the loss due to the above feature extraction and countermeasures related to the protection of the codebook against the impersonation attack, we will consider the performance of simple lossless source coding based authentication presented in Figure 2 accompanied by a generic random projection operator $\mathbf{\Phi}$ shown in Figure 6. Such kind of a projection into a secure key-defined domain besides the security insures the dimensionality reduction, complexity as well as memory storage. The transform $\mathbf{\Phi}$ produces vectors $\tilde{\mathbf{x}}(m)$ and $\tilde{\mathbf{y}}$ of dimensionality $L$, where $L \leq N$. Additionally, the transform can be chosen in such a way to guarantee a certain robustness to the legitimate distortions. In the rest, this protocol is similar to one from Figure 2.

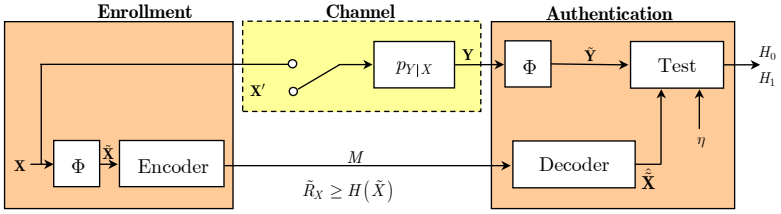



**Figure 6.** Authentication setup with random projections: $\mathbf{\Phi}$ is the key-based random projection operator.

The main goal of the paper is to compare the performance of the authentication setup from Figure 2 with one based on random projections shown in Figure 6 in terms of probability of false acceptance $P_F$ and probability of correct acceptance $P_D$ that form a receiver operation characteristic (ROC).

The paper has the following structure. The generic authentication problem formulation is considered in Section 2. The authentication in the direct domain according to Figure 2 is presented in Section 3 while in the random projections domain according to Figure 6 in Section 4. The results of computer simulation are given in Section 5. Finally, Section 6 concludes the paper.

## 2. GENERIC AUTHENTICATION PROBLEM

A generic authentication problem can be considered as a hypothesis testing[11] that requires the selection of authentication criteria and assumptions behind the statistics of genuine and faked items. In the most general case, the authentication problem can be considered as a decision making that the observed codeword $\mathbf{y}$ is in some proximity to the genuine codeword $\mathbf{x}(m)$, for example specified in the Euclidean space as $\|\mathbf{x}(m) - \mathbf{y}\|^2 \leq e_m$,

where $e_m$ defines the acceptable distortions as well as the acceptance region $\mathcal{R}_1$, while $\mathcal{R}_0$ is considered to be the rejection region. This can be schematically shown as in Figure 7 for all realizations or codewords.

To design the decision rule for the binary hypothesis testing, we will use an approach similar to one exploited in digital communications for the analysis of upper bounds on probability of error attained by linear codes. In particular, union bound limits probability of error of such codes based on the first component of their spectrum, i.e., the minimum distance of the code.[5, 12] Therefore, we will analyze the problem of the binary hypothesis testing in the worst case condition for the selection of the alternative hypothesis. We will assume that given the enrolled database of all item forensics and specified index $m$ or equivalently $\mathbf{x}(m)$, one needs to ensure the desired ROC for the closest possible codeword denoted as $\mathbf{x}(n)$ in the above mentioned Figure among all $M$ codewords. It should be noticed that one can also ensure the specified ROC taking into account all codewords and their corresponding probabilities of appearance that corresponds to the Bayessian framework. However, to avoid cumbersome integrations that reduces tractability, we will follow the worst case approach.[†]

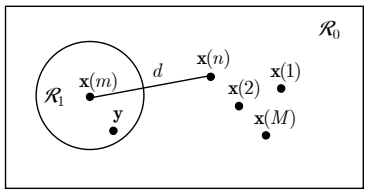



**Figure 7.** Authentication setup in the codeword space.

## 3. AUTHENTICATION AS BINARY HYPOTHESIS TESTING

We will formulate the authentication problem as the hypothesis testing with two hypothesis, i.e., $H_1$ corresponds to the case that the item is authentic and $H_0$ faked, for the genuine codeword $\mathbf{x}(m)$ and its worst case counterpart $\mathbf{x}(n)$:

$$\begin{cases} H_0: & \mathbf{y} = \mathbf{x}(n) + \mathbf{z}, \\ H_1: & \mathbf{y} = \mathbf{x}(m) + \mathbf{z}, \end{cases} \tag{3}$$

where $\mathbf{z}$ is the noise component corresponding to the DMCs $p_{Y|X}$.

We will use the Neyman-Pearson decision rule that maximizes $P_D$ subject to the constraint $P_F \leq \alpha$ that can be formulated as the likelihood ratio test:

$$\Lambda(\mathbf{y}) = \frac{p(\mathbf{y}|H_1)}{p(\mathbf{y}|H_0)} \lessgtr \eta, \tag{4}$$

with the threshold $\eta$ chosen to satisfy the constraint $P_F = \int_{\Lambda(\mathbf{y})>\eta} p(\mathbf{y}|H_0)d\mathbf{y} = \alpha$, where $p(\mathbf{y}|.)$ is the distribution $\mathbf{y}$ under the corresponding hypothesis.

Under the Gaussian assumption about the noise $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2\mathbf{I}_N)$ and known signals $\mathbf{x}(m)$ and $\mathbf{x}(n)$, we have [‡]:

$$\begin{cases} H_0: & p(\mathbf{y}|H_0) = \mathcal{N}(\mathbf{x}(n), \sigma_Z^2\mathbf{I}_N), \\ H_1: & p(\mathbf{y}|H_1) = \mathcal{N}(\mathbf{x}(m), \sigma_Z^2\mathbf{I}_N). \end{cases} \tag{5}$$

The decision rule (4) can be reformulated by taking the logarithm as:

$$\log p(\mathbf{y}|H_1) - \log p(\mathbf{y}|H_0) \lessgtr \log \eta. \tag{6}$$

The test (6) can be reduced to the sufficient statistic $t$:

[†]Alternatively, one can also consider generalized maximum likelihood approach.

[‡]The selection of the Gaussian noise is explained by the largest differential entropy (worst case conditions for the authentication) among all distributions with the bounded variance.

$$t(\mathbf{y}) := \mathbf{y}^T \left(\mathbf{x}(m) - \mathbf{x}(n)\right) - \frac{1}{2}(\epsilon(m) - \epsilon(n)) \lessgtr \gamma, \tag{7}$$

where $\gamma = \sigma_Z^2 \log \eta$ and $\epsilon(m) = \mathbf{x}^T(m)\mathbf{x}(m) = \|\mathbf{x}(m)\|^2$ is the energy of signal $\mathbf{x}(m)$ and $\epsilon(n) = \mathbf{x}^T(n)\mathbf{x}(n) = \|\mathbf{x}(n)\|^2$ of $\mathbf{x}(n)$, which is characterized by:

$$\begin{cases} H_0: & T \sim \mathcal{N}(-\frac{1}{2}d^2, \sigma_Z^2 d^2), \\ H_1: & T \sim \mathcal{N}(+\frac{1}{2}d^2, \sigma_Z^2 d^2), \end{cases} \tag{8}$$

where $d^2 = \|\mathbf{x}(m) - \mathbf{x}(n)\|^2$.

The probability of false alarm $P_F$ and correct detection $P_D$ can be now found as:

$$\begin{cases} P_F = \Pr[T > \gamma | H_0] = Q\left(\frac{\gamma + \frac{1}{2}d^2}{\sqrt{\sigma_Z^2 d^2}}\right), \\ P_D = \Pr[T > \gamma | H_1] = Q\left(\frac{\gamma - \frac{1}{2}d^2}{\sqrt{\sigma_Z^2 d^2}}\right). \end{cases} \tag{9}$$

To determine a threshold $\gamma$, we set $P_F = \alpha$, which yields:

$$\gamma = \sigma_Z d Q^{-1}(\alpha) - \frac{1}{2}d^2, \tag{10}$$

where $Q(.)$ is the $Q$-function, that results in:

$$P_D(\alpha) = Q\left(Q^{-1}(\alpha) - \sqrt{\frac{d^2}{\sigma_Z^2}}\right). \tag{11}$$

Let $\bar{\epsilon} = \frac{1}{2}(\epsilon(m) + \epsilon(n))$, which assumes equals prior probabilities. Then:

$$d^2 = \|\mathbf{x}(m) - \mathbf{x}(n)\|^2 = 2\bar{\epsilon} - 2\mathbf{x}^T(m)\mathbf{x}(n) = 2\bar{\epsilon}(1 - \kappa_X), \tag{12}$$

where $\kappa_X = \frac{\mathbf{x}^T(m)\mathbf{x}(n)}{\frac{1}{2}(\mathbf{x}^T(m)\mathbf{x}(m) + \mathbf{x}^T(n)\mathbf{x}(n))}$. If $\kappa_X = 0$, $\mathbf{x}^T(m)\mathbf{x}(n) = 0$ and two vectors are orthogonal.

If we also assume that both signals have the same energy, i.e., $\epsilon(m) = \epsilon(n) = \epsilon$, then:

$$P_D(\alpha) = Q\left(Q^{-1}(\alpha) - \sqrt{\frac{2\epsilon(1 - \kappa_X)}{\sigma_Z^2}}\right). \tag{13}$$

For $\kappa_X = 0$ that corresponds to the case of well-known orthogonal signaling in digital communications, it yields:

$$P_D(\alpha) = Q\left(Q^{-1}(\alpha) - \sqrt{2\xi}\right). \tag{14}$$

where $\xi = \frac{\epsilon}{\sigma_Z^2}$ (we also define $SNR = 10 \log_{10} \xi$).

The average probability of error is:

$$P_e = \frac{1}{2}P_F + \frac{1}{2}(1 - P_D) = Q\left(\sqrt{\frac{1}{2}\xi}\right). \tag{15}$$

## 4. AUTHENTICATION BASED ON RANDOM PROJECTIONS

In this section, we will consider the above authentication setup according to Figure 6, where the protocol is based on a sort of hashes computed from $\mathbf{y}$ and $\mathbf{x}(m)$ using key-dependent mapping:

$$\tilde{\mathbf{y}} = \mathbf{\Phi}\mathbf{y}, \tag{16}$$

$\mathbf{y} \in \mathbb{R}^N$, $\tilde{\mathbf{y}} \in \mathbb{R}^L$, $\mathbf{\Phi} \in \mathbb{R}^{L \times N}$ and $L \leq N$. The matrix $\mathbf{\Phi}$ has the elements $\varphi_{i,j}$ that are generated from some specified distribution and it is known as a random projection. $L \times N$ random matrices $\mathbf{\Phi}$ whose entries $\varphi_{i,j}$ are

independent realizations of Gaussian random variables $\Phi_{i,j} \sim \mathcal{N}(0, \frac{1}{N})$ represent a particular interest for our study. In this case, such a matrix can be considered as an orthoprojector, for which $\mathbf{\Phi}\mathbf{\Phi}^T \approx \mathbf{I}_L$.

The corresponding hypotheses can be reformulated as:

$$\begin{cases} \tilde{H}_0: & \tilde{\mathbf{y}} = \mathbf{\Phi}(\mathbf{x}(n) + \mathbf{z}) = \tilde{\mathbf{x}}(n) + \tilde{\mathbf{z}}, \\ \tilde{H}_1: & \tilde{\mathbf{y}} = \mathbf{\Phi}(\mathbf{x}(m) + \mathbf{z}) = \tilde{\mathbf{x}}(m) + \tilde{\mathbf{z}}, \end{cases} \tag{17}$$

that leads to the test:

$$\Lambda(\tilde{\mathbf{y}}) = \frac{p(\tilde{\mathbf{y}}|\tilde{H}_1)}{p(\tilde{\mathbf{y}}|\tilde{H}_0)} \lessgtr \tilde{\eta}, \tag{18}$$

with the distributions under hypothesis:

$$\begin{cases} \tilde{H}_0: & p(\tilde{\mathbf{y}}|\tilde{H}_0) = \mathcal{N}(\tilde{\mathbf{x}}(n), \sigma_Z^2\mathbf{C}), \\ \tilde{H}_1: & p(\tilde{\mathbf{y}}|\tilde{H}_1) = \mathcal{N}(\tilde{\mathbf{x}}(m), \sigma_Z^2\mathbf{C}), \end{cases} \tag{19}$$

where $\mathbf{C} = \mathbf{\Phi}\mathbf{\Phi}^T$.

Similarly, one can deduce the sufficient statistic $\tilde{t}$:

$$\tilde{t}(\tilde{\mathbf{y}}) := \tilde{\mathbf{y}}^T\mathbf{C}^{-1}\left(\tilde{\mathbf{x}}(m) - \tilde{\mathbf{x}}(n)\right) - \frac{1}{2}\Delta\tilde{\epsilon} \lessgtr \tilde{\gamma}, \tag{20}$$

where $\tilde{\gamma} = \sigma_Z^2 \log\tilde{\eta}$ and $\Delta\tilde{\epsilon} = \tilde{\mathbf{x}}^T(m)\mathbf{C}^{-1}\tilde{\mathbf{x}}(m) - \tilde{\mathbf{x}}^T(n)\mathbf{C}^{-1}\tilde{\mathbf{x}}(n)$, which is characterized by:

$$\begin{cases} \tilde{H}_0: & \tilde{T} \sim \mathcal{N}(-\frac{1}{2}\tilde{d}^2, \sigma_Z^2\tilde{d}^2), \\ \tilde{H}_1: & \tilde{T} \sim \mathcal{N}(+\frac{1}{2}\tilde{d}^2, \sigma_Z^2\tilde{d}^2), \end{cases} \tag{21}$$

where $\tilde{d}^2 = \left(\mathbf{x}(m) - \mathbf{x}(n)\right)^T\mathbf{\Phi}^T\mathbf{C}^{-1}\mathbf{\Phi}\left(\mathbf{x}(m) - \mathbf{x}(n)\right)$.

The probabilities of false alarm $P_F$ and correct detection $P_D$ can be now found as:

$$\begin{cases} P_F = \Pr[\tilde{T} > \tilde{\gamma}|\tilde{H}_0] = Q\left(\frac{\tilde{\gamma}+\frac{1}{2}\tilde{d}^2}{\sqrt{\sigma_Z^2\tilde{d}^2}}\right), \\ P_D = \Pr[\tilde{T} > \tilde{\gamma}|\tilde{H}_1] = Q\left(\frac{\tilde{\gamma}-\frac{1}{2}\tilde{d}^2}{\sqrt{\sigma_Z^2\tilde{d}^2}}\right). \end{cases} \tag{22}$$

Assuming $P_F = \alpha$, one obtains:

$$P_D(\alpha) = Q\left(Q^{-1}(\alpha) - \sqrt{\frac{\tilde{d}^2}{\sigma_Z^2}}\right). \tag{23}$$

Assuming the condition of orthoprojection for $\mathbf{\Phi}$ one obtains $\mathbf{C} = \mathbf{\Phi}\mathbf{\Phi}^T = \mathbf{I}_L$ and for the distance $\tilde{d}^2 = \left(\mathbf{x}(m) - \mathbf{x}(n)\right)^T\mathbf{\Phi}^T\mathbf{\Phi}\left(\mathbf{x}(m) - \mathbf{x}(n)\right) = \left\|\mathbf{\Phi}\left(\mathbf{x}(m) - \mathbf{x}(n)\right)\right\|^2$

To introduce the bounds on the distance $\tilde{d}^2$ we will use the results of Johnson-Lindenstrauss lemma,[7] which states that with high probability the geometry of a point cloud is not disturbed by certain Lipschitz mappings onto a space of dimension logarithmic in the number of points. In particular, some existing proofs of the lemma show that the mapping $\mathbf{\Phi}$ can be taken as a linear mapping represented by an $L \times N$ matrix whose entries are randomly drawn from certain probability distributions. More particularly, $M$ vectors in the Euclidean space can be projected down to $L = O(\zeta^{-2}\log_2 M)$ dimensions while incurring a distortion of at most $1 + \zeta$ in their pairwise distances, where $0 < \zeta < 1$. In principle, this can be achieved by a dense $L \times N$ matrix and such a mapping takes $O(N \log_2 M)$ (for fixed $\zeta$). We refer interested readers to[1] for more details.

According to Johnson-Lindenstrauss result[7]:

$$(1-\zeta)\sqrt{\frac{L}{N}} \le \frac{||\mathbf{\Phi}\mathbf{x}||}{||\mathbf{x}||} \le (1+\zeta)\sqrt{\frac{L}{N}}, \tag{24}$$

with high probability.

This allows to use the approximation for the random orthoprojector $\mathbf{\Phi}$ as:

$$(1-\zeta)\sqrt{\frac{L}{N}}||\mathbf{x}|| \leq ||\mathbf{\Phi x}|| \leq (1+\zeta)\sqrt{\frac{L}{N}}||\mathbf{x}||. \tag{25}$$

Thus, with high probability one can approximate (23) as follows:

$$P_D(\alpha) \approx Q\left(Q^{-1}(\alpha) - \sqrt{\frac{L}{N}}\sqrt{\frac{d^2}{\sigma_Z^2}}\right), \tag{26}$$

that makes possible to estimate the corresponding loss with respect to the equation (11). The random projections introduce the loss in the distance between codewords proportional to $\sqrt{\frac{L}{N}}$.

Equivalently to (14) for the equiprobable orthogonal signals with the same energy, one can rewrite the above approximation as:

$$P_D(\alpha) = Q\left(Q^{-1}(\alpha) - \sqrt{\frac{L}{N}}\sqrt{2\xi}\right). \tag{27}$$

Finally, the average probability of error computed for the direct domain according to (15) can be found for the random projections domain as:

$$P_e = Q\left(\sqrt{\frac{1}{2}\frac{\mathbf{x}^T(m)\mathbf{\Phi}^T\mathbf{\Phi x}(m)}{\sigma_Z^2}}\right), \tag{28}$$

with the approximation:

$$P_e \approx Q\left(\sqrt{\frac{L}{N}}\sqrt{\frac{1}{2}\xi}\right). \tag{29}$$

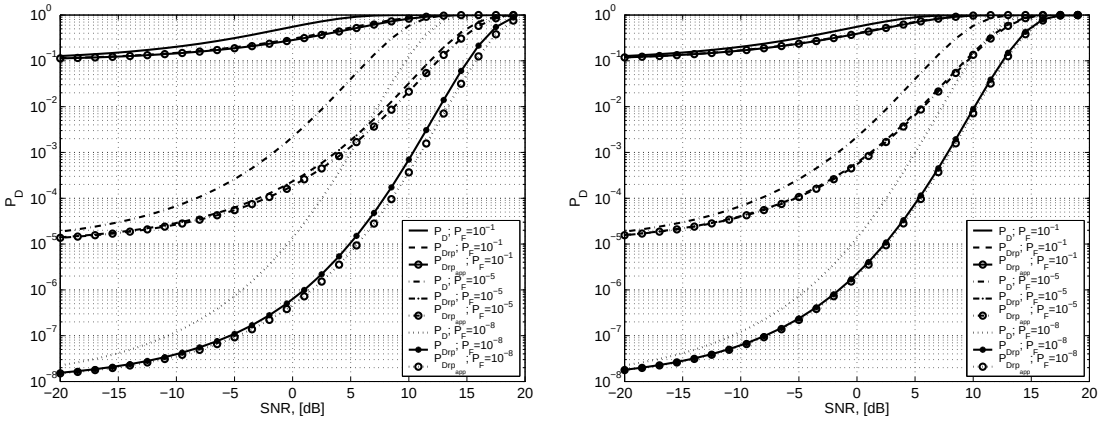
## 5. COMPUTER SIMULATION

In this section, the impact of dimensionality reduction based on the random projections and approximation accuracy was investigated using both analytical formulas and Monte Carlo simulation for Gaussian data of lengths $N_X = N_Y = 3500$. The orthoprojectors $\mathbf{\Phi_x}$ and $\mathbf{\Phi_y}$ have been generated according to the Gaussian distribution with the parameters described in Section 4. We plot the operational characteristic of authentication scheme in Figure 8 for the authentication without transform $\mathbf{\Phi}$ (14) (denoted as $P_D$), with the transform (27) (denoted as $P_{Drp}$) and its approximation (26) (denoted as $P_{Drp_{app}}$) for three ratios $L/N$ equal 0.25, 0.50 and 0.75. Obviously, the decrease of dimensionality causes a degradation in performance. However, in relatively high SNR, the authentication based on the random projections can perform closely to the traditional authentication.

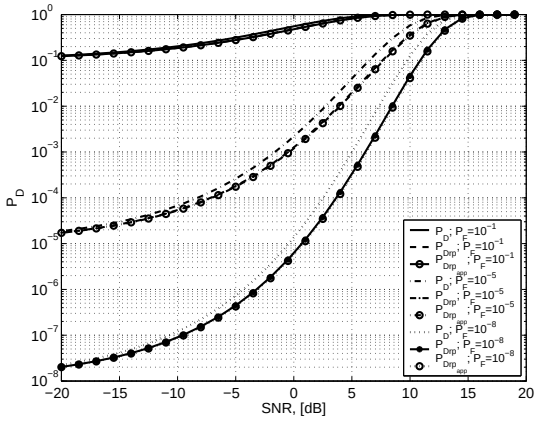
Moreover, the random projections approximation based on the Johnson-Lindenstrauss lemma demonstrates quite accurate results in all experimants and can be used for the estimation of performance.

## 6. CONCLUSIONS

In this paper, we considered the item authentication based on random projections and distributed coding. In particular, we investigated the impact of dimensionality reduction performed using random orthoprojectors and proposed the corresponding approximations using the Johnson-Lindenstrauss lemma. It was established that the orthoprojectors reduce the vector and distribution distances proportionally to the ratio of the vector lengths after and before projection that provides the hints about fusion techniques based on feature extraction and confirmed the well-known general information-theoretic result of data processing inequality. These findings might be of interest for the design of practical authentication systems. In future, we plan to consider a practical implementation of distributed source coding based authentication framework analyzed in this paper using LDPC codes and investigate the impact of lossy source coding based on Wyner-Ziv approach on the distribution under hypothesis $H_1$ and corresponding performance as well as practically validate the considered theoretical setup for the person authentication based on several biometrics and packaging authentication using sampling in several key-defined locations. Not less important problem would be the investigation of security of the considered setup and study of possible attacks.




(a) (b)




(c)

**Figure 8.** Probability of correct detection $P_D$ for $P_F$ equals $10^{-1}, 10^{-5}$ and $10^{-8}$ for $L/N$ ratios equal (a) 0.25, (b) 0.50 and (c) 0.75.

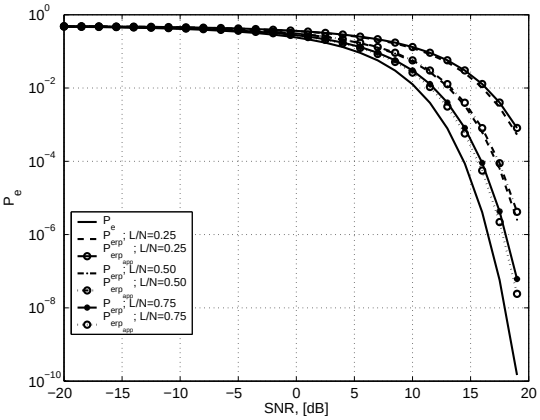



**Figure 9.** Average probability of error for $L/N$ ratios equal 0.25, 0.50 and 0.75.

## 7. ACKNOWLEDGMENTS

This paper was partially supported by SNF PB grant 114613 and SNF 200021–119770, 20020–121635 and Swiss IM2 project.

## REFERENCES

1. D. Achlioptas. Database-friendly random projections: Johnson-Lindenstrauss with binary coins. *JOURNAL OF COMPUTER AND SYSTEM SCIENCES*, 66(4):671–687, 2003.
2. R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography - Part I: secret sharing. *IEEE Trans. Inform. Theory*, 39(4):1121–1132, 1993.
3. F. Beekhof, S. Voloshynovskiy, O. Koval, R. Villan, and T.Pun. Secure surface identification codes. In *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, San Jose, CA, USA, Jan 27–31 2008.
4. T. Cover and J. Thomas. *Elements of Information Theory*. Wiley and Sons, New York, 1991.
5. H.Herzberg and G.Poltyrev. Techniques of bounding the probability of decoding error for block coded modulation structures. *IEEE Trans. Information Theory*, 44(4):427–433, April 1996.
6. T. Ignatenko and F.M.J. Willems. On the security of xor-method in biometric authentication systems. In *The twenty-seventh symposium on Information Theory in the Benelux*, pages 197–204, Noordwijk, The Netherlands, June 8-9 2006.
7. W. B. Johnson and J. Lindenstrauss. Extensions of Lipschitz mappings into Hilbert space. *Contemporary Mathematics*, (26):189–206, 1984.
8. Y.-C. Lin, D. Varodayan, and B. Girod. Image authentication based on distributed source coding. In *IEEE International Conference on Image Processing (ICIP2007)*, San Antonio, USA, September 2007.
9. E. Martinian, S. Yekhanin, and J.S. Yedidia. Secure biometrics via syndromes. In *43rd Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, USA, October 2005.
10. U. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory*, 39:733–742, 1993.
11. U. Maurer. A unified and generalized treatment of authentication theory. In *Proc. 13th Symp. on Theoretical Aspects of Computer Science (STACS'96)*, volume 1046 of *Lecture Notes in Computer Science*, pages 387–398. Springer-Verlag, Feb 1996.
12. G. Poltyrev. Bounds on the decoding error probability of binary linear codes via their spectra. *IEEE Trans. on Information Theory*, 40(4):1284–1293, April 1994.
13. D. Slepian and J.K. Wolf. Noiseless encoding of correlated information sources. *IEEE Trans. Information Theory*, 19:471–480, July 1973.
14. P. Tuyls, B. Skoric, and T. Kevenaar (Eds.). *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer, 2007.
15. A. Wyner and J. Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. Information Theory*, 22(1):1–10, January 1976.