Privacy enhancement of common randomness based authentication: key rate maximized case

Voloshynovskyy, Svyatoslav; Koval, Oleksiy; Holotyak, Taras; Beekhof, Fokko Pieter

PRIVACY ENHANCEMENT OF COMMON RANDOMNESS BASED AUTHENTICATION: KEY RATE MAXIMIZED CASE

Sviatoslav Voloshynovskiy, Oleksiy Koval, Taras Holotyak and Fokko Beekhof

University of Geneva
Department of Computer Science
7 route de Drize, CH 1227, Geneva, Switzerland

ABSTRACT

In this paper, we consider security-privacy issues in authentication techniques based on the extraction of common randomness. We demonstrate that the key rate-privacy leak pairs can be enhanced using reliable components extraction from specially designed random projections. The decrease of bit error probability is estimated and its impact on the key rate and privacy leak is evaluated. Several authentication schemes with new helper data protocol are proposed.

1. INTRODUCTION

Recently, the authentication of humans and physical objects based on *biometrics* and *physically unclonable functions* (PUFs) underwent a considerable evolution enabling to introduce crypto-based security into the analog noisy world [1]. These new techniques are able to overcome the fundamental sensitivity issue of classical cryptographic encryption and one-way functions to small noise in input data by trade-offing the security and robustness to noise. The inherent feature of practically all state-of-the-art authentication protocols robust to noise is the storage of some additional information (a.k.a. *helper data*) assisting in the reliable extraction of a *common secret* at the enrollment (encoder) and authentication (decoder) sides [1, 2, 3]. At the same time, since the helper data is somehow input dependent, it raises natural concerns that it should provide little information about the secret extracted from the noisy data (*secrecy leak*) and input itself (*privacy leak*). The secrecy leak needs to be small to prevent system abuse by the *impersonation attack*, when the attacker tries to construct artificial biometrics or PUFs that can pass the authentication based on the disclosed templates. A small privacy leak is required to protect some sensitive information that can be extracted from the inputs. The schematic diagram of helper data based authentication is shown in Fig. 1. The main idea behind this kind of authentication is based on the Wyner-Ziv binning principle used for source coding with side information [4], when a compressed version $\mathbf{U}$ of input data $\mathbf{X}$ is constructed and the key S and helper data M are generated as functions of $\mathbf{U}$. Roughly $2^{NI(U;X)}$ $\mathbf{U}$ sequences are generated and randomly distributed into approximately $2^{N(I(U;X)-I(U;Y))}$ bins, each containing about $2^{NI(U;Y)}$ sequences. The bin index M serves as the helper data and the sequence index S within the bin is the key. The secure sketch approach [3] and Slepian-Wolf based authentication using syndrome coding [2] are exactly based on this architecture. The authentication layer is based on the classical cryptographic authentication as for the noiseless digital inputs. At the same time, the authentication system should satisfy:

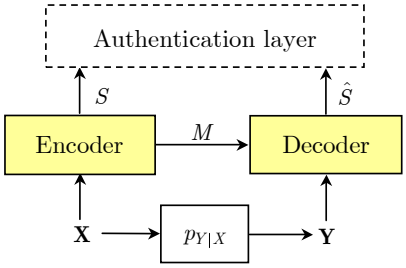

Fig. 1. Authentication based on helper data.

$$\text{reliability: } \Pr[\hat{S} \neq S] \leq \epsilon, \tag{1}$$

$$\text{key rate: } N^{-1}H(S) \geq R_s, \tag{2}$$

$$\text{secrecy leak: } I(S;M) \leq N\epsilon, \tag{3}$$

$$\text{privacy leak: } I(\mathbf{X};M) \leq N(L_p+\epsilon), \tag{4}$$

with small nonnegative ϵ. The secrecy leak $I(S;M)$ can be made arbitrary small by proper randomization and one can control the trade-off between the privacy leak L_p and key rate R_s by the different choices of $\mathbf{U}$. It was demonstrated that this trade-off can be [5, 6]:

$$R_s \leq I(U;Y), \tag{5}$$

$$L_p \geq I(U;X) - I(U;Y). \tag{6}$$

The key rate can be maximized by setting $U = X$ that yields:

$$R_s \leq I(X;Y), \tag{7}$$

$$L_p \geq H(X|Y). \tag{8}$$

The contact author is S. Voloshynovskiy (email: svolos@unige.ch). http://sip.unige.ch. This work is supported by SNF projects 111643 and 1119770

Such a selection of a compressed version U mimics the Slepian-Wolf lossless distributed source coding of discrete sources used in [2]. For the i.i.d. Gaussian setup with $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$ and $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, \sigma_X^2 \mathbf{I}_N)$ and $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma_Z^2 \mathbf{I}_N)$, it reduces to:

$$R_s^G \leq \frac{1}{2} \log_2 \frac{1}{1 - \rho_{XY}^2} = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_X^2}{\sigma_Z^2}\right), \quad (9)$$

$$L_p^G \geq \frac{1}{2} \log_2 (2\pi e \sigma_{X|Y}^2) \quad (10)$$

where $\rho_{XY}^2 = \frac{\sigma_X^2}{\sigma_X^2 + \sigma_Z^2}$ is the squared correlation coefficient between X and Y and $\sigma_{X|Y}^2 = \frac{\sigma_X^2 \sigma_Z^2}{\sigma_X^2 + \sigma_Z^2}$. If the above setup is converted into binary form based on binary quantization, one obtains the Slepian-Wolf scheme with:

$$R_s^B \leq I(B_{\mathbf{x}}; B_{\mathbf{y}}) = 1 - H(B_{\mathbf{x}}|B_{\mathbf{y}}), \quad (11)$$

$$L_p^B \geq H(B_{\mathbf{x}}|B_{\mathbf{y}}), \quad (12)$$

where $H(B_{\mathbf{x}}|B_{\mathbf{y}}) = H_2(\bar{P}_b) = -\bar{P}_b \log_2 \bar{P}_b - (1-\bar{P}_b) \log_2 (1-\bar{P}_b)$ that is the binary entropy; and for the equilikely bits $H(B_{\mathbf{x}}) = 1$ and the bit error probability $\bar{P}_b$ (cross-over probability for Binary Symmetric Channel (BSC) linking $B_{\mathbf{x}}$ and $B_{\mathbf{y}}$) is found as:

$$\bar{P}_b = \frac{2}{\pi} \arctan \left(\sqrt{\frac{1 - \rho_{XY}}{1 + \rho_{XY}}}\right) = \frac{1}{\pi} \arccos(\rho_{XY}). \quad (13)$$

Therefore, the key rate-privacy leak pair is completely defined by $\bar{P}_b$ that in turn is defined by ρ_{XY}^2.

Tuyls *et. al.* considered two practical setups based on the above theoretical framework of helper data assisted authentication [7]. The first setup is based on the *secret extraction from significant components* [8] and the second one is based on the *secret extraction from binarized data* considered above using error-correction codes (ECC). The main idea behind the first setup is to apply the Fisher discriminative transform to the input data and to extract the most reliable components possessing a magnitude higher then a certain threshold. Thus, the helper data M is used to communicate the information about these components to the decoder. The scheme is 0-secrecy leaking, i.e., $I(S; M) = 0$, ans its robustness in terms of $\bar{P}_b$ was upper bounded according to Bernstein's inequality. The privacy of this scheme was not theoretically analyzed. The second setup is based on the ECC implementation, where it was also shown that $I(S; M) = 0$ and the key rate-privacy leak pair coincides with (11)-(12). The rate of ECC is proportional to $H_2(\bar{P}_b)$ that should ensure reliable key retrieval at the decoder side.

Both techniques are facing several deficiencies that we will address in this paper. In the first case, the application of Fisher transform requires knowledge of the input data and noise statistics in terms of their covariance matrices to perform the diagonalization. It can be estimated off-line but it still requires a quite significant amount of training data. Such a transform is data-dependent and the addition of new entries might also request the re-training that does not ensure backward compatibility. Moreover, the independence and Gaussianity of the transformed coefficients are desirable. Additionally, the extraction of significant components based on the absolute value thresholding leads to a variable template length. This requires an additional coefficient selection and the synchronization between the encoder and decoder. Finally, even though the significant component extraction based on the public-based Fisher transform is 0-secure, it raises certain privacy preserving issues. In this paper, we will show that the significant components are collinear to the basis vectors of the Fisher transform. The public information about these basis vectors even with the secret preservation of their signs reveals significant information to the attacker about $\mathbf{X}$. The second setup is based on the binarized data and information about the reliability is completely disregarded thus leading to relatively high $\bar{P}_b$ and sequentially to the reduction of key rate and increase of the privacy leak.

Therefore, the goal of this paper is to design a data-independent transform for the significant component extraction and reduce the privacy leak due to the helper data. To achieve this goal, we introduce a generic random transform with a fixed number of reliable coefficients and demonstrate the impact of side information accuracy about the significant components on $\bar{P}_b$ in Section 2.1. Based on these results, we propose several authentication schemes with enhanced privacy in Section 2.2. The results of computer simulation are presented in Section 3. Section 4 concludes the paper.

2. PROPOSED AUTHENTICATION SYSTEM

In this paper, we will target the key rate maximization approach described in Section I that results in the selection $U = X$ with the upper bound on the key rate R_s (7). Therefore, our primary goal is to reduce the privacy leak of both practical systems considered above.

2.1. Reliable components extraction

The extraction of significant components in the scope of this paper is performed based on the random projection transform. This transform can also be considered as a mapping of the original data $\mathbf{x}$ to some *secure* and *robust* domain:

$$\tilde{\mathbf{x}} = \mathbf{W}\mathbf{x}, \quad (14)$$

where $\mathbf{x} \in \mathbb{R}^N$, $\tilde{\mathbf{x}} \in \mathbb{R}^L$, $\mathbf{W} \in \mathbb{R}^{L \times N}$ and $L \leq N$ and $\mathbf{W} = (\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_L)^T$ consists of a set of projection basis vectors $\mathbf{w}_i \in \mathbb{R}^N$ with $1 \leq i \leq L$. Instead of following a particular consideration of mapping $\mathbf{W}$, we will assume that $\mathbf{W}$ is a random matrix. The matrix $\mathbf{W}$ has the elements $w_{i,j}$ that are generated from some specified distribution. $L \times N$ random matrix $\mathbf{W}$ whose entries $w_{i,j}$ are independent realizations of Gaussian random variables $W_{i,j} \sim \mathcal{N}(0, \frac{1}{N})$ presents a particular interest for our study. In this case, such a matrix can be considered as an almost *orthoprojector*, for which

$\mathbf{W}\mathbf{W}^T \approx \mathbf{I}_L$. Moreover, the selection of basis vectors with Gaussian distribution also guarantees the Gaussian distribution of projected coefficients.

The second step also uses a possibly key-dependent labeling or Grey codes to ensure closeness of labels for close vectors. The most simple quantization or binarization of extracted features is known as *sign random projections*:

$$b_{\mathbf{x}_i} = sign(\mathbf{w}_i^T \mathbf{x}), \tag{15}$$

where $b_{\mathbf{x}_i} \in \{0,1\}$, with $1 \leq i \leq L$ and $sign(a) = 1$, if $a \geq 0$ and 0, otherwise. The vector $\mathbf{b}_\mathbf{x} \in \{0,1\}^L$ computed for all projections represents a *binary template* of the vector $\mathbf{x}$. Since all projections are independent, it can be assumed that all bits in $\mathbf{b}_\mathbf{x}$ will be independent and equiprobable.

Obviously, the template computed from some distorted version $\mathbf{y}$ of $\mathbf{x}$ denoted as $\mathbf{b}_\mathbf{y}$ might contain some bits different from those in $\mathbf{b}_\mathbf{x}$. Therefore, the link between the binary representation $\mathbf{b}_\mathbf{x}$ of vector $\mathbf{x}$ and its noisy counterpart $\mathbf{b}_\mathbf{y}$ of vector $\mathbf{y}$ is defined according to the BSC with average probability $\bar{P}_b$. The bit error probability indicates the mismatch of signs between $\tilde{x}_i$ and $\tilde{y}_i$ according to (15), i.e., $\Pr[sign(\tilde{x}_i) \neq sign(\tilde{y}_i)]$. For a given $\mathbf{x}$ and $\mathbf{w}_i$, the probability of bit error is:

$$P_{b|\tilde{x}_i} = \frac{1}{2}(\Pr[\tilde{Y}_i \geq 0 | \tilde{X}_i < 0] + \Pr[\tilde{Y}_i < 0 | \tilde{X}_i \geq 0]), \tag{16}$$

or by symmetry as:

$$P_{b|\tilde{x}_i} = \Pr[\tilde{Y}_i < 0 | \tilde{X}_i \geq 0]. \tag{17}$$

For a given $\tilde{x}_i$ and Gaussian noise[1], the distribution of the projected vector is $\tilde{Y}_i \sim \mathcal{N}(\tilde{x}_i, \sigma_Z^2 \mathbf{w}_i^T \mathbf{w}_i)$ that reduces to $\tilde{Y}_i \sim \mathcal{N}(\tilde{x}_i, \sigma_Z^2)$ for the orthoprojector ($\mathbf{w}_i^T \mathbf{w}_i = 1$) and:

$$P_{b|\tilde{x}_i} = \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi\sigma_Z^2}} e^{\frac{-(\tilde{y}_i - \tilde{x}_i)^2}{2\sigma_Z^2}} d\tilde{y}_i = Q\left(\frac{\tilde{x}_i}{\sigma_Z}\right). \tag{18}$$

The origin of $P_{b|\tilde{x}_i}$ can be explained considering the mutual configuration of $\mathbf{x}$ and $\mathbf{w}_i$ (Fig. 2). The vector $\mathbf{x}$ forms the angle θ_{XW_i} with the basis vector $\mathbf{w}_i$ and the projection results into the scalar value $\tilde{x}_i$. The closer angle θ_{XW_i} is to $\pi/2$, the smaller value $\tilde{x}_i$. This leads to a larger probability that the sign of $\tilde{y}_i$ will be different from the sign of $\tilde{x}_i$. One can immediately note that since the projections are generated at random there is generally no guaranty that two vectors can be collinear. However, at the same time some of the projections might form angles with $\mathbf{x}$ that deviate from $\pi/2$ thus leading to smaller bit error probability. This observation makes it possible to assume that some projections can be more preferable than others and the equation (18) can be a good measure of bit *reliability* or *significance*.

The above analysis only refers to a single realization of $\mathbf{x}$. Since $\mathbf{X}$ is a random vector following some distribution $p(\mathbf{x})$, one should find the average probability of error for all possible realizations. Assuming $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, \sigma_X^2 \mathbf{I}_N)$, the statistics of data in the projection domain are $\tilde{X}_i \sim \mathcal{N}(0, \sigma_X^2)$ and:

$$\bar{P}_b = 2\int_0^\infty P_{b|\tilde{x}_i} p(\tilde{x}_i) d\tilde{x}_i \tag{19}$$

$$= 2\int_0^\infty Q\left(\frac{\tilde{x}_i}{\sigma_{Z_r}}\right) \frac{1}{\sqrt{2\pi\sigma_X^2}} e^{\frac{-\tilde{x}_i^2}{2\sigma_X^2}} d\tilde{x}_i = \frac{1}{\pi}\arccos(\rho_{XY}). \tag{20}$$

It should be noticed that all possible values $\tilde{x}_i$ in (19) originating from both "unreliable", i.e., values close to zero, and "reliable", i.e., values far away from zero, projections are taken into account with the same weight to form the resulting binary vector $\mathbf{b}_\mathbf{x}$. Obviously, for a given set of enrollment data one can always find a set of vectors $\mathbf{w}_i$, $1 \leq i \leq L$ minimizing the overall bit error probability like in the case of the Fisher transform. However, keeping in mind the facts that the number of classes might be in the order of millions and constantly updated such an optimization problem looks highly unfeasible. Therefore, in the scope of this paper we

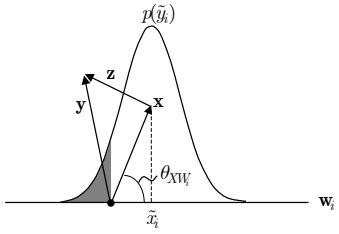

Fig. 2. The bit error probability for a given $\mathbf{x}$ and some $\mathbf{w}_i$.

will consider another approach when one generates the *overcomplete set of random projections* J and select among them only those L projections that are the largest in the absolute magnitude, if a fixed number of template bits is requested, or those that are higher then a certain threshold $T_{\tilde{x}}$ for a given $\mathbf{x}$ like in [8]. We will form a vector $\mathbf{P}_\mathbf{x} \in \{0,1\}^J$ containing the positions of significant components marked with 1s. In case of the above thresholding approach, the corresponding average probability of bit error is:

$$\bar{P}_{b_T} = \frac{1}{\int_{T_{\tilde{x}}}^\infty p(\tilde{x}_i) d\tilde{x}_i} \int_{T_{\tilde{x}}}^\infty P_{b|\tilde{x}_i} p(\tilde{x}_i) d\tilde{x}_i \tag{21}$$

$$= Q^{-1}\left(\frac{T_{\tilde{x}}}{\sigma_X}\right) \int_{T_{\tilde{x}}}^\infty Q\left(\frac{\tilde{x}_i}{\sigma_{Z_r}}\right) \frac{1}{\sqrt{2\pi\sigma_X^2}} e^{\frac{-\tilde{x}_i^2}{2\sigma_X^2}} d\tilde{x}_i, \tag{22}$$

where the multiplier is the normalization constant corresponding to the fraction of distribution behind the threshold.

It is easy to verify that the number of coefficients L of random variable $\tilde{X}_i$ following Gaussian distribution and exceeding the threshold $T_{\tilde{x}}$ in J projections satisfies with high probability the following equation:

$$\Pr[L \geq \ell] = 1 - F_{B_X}(J, \ell, \Pr[\tilde{X}_i > T_{\tilde{x}}]), \tag{23}$$

[1] In the case of assumed Gaussian random basis vectors $\mathbf{w}_i$ any distribution will be mapped into Gaussian one for both entry and noisy data.

where ℓ is the necessary number of reliable coefficients (like 32, 64 or 128), $F_{B_X}(J, \ell, \Pr[\tilde{X}_i > T_{\tilde{x}}])$ designates binomial cumulative distribution function and $\Pr[\tilde{X}_i > T_{\tilde{x}}] = Q\left(\frac{T_{\tilde{x}}}{\sigma_X}\right)$. In the case of selection of L largest components out of J, we will only assume that J is sufficiently large with respect to L to ensure the desirable bit error probability $\bar{P}_b'$.

2.2. Helper data communication: generalized protocol

The considered extraction of L significant components is used in the generalized authentication protocol shown in Fig. 3 [2] . The proposed protocol contains two types of helper data M_1 and M_2. The helper data M_1 is dedicated to the communication of side information about the significant components $\mathbf{P_x}$. The helper data M_2 serves for the errorless key recovery at the decoder based on $\mathbf{B_y}$.

Depending on the rate of helper data M_1, one can design different coding strategies for the desired key rate-privacy trade-off: (a) no side information about the reliable components, i.e., $H(\mathbf{P_x}) = 0$ with the overall helper data privacy leak $H_2(\bar{P}_b)$ from M_2; (b) the directly compressed significant components index vector $\mathbf{P_x}$ with the entropy $H(\mathbf{P_x})$ and reduced M_2 leak $H_2(\bar{P}_b')$; (c) the vector $\mathbf{P_x}$ compressed in the distributed way using $\mathbf{P_y}$ as the noisy side information with the entropy $H(\mathbf{P_x}|\mathbf{P_y})$ and the same M_2 leak $H_2(\bar{P}_b')$. The first strategy corresponds to the direct implementation of the Slepian-Wolf scheme considered in Section 1 with the relatively high privacy leak via M_2. The second strategy corresponds to the system considered in [8] with the difference in the procedure of significant components extraction described in the previous section. Moreover, contrary to the considered random projections, the publicly known basis vectors of the Fisher transform $\mathbf{w}_j$, $1 \le j \le J$ enforced by the information about the significant components $P_{\mathbf{x}_j}$ in [8] can leak up to $I(\mathbf{X}; \mathbf{W}_1 P_{\mathbf{x}_1}, \cdots, \mathbf{W}_J P_{\mathbf{x}_J})$= $I(\mathbf{X}; \mathbf{W}_1', \cdots, \mathbf{W}_L') \le \sum_{i=1}^{L} I(\mathbf{X}; \mathbf{W}_i')$ bits about $\mathbf{x}$, where $\mathbf{W}_i'$, $1 \le i \le L$ denote the basis vectors corresponding to the significant components. This mutual information is nonzero and this issue was not addressed in [8]. The third scheme only reveals $H(\mathbf{P_x}|\mathbf{P_y})$ bits about the positions of significant components contrarily to the previous one. Moreover, we will show in the next section that privacy leak in part of M_2 can be close to zero for a certain operation regime. It should be also pointed out that the use of described key-dependent orthoprojector $\mathbf{W}$ does not require any training and reveal any information about the basis vectors contrarily to the Fisher transform. Additionally, if the number of future items/users is essentially larger than the cardinality of training set, the performance of random orthoprojector asymptotically approaches those of Fisher transform in terms of $\bar{P}_b'$.

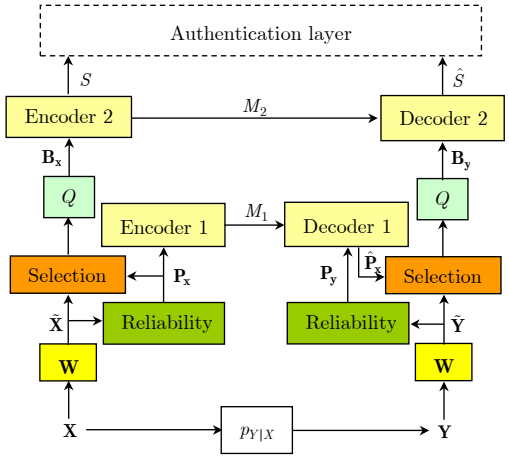

Fig. 3. Authentication based on helper data.

3. RESULTS OF COMPUTER SIMULATION

In this section, we present the results of computer simulation for the considered key rate-privacy leak formulation under the Gaussian observation and binarized setup. The observation model is considered in terms of signal-to-noise ratio (SNR) defined as SNR $= 10\log_{10}\frac{\sigma_X^2}{\sigma_Z^2}$. All results are obtained for 10000 noise realizations and 100 input vectors. First, we show the impact of significant components extraction on $\bar{P}_b$ according to the proposed overcomplete random projections transform with $J = 1500$ and $L = 32$ for $N = 1024$ length Gaussian input vectors versus the blind ransom transform (19) (Fig. 4). To estimate the privacy leak due to

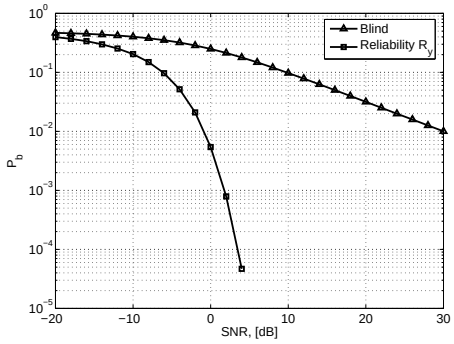

Fig. 4. Average bit error probability for blind and significant components based binarization based on $\mathbf{P_x}$.

the distributed coding of helper data M_1, we performed the simulations shown in Fig. 5. Obviously, this leak depends on the SNR and asymptotically converges to zero with the SNR increase. The key rate increase due to the usage of significant

[2] Since the mapping (14)-(15) does not generally guarantee the bit independence, one can apply privacy amplification. The privacy amplification can be accomplished in two different ways: (a) by applying diagonalization transform to the data $\tilde{\mathbf{X}}$ after (14) that closely follows Gaussian distribution or (b) by applying universal hashing that ensures the extraction of uniform binary template $\mathbf{B_x}'$ of length L' from $\mathbf{B_x}$ with $L > L'$.

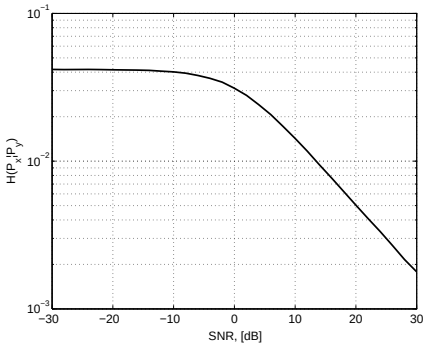

Fig. 5. Position information leak based on M_1 for significant components communication $H(P_{\mathbf{x}}|P_{\mathbf{y}})$.

components versus the blind random projection transform is shown in Fig. 6. Finally, to investigate the privacy leak due

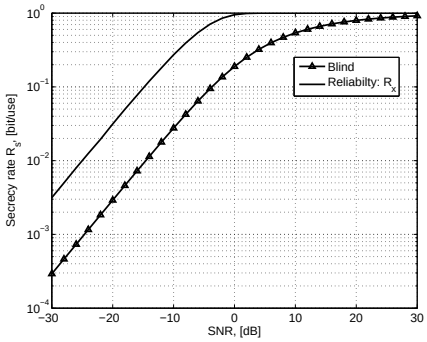

Fig. 6. Key rate R_s for blind and significant components based binarization based on $\mathbf{P_x}$.

to the helper data M_2 in different protocols, we obtained the results shown in Fig. 7. The privacy leak due to the significant component selection based on $\mathbf{P_x}$ is considerably reduced in comparison to the blind scheme. Moreover, one can expect even 0-privacy leak for SNR higher 10 dB.

4. CONCLUSIONS

We considered the generalized key rate maximizing authentication setup with two types of helper data based on the significant component positions and secure key encoding. The different coding schemes are analyzed to minimize the privacy leak due to the helper data. In particular, we established that one can achieve zero privacy leak in part of significant components helper data by their direct extraction from the noisy data. Moreover, the privacy leak in part of secret key extraction can be significantly reduced thanks to the proposed overcomplete random projection transform with the selection of fixed length template vector.

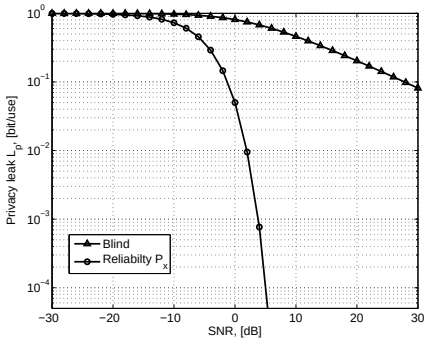

Fig. 7. Privacy leak L_p based on M_2 for blind and significant components based binarization based on $\mathbf{P_x}$.

5. REFERENCES

[1] P. Tuyls, B. Skoric, and T. Kevenaar (Eds.), *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer, 2007.

[2] 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.

[3] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 503–512, 2007.

[4] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Information Theory*, vol. 22, no. 1, pp. 1–10, January 1976.

[5] L. Lai, S.W. Ho, and H.V. Poor, "Privacy-security tradeoffs in biometric security systems," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, USA, 23-26 Sept. 2008, pp. 268–273.

[6] T. Ignatenko and F.M.H. Willems, "Privacy leakage in biometric secrecy systems.," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Urbana, USA, 23-26 Sept. 2008, pp. 850–857.

[7] P. Tuyls, E. Verbitskiy, J. Goseling, and D. Denteneer, "Privacy protecting biometric authentication systems: An overview," in *12th European Signal Processing Conference*, Vienna, Austria, 6-10 Sept. 2004, pp. 1397–1400.

[8] E. Verbitskiy, P. Tuyls, D. Denteneer, and J. P. Linnartz, "Reliable biometric authentication with privacy protection," in *24th Benelux Symposium on Information Theory*, 2003, pp. 125–132.