Privacy amplification of content identification based on fingerprint bit reliability

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

How to cite

VOLOSHYNOVSKYY, Svyatoslav et al. Privacy amplification of content identification based on fingerprint bit reliability. In: 2010 IEEE International Workshop on Information Forensics and Security (WIFS). Seattle (The USA). [s.l.] : Institute of Electrical and Electronics Engineers (IEEE), 2010. p. 1–6. doi: 10.1109/WIFS.2010.5711461

This publication URL: https://archive-ouverte.unige.ch//unige:47637
Publication DOI: 10.1109/WIFS.2010.5711461

Privacy Amplification of Content Identification Systems Based on Fingerprint Bit Reliability

Sviatoslav Voloshynovskiy, Oleksiy Koval, Taras Holotyak, Fokko Beekhof, Farzad Farhadzadeh

Department of Computer Science, University of Geneva
7 route de Drize, CH 1227, Geneva, Switzerland
{svolos, Oleksiy.Koval, Taras.Holotyak, Fokko.Beekhof, Farzad.Farhadzadeh}@unige.ch

***Abstract*—In many problems such as biometrics, multimedia search, retrieval, recommendation systems requiring privacy-preserving similarity computations and identification, some binary features are stored in the public domain or outsourced to third parties that might raise certain privacy concerns about the original data. To avoid this privacy leak, privacy amplification is used. In the most cases, the privacy amplification is uniformly applied to all binary features resulting in the data degradation and corresponding loss of performance. To avoid this undesirable effect we propose a new privacy amplification technique that benefits from side information about bit reliability. In this paper, we investigate the identification rate-privacy leak trade-off. The analysis is performed for the case of perfect match between the side information shared between the encoder and decoder as well as for the case of imperfect side information.**

I. Introduction

Content identification systems are widely used in various emerging applications ranging from identification of physical objects and humans to multimedia management (content filtering, content tagging) and security (copyright protection, broadcast monitoring, etc.). Most identification techniques are based on binary digital fingerprinting. A digital fingerprint represents a short, robust and distinctive content description allowing fast and privacy-preserving operations. In this case, all operations are performed on the fingerprint instead of on the original large and privacy-sensitive data thus enabling to introduce crypto-based security into the analog or noisy digital 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.

During last years, certain important practical and theoretical achievements were reported. The main efforts on the side of practical algorithms have been concentrated on robust feature selection and fast indexing techniques mostly borrowed from content-based retrieval applications [2], [3]. The information-theoretic limits of content identification under infinite length and ergodic assumptions and noisy enrollment have been investigated by Willems et. al. [4] using the jointly typical decoder. The impact of additional constraints on the fingerprint storage rate that can be also considered as a sort of enrollment distortions under the same asymptotic assumptions have been studied by Westover and O'Sullivan [5] and Tuncel *et. al.* [6]. The detection-theoretic limits have been first studied in [7] under geometrical desynchronization distortions and a further extension of this framework was proposed in [8] for the case of finite-length fingerprinting and null hypothesis. The used decision rule is based on minimum Hamming distance decoder with a fidelity constraint under Binary Symmetric Channel (BSC) model. Since this decision rule requires the computation of likelihoods/distances between the query and all database entries, the complexity of the considered identification is exponential with the input length. Due to the additional fact that identification services are often outsourced to third parties and state authorities, the privacy of data owners is an important issue and remains largely unexplored.

For the completeness of state-of-the-art analysis it is worth mentioning that privacy issues have been mainly studied in the authentication applications due to the public sharing of *helper data* and extended to various practical implementations based on Slepian-Wolf and Wyner-Ziv distributed coding [1], [9], [10]. 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.

Due to the essential difference in the formulation of privacy leaks in the authentication and identification problems, there is a necessity to protect not only the helper data as in the authentication problem but also the entire fingerprint. In our previous work [11] we have considered the rate-privacy-complexity trade-off for identification applications. This approach is based on global privacy amplification, where all bits of stored fingerprint are randomized with the same probability disregarding their reliabilities. This approach is similar in spirit to the compression based approaches [5], [6]. However, contrary to the previous approach a concept of bit reliability was introduced to reduce the identification complexity based on a bounded distance decoder (BDD). Obviously, such a construction does not fully benefit from the fact that the information about the reliable bits can be

WIFS'2010, December 12-15, 2010, Seattle, WA, USA.
978-1-4244-9080-6/10/$26.00

present at the encoder and decoder that can be used not only for the efficient decoding but also for the enhanced privacy amplification.

Therefore, in this paper we introduce an information-theoretic framework for the analysis of private content identification based on finite length fingerprinting with bit reliability side information. Contrary to previous works, we propose a privacy amplification mechanism, which is adaptive to the bit reliability, and demonstrate its advantages over the state-of-the-art privacy amplification in the identification problem. We present and analyze a privacy-preserving technique, which asymptotically achieves the theoretical identification performance limits in terms of identification rate. The proposed technique is based on Forney's type of erasure/list decoding [12] implemented in the form of BDD. The analysis is performed for the case of perfect match between the side information shared between the encoder and decoder as well as for the case of imperfect side information.

Notations. We use capital letters to denote scalar random variables X, bold capital letters to denote vector random variables $\mathbf{X}$, corresponding small letters x and small bold letters $\mathbf{x}$ to denote the realizations of scalar and vector random variables, respectively, i.e., $\mathbf{x} = \{x(1), x(2), ..., x(N)\}$. $\mathbf{b_x}$ is used to denote the binary version of $\mathbf{x}$. We use $X \sim p(x)$ to indicate that a random variable X follows $p_X(x)$.

II. Identification problem formulation

We will assume that the *data owner* has M entries in the database indexed by an index m, i.e., $\mathbf{x}(m) \in \mathbb{R}^N$, $1 \leq m \leq M$, where $M = 2^{LR}$ with R to be the identification rate of (M, L)-fingerprinting code and L stands for the fingerprint length. The index m is associated to all identification information (ownership, time of creation, distribution channel, etc.) and the data $\mathbf{x}(m)$ is some privacy sensitive part of the database represented by image, video, audio, biometric, PUFs, etc. At the same time, the *data user* has a query data $\mathbf{y} \in \mathbb{R}^N$ that can be in some relationship with $\mathbf{x}(m)$ via a probabilistic model $p(\mathbf{y}|\mathbf{x})$ or can represent some irrelevant input $\mathbf{x}'$. The data user wishes to retrieve the identification information of $\mathbf{x}(m)$ that is the closest to the query $\mathbf{y}$ or reject the query, if no relevant database entry is found. For complexity and privacy reasons, the above identification is performed in the domain of digital fingerprints $\mathbf{b_x} \in \{0,1\}^L$ and $\mathbf{b_y} \in \{0,1\}^L$ that are short length, secure and robust counterparts of $\mathbf{x}$ and $\mathbf{y}$, respectively (Fig. 1). Moreover, to ensure adequate privacy protection of digital fingerprints, the data owner applies privacy amplification (PA) to produce protected version $\mathbf{b_u}(m)$ of $\mathbf{b_x}(m)$. The resulting fingerprints can be shared with third parties for various security and management services. In particular, the storage of the resulting codebook/database of protected fingerprints $\mathbf{b_u}(m)$, $1 \leq m \leq M$, and the content identification can be performed on a remote server that can be honest in terms of claimed functionalities but curious in terms of observing, analyzing or leaking the stored data. The result of identification should be an estimate of index $\hat{m}$ of the corresponding closest entry or the erasure, i.e., null hypothesis. If the query is properly identified, the corresponding encrypted content $\mathbf{x}(m)$ or associated identification information is delivered to the data user using the predefined data exchange protocol.

In the scope of this paper, we will assume that the binary fingerprints are obtained by a dimensionality reduction transform $\mathbf{W}$ and binarization Q (Fig.1). The projected vectors of lower dimensionality $\tilde{\mathbf{x}}(m) \in \mathbb{R}^L$ and $\tilde{\mathbf{y}} \in \mathbb{R}^L$ are obtained from $\mathbf{x}(m)$ and $\mathbf{y}$ based on the dimensionality reduction transform:

$$\tilde{\mathbf{x}}(m) = \mathbf{W}\mathbf{x}(m), \tag{1}$$

$$\tilde{\mathbf{y}} = \mathbf{W}\mathbf{y}, \tag{2}$$

where $\mathbf{W} \in \mathbb{R}^{L \times N}$ with $L \leq N$ 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 $1 \leq i \leq L$. The dimensionality reduction transform is based on any randomized orthogonal matrix $\mathbf{W}$ (random projection transform) whose elements $w_{i,j}$ are generated from some specified distribution. An $L \times N$ 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 $\mathbf{W}\mathbf{W}^T \approx \mathbf{I}_L$ [1]. The selection of basis vectors with a Gaussian distribution also guarantees the Gaussian distribution of the projected coefficients. This will also be true for other statistics of the projection coefficients for sufficiently large N according to the Central Limit Theorem.

The binarization is performed as:

$$b_{\mathbf{x}_i} = sign(\mathbf{w}_i^T \mathbf{x}), \tag{3}$$

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. Since all projections are independent, it can be assumed that all bits in $\mathbf{b_x}$ will be independent and equiprobable for sufficiently large L.[2]

The mismatch between the data owner fingerprint $\mathbf{b_x}$ and data user query fingerprint $\mathbf{b_y}$ can be modeled based on memoryless BSC model with a probability of bit error P_b. It was shown that $P_b = \frac{1}{\pi}\arccos(\rho_{\tilde{X}\tilde{Y}})$, where $\rho_{\tilde{X}\tilde{Y}}$ is a correlation coefficient between $\tilde{X}$ and $\tilde{Y}$ [11].

Therefore, the main issues are: (a) the accuracy of identification defined in terms of probability of false acceptance of irrelevant entries and probability of wrong estimation of queries corresponding to the existing entries; (b) the complexity of identification; (c) the memory storage of resulting fingerprints; (d) the maximum number of correctly identifiable entries under the measures defined in (a) and length of fingerprints L; (e)

[1] Otherwise, one can apply special orthogonalization techniques to ensure perfect orthogonality.

[2] This assumption is only possible for independent input data. Since the transformed vectors will closely follow the Gaussian pdf but will not necessarily be decorrelated, one can apply the principle component analysis to decorrelate them, that, for the case of Gaussian data, will also provide their independence.

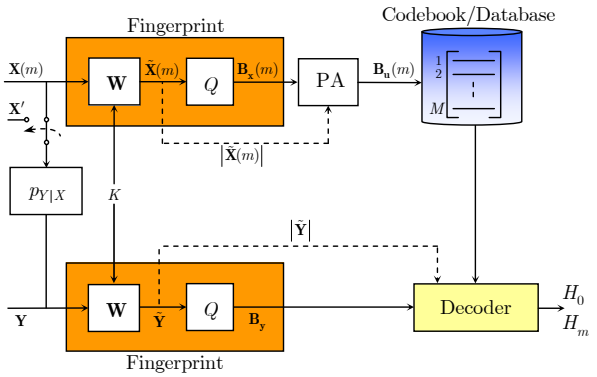

Fig. 1. Generalized block-diagram of private content identification based on digital fingerprinting.

the identification capacity under infinite L and (f) the privacy leak due to the fingerprint disclosure. [3]

In [11], we formulated the identification problem with the global privacy amplification as a composite hypothesis test:

$$\begin{cases} H_0: & p(\mathbf{b_y}|H_0) = p(\mathbf{b_y}|\mathbf{b_x}'), \\ H_m: & p(\mathbf{b_y}|H_m) = p(\mathbf{b_y}|\mathbf{b_u}(m)), m = 1, \cdots, M. \end{cases} \tag{4}$$

In the binary fingerprinting domain, the link between $\mathbf{b_x}$ and between $\mathbf{b_y}$ and $\mathbf{b_x}$ and $\mathbf{b_u}$ can be considered based on the BSC models with corresponding bit error probabilities P_b and λ. The parameter λ corresponds to the BSC serving as a test channel for the compressed version $\mathbf{b_u}$ considered as the privacy amplification [13]. Under the above assumption, these two BSCs $\mathbf{b_x} \to \mathbf{b_u}$ and $\mathbf{b_x} \to \mathbf{b_y}$ can be considered as an equivalent channel $\mathbf{b_u} \to \mathbf{b_y}$ obtained by their concatenation with the cross-probability P_{b_e} equals to the convolution $P_{b_e} = P_b * \lambda = P_b(1-\lambda) + \lambda(1-P_b)$. Under these conditions, the corresponding hypothesis (4) are:

$$\begin{cases} H_0: & p(\mathbf{b_y}|\mathbf{b_x}') = \frac{1}{2^L}, \\ H_m: & p(\mathbf{b_y}|\mathbf{b_u}(m)) = \left(\frac{P_{b_e}}{1-P_{b_e}}\right)^{d^H(\mathbf{b_y}, \mathbf{b_u}(m))} (1-P_{b_e})^L, \end{cases} \tag{5}$$

where $d^H(.,.)$ denotes the Hamming distance.

Let the decision rule based on the public version $\mathbf{b_u}$ of $\mathbf{b_x}$ corresponds to the Forney's erasure decoder [12]:

$$p(\mathbf{b_y}|\mathbf{b_u}(m)) \geq 2^{\tau L}, \tag{6}$$

where τ is the threshold. We will show that this threshold should satisfy $\tau \leq -H_2(P_{b_e})$, where $H_2(.)$ denotes the binary entropy, for the unique decoding of index m and rejection hypothesis H_0.

Under (5), the decision rule (6) can be rewritten as:

$$d^H(\mathbf{b_y}, \mathbf{b_u}(m)) \leq L\gamma, \tag{7}$$

where $\gamma = \frac{-\tau + \log_2(1-P_{b_e})}{\log_2 \frac{1-P_{b_e}}{P_{b_e}}}$. We will refer to this decision rule as the BDD that produces a unique $\hat{m}$. To minimize the overall identification error and to achieve the identification capacity that coincides with the capacity of the corresponding BSC, it was shown that the threshold should satisfy $\gamma_{\text{opt}} = \frac{1-R+\log_2(1-P_{b_e})-1/L}{\log_2\left(\frac{1-P_{b_e}}{P_{b_e}}\right)}$ [11]. The efficient implementation of identification search strategy based on the Hamming sphere-based BDD interpretation was demonstrated in the same paper along the conditions on P_{b_e} under which this search outperforms the exhaustive one.

For the case of asymptoticly large L, it was also shown that:

Proposition 1: For $P_{b_e} \leq \gamma \leq \frac{1}{2}$ and if $H_2(\gamma) \leq 1 - R$ there exist codes with rate R and error probability P_e such that:

$$\lim_{L \to \infty} P_e = 0. \tag{8}$$

As soon as γ is arbitrarily close to P_{b_e}, the rate $R = 1 - H_2(P_{b_e})$ is achievable, and it is referred to as private identification capacity:

$$C_{id} = 1 - H_2(P_{b_e}). \tag{9}$$

The privacy leak L_p about $\mathbf{B_x}$ from the public $\mathbf{B_u}$ is defined by the mutual information between them [4]:

$$L_p = I(B_{\text{u}}; B_{\text{x}}) = 1 - H_2(\lambda). \tag{10}$$

The trade-off between the identification rate and privacy leak is achieved by the selection of parameter λ. This parameter is applied to all bits disregarding their actual bit reliability shown to be equal to [11]:

$$P_{b|\tilde{x}} = Q\left(\frac{|\tilde{x}|}{\sigma_{\tilde{Z}}}\right), \tag{11}$$

which stands for the bit error probability for a given projection coefficient $\tilde{x}$ under the assumption that $p(\tilde{x}, \tilde{y})$ corresponds to jointly Gaussian distribution in the random projection domain and $\sigma_{\tilde{Z}}$ denotes a standard deviation of additive Gaussian noise in the random projection domain. [5] Such a global interpretation corresponds to the assumption that all bits pass via the same channel and there is no any side information about the probability to be randomly flipped. However, in reality such kind of information is available and in the next section we will investigate the possible benefits of its usage based on the simplified model of subchannel consideration that we will refer to as *channel splitting*.

III. Channel Splitting Model

In the first part of this section we consider theoretical limits of reliable identification with various types of side information about bit reliability without privacy amplification, i.e., $L_p = 1$, and then present the practical privacy-preserving coding schemes in the second part.

The binary fingerprinting problem in the projected domain can be represented according to *sign-magnitude decomposition*

[3] In this paper, we do not analyze the identification from partial data such as block of image or frame of video due to the straightforward extension of our results to these cases under corresponding matching conditions.

[4] A more conservative definition of privacy leak would be $I(B_{\text{u}}; X)$.

[5] The Gaussianity assumption about the statistics of projected coefficients is due to the Gaussian basis vectors of $\mathbf{W}$ and consequence of central limit theorem.

when $\tilde{x} = sign(\tilde{x})|\tilde{x}| = b_x|\tilde{x}|$, where $b_x = sign(\tilde{x})$. This decomposition makes it possible to redefine the identification channel by the equivalent model presented in Fig. 2 with $P_{b|\tilde{x}}$ defined by (11) and $\tilde{y} = \tilde{x} + \tilde{z}$, where $\tilde{z}$ represents the zero-mean Gaussian noise with the variance $\sigma^2_{\tilde{Z}}$ in the projected domain.

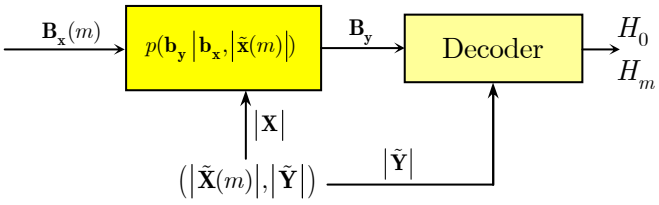

Fig. 2. Equivalent model of binary fingerprint identification based on sign-magnitude decomposition.

The magnitude component $|\tilde{x}|$ defines the bit reliability and is considered as a random parameter of the binary identification channel of interest. Depending on the availability of information about $|\tilde{x}|$ at the decoder one can distinguish 3 major cases[6]: (a) only distribution $p(\tilde{x})$ is known; (b) perfect information about realization of magnitudes $|\tilde{x}|$ and (c) noisy (imperfect) bit reliabilities given by $|\tilde{y}|$.

Remark 1: The identification rate under the absence of information about the bit reliability (traditional binary fingerprinting or blind setup) is:

$$R_{id|0} = (1 - H_2(P_b)), \tag{12}$$

where $P_b = E_{p(\tilde{x})}[P_{b|\tilde{x}}]$ is the average probability of bit error.

Remark 2: The identification rate under the perfect information about the random parameter:

$$R_{id|x} = 2\int_0^{+\infty}\left[1 - H_2\left(Q\left(\frac{\tilde{x}}{\sigma_{\tilde{Z}}}\right)\right)\right]p(\tilde{x})d\tilde{x}. \tag{13}$$

Remark 3: The identification rate under the imperfect (noisy) information about the bit reliability is:

$$R_{id|y} = 2\times$$
$$\int_0^{+\infty}\left[1 - H_2\left(\int_{-\infty}^{+\infty} Q\left(\frac{\tilde{x}+\tilde{z}}{\sigma_{\tilde{Z}}}\right)p(\tilde{z})d\tilde{z}\right)\right]p(\tilde{x})d\tilde{x}. \tag{14}$$

The identification rates under the blind, perfect and imperfect (noisy) information about the bit reliability are shown in Fig. 3. The observation model is considered in terms of the signal-to-noise ratio (SNR) defined as $SNR = 10\log_{10}\frac{\sigma^2_{\tilde{X}}}{\sigma^2_{\tilde{Z}}}$. It is important to note that the presence of perfect information about bit reliability at the decoder essentially enhances the identification rate. The noisy side information provides also certain enhancement in the region of positive SNRs with respect to the blind identification setup. However, even this enhancement is not so high in terms of achievable identification rate, the privacy gain can be still essential.

[6]We do not consider here the compressed case as in [14].

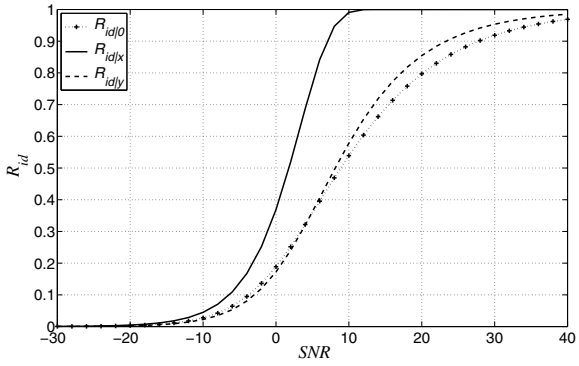

Fig. 3. Identification rates under various side informations about bit reliability.

To present practical coding schemes enabling reliability dependent privacy amplification, we introduce a *channel splitting* model. We will assume that the random projections transform produces J coefficients. Although all these coefficients can be used to produce information bits and will be considered in our theoretical analysis of binary fingerprint identification, it is assumed that only L of them form the actual fingerprint that will be used for the identification in practical schemes.

The channel splitting model assumes the encoding, storage and privacy amplification of J bits depending on their reliabilities, defined by the side information $|\tilde{x}|$, into S independent channels. Each channel contains S_j components, $1 \le j \le S$ such that $J = \sum_{j=1}^{S} S_j$, obtained based on the sorting of the reliabilities of corresponding bits as shown in Fig 4.

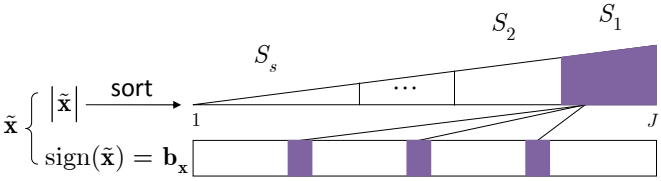

Fig. 4. Channel splitting model based on bit reliabilities.

Proposition 2 *(channel splitting):* Assume that the perfect information about bit reliabilities defined by $|\tilde{x}|$ is shared between the encoder and decoder. Then, each BSC is characterized by its own average probability of bit error P_{b_j} and corresponding achievable rates $R_j = 1 - H_2(P_{b_j})$ with the use probability to be p_j. Therefore, the overall bit error probability without any information about $|\tilde{x}|$ is defined as $P_b = \sum_{j=1}^{S} P_{b_j}p_j$ and the identification rate is given by:

$$R_{id} = \sum_{j=1}^{S}(1 - H_2(P_{b_j}))p_j, \tag{15}$$

which asymptotically approaches (14) as the number of channels increases. This model is schematically shown in Fig. 5a.

Proposition 3 *(2-channel splitting):* Assuming the perfect shared side information based on $|\tilde{x}|$ with $S = 2$ and

choosing $S_1 = L$ to be the most reliable bits representing the actual fingerprint communicated via the BSC with P_{b_G} (good channel) and stored with the amplification factor λ_G in the database, while assigning the remaining $S_2 = J-L$ bits to the second BSC with P_{b_B} (bad channel) that are also stored with the amplification factor λ_B, and denoting $P_{b_{eG}} = P_{b_G} * \lambda_G$ and $P_{b_{eB}} = P_{b_B} * \lambda_B$, the identification rate-privacy leak pair yields[7]:

$$R_{id} = \frac{1}{J}\left(L(1-H_2(P_{b_{eG}})) + (J-L)(1-H_2(P_{b_{eB}}))\right), \tag{16}$$

$$L_p = 1 - H_2(\bar{\lambda}), \tag{17}$$

with $\bar{\lambda} = \frac{1}{J}(L\lambda_G + (J-L)\lambda_B)$.

Remark 4: One possible strategy for trading-off identification rate-privacy leak consists in the constraint optimization similar to the distortion allocation in the rate-distortion theory that consists in fixing the desired L_p resulting in $\bar{\lambda}$ and maximizing R_{id} by allocating different λ_G and λ_B distortions to each channel.

Remark 5 *(practical solution):* Due to the fact that the attacker has no access to the information defining the bit reliabilities and corresponding randomization strategy one can simply randomize all $(J-L)$ bits with λ_B keeping $\lambda_G = 0$ for L good bits that yields:

$$R_{id} = \frac{L}{J}(1-H_2(P_{b_G})), \tag{18}$$

$$L_p = 1 - H_2\left(\frac{J-L}{J}\lambda_B\right). \tag{19}$$

One can also hide the positions of the reliable bits by assigning $\lambda_B = 0.5$ and leaving the attacker with the only option of guessing strategy that would require:

$$\binom{J}{L} \leq 2^{JH_2(\frac{L}{J})}, \tag{20}$$

trails which results for example for $J = 1024$ and $L = 32$ into 2^{205} trials that makes this strategy unfeasible.

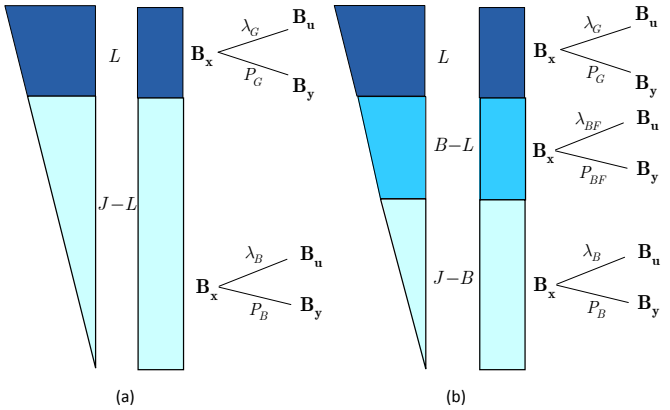

Fig. 5. Channel splitting model: (a) 2-channel splitting and (b) 3-channel splitting with buffering.

[7]We assume here that P_{b_G} and P_{b_B} include the effect of misplacement error due to the noisy $\tilde{y}$.

IV. Privacy Amplification Based on Buffering

In the previous analysis, we have assumed that the bit reliability information $|\tilde{x}|$ is shared between the encoder and decoder. This assumption was used in early techniques such as in [15], but it was shown that it is privacy revealing if the information about the positions of reliable components is available in the public domain [14] along with the proposal how to minimize this leak based on distributed coding.

Therefore, to overcome this shortcoming, in this paper we propose to extract this information directly from the noisy observations $|\tilde{y}|$ thus avoiding any additional storage in the public domain. Unfortunately, this leads to a certain inaccuracy with respect to the case of available $|\tilde{x}|$, which can be resolved based on *buffering*.

Proposition 4 *(buffering):* Assuming the encoder has access to the side information based on $|\tilde{x}|$ and the decoder to the noisy counterpart $|\tilde{y}|$, the buffering equivalent to the 3-channel splitting suggests $S = 3$ and choosing $S_1 = L$ to be the most reliable bits representing the actual fingerprint communicated via the BSC with P_{b_G} (good channel) and stored with the factor λ_G in the database, $S_2 = B - L$ to be the buffer with B bits assigned to the buffer and reliable components; the buffer bits are communicated via the BSC with $P_{b_{BF}}$ (buffer channel) and stored with the factor λ_{BF} in the database, while assigning the remaining $S_3 = J - B$ bits to the third BSC with P_{b_B} (bad channel) that are also stored with the factor λ_B, and denoting $P_{b_{eG}} = P_{b_G} * \lambda_G$, $P_{b_{eBF}} = P_{b_{BF}} * \lambda_{BF}$ and $P_{b_{eB}} = P_{b_B} * \lambda_B$, the identification rate-privacy leak pair yields:

$$\begin{aligned} R_{id} &= \tfrac{1}{J}(L(1-H_2(P_{b_{eG}})) + (B-L)(1-H_2(P_{b_{eBF}})) \\ &\quad +(J-B)(1-H_2(P_{b_{eB}}))), \\ L_p &= 1 - H_2(\bar{\lambda}), \end{aligned} \tag{21}$$

with $\bar{\lambda} = \frac{1}{J}(L\lambda_G + (B-L)\lambda_{BF} + (J-L)\lambda_B)$. This model is schematically shown in Fig. 5,b.

Remark 6: One practical strategy to the selection of privacy parameters consists in selection $\lambda_G = \lambda_{BF} = 0$ and $\lambda_B = 0.5$ that yields[8]:

$$R_{id} = \frac{1}{J}(L(1-H_2(P_{b_{bG}})) + (B-L)(1-H_2(P_{b_{BF}}))), \tag{22}$$

$$L_p = 1 - H_2\left(\frac{J-L}{J}\lambda_B\right). \tag{23}$$

The fast identification based on reliable bits and the maximum likelihood counterpart of the BDD was presented in our previous work [16]. The reliable bits are selected from the noisy observation and the BDD decoding is performed only based on these bits.

V. Results of Computer Simulation

In this section, we present the results of computer simulations for the considered identification rate-privacy leak

[8]The selection of $\lambda_B = 0.5$ aims at protecting all bits of fingerprint that are the least reliable and not used for the further identification but whose positions are very important for the correct identification.

formulation under the Gaussian observation and binarized setup. All results are obtained for 10000 noise realizations and 100 input vectors.

To demonstrate the relationship between different considered privacy preserving strategies, we have selected SNR $= 10$ dB that corresponds to $P_b = 0.1$ and performed the simulation for the cases of traditional non-adaptive privacy amplification (9)-(10), 2-channel splitting model (18) with the perfect side information shared between the encoder and decoder and mismatched side information about bit reliabilities, 3-channel model (22) based on the mismatched side information and buffer lengths of $B = 128$ and $B = 256$. The results of modeling are shown in Fig. 6. The presence of side information

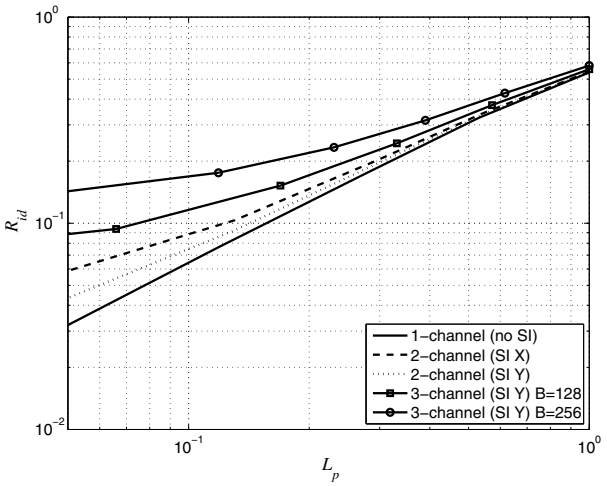

Fig. 6. Identification rate-privacy leak trade-off for $J = 1024$ and $L = 32$ with $P_b = 0.1$ for different channel splitting models: no splitting (1-channel model), 2-channel splitting and different side information and 3-channel splitting based on buffering.

clearly enhances the identification rate-privacy trade-off for all cases. The impact of side information mismatch in a simple 2-channel splitting model degrades the performance with respect to the perfect side information in the region of small privacy-leak rates. The increase of the amount of channels in the 3-channel splitting model leads to better approximation of real channel model (14). The results obtained even for the imperfect side information clearly indicate the increase in performance that is especially important for the region of small privacy leak rates.

VI. Conclusions

We considered the privacy amplification mechanism based on the bit reliability. Several techniques are analyzed for the case of perfect and imperfect side information shared between the encoder and decoder. In particular, we established that one can achieve considerable privacy amplification using even imperfect side information without the identification rate loss. We demonstrated that the privacy amplification can be solved without any publicly stored information about reliable bits contrary to the state-of-the-art methods. The next stage of our study will be dedicated to the solution of optimal amplification parameter allocation based on the constraint optimization problem.

Acknowledgment

This work is supported by SNF projects 121635 and 1119770.

References

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

[2] J. Haitsma, T. Kalker, and J. Oostveen, "Robust audio hashing for content identification," in *International Workshop on Content-Based Multimedia Indexing*, Brescia, Italy, September 2001, pp. 117–125.

[3] F. Lefebvre and B. Macq, "Rash : RAdon Soft Hash algorithm," in *Proceedings of EUSIPCO - European Signal Processing Conference*, Toulouse, France, 2002.

[4] F. Willems, T. Kalker, J. Goseling, and J.-P. Linnartz, "On the capacity of a biometrical identification system," in *Proc. 2003 IEEE Int. Symp. Inform. Theory*, Yokohama, Japan, June 29 - July 4 2003, p. 82.

[5] M. Westover and J. O'Sullivan, "Achievable rates for pattern recognition," *EEE Trans. Information Theory*, vol. 54, no. 1, pp. 299–320, 2008.

[6] E. Tuncel, P. Koulgi, and K. Rose, "Rate-distortion approach to databases: Storage and content-based retrieval," *EEE Trans. Information Theory*, vol. 50, no. 6, pp. 953–967, 2004.

[7] S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Robust perceptual hashing as classification problem: decision-theoretic and practical considerations," in *Proceedings of the IEEE 2007 International Workshop on Multimedia Signal Processing*, Chania, Crete, Greece, October 1–3 2007.

[8] A. L. Varna, A. Swaminathan, and M. Wu, "A decision theoretic framework for analyzing hash-based content identification systems," in *ACM Digital Rights Management Workshop*, Oct. 2008, pp. 67–76.

[9] E. Martinian, S. Yekhanin, and J. Yedidia, "Secure biometrics via syndromes," in *43rd Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, USA, October 2005.

[10] 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.

[11] S. Voloshynovskiy, O. Koval, F. Beekhof, F. Farhadzadeh, and T. Holotyak, "Information-theoretical analysis of private content identification," in *IEEE Information Theory Workshop, ITW2010*, Dublin, Ireland, Aug.30-Sep.3 2010.

[12] G. D. Forney, "Exponential error bounds for erasure, list, and decision feedback schemes," *IEEE Trans. Inf. Theory*, vol. 14, pp. 206–220, March 1968.

[13] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[14] S. Voloshynovskiy, O. Koval, T. Holotyak, and F. Beekhof, "Privacy enhancement of common randomness based authentication: key rate maximized case," in *Proceedings of IEEE International Workshop on Information Forensics and Security*, London, UK, December 6–9 2009.

[15] 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.

[16] T. Holotyak, S. Voloshynovskiy, F. Beekhof, and O. Koval, "Fast identification of highly distorted images," in *Proceedings of SPIE Photonics West, Electronic Imaging 2010 / Media Forensics and Security XII*, San Jose, USA, January 21–24 2010.