Odyssey 2018 The Speaker and Language Recognition Workshop
26-29 June 2018, Les Sables d'Olonne, France

Homomorphic Encryption for Speaker Recognition: Protection of Biometric Templates and Vendor Model Parameters

Andreas Nautsch, Sergey Isadskiy, Jascha Kolberg, Marta Gomez-Barrero, Christoph Busch

da/sec – Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany

{andreas.nautsch,sergey.isadskiy,jascha.kolberg}@h-da.de
{marta.gomez-barrero,christoph.busch}@h-da.de

Abstract

Data privacy is crucial when dealing with biometric data. Accounting for the latest European data privacy regulation and payment service directive, biometric template protection is essential for any commercial application. Ensuring *unlinkability* across biometric service operators, *irreversibility* of leaked encrypted templates, and *renewability* of e.g., voice models following the i-vector paradigm, biometric voice-based systems are prepared for the latest EU data privacy legislation. Employing Paillier cryptosystems, Euclidean and cosine comparators are known to ensure data privacy demands, without loss of discrimination nor calibration performance. Bridging gaps from template protection to speaker recognition, two architectures are proposed for the two-covariance comparator, serving as a generative model in this study. The first architecture preserves privacy of biometric data capture subjects. In the second architecture, model parameters of the comparator are encrypted as well, such that biometric service providers can supply the same comparison modules employing different key pairs to multiple biometric service operators. An experimental proof-of-concept and complexity analysis is carried out on the data from the 2013 – 2014 NIST i-vector machine learning challenge.

1. Introduction

The latest EU data privacy regulation [1] declares biometric information as *personal data*, i.e. highly sensitive and entitled to the right of privacy preservation. Similarly, the current payment service directive [2] also requires biometric template protection to be employed in biometric systems utilized for banking services. To that end, the ISO/IEC IS 24745 [3] on biometric information protection provides guidance on how to preserve the subject's privacy by defining the following three main properties to be fulfilled by protected biometric templates:

- *unlinkability*: stored biometric templates shall not be linkable across applications or databases,
- *irreversibility*: biometric samples cannot be reconstructed from protected biometric templates,
- *renewability*: multiple biometric references can be independently transformed, when they are created from one or more samples of a biometric data capture subject.

In addition to these properties, other performance metrics, such as recognition accuracy, should be preserved.

Even if some works argue that there is no need for template protection depending on the feature extraction [4], sensitive information can be derived from unprotected templates, as it has already been proved for other biometric characteristics [5, 6]. In particular, linkability of state-of-the-art speaker recognition features is demonstrated in [7] with the motivation of interchanging features among different voice biometric services. The interchange of biometric data across services is recently addressed ethically in [8], especially when targeting forensic and investigatory scenarios. Accounting for latest data privacy legislations, we motivate template protection, especially in commercial but also in other dual-use case application scenarios.

Current approaches to biometric template protection can be broadly classified into three categories [9], namely: i) cancelable biometrics [10], where irreversible transformations are applied at sample or template level; ii) cryptobiometric systems [11], where a key is either bound or extracted from the biometric data; and iii) biometrics in the encrypted domain [12], where techniques based on homomorphic encryption (HE) and garbled circuits are used to protect the data. Whereas cancelable biometrics and cryptobiometric systems usually report some accuracy degradation [9], the use of HE schemes prevents such loss, since the operations carried out in the encrypted domain are equivalent to those performed with plaintext data. For this reason, we apply in this work HE schemes similar to the ones proposed in [13, 14, 15, 16] to speaker recognition relying on generative comparators, such as probabilistic linear discriminant analysis (PLDA). We thereby ensure data privacy for data capture subjects for comparison models utilizing the two-covariance (2Cov) approach [17, 18] (i.e. full subspace PLDA) as a prototype generative comparison algorithm.

Comparison scores of generative and discriminative models can be probabilistic. In contrast to discriminative comparators, generative models can emit features with associated likelihoods based on pre-trained models, and thus estimate probabilistic similarity. The parameters of pre-trained models deserve protection by the biometric service vendors, who distribute these sensitive parameters to various biometric service operators. We further propose a mutual encryption scheme granting subject and vendor data privacy by employing well-established Paillier homomorphic cryptosystems [19, 20], blindfolding operators. Worth noting, while conventional image based biometric systems employ comparators operating either on binary or non-negative integers [15, 16, 21, 22], the generative comparators used in speaker recognition applications make assumptions on underlying distributions, such as normal distribution [23, 24], consequently operating on normal distributed float values.

In the following, we make HE available to speaker recognition, targeting data privacy for subjects and vendors. Secs. 2, 3, 4 depict related work on homomorphic cryptosystems and speaker recognition. Sec. 5 proposes two architectures for HE protected 2Cov comparators. A proof-of-concept study is discussed in Sec. 6 with conclusions drawn in Sec. 7.

10.21437/Odyssey.2018-3

2. Related Work

In order to apply standardized biometric template protection schemes, binarization can be employed [3]. Related work on the binarization of traditional speaker recognition systems utilizing universal background models (UBMs) targeting the GMM–UBM approach can be found in [25, 26, 27]. In addition, in our earlier work [28], we proposed a biometric template protection scheme for speaker recognition, based on binarized Gaussian mixture model (GMM) supervectors.

However, due to the binarization process, the biometric performance usually declines, and calibration properties are lost. Contrary to performance-lossy template protection approaches as biometric cryptosystems and cancelable biometrics [9], HE completely preserves biometric accuracy. Therefore, we investigate on Paillier HE schemes, which are already introduced to other biometric modalities, such as signature [13], iris [21], and fingerprint [22] recognition, considering Hamming distances (XOR operator), dynamic time warping (DTW), the Euclidean distance, and the cosine similarity. We thus focus on homomorphic cryptosystems for the remainder of the article.

In [29] and [30], the authors provide an overview of several biometric template protection schemes based on homomorphic encryption and garbled circuits. Barni et al. [22] present a way to protect fixed-length fingercodes [31] using homomorphic encryption. This system was modified in [32] to accelerate the process by reducing the size of the fingercode. However, a reduction of information also leads to a degradation of biometric recognition performance. Ye et al. present an anonymous biometric access control (ABAC) system [33] for iris recognition. Their system setup verifies only whether a subject is enrolled without revealing the identity and thus grants anonymity towards the subjects. Another ABAC protocol is proposed in [34] by Luo et al. and a secure similarity search algorithm is presented for anonymous authentication. Combining homomorphic encryption with garbled circuits, Blanton and Gasti [35] implement secure protocols for iris and fingerprint recognition.

Among the existing cryptosystems in the literature, encryption algorithms based on lattices are assumed to be post-quantum secure [36, conjecture 2], which is a convenient property for a public key encryption scheme. Using ideal lattices in a somewhat homomorphic encryption (SHE) scheme, Yasuda et al. [37] compute the Hamming distance of encrypted templates in an efficient way by using a packing method before the encryption. By using binary feature vectors with a constant size of $2\,048\,\mathrm{bits}$ for every biometric data, again Yasuda et al. [38] present a new packing method in a SHE scheme for biometric authentication based on a special version of the ring learning with errors assumption. Another privacy-preserving biometric authentication approach [39] splits a $2\,048\,\mathrm{bits}$ iris code into 64 blocks with $32\,\mathrm{bits}$ each and encrypts these blocks using n-th degree truncated polynomial ring (NTRU). As in the aforementioned works, scores are computed in the encrypted domain without disclosure of biometric information.

3. Homomorphic Cryptosystems

Homomorphic encryption [40, 41, 42] has the property that computations on the ciphertext are equivalent to those carried out on the plaintext. In particular, homomorphisms are functions which preserve algebraic structures of groups [43]. The function $f : G \to H$ is a homomorphism for groups $(G, \diamond), (H, \square)$ with sets G, H and operators $\diamond, \square$ if:

$$f(g \diamond g') = f(g) \square f(g') \qquad \forall g, g' \in G. \tag{1}$$

Public-key cryptosystems $(K, M, C, \mathrm{enc}, \mathrm{dec})$ with sets of keys K, plaintexts M, ciphertexts C, and functions representing encryption enc and decryption dec are homomorphic if:

$$\begin{aligned} &\forall m_1, m_2 \in M, \forall pk \in K : \\ &\mathrm{enc}_{pk}(m_1) \square \mathrm{enc}_{pk}(m_2) = \mathrm{enc}_{pk}(m_1 \diamond m_2), \end{aligned} \tag{2}$$

where the public key *pk* is used for encryption and the secret key *sk* for the decryption functions, respectively:

$$\begin{aligned} \mathrm{enc}_{pk} &: M \to C, \\ \mathrm{dec}_{sk} &: C \to M. \end{aligned} \tag{3}$$

3.1. Paillier HE Scheme

Motivated by asymmetric Paillier cryptosystems [19, 20], HE has been made available to biometric template protection [13, 15, 16]. Paillier cryptosystems are homomorphic probabilistic encryption schemes based on the decisional composite residuosity assumption (DCRA): for integers n, z it is hard to decide, whether z is an n-residue modulo n^2. Due to this assumption, the Paillier cryptosystem is secure against *honest but curious users* conducting chosen ciphertext attacks [19, 44, 45].

In the Paillier cryptosystem, the public key $pk = (n, g)$ is defined by $n = p\,q$ and $g \in \mathbb{Z}^*_{n^2}$, where p, q are two large prime numbers, such that $\gcd(p\,q, (p-1)\,(q-1)) = 1$, and with $\mathbb{Z}^*_{n^2}$ as the set of module n^2 integers having a modular multiplicative inverse. The modular multiplicative inverse $\overline{\varrho}$ to ϱ is required with $\gcd(\varrho, \overline{\varrho}) = 1$: $\varrho\,\overline{\varrho} \equiv 1 \pmod{n^2}$. Based on p, q, the secret key $sk = (\lambda, \mu)$ is defined by $\lambda = \mathrm{lcm}(p-1, q-1)$ and $\mu = \overline{\varrho} \mod n$ with $\varrho = L(g^\lambda \mod n^2)$ and $L(x) = \frac{x-1}{n}$.

During encryption $c = \mathrm{enc}_{pk}(m, s) \in \mathbb{Z}^*_{n^2}$ of a message $m \in \mathbb{Z}_n$ with public key *pk*, a random number $s \in \mathbb{Z}^*_n$ provides the probabilistic nature of the cryptosystem, i.e. $\mathrm{enc}_{pk}(m, s_1) \neq \mathrm{enc}_{pk}(m, s_2)$ for two different $s_1, s_2 \in \mathbb{Z}^*_n$:

$$c = \mathrm{enc}_{pk}(m, s) = g^m\, s^n \mod n^2, \tag{4}$$

which is abbreviated in the following as $\mathrm{enc}_{pk}(m)$.

Ciphertexts are decrypted as:

$$m = \mathrm{dec}_{sk}(c) = L\left(c^\lambda \mod n^2\right) \mu \mod n. \tag{5}$$

Similarly to [13, 15, 16, 20], we utilize the additive homomorphic properties of the Paillier cryptosystem regarding plaintexts m_1, m_2 and corresponding ciphertexts c_1, c_2:

$$\begin{aligned} &\mathrm{dec}_{sk}\,(c_1\, c_2) = m_1 + m_2 \mod n, \\ &\mathrm{dec}_{sk}\left({c_1}^l\right) = m_1\, l \mod n, \text{ with a constant } l. \end{aligned} \tag{6}$$

In other words, whereas the decrypted product of two ciphertexts is equivalent to the sum of two plaintexts, the corresponding exponentiation of a ciphertext results in the product of the corresponding plaintext and constant as exponent.

3.2. Homomorphic Template Protection

Targeting biometric template protection, data privacy friendly comparison schemes are sought, in which only encrypted references, i.e. no plaintexts, are stored in databases. As such, the Euclidean and cosine similarity comparison scores S_{Euc}, S_{cos} between two F-dimensional vectors $\boldsymbol{X} = \{x_1, \ldots, x_F\}, \boldsymbol{Y} = \{y_1, \ldots, y_F\}$ are computationally derived as [13, 15, 16]:

$$S_{Euc}\,(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{f=1}^{F} x_f^2 + \sum_{f=1}^{F} y_f^2 - 2 \sum_{f=1}^{F} x_f\, y_f, \tag{7}$$

and the corresponding encrypted score $\mathrm{enc}_{pk}\left(S_{Euc}\left(\boldsymbol{X},\boldsymbol{Y}\right)\right)$:

$$\mathrm{enc}_{pk}\left(S_{Euc}\left(\boldsymbol{X},\boldsymbol{Y}\right)\right) = \mathrm{enc}_{pk}\left(\sum_{f=1}^{F} x_f^2\right) \mathrm{enc}_{pk}\left(\sum_{f=1}^{F} y_f^2\right) \prod_{f=1}^{F} \mathrm{enc}_{pk}\left(y_f\right)^{-2\,x_f}, \tag{8}$$

where the protected reference $\boldsymbol{Y}_{Euc}^{\mathrm{enc}_{pk}}$ is defined as:

$$\boldsymbol{Y}_{Euc}^{\mathrm{enc}_{pk}} = \left(\mathrm{enc}_{pk}\left(\sum_{f=1}^{F} y_f^2\right), \left(\mathrm{enc}_{pk}\left(y_f\right)\right)_{f=1}^{F}\right). \tag{9}$$

On the other hand, the cosine comparison is derived as [13, 15]:

$$S_{cos}\left(\boldsymbol{X},\boldsymbol{Y}\right) = \frac{\boldsymbol{X}'\,\boldsymbol{Y}}{\|\boldsymbol{X}\|\,\|\boldsymbol{Y}\|} = \sum_{f=1}^{F} \frac{x_f}{\|\boldsymbol{X}\|}\,\frac{y_f}{\|\boldsymbol{Y}\|},$$

$$\mathrm{enc}_{pk}\left(S_{cos}\left(\boldsymbol{X},\boldsymbol{Y}\right)\right) = \prod_{f=1}^{F} \mathrm{enc}_{pk}\left(\frac{y_f}{\|\boldsymbol{Y}\|}\right)^{\frac{x_f}{\|\boldsymbol{X}\|}}, \tag{10}$$

where the protected reference $\boldsymbol{Y}_{cos}^{\mathrm{enc}_{pk}}$ is defined for length-normalized features as:

$$\boldsymbol{Y}_{cos}^{\mathrm{enc}_{pk}} = \left(\left(\mathrm{enc}_{pk}\left(y_f\right)\right)_{f=1}^{F}\right) = \mathrm{enc}_{pk}(\boldsymbol{Y}). \tag{11}$$

In [13, 15], solely positive integers are considered. Accommodating a broader range of only positive float values, a 10^{12} scaling factor is employed. Accounting for negative float values, this study relies on an alternative float representation.

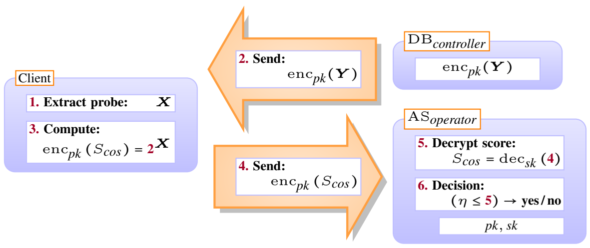

Figure 1: Architecture of homomorphic encrypted cosine similarity comparison for length-normalized features, cf. [13], with client, servers (blue) and communication channels (orange).

Fig. 1 illustrates a distributed client – server architecture employing HE with a cosine comparison: a client C extracts the probe feature vector $\boldsymbol{X}$ and requests the encrypted reference feature vector $enc_{pk}(\boldsymbol{Y})$ from the database $\mathrm{DB}_{controller}$. Then, scores are calculated on the client, and sent to the authentication server $\mathrm{AS}_{operator}$, which holds the key pair (pk, sk). Based on pre-defined threshold, $\mathrm{AS}_{operator}$ outputs the decision D of whether the decrypted score S_{cos} is greater or equal to a threshold η, or not. Ideally, $\mathrm{DB}_{controller}$ is in the domain of an independent data controller, restricting access to operators among others. Tab. 1 provides an overview to the complexity of the encrypted Euclidean and cosine comparison, where numbers diverge from [13] as in the signature recognition scenario, five reference templates are encrypted rather than e.g., an averaged template model. As references are encrypted during enrolment, cosine-based biometric comparisons require no additional encryptions, whereas in Euclidean-based comparisons, the probe templates need to be encrypted.

Table 1: Complexity analysis for the Euclidean and cosine comparators during verification, cf. [13], assuming $F = 250$ dimensional features, the size of an encrypted feature $\nu = 0.5\,\mathrm{KiB}$, and the plain feature size $p = 64$ bits.

	Euclidean	Cosine
N° encryptions	F	0
N° decryptions	1	1
N° additions	$F-1$	0
N° products	$2\,F+4$	$F-1$
N° exponentiations	$2\,F$	F
Plain template size	$p\,F$ $\approx 2.0\,\mathrm{KiB}$	$p\,F$ $\approx 2.0\,\mathrm{KiB}$
Protected template size	$\nu\,(F+1)$ $= 125.5\,\mathrm{KiB}$	$\nu\,F$ $= 125.0\,\mathrm{KiB}$
Channels: amount of protected data exchanged	$\nu\,(F+2)$ $= 126.0\,\mathrm{KiB}$	$\nu\,(F+1)$ $= 125.5\,\mathrm{KiB}$

4. Speaker Recognition: 2Cov Comparator

Recent speaker recognition approaches rely on intermediate-sized vectors (i-vectors), representing the characteristic speaker offset from an UBM, which models the distribution of acoustic features, such as Mel-Frequency Cepstral Coefficients (MFCCs) [46]. UBM components' mean vectors are concatenated to a *supervector* $\boldsymbol{\mu}_{\mathrm{UBM}}$. Seeking non-sparse features, session supervectors $\boldsymbol{s}$ are decomposed by a total variability matrix $\mathbf{T}$ into a lower-dimensional and higher-discriminant i-vectors $\boldsymbol{i}$ as an offset to the UBM supervector $\boldsymbol{\mu}_{\mathrm{UBM}}$:

$$\boldsymbol{s} = \boldsymbol{\mu}_{\mathrm{UBM}} + \boldsymbol{T}\,\boldsymbol{i}. \tag{12}$$

The total variability matrix is trained on a development set using an expectation maximization algorithm [23, 24]. Then, i-vectors are projected onto a unit-spherical space by whitening transform and length-normalization [47, 48].

State-of-the-art i-vector comparators belong to the PLDA family [18, 48]. PLDA comparators conduct a likelihood ratio scoring comparing the probabilities of the hypotheses that reference and probe i-vectors $\boldsymbol{X}, \boldsymbol{Y}$ stem from (a) the same source or (b) different sources. Therefore, within and between speaker variabilities are examined in a latent feature subspace. In this work, emphasis is put on the 2Cov approach [17, 18], the full-subspace Gaussian PLDA. Notably, the 2Cov comparator can also be related to pairwise support vector machines [17, 18]. For the sake of tractability, this study focuses on the generative 2Cov model. Also, i-vectors are solely considered as point estimates, assuming ideal precision during feature extraction. The closed-form solution to the 2Cov scoring is denoted regarding within and between covariances $\boldsymbol{W}^{-1}, \boldsymbol{B}^{-1}$ with mean $\boldsymbol{\mu}$ [17]:

$$\begin{aligned}
S_{2Cov}\left(\boldsymbol{X},\boldsymbol{Y}\right) &= \boldsymbol{X}'\,\boldsymbol{\Lambda}\,\boldsymbol{Y} + \boldsymbol{Y}'\,\boldsymbol{\Lambda}\,\boldsymbol{X} + \boldsymbol{X}'\,\boldsymbol{\Gamma}\,\boldsymbol{X} + \\
&\quad \boldsymbol{Y}'\,\boldsymbol{\Gamma}\,\boldsymbol{Y} + \boldsymbol{c}'\left(\boldsymbol{X}+\boldsymbol{Y}\right) + k, \\
\boldsymbol{\Lambda} &= \frac{1}{2}\boldsymbol{W}'\,\tilde{\boldsymbol{\Lambda}}\,\boldsymbol{W}, \qquad \boldsymbol{\Gamma} = \frac{1}{2}\boldsymbol{W}'\left(\tilde{\boldsymbol{\Lambda}} - \tilde{\boldsymbol{\Gamma}}\right)\boldsymbol{W}, \\
\boldsymbol{c} &= \boldsymbol{W}'\left(\tilde{\boldsymbol{\Lambda}} - \tilde{\boldsymbol{\Gamma}}\right)\boldsymbol{B}\,\boldsymbol{\mu}, \\
k &= \tilde{k} + \frac{1}{2}\left(\left(\boldsymbol{B}\,\boldsymbol{\mu}\right)'\left(\tilde{\boldsymbol{\Lambda}} - 2\,\tilde{\boldsymbol{\Gamma}}\right)\boldsymbol{B}\,\boldsymbol{\mu}\right), \\
\tilde{\boldsymbol{\Lambda}} &= \left(\boldsymbol{B} + 2\,\boldsymbol{W}\right)^{-1}, \quad \tilde{\boldsymbol{\Gamma}} = \left(\boldsymbol{B} + \boldsymbol{W}\right)^{-1}, \\
\tilde{k} &= 2\,\log|\tilde{\boldsymbol{\Gamma}}| - \log|\tilde{\boldsymbol{\Lambda}}| - \log|\boldsymbol{B}| + \boldsymbol{\mu}'\,\boldsymbol{B}\,\boldsymbol{\mu}.
\end{aligned} \tag{13}$$

5. Proposed Architecture

In the following, two discriminative HE schemes are proposed. The first puts emphasis on HE for i-vectors during 2Cov comparison, seeking data privacy for end-users, whereas the second scheme focuses on the encryption of i-vectors as well as 2Cov model parameters, targeting data protection for subjects and vendors. An auxiliary float representation is implemented, encoding float values as nonnegative integers for the purpose of providing Paillier properties, cf. Eq. (6).

5.1. Auxiliary Float Representation: nonnegative Integers

For the purpose of representing float values of i-vectors as nonnegative integer values, i.e. seeking conformance to Paillier cryptosystems, the integer encoding scheme standardized in IEEE 754 is employed [49]. Floats are encoded in terms of a sign S, a mantissa M times a base $B = 16$ raised to an exponent E. Nonnegative integers are derived by seeking congruent positive representations in modulo n^2, i.e. regarding the public key domain. Accounting for negative values [50], the plaintext integer domain is divided into four intervals: $[0, \frac{n}{3})$ for positive float representations, $[\frac{2n}{3}, n)$ for negative float representations, and $[\frac{n}{3}, \frac{2n}{3})$ as well as $[n, \infty)$ for the purpose of detecting overflows resulting from previous Paillier HE operations. Targeting Paillier HE, same exponents of m_1, m_2 are required, hence the mantissa is encrypted as a nonnegative integer representation. The plaintext exponent of the depending mantissa encoding is kept auxiliary. Security is satisfied due to the DCRA employing randomized mantissa obfuscation during encryption. In Paillier addition, encrypted mantissae are scaled for equivalent addend exponents. In Paillier multiplication, modular exponentiation of $c = \text{enc}_{pk}(M, s)$ is conducted, during which mantissae are kept rather small by iterative multiplications than by right-away exponentiation.

5.2. Data Privacy: Protecting Subjects

For the sake of tractability, we assume a zero mean, causing $\boldsymbol{c} = \mathbf{0}$, and neglect the normalization term, i.e. $k = 0$, such that the following scheme solely holds for discriminative 2Cov, however calibrated scores can be easily achieved by adding the k term after score decryption:

$$
\begin{aligned}
S_{2Cov}\left(\boldsymbol{X}, \boldsymbol{Y}\right) &= \boldsymbol{X}'\,\boldsymbol{\Lambda}\,\boldsymbol{Y} + \boldsymbol{Y}'\,\boldsymbol{\Lambda}\,\boldsymbol{X} + \boldsymbol{X}'\,\boldsymbol{\Gamma}\,\boldsymbol{X} + \boldsymbol{Y}'\,\boldsymbol{\Gamma}\,\boldsymbol{Y}, \\
&= \left(\boldsymbol{X}'\,\boldsymbol{\Lambda}\right)\,\boldsymbol{Y} + \boldsymbol{Y}'\,\left(\boldsymbol{\Lambda}\,\boldsymbol{X}\right) + \\
&\quad \boldsymbol{X}'\,\boldsymbol{\Gamma}\,\boldsymbol{X} + \boldsymbol{Y}'\,\boldsymbol{\Gamma}\,\boldsymbol{Y}.
\end{aligned} \tag{14}
$$

For the discriminative 2Cov, HE is employed motivated by the (symmetric) dot product for vector multiplication:

$$
\begin{aligned}
\text{enc}_{pk}(\boldsymbol{Y})^{\boldsymbol{X}} &= \prod_{f=1}^{F} \text{enc}_{pk}(y_f)^{x_f} = \text{enc}_{pk}(\boldsymbol{X}'\,\boldsymbol{Y}) \\
&= \text{enc}_{pk}(\boldsymbol{Y}'\,\boldsymbol{X}) = \prod_{f=1}^{F} \text{enc}_{pk}(x_f)^{y_f} = \text{enc}_{pk}(\boldsymbol{X})^{\boldsymbol{Y}}, \\
\text{enc}_{pk}\left(S_{2Cov}\left(\boldsymbol{X}, \boldsymbol{Y}\right)\right) &= \text{enc}_{pk}(\boldsymbol{Y})^{(\boldsymbol{X}'\,\boldsymbol{\Lambda})}\ \text{enc}_{pk}(\boldsymbol{Y})^{(\boldsymbol{\Lambda}\,\boldsymbol{X})} \\
&\quad \text{enc}_{pk}(\boldsymbol{X}'\,\boldsymbol{\Gamma}\,\boldsymbol{X})\ \text{enc}_{pk}(\boldsymbol{Y}'\,\boldsymbol{\Gamma}\,\boldsymbol{Y}), \\
\text{enc}_{pk}(\boldsymbol{Y}) &= \left(\text{enc}_{pk}(y_f)\right)_{f=1}^{F},
\end{aligned} \tag{15}
$$

with auxiliary vectors are denoted as $(\boldsymbol{X}'\,\boldsymbol{\Lambda})$, $(\boldsymbol{\Lambda}\,\boldsymbol{X})$, and the protected reference $\boldsymbol{Y}_{2Cov}^{\text{enc}_{pk}} = \left(\text{enc}_{pk}(\boldsymbol{Y}), \text{enc}_{pk}(\boldsymbol{Y}'\,\boldsymbol{\Gamma}\,\boldsymbol{Y})\right)$.

Fig. 2 illustrates the proposed HE architecture for a distributed system. Similarly to the cosine comparison HE approach, the scores are computed in the encrypted domain on the client, and decrypted on the authentication server. Thereby, the 2Cov score is computed in four parts.

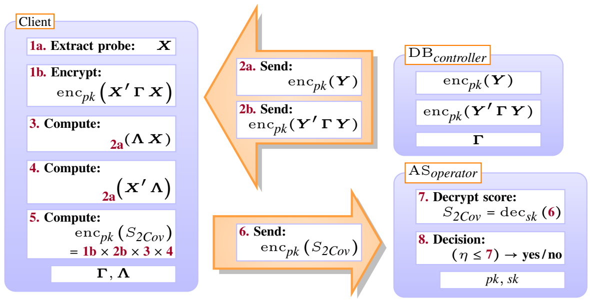

Figure 2: Architecture of homomorphic encrypted 2Cov comparison solely protecting subject data, with client, servers (blue) and communication channels (orange).

5.3. Data Privacy: Protecting Subjects and Vendors

Contrary to established biometric HE approaches employing non-generative comparators, generative comparators require trained hyper-parameters e.g., between and within covariance matrices in terms of the 2Cov comparator. For the purpose of protecting both subject and vendor data, two key sets are employed $(pk1, sk1), (pk2, sk2)$. Utilizing the Frobenius inner product [1], Eq. (13) can be reformulated [17]:

$$
\begin{aligned}
S_{2Cov}\left(\boldsymbol{X}, \boldsymbol{Y}\right) &= \langle \boldsymbol{\Lambda}, \boldsymbol{X}\,\boldsymbol{Y}' + \boldsymbol{Y}\,\boldsymbol{X}' \rangle + \langle \boldsymbol{\Gamma}, \boldsymbol{X}\,\boldsymbol{X}' + \boldsymbol{Y}\,\boldsymbol{Y}' \rangle + \\
&\quad \boldsymbol{c}'\ \left(\boldsymbol{X} + \boldsymbol{Y}\right) + k, \\
&= \boldsymbol{w}_{\boldsymbol{\Lambda}}'\,\varphi_{\boldsymbol{\Lambda}}(\boldsymbol{X}, \boldsymbol{Y}) + \boldsymbol{w}_{\boldsymbol{\Gamma}}'\,\varphi_{\boldsymbol{\Gamma}}(\boldsymbol{X}, \boldsymbol{Y}) + \\
&\quad \boldsymbol{w}_{\boldsymbol{c}}'\,\varphi_{\boldsymbol{c}}(\boldsymbol{X}, \boldsymbol{Y}) + \boldsymbol{w}_k'\,\varphi_k(\boldsymbol{X}, \boldsymbol{Y}), \\
&= \boldsymbol{w}'\,\varphi(\boldsymbol{X}, \boldsymbol{Y}),\ \textit{with:} \\
\varphi(\boldsymbol{X}, \boldsymbol{Y}) &= \begin{bmatrix} \text{vec}(\boldsymbol{X}\,\boldsymbol{Y}' + \boldsymbol{Y}\,\boldsymbol{X}') \\ \text{vec}(\boldsymbol{X}\,\boldsymbol{X}' + \boldsymbol{Y}\,\boldsymbol{Y}') \\ \boldsymbol{X} + \boldsymbol{Y} \\ 1 \end{bmatrix} = \begin{bmatrix} \varphi_{\boldsymbol{\Lambda}}(\boldsymbol{X}, \boldsymbol{Y}) \\ \varphi_{\boldsymbol{\Gamma}}(\boldsymbol{X}, \boldsymbol{Y}) \\ \varphi_{\boldsymbol{c}}(\boldsymbol{X}, \boldsymbol{Y}) \\ \varphi_k(\boldsymbol{X}, \boldsymbol{Y}) \end{bmatrix}, \\
\boldsymbol{w} &= \begin{bmatrix} \text{vec}(\boldsymbol{\Lambda}) \\ \text{vec}(\boldsymbol{\Gamma}) \\ \boldsymbol{c} \\ k \end{bmatrix} = \begin{bmatrix} \boldsymbol{w}_{\boldsymbol{\Lambda}} \\ \boldsymbol{w}_{\boldsymbol{\Gamma}} \\ \boldsymbol{w}_{\boldsymbol{c}} \\ \boldsymbol{w}_k \end{bmatrix}.
\end{aligned} \tag{16}
$$

For the simplified 2Cov comparator, a mutual HE scheme sustaining data privacy for subjects and vendors can be employed by extending the inner product of vectors to the Frobenius inner product of matrices $\boldsymbol{A}, \boldsymbol{B}$, which can be reformulated via the $\text{vec}(\cdot)$ operator as the inner product of (column-stacked) vectors, such that the dot product can be employed as well with a public key *pk*:

$$
\text{enc}_{pk}\left(\boldsymbol{A}\right)^{\langle\rangle(\boldsymbol{B})} = \text{enc}_{pk}\left(\text{vec}\left(\boldsymbol{A}\right)\right)^{\text{vec}(\boldsymbol{B})}, \tag{17}
$$

where the encryption of a matrix $\boldsymbol{A}$ is denoted as:

$$
\text{enc}_{pk}\left(\boldsymbol{A}\right) = \left(\left(\text{enc}_{pk}(a_{i,j})\right)_{i=1}^{F}\right)_{j=1}^{F}. \tag{18}
$$

[1]The inner Frobenius product denotes $\boldsymbol{x}'\,\boldsymbol{A}\,\boldsymbol{y} = \langle \boldsymbol{A}, \boldsymbol{x}\,\boldsymbol{y}' \rangle = \text{vec}(\boldsymbol{A})'\,\text{vec}(\boldsymbol{x}\,\boldsymbol{y}')$, where $\text{vec}(\cdot)$ denotes the operator stacking matrices into a vector and $\langle \boldsymbol{A}, \boldsymbol{B} \rangle$ is the dot product between matrices, cf. [17].

In the simplified 2Cov comparator, the encrypted vendor and operator communication takes the form:

$$S_{2Cov}(\boldsymbol{X}, \boldsymbol{Y}) = \boldsymbol{w}'_{\boldsymbol{\Lambda}}\, \varphi_{\boldsymbol{\Lambda}}(\boldsymbol{X}, \boldsymbol{Y}) + \boldsymbol{w}'_{\boldsymbol{\Gamma}}\, \varphi_{\boldsymbol{\Gamma}}(\boldsymbol{X}, \boldsymbol{Y}),$$
$$\mathrm{enc}_{pk2}\left(S_{2Cov}(\boldsymbol{X}, \boldsymbol{Y})\right) = \mathrm{enc}_{pk2}(\boldsymbol{\Lambda})^{\langle\rangle(\boldsymbol{c_1})}\mathrm{enc}_{pk2}(\boldsymbol{\Gamma})^{\langle\rangle(\boldsymbol{c_2}+\boldsymbol{c_3})},$$
$$\textit{with: } \boldsymbol{c_1} = \boldsymbol{X}\,\boldsymbol{Y}' + \boldsymbol{Y}\,\boldsymbol{X}', \boldsymbol{c_2} = \boldsymbol{X}\,\boldsymbol{X}',\ \boldsymbol{c_3} = \boldsymbol{Y}\,\boldsymbol{Y}', \tag{19}$$

where the computation of $\boldsymbol{c_1}, \boldsymbol{c_2}, \boldsymbol{c_3}$ is subdue to the encrypted operator, controller and end-user communication:

$$\mathrm{enc}_{pk1}(\boldsymbol{c_1}) = \mathrm{enc}_{pk1}(\boldsymbol{Y})^{\boldsymbol{X}'} \circ \mathrm{enc}_{pk1}(\boldsymbol{Y}')^{\boldsymbol{X}},$$
$$\mathrm{enc}_{pk1}(\boldsymbol{c_2} + \boldsymbol{c_3}) = \mathrm{enc}_{pk1}(\boldsymbol{X}\,\boldsymbol{X}') \circ \mathrm{enc}_{pk1}(\boldsymbol{Y}\,\boldsymbol{Y}'), \tag{20}$$

where $\circ$ denotes the Hadamard product [2], and the terms $\mathrm{enc}_{pk1}(\boldsymbol{Y})^{\boldsymbol{X}'}$, $\mathrm{enc}_{pk1}(\boldsymbol{Y}')^{\boldsymbol{X}}$ represent exponentiations in an outer product fashion, resulting in the matrices $\mathrm{enc}_{pk1}(\boldsymbol{Y}\,\boldsymbol{X}')$ and $\mathrm{enc}_{pk1}(\boldsymbol{X}\,\boldsymbol{Y}')$, respectively. Finally, the protected reference is $\boldsymbol{Y}^{\mathrm{enc}_{pk1}}_{2Cov} = (\mathrm{enc}_{pk1}(\boldsymbol{Y}), \mathrm{enc}_{pk1}(\boldsymbol{Y}\,\boldsymbol{Y}'))$.

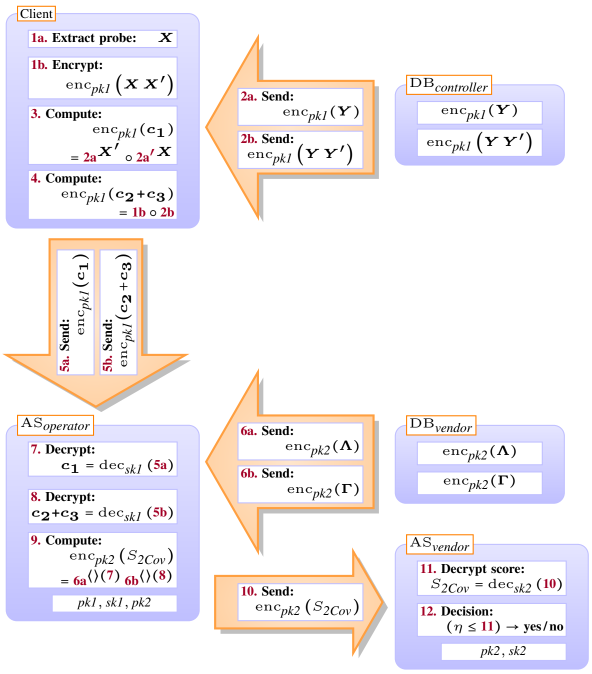

Figure 3: Architecture of protected templates and hyper-parameters, with client, servers (blue) and communication channels (orange).

Fig. 3 presents the proposed architecture. The previously proposed architecture is extended by additional communication channels between operators and vendors. Applications employ two key pairs, such that template protection can be achieved dependent on both: (a) different biometric services of an operator, and (b) multiple provisions of a biometric system to service operators by a vendor. Consequently, additional servers are necessary on the vendor site in terms of a database DB_{vendor} and an authentication server AS_{vendor}, respectively.

[2] The Hadamard product is an entrywise product of two matrices $\boldsymbol{A}, \boldsymbol{B}$ having the same dimension: $\boldsymbol{A} \circ \boldsymbol{B} = (\boldsymbol{A})_{i,j}\,(\boldsymbol{B})_{i,j}$.

6. Experimental Analysis and Discussion

An experimental validation is conducted on the 2013 – 2014 NIST i-vector machine learning challenge [51, 52] phase III database (i.e. with labeled development data), where 600 dimensional i-vectors are supplied, comprising a development set of 36 572 i-vectors, 1 306 references with each five enrolment i-vectors, and 9 634 probes, conducting 12 582 004 comparisons on averaged reference i-vectors as template models. The prototype system comprises a dimension reduction to $F = 250$ by linear discriminant analysis, within class covariance normalization, length normalization, and 2Cov comparison. For the Paillier cryptosystem, $n = 2\,048$ bits keys are utilized, in accordance with the NIST recommendation [53]. In contrast, plaintext operations consider double floating-point precision, i.e. $p = 64$ bits per plain real feature value. Implementations are based on the freely available *sidekit* [54] and *Python Paillier* [50]. Fig. 4 illustrates the DET performance of conventional and HE 2Cov comparators on the evaluation set in terms of false non-match rate (FNMR) and false match rate (FMR): the baseline performance is preserved across all operating points (same for all systems). The DET is depicted in terms of the convex hull of the receiver operating characteristic (ROCCH). For the exemplary 2Cov system, a 2.5% equal error rate (ROCCH-EER), a 0.050 minDCF (parameterized according to [51]), and a 0.099 $C_{\mathrm{llr}}^{\mathrm{min}}$ are preserved in the protected domain. As the k normalization term is neglected in this set-up, the baseline system yielded a 9.560 C_{llr}. Calibration loss can be reduced by a post score re-bias, or by employing conventional score calibration methods, cf. [55]. By utilizing linear score calibration trained on the development set with known labels, C_{llr} is reduced to 0.284.

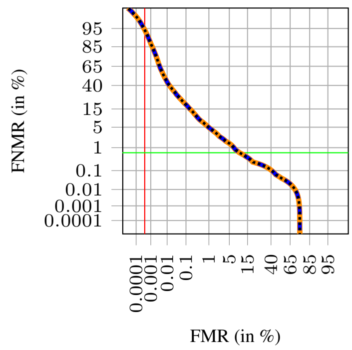

Figure 4: DET comparison of the baseline 2Cov system (orange), and the proposed HE 2Cov schemes, focusing on subject data protection (blue, dashed), and the protection of subject and vendor data (black, dotted) with rule of 30 bounds (red, green).

As the verification performance is preserved, the proposed schemes are further examined regarding requirements of the biometric template protection standard [3] in terms of [13]: $i)$ *only the client can have access to the plain probe template,* $ii)$ *the plain reference template should not be seen by the client, and only its encryption should be stored or handled during verification, and* $iii)$ *the score should also be protected in order to prevent hill-climbing and inverse-biometrics attacks*. Firstly, both employed homomorphic Paillier cryptosystem provide semantic security: only secret keys are able to derive the plain probe after encryption, where the client solely communicates the encrypted score $(\mathrm{enc}_{pk}(S_{2Cov}(\boldsymbol{X}, \boldsymbol{Y})))$ or auxiliary matrices $(\mathrm{enc}_{pk1}(\boldsymbol{c_1}), \mathrm{enc}_{pk1}(\boldsymbol{c_2} + \boldsymbol{c_3}))$. Secondly, biometric references are communicated from the controller database server to the client in the encrypted domain, assuming the authentication server being able to protect the secret key $sk1$, no other entities will be able to relate the protected biometric information. Similarly, the vendor data is protected in the sense, that the vendor authentication server is assumed to be able to protect $sk2$. Finally, scores are computed in the protected domain, and can solely be decrypted utilizing secret key $sk2$. Thus, the irreversibility criterion is met. Renewability is granted as depicted in [13]: if templates are lost, new key pairs can be generated for the purpose of re-encrypting the database, such that (a) re-acquisitions of enrollment samples are avoided when revoking corrupted templates, and (b) comparisons of corrupt to renewed templates result in non-matches, granting security and data privacy. Thus, templates can easily be revoked, thereby providing data privacy. Unlinkability is granted due to the probabilistic nature of the Paillier cryptosystem, where random numbers are utilized for different encryptions, i.e. encrypting the same data $\boldsymbol{Y}$ twice, two different random numbers s_1, s_2 are drawn, such that: $\mathrm{enc}_e(\boldsymbol{Y}, s_1) \neq \mathrm{enc}_e(\boldsymbol{Y}, s_2)$, cf. [13, 19].

Table 2: Complexity analysis for the proposed 2Cov HE schemes (verification) with the data sizes of the exemplary employed system (p = 64 bits, ν = 0.5 KiB, F = 250).

Comparator Protection	2Cov subject	2Cov subject & vendor
N^o encryptions	1	F^2
N^o decryptions	1	$2\,F^2 + 1$
N^o additions	$4\,F\,(F-1)$	0
N^o products	$4\,F^2 + 2\,F + 1$	$5\,F^2 - 1$
N^o exponentiations	$2\,F$	$4\,F^2$
Plain template size	$p\,F$ $\approx 2.0\,\mathrm{KiB}$	$p\,F$ $\approx 2.0\,\mathrm{KiB}$
Protected template size	$\nu\,(F+1)$ $= 125.5\,\mathrm{KiB}$	$\nu\,(F^2 + F)$ $\approx 30.6\,\mathrm{MiB}$
Plain model size	$2\,p\,F^2$ $\approx 1.0\,\mathrm{MiB}$	$2\,p\,F^2$ $\approx 1.0\,\mathrm{MiB}$
Protected model size	0 $= 0\,\mathrm{KiB}$	$2\,\nu\,F^2$ $\approx 61.0\,\mathrm{MiB}$
Channels: amount of protected data exchanged	$\nu\,(F+2)$ $= 126.0\,\mathrm{KiB}$	$\nu\,(5\,F^2 + F + 1)$ $\approx 152.7\,\mathrm{MiB}$

In terms of complexity, each approach can be analyzed regarding the amount of required resources, i.e. the number of operations performed in the encrypted domain as well as the size of encrypted data sent over a channel. For a single verification attempt, the chipertext channel bandwidth is $\nu = 2\,n$ due to the Paillier ciphertext length in modulo n^2 domain [13], i.e. $\nu = 4\,096\,\mathrm{bits}\,\frac{1\,\mathrm{KiB}}{8\,192\,\mathrm{bits}} = 0.5\,\mathrm{KiB}$ for the examined system. Tab. 2 summarizes the proposed HE schemes' complexity. Regarding to an i-vector dimension $F = 250$, the cosine HE approach requires $\nu\,F = 125\,\mathrm{KiB}$ for storing a reference i-vector. For transmitting the protected score to the authentication server, $0.5\,\mathrm{KiB}$ are necessary, i.e. a protected scalar. The subject protective 2Cov HE scheme stores a reference tuple with $\nu\,(F+1) = 125.5\,\mathrm{KiB}$, communicating a protected scalar as well to the authentication server. However, the subject and vendor protective 2Cov HE scheme stores protected auxiliary matrices, requiring $\nu\,(F^2 + F) \approx 30.6\,\mathrm{MiB}$. Therefore, the channel between client and authentication server considers two protected matrices, requiring $2\,\nu\,F^2 \approx 61.0\,\mathrm{MiB}$, alike for the vendor database to operator authentication server channel. Regarding the protected data exchanged over the communication channels, the first proposed scheme comprises $\nu\,(F+2) = 126\,\mathrm{KiB}$ as the protected template and score are transmitted. The second proposed scheme demands higher requirements: as the model hyper-parameters are protected, the client to authentication server channel transmits auxiliary matrices comprising $2\,\nu\,(F^2) \approx 61.0\,\mathrm{MiB}$, whereas the same data amount is loaded for the protected model from the vendor database server. Finally, a protected score is transmitted to the vendor authentication server, making application decisions. Afterwards, conventional security protocols can be employed.

7. Conclusion

Employing HE, *data privacy* is protected: non-HE comparisons solely carried out by biometric service operators permit operators to utilize plaintext biometric templates for other (non-biometric) purposes. HE prohibits operators to exploit *data privacy* by preserving *unlinkability*, *irreversibility*, and *renewability*. Additionally one may assure *data security*, i.e. by utilizing transport layer security (TLS), e.g. with RSA.

Homomorphic template protection is made available to generative comparators, i.e. comparators employing statistical models, where the related biometrics work solely considers non-generative comparators, such as XOR, DTW, Euclidean distance, and cosine similarity. Extending the HE scheme for cosine similarity comparison, template protection is made available to the 2Cov comparator in two architectures. The first proposed HE architecture solely puts emphasis on the protection of templates, which can be sustained under a fair complexity tradeoff. Contrastively, the second proposed HE 2Cov scheme provides subject and vendor data protection. However, the required complexity increases by a quadratic term. By pre-loading both protected model parameters the channel bottleneck is reduced to $\nu\,(3\,F^2 + F + 1) \approx 91.7\,\mathrm{MiB}$ for a single verification attempt, which however limits the application scope to well-equipped infrastructures e.g., call center and forensic scenarios. Depending on the application scenario, protected templates may also be pre-loaded, further reducing the overall transmitted data amount to $\nu\,(2\,F^2 + 1) \approx 61.0\,\mathrm{MiB}$. For mobile device voice biometrics, one may prefer to employ the first proposed architecture. Both approaches ensure biometric template protection requirements as of the ISO/IEC 24745 standard.

As the proposed schemes target 2Cov as prototype generative comparators, i.e. the full-subspace Gaussian PLDA special case, extensions to other members of the PLDA family and related comparators can be easily developed. Accounting for i-vectors not only as single point estimate features but also as latent variables, uncertainties associated to the single point estimation can be incorporated as well, e.g. targeting full-posterior PLDA. Also, HE schemes seem promising for end-to-end neural network system architectures, as the inner Frobenius product is computable in the protected domain. Extensions of the proposed architectures and implementations of alternative HE schemes is left to future work.

8. Acknowledgements

This work was supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts within the Center for Research in Security and Privacy (`www.crisp-da.de`), and the BioMobile II project (no. 518/16-30).

9. References

[1] European Council, "Directive 2016/680 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA," April 2016.

[2] European Parliament and European Council, "Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market," November 2015.

[3] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection*, International Organization for Standardization, 2011.

[4] C. Vaquero and P. Rodríguez, "On the need of template protection for voice authentication," in *Proc. Annual Conf. of the Intl. Speech Communication Association (INTERSPEECH)*, 2015, pp. 219–223.

[5] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, 2007.

[6] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[7] O. Glembek, P. Matejka, O. Plchot, J. Pesan, L. Burget, and P. Schwarz, "Migrating i-vectors between speaker recognition systems using regression neural networks," in *Proc. Annual Conf. of the Intl. Speech Communication Association (INTERSPEECH)*, 2015, pp. 2327–2331.

[8] E. Moyakine, C. Colonnello, J. Butler, and C. Jasserand, "Discussion panel: SIIP and INGRESS research projects: Developing effective and sustainable biometric systems with a global reach," 2017, EAB Research Projects Conference, [Online] `https://www.eab.org/upload/documents/1279/08-eabrpc2017_SIIP_INGRESS.zip?ts=1517990107115`, last accessed: 2018-02-07.

[9] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 3, 2011.

[10] V. M. Patel, N. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Proc. Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[11] P. Campisi, Ed., *Security and Privacy in Biometrics*, Springer, 2013.

[12] C. Aguilar-Melchor, S. Fau, C. Fontaine, et al., "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 108–117, 2013.

[13] M. Gomez-Barrero, J. Fierrez, J. Galbally, E. Maiorana, and P. Campisi, "Implementation of fixed length template protection based on homomorphic encryption with application to signature biometrics," in *Proc. Conf. on Computer Vision and Pattern Recognition Workshops (CVPR)*, 2016, pp. 191–198.

[14] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Information Sciences*, vol. 370–371, pp. 18–32, 2016.

[15] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognition*, vol. 67, pp. 149–163, 07 2017.

[16] M. Gomez-Barrero, J. Galbally, A. Morales, and J. Fierrez, "Privacy-preserving comparison of variable-length data with application to biometric template protection," *IEEE Access*, vol. 5, no. 1, pp. 8606–8619, 12 2017.

[17] S. Cumani, N. Brümmer, L. Burget, P. Laface, O. Plchot, and V. Vasilakakis, "Pairwise discriminative speaker verification in the i-vector space," *IEEE Trans. on Audio, Speech, and Language Processing (TASLP)*, vol. 21, no. 6, pp. 1217–1227, 2013.

[18] S. Cumani and P. Laface, "Generative pairwise models for speaker recognition," in *Proc. Odyssey 2014: The Speaker and Language Recognition Workshop*, 2014, pp. 273–279.

[19] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Advances in Cryptology — EUROCRYPT*, 1999, pp. 223–238.

[20] H. Zhu, X. Meng, and G. Kollios, "Privacy preserving similarity evaluation of time series data," in *Proc. Intl. Conf. on Extending Database Technology (EDBT)*, 2014, pp. 499–510.

[21] G. M. Penn, G. Pötzelsberger, M. Rohde, and A. Uhl, "Customisation of paillier homomorphic encryption for efficient binary biometric feature vector matching," in *Proc. IEEE Intl. Conf. Biometrics Special Interest Group (BIOSIG)*, 2014, pp. 1–6.

[22] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, et al., "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in *Proc. Intl. Conf. on Biometrics: theory applications and systems (BTAS)*. IEEE, 2010, pp. 1–7.

[23] N. Dehak, P. J. Kenny, R. Dehak, P. Dumouchel, and P. Ouellet, "Front-end factor analysis for speaker verification," *IEEE Trans. on Audio, Speech, and Language Processing (TASLP)*, vol. 19, no. 4, pp. 788–798, 2011.

[24] P. Kenny, "Joint factor analysis of speaker and session variability: Theory and algorithms," Tech. Rep. CRIM-06/08-13, CRIM, Montreal, 2005.

[25] X. Anguera and J. F. Bonastre, "A novel speaker binary key derived from anchor models," in *Proc. Annual Conf. of the Intl. Speech Communication Association (INTERSPEECH)*, 2010, pp. 2118–2121.

[26] J. F. Bonastre, P. M. Bousquet, D. Matrouf, and X. Anguera, "Discriminant binary data representation for speaker recognition," in *Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, 2011, pp. 5284–5287.

[27] G. Hernández-Sierra, J. F. Bonastre, and J. Calvo de Lara, "Speaker recognition using a binary representation and specificities models," in *Proc. Iberoamerican Congress on Pattern Recognition (CIARP)*, 2012, pp. 732–739.

[28] M. Paulini, C. Rathgeb, A. Nautsch, H. Reichau, H. Reininger, and C. Busch, "Multi-bit allocation: Preparing voice biometrics for template protection," in *Proc. Odyssey 2016: The Speaker and Language Recognition Workshop*, 2016, pp. 291–296.

[29] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 66–76, 2015.

[30] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 42–52, 2013.

[31] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," *Proc. of the IEEE*, vol. 85, no. 9, pp. 1365–1388, 1997.

[32] T. Bianchi, S. Turchi, A. Piva, R. D. Labati, V. Piuri, and F. Scotti, "Implementing fingercode-based identity matching in the encrypted domain," in *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, 2010, pp. 15–21.

[33] S. Ye, Y. Luo, J. Zhao, and S. Cheung, "Anonymous biometric access control," *EURASIP Journal on Information Security*, vol. 2009, no. 1, pp. 1–17, 2009.

[34] Y. Luo, S. C. Sen-ching, and S. Ye, "Anonymous biometric access control based on homomorphic encryption," in *Proc. Intl. Conf. on Multimedia and Expo (ICME)*, 2009, pp. 1046–1049.

[35] M. Blanton and P. Gasti, *Secure and Efficient Protocols for Iris and Fingerprint Identification*, pp. 190–209, Springer Berlin Heidelberg, 2011.

[36] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Springer Science & Business Media, 2009.

[37] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, "Packed homomorphic encryption based on ideal lattices and its application to biometrics," in *Proc. Intl. Conf. on Availability, Reliability, and Security*, 2013, pp. 55–74.

[38] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, "New packing method in somewhat homomorphic encryption and its applications," *Security and Communication Networks*, vol. 8, no. 13, pp. 2194–2213, 2015.

[39] C. Patsakis, van J. Rest, M. Choraś, and M. Bouroche, "Privacy-preserving biometric authentication and matching via lattice-based encryption," in *Proc. Intl. Workshop on Data Privacy Management*, 2015, pp. 169–182.

[40] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 168–180, 1978.

[41] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP Journal on Information Security*, vol. 2007, 2007.

[42] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008.

[43] T. W. Hungerford, *Algebra*, Springer Graduate Texts in Mathematics, 1974.

[44] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in *Proc. Advances in Cryptology (CRYPTO)*, 1998, pp. 26–45.

[45] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems provably secure against active adversaries," in *Proc. Advances in Cryptography — ASIACRYPT*, 1999, pp. 165–179.

[46] D. A. Reynolds, T. F. Quatieri, and R. B. Dunn, "Speaker verification using adapted gaussian mixture models," *Conversational Speech, Digital Signal Processing*, vol. 10, pp. 19–41, 2000.

[47] D. Garcia-Romero and C.Y. Epsy-Wilson, "Analysis of i-vector length normalization in speaker recognition systems," in *Proc. Annual Conf. of the Intl. Speech Communication Association (INTERSPEECH)*, 2011, pp. 249–252.

[48] P.-M. Bousquet, J.-F. Bonastre, and D. Matrouf, *Identify the Benefits of the Different Steps in an i-Vector Based Speaker*, chapter CIARP, Part II, pp. 278–285, Springer-Verlag Berlin Heidelberg, 2013.

[49] IEEE Standards Association, *754-2008 IEEE standard for Floating-Point Arithmetic*, 2008.

[50] B. Thorne, "Python Paillier," 2017, [Online] `https://github.com/n1analytics/python-paillier/`, last accessed: 2018-01-11.

[51] National Institute of Standards and Technology (NIST), "The 2013-2014 speaker recognition i-vector machine learning challenge," Tech. Rep., National Institute of Standards and Technology, 2014.

[52] D. Bansé, G. R. Doddington, D. Garcia-Romero, J. J. Godfrey, C. S. Greenberg, et al., "Summary and initial results of the 2013-2014 speaker recognition i-vector machine learning challenge," in *Proc. Annual Conf. of the Intl. Speech Communication Association (INTERSPEECH)*, 2014, pp. 368–372.

[53] E. Barker, L. Chen, A. Roginsky, and M. Smid, "Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography," Tech. Rep. SP 800-56A Rev. 2, NIST, May 2013.

[54] A. Larcher, K.A. Lee, and S. Meignier, "An extensible speaker identification SIDEKIT in Python," in *Proc. IEEE Intl. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2016, pp. 5095–5099, `http://lium.univ-lemans.fr/sidekit`, last accessed: 2017-05-15.

[55] N. Brümmer and E. de Villiers, "The BOSARIS toolkit user guide: Theory, algorithms and code for binary classifier score processing," Tech. Rep., AGNITIO Research, South Africa, December 2011.