Privacy-Preserving Multibiometric Authentication in Cloud with Untrusted Database Providers

Christina-Angeliki Toli, Abdelrahaman Aly, Bart Preneel

Department of Electrical Engineering
KU Leuven COSIC and imec
Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven-Heverlee, Belgium
{fistname.lastename}@esat.kuleuven.be
http://www.esat.kuleuven.be/cosic/

Abstract

This paper introduces a secure and privacy-preserving mechanism for biometric-based user authentication in a distributed manner. The design combines three modalities (face, iris and fingerprint) according to user's performance strength parameters (False Acceptance and False Rejection Rates). We use a user-specific weighted score level fusion strategy to determine the final multimodal result. The stored unimodal templates are held by distinct database providers that can be malicious. Privacy regulations recognize biometric data as sensitive, hence their handling and storage in an untrusted environment with third parties are challenging. Therefore, we utilize Multi-Party Computation to enhance security among authentication stages. In contrast to the existing research, the novelty of this approach lies in performing multimodal authentication without storing private information in a single database, nor transferring the calculation results to any third party. The proposed protocol is analyzed to assess its usability, security and efficiency (execution time is less than a second under the studied scenario).

Keywords: Biometrics, Identity authentication, Secret sharing, Multi-Party Computation, Secure distributed systems, Cloud cryptography, Privacy-aware architecture

1 Introduction

Secure authentication is a primary goal when users access a multiplicity of services. Biometric technologies have become a natural fit for several applications in the cloud domain. Multibiometrics can improve identification efficiency by expanding the feature space to increase reliability [29]. However, multimodal incorporation (fusion) is viewed as an open problem. The starting point, for different studies in the literature, is to define the conditions, under which, a fusion model is most likely to be characterized as optimal and accurate in terms of performance rates [17]. The suitability of a biometric design is determined by two probabilistic measures: i) The False Acceptance Rates (FAR), and ii) The False Rejection Rates (FRR). Note that any biometric information can be seen as sensitive personal data, and their transmission across cloud parties poses serious security and privacy threats [20]. Although, it is possible to use cryptographic techniques to communicate and store the templates, for instance using Public Key Infrastructure (PKI); this is not enough for a completely secure process, taking into account the privacy issues related to the biometric information leakage.

Motivated by cloud applications that require privacy-aware design, we propose a secure protocol for multimodal biometric authentication mechanism in cloud domain. The studied scenario represents a general layout, used in practice, that involves a user, an untrusted intermediary entity who wants to authenticate the user and three malicious cloud-based providers that hold unimodal databases for unibiometric recognition services. The aim is to biometrically authenticate the user by following a score level multimodal fusion strategy. We combine three modalities on a user's performance rates basis, taking into account the severity of the privacy concerns that may limit the design and implementation [23].

We address these concerns by using Secure Multi-Party Computation (MPC) to build a protocol that securely combines the multiple unibiometric characteristics of the model and provides the final fusion result securely. The term "securely" means that no sensitive privately held data are exposed to any untrusted intermediary party involved in the computation, or platform nor any other third party. Our protocol is designed for authentication, in the context of systems that integrate unimodal biometrics coming from different service providers, such as log in to biometric-based mobile applications. Moreover, it can operate in cloud-based identification services for lawful surveillance purposes. In this work we focus solely on the security of the biometric template(s) and not on the user's identity anonymization.

The ***contribution*** of this paper is as follows:

- We introduce a protocol for biometric authentication that exploits prior stored unimodal templates being collected by three service providers. In the context of fusion, as this is determined in Section 3.4; we compute the multimodal result, avoiding the auxiliary, temporary or permanent storage of information in a single database, either at rest or at transit.
- In Section 4.3, we expand on the selection of fusion technique by following a user-specific weighted score level fusion strategy. According to this method, weights as factors are assigned to each modality based on the performance parameters for each user, increasing or reducing its importance at the final score.
- By using MPC, we avoid the reliance on any centralized repository and utilize the stored templates in a privacy-preserving decentralized manner. This could be viewed as if the parties use a virtualized trusted "third party", but that in reality is centralized and is composed of untrusted parties with competing interests to avoid collusion.

Regarding ***privacy***, by using this virtualized computation environment, we achieve the following properties:

- Service providers do not learn the raw acquired biometric data, nor any derived information from them.
- The untrusted intermediary entity does not learn the stored templates, nor any information derived from them, except of the unique output $\texttt{out} \in \{0,1\}$.

The ***general assumptions*** and ***non-goals*** are as follows:

- We assume the parameters of reference, thresholds and rates are already held by the unibiometric cloud-based service providers and secretly shared by them during the execution of the protocol.
- We assume that the biometric sensors are tamper-proof devices and use available Public Key Infrastructure (PKI) framework. In this way, the data are secretly trans-

mitted, being encrypted with the key of user *u*, for preserving protection of the raw biometric information from the untrusted intermediary entity.

- Regarding training, as this is determined in Section 3.2, we assume that service providers hold and calculate FAR and FRR parameters. We assume that they train their unimodal datasets by regulating the reference thresholds, while they also utilize established training algorithms to handle user-specific error rates. Because of its large scope, any privacy challenges on securely computing such rates are outside the scope of this paper and should be the subject of further research.

2 Related Work and Motivation

The use of online recognition schemes, have resulted in an increase of security and privacy risks. this mainly occurs due to the way that information is recollected and stored, Pan et al. [27]. These concerns have reduced public acceptance of biometric technologies, pointing out the problem of trust in cloud environment. Along these lines, several privacy-by-design approaches have been presented from biometric secret sharing and fuzzy extractors methods to privacy-preserving protocols. Indicatively, we may mention the work by Wang et al. [33] who introduces a privacy-friendly fingerprint matching protocol. Approaches that use secure computation in different settings can be found in [5, 6, 34]. Yuan and Yu [35] design a biometric identification scheme for cloud computing. However, these studies do not address the question of fusion or approach the field from a multimodal perspective. For our privacy-aware protocol, we take into consideration the findings provided by Bringer et al. [9] regarding the impact of secure MPC techniques on identification schemes in terms of accuracy and privacy.

Finally, the paper introduced by Toli et al. in [32] describes a succinct fusion model for cloud-based access control. This introductory work mainly discusses the advantages and conditions of using MPC in such settings without introducing any protocol, formal solution or implementation besides general discussion. Our work is based on their basic conditions and present concrete results that complete such assertions. Our privacy-aware protocol addresses all the model inputs, providing an efficient and viable solution for enhancing privacy during the calculation phases.

3 Background and Preliminaries

3.1 Unimodal Biometric Recognition

Face Recognition: Face recognition based on Euclidean Distance and facial texture features is a technique that is familiar to its overall recognition accuracy at face biometric systems. In literature, there are several approaches that take the advantage of using statistical facial characteristics that could present strong resistibility to noise. These methods by training their datasets have managed to present notable face recognition schemes that outperform the classical Euclidean Distance approaches.

Fingerprint Recognition: During the last decade, the matching of unequal number of minutia features and ridges of the fingerprints are the most important and challenging field in fingerprint based biometrics recognition systems. Recently, the technique and algorithms suggested by [26] showed that can offer promising recognition accuracy. Findings compared with classical Euclidean Distances presenting better matching scores. The performance of the proposed image alignment and the minutia matching algorithms are evaluated to constitute the basis for the next generation fingerprint-based schemes.

Iris Recognition: A new method for iris recognition collarates the zigzag area of iris for the extraction of the feature [28]. In this way captures the most important information of the pattern. HAAR wavelet and 1D Log Gabor filter used for feature extraction and managed to improve performance. Support vector machine techniques and Hamming Distance approach is used to eyelid and eyelash detection. The recognition accuracy of the proposed system was compared with the previous reported approaches, offering significant results. For that reason, this method could be characterized as novelty at the field of iris recognition.

Biometrics are based on pattern recognition techniques, used on statistically unique parts of modalities in order to allow recognition. The process includes the feature extraction stage, where the user presents raw biometrics (new template) at the sensor(s), and the matching phase where an extracted feature is compared with a stored template. In this work, we assume that the matching process is performed by Hamming Distances algorithms. The technique is widely used in current biometric commercial deployments on face, iris and fingerprint, presenting highly reliable results in terms of performance [9, 21], and it can be easily adapted for privacy-preserving scenarios. Other methods that can be calculated over an arithmetic or boolean circuit could be also used [5, 6].

3.2 Thresholds and Performance Rates

The confidence in the functionality of a biometric scheme is determined by specific measures that are used to evaluate the accuracy and effectiveness. Thresholds are defined to decide if a user does or does not correspond to a claimed identity. In biometric deployments, after the recognition process for each user u, the generated match score s between the new and stored templates is analyzed on the basis of a predefined decision threshold $\perp$. The process is represented as:

$$\begin{aligned} s_u &\geq \perp \quad Accept \\ s_u &\leq \perp \quad Reject \end{aligned} \tag{1}$$

The statistical calculation of a threshold is related to the extraction and validation of performance rates [24]. Following the analysis of Ross et al. [29], given a threshold $\perp$, for a match score s, the $p(s \mid \text{genuine})$ represents the probability of dissimilarity values for a given s, between the raw data and the template, under the genuine conditions; and similarly $p(s \mid \text{impostor})$ indicates the probability for the impostor conditions. Consider an impostor who is not enrolled in the system, FAR for a threshold $\perp$ can be computed as follows:

$$\text{FAR}(\perp) = \int_{-\infty}^{\perp} p(s \mid \text{impostor})\, ds \tag{2}$$

The FRR is given by:

$$\mathrm{FRR}(\perp) = \int_{\perp}^{\infty} p(s \mid \text{genuine})\, ds \tag{3}$$

A system's accuracy is associated with the ability of the involved parties (manufacturers) to test on their datasets for the purposes of the scheme. Tuning the system's threshold $\perp$, also known as reference threshold for the performance rates, is a common technique referred as the *training* of datasets to perform under a given procedure; a process that always effects on the corresponding rates of the system [24, 29].

3.3 Score Normalization Technique

The match scores obtained from the biometric matchers are non-homogenous, similarity measures, in different scales, where $\{-1,+1\}$ is typically used for faces, a unit interval $\{0,1\}$ for irides, and $\{0,100\}$ is the range for fingerprints. Hence, it is necessary to normalize the scores using an adaptive technique prior to their combination. Compared to other approaches, *Min-Max Normalization* technique has not presented disadvantages regarding viability and computational complexity from a biometric perspective [18]. Due to its simple applicability, it is perfectly adequate to work for our protocol. The normalized scores, where minimum is 0 and maximum is 1, are computed as:

$$ns^t_j = \frac{s^t_j - min^N_{i=1} s^i_j}{max^N_{i=1} s^i_j - min^N_{i=1} s^i_j} \tag{4}$$

Here s^t_i denotes the i^{th} score obtained by the j^{th} matcher, N is the number of match scores $i = 1,...,N$ available in the set, and R the number of matchers $j = 1,...,R$ for each modality.

3.4 User-Specific Weighted Score Fusion

In the context of multibiometrics, data fusion represents an active area with numerous approaches and can be accomplished at various levels and by several strategies in a biometric deployment (more information can be found in Ross et al. *"Handbook of Multibiometrics"* [29]). However, multimodal designs are governed by the information type and sources, the acquisition; the processing stages; and the final application. In this paper, we use the term of "fusion" to describe the consolidation of matched unimodal templates in a single score that we call "multimodal result".

Match score level fusion, also known as fusion at measurement or confidence level, is a widely used fusion approach. It provides improved performance in comparison to decision-level fusion, while it allows an easy integration for different modalities [18]. In a fusion model, performance rates can be applied in such a way that they assign different degrees of importance to the various modalities on a user-by-user basis [30]. In our protocol, fusion is computed following a weighted match score level strategy. For determining the set of weights, we follow the user-specific weighted sum rule presented in [29]. In a system with M modalities, where modality i has weight w_i for the user u, and the match score is equal to s_i, then the score of fusion is computed as follows:

$$sf_u = \sum_{i=1}^{M} w_i s_i \tag{5}$$

The factors w_i are in the range of $\{0,1\}$ and being applied such as the constraint $w_i + ... + w_M = 1$ is satisfied.

3.5 Achievable Security under MPC

Security under MPC addresses the confidentiality of the private inputs with respect to the parties involved in any computational stage of the protocol. MPC is used for security reasons against typical privacy adversarial models, such as honest but curious and malicious adversaries, offering various security levels, from computation to perfect security [3, 15]. We define security under MPC as follows:

Definition 1. *(**Security**): Consider $I = P_1, ..., P_n$ being the parties who want to compute a function $y = f(x_1, ..., x_n)$, where x_i is the secret input of P_i. Then, any protocol π that computes y is secure if the parties do not learn anything but the output y and what can be inferred from y.*

This definition implies that no party P_i should learn any information from the private inputs of $P_j \quad \forall j \in I$, where $i \neq j$, except what can be inferred from the output. Notice that in our case, we assume all parties involved in the computation have knowledge of who the user is, or the index being analyzed. Finally, access patterns towards the protocol could also be statistically hidden, as explained in the following sections. To ease security analysis and the protocol description, we use the following arithmetic black-box.

Arithmetic Black-Box.

We use and extend the arithmetic black-box of Damgård and Nielsen [14] based on a composable efficient MPC from threshold homomorphic encryption, assuming its functionality can be accessed by our secure protocol. The original arithmetic black box was built under Canetti's composability hybrid model [10] and proved secure against passive and active adversaries. This makes simulation proofs straightforward, where the simulated view of any P_i is the same as the adversary view, reducing the complexity of our security analysis. The black box in [14] could be seen as a virtualized entity capable to store field elements over $\mathbb{Z}_{|}$, where p is any sufficiently large prime number or RSA modulus. It also provides secure addition and multiplication with a scalar and between secretly stored values. The basic functionality of our arithmetic black-box $\mathscr{F}_{ABB}$ can be achieved by well-known protocols for homomorphic encryption (see Paillier's cryptosystem [25]), or linear secret sharing schemes, such as Shamir's scheme [31]. The addition and multiplication provided by the $\mathscr{F}_{ABB}$ can exploit the advantages of well-known MPC protocols, based on the properties of the cryptographic sharing primitive selected. This category includes the BGW protocol by Ben-Or et al. [3], BDOZ by Bendlin et al. [4] or SPDZ by Damgård et al. [15], and recent works, such as MASCOT by Keller et al. [19] and other highly specialized 3-party protocols [2, 7].

Arithmetic Black-Box Extension.

Following the work introduced by Lipmaa and Toft in [22], we proceed to extend our black box, in order to have inequality tests, being needed by our protocol. Arithmetic circuits and protocols for ***secure comparison*** have been introduced by [12, 13], among others. We could cite for instance the inequality tests that can be found in [22], where the authors use the same $\mathscr{F}_{ABB}$ conceptualization. In the context of our $\mathscr{F}_{ABB}$ extension, the following operations are provided:

$$[z] \leftarrow [x] \overset{?}{=} [y] \mid [z] \in \{0,1\} \tag{6}$$

$$[z] \leftarrow [x] \overset{?}{<} [y] \mid [z] \in \{0,1\} \tag{7}$$

3.6 Security Notation and Assumptions

We assume that all inputs and intermediary values are elements of a finite field bounded by p ($\mathbb{Z}_l$), such that $x \ll p$, for any value x in $\mathbb{Z}_l$, so that no overflows occur. For simplicity reasons, we assume that the underlying cryptographic primitive is secret sharing. Additionally, we use the notation introduced by Damgård and Nielsen [14], where $[x]$ represents the secretly shared value of $[x]$. To express operations provided by the $\mathscr{F}_{ABB}$, we use the infix representation $[z] \leftarrow [x] + [y]$. In reality, the operations (addition, multiplication gates) are provided by the underlying protocols, such as [2, 3, 4, 15, 19] and executed by the involved parties. Practically, our protocol is as secure as the underlying MPC functionality that is implemented. Negative numbers are represented in the typical way, where the lower half of the $\mathbb{Z}_l$ field represents the positives and the other half the negatives.

Under the $\mathscr{F}_{ABB}$ model, complexity is measured by the number of non-concurrent black-box operations that are executed. MPC protocols based on linear secret sharing schemes can offer addition of shares and scalar multiplication, approximately at the same cost of similar *"plain-text"* operations. Nonetheless, multiplications require some level of information exchange between the computational parties.

Concurrent operations that require information exchange between parties is referred to as a communication round. Comparisons are by themselves arithmetic circuits, composed of addition and multiplication gates. Their computational and communication cost is much higher than a multiplication, and thus is on the interest of the algorithm designer to minimize their use.

4 Multimodal Mechanism Layout

In this section, we present the general layout of our multimodal authentication mechanism, the roles and parties involved in the process. The studied scenario describes the authentication procedure being performed biometrically, where the fusion strategy is based on the optimum low FAR. Figure 1 illustrates the interaction of the parties.

4.1 Parties and Roles

Intermediary Entity: Party who is interested on authenticate the user. It holds the new templates of the raw acquired biometric data, obtained directly by the recognition sensors. It also holds the threshold of decision $\perp$. The entity does not actively participate in the computation. We assume that the sensors use a PKI framework for the secure transmission of the templates to the parties in charge of the computation. Any further analysis on protection against data tampering on the entity's behalf is outside the scope of this paper.

Service Providers: These parties are considered to be malicious. They hold their respective unimodal templates stored in unimodal databases and they are in charge of

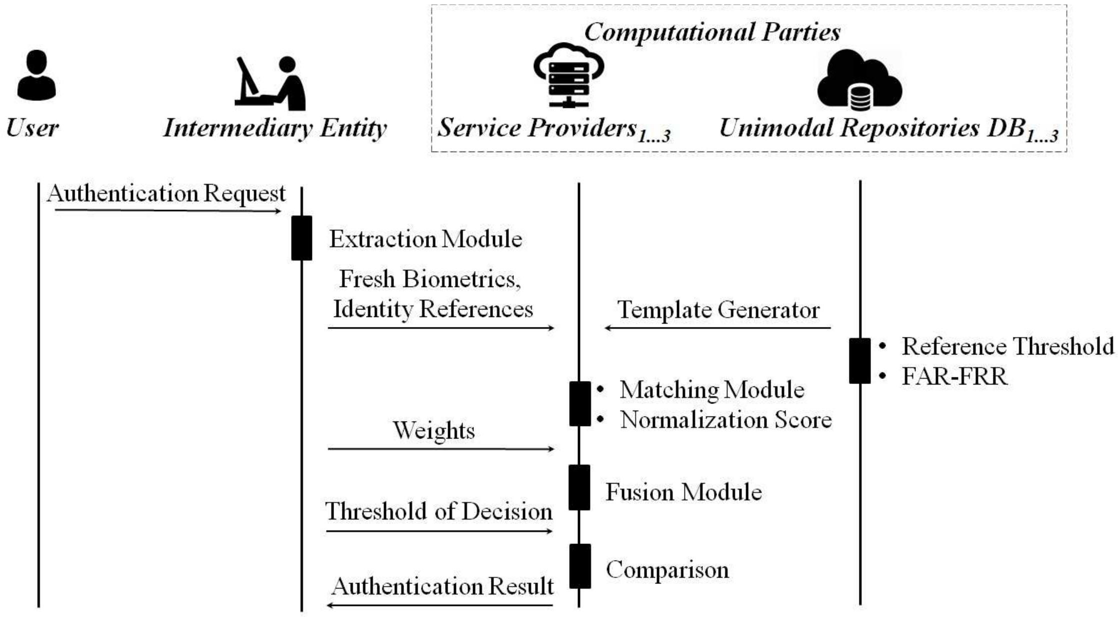

Fig. 1: Mechanism for Multimodal Authentication in Cloud.

storing and regulating the FAR and FRR parameters. We consider the maintenance of the templates to be an orthogonal problem. In case the stored templates have to be updated, this can to be directly managed by the service providers who can adjust the biometric data of their users and recalculate the performance metrics of their schemes.

Input Data: All the input data of the parties are considered to be private. In our privacy-preserving protocol, biometric information are represented in binary form; and they are sent to the computational parties using private channels. We assume that input data are integers and they are included in $\mathbb{Z}_p$. In case fixed point precision is needed, data can be multiplied by a sufficiently large decimal constant. This procedure takes place to prevent the computation of what can be considered complex decimal arithmetic with arithmetic circuits.

Dealers: They have to provide inputs to the protocol for the computation in shared form. In our case, the intermediary entity extracts the biometric information and transmits the secret shares of the new templates. The cloud-based service providers have to deal with the shares of the stored templates and communicate the parametrization.

Computational Parties: They are the set of servers in charge of computing the protocol. Note that there is no upper bound on the number of the involved computational parties. They receive the shares from the dealers and execute the computation. Due to their role, computational parties are considered to be distrustful with conflicting interests, creating incentives for collusion. Without loss of generality, the role of the computational parties can be executed by the service providers. Our protocol is generic, thus the selection of the computational parties is rather tied to the scenario and orthogonal to our analysis.

Output Parties: The parties that learn the final output. In our case, the intermediary entity plays this role, while no other party, including computational parties, learns any other information besides their original input.

4.2 Identity Authentication Stages

The authentication process is executed as follows:

1. A user claims access and presents to the sensors (hosted by the untrusted entity) his/her biometric inputs and an identification document or a personal credential.
2. After the feature extraction phase the new templates of the raw acquired biometrics are generated. The intermediary entity sends secret shares of user's private information to the computational parties.
3. Matching algorithms are used by the computational parties in order to compare the new template with stored templates. The service providers choose and transmit the corresponding reference thresholds. According to this, the match score is computed in order to represent the closest similarity between raw data and stored modalities.
4. Match scores are normalized following (4).
5. The service providers, according to the reference threshold for the specific user, choose and transmit their private inputs of FAR following (2).
6. For the given performance rates, the normalized match scores are fused, applying the user-specific weighted sum rule (5) that determines the final fusion result. Section 4.3 presents the fusion strategy.
7. The output party determines and secretly shares the threshold of decision to the computational parties. A binary decision result returns to the intermediary entity according to the conditions of (1).

For the studied scenario of authentication specifically, the fact of rejection occurs when the mechanism fails to correspond the raw data to the stored templates at one or any of the databases, or the match scores were poor, resulting a final fusion score that failed to surpass the threshold of decision. For authentication and identification applications, the case where a user is not registered; and his/her biometric data are not stored in unimodal cloud-based service providers, is considered indistinguishable.

4.3 Fusion Strategy

Following the literature on the fusion field [29], we use user-specific performance-dependent weights to signal the performance of each biometric modality after matching, increasing or reducing its importance at the final score. Algorithm 1 presents the selection of weights according to FAR that each user exhibits for a given reference threshold in the unimodal deployments of the service providers in cloud. For setting the weights, the algorithm sorts in ascending order the FAR rates for the given three modalities, such as w_i is the weight for the i^{th} modality, where $w_i \in \{0,1\}$ and $w_i + w_{i+1} + w_{i+2} = 1$ is satisfied. For every given higher value of FAR, a smaller weight is selected for the reduction of the influence of the less reliable modality. On the contrary, for the user-specific FRR-dependent fusion of Algorithm 2, FRR rates and weights are directly proportional parameters that are used to expand the identification range of the mechanism. Note that for three variables, each one with three states: $>, \approx or <$, there are $3^3 = 27$ permutations, where only 13 are possible.

Accuracy.

Our protocol is considered to be as accurate as its non-secure counterpart; and it depends on the values of the selected match scores, FAR, FRR and weights parameters, hence per instantiation. We refer the reader to the experimental results presented in [29], and their conclusions on the topic. Namely that user-specific weighted fusion methods are a beneficial approach when biometric information are provided by different sub-schemes and the performance varies across users. Such a multimodal

Algorithm 1: User-Specific FAR-Dependent Weights.

```
Compare and sort FAR performance rates.
if $FAR_i < FAR_{i+1} \mid FAR_i < FAR_{i+2} \mid FAR_{i+1} < FAR_{i+2}$ then $w_i > w_{i+1} > w_{i+2}$ ;
if $FAR_i \approx FAR_{i+1} \mid FAR_i < FAR_{i+2} \mid FAR_{i+1} < FAR_{i+2}$ then $w_i = w_{i+1}$ AND $w_i > w_{i+2}$ ;
if $FAR_i > FAR_{i+1} \mid FAR_i < FAR_{i+2} \mid FAR_{i+1} < FAR_{i+2}$ then $w_{i+1} > w_i > w_{i+2}$ ;
if $FAR_i > FAR_{i+1} \mid FAR_i \approx FAR_{i+2} \mid FAR_{i+1} < FAR_{i+2}$ then $w_i = w_{i+2}$ AND $w_i < w_{i+1}$ ;
if $FAR_i > FAR_{i+1} \mid FAR_i > FAR_{i+2} \mid FAR_{i+1} < FAR_{i+2}$ then $w_{i+1} > w_{i+2} > w_i$ ;
if $FAR_i < FAR_{i+1} \mid FAR_i < FAR_{i+2} \mid FAR_{i+1} \approx FAR_{i+2}$ then $w_{i+1} = w_{i+2}$ AND $w_{i+1} < w_i$ ;
if $FAR_i \approx FAR_{i+1} \mid FAR_i \approx FAR_{i+2} \mid FAR_{i+1} \approx FAR_{i+2}$ then $w_i = w_{i+1} = w_{i+2}$ ; ▷ equal-weighted fusion
if $FAR_i > FAR_{i+1} \mid FAR_i > FAR_{i+2} \mid FAR_{i+1} \approx FAR_{i+2}$ then $w_{i+1} = w_{i+2}$ AND $w_{i+1} > w_i$ ;
if $FAR_i < FAR_{i+1} \mid FAR_i < FAR_{i+2} \mid FAR_{i+1} > FAR_{i+2}$ then $w_i > w_{i+2} > w_{i+1}$ ;
if $FAR_i < FAR_{i+1} \mid FAR_i \approx FAR_{i+2} \mid FAR_{i+1} > FAR_{i+2}$ then $w_i = w_{i+2}$ AND $w_i > w_{i+1}$ ;
if $FAR_i < FAR_{i+1} \mid FAR_i > FAR_{i+2} \mid FAR_{i+1} > FAR_{i+2}$ then $w_{i+2} > w_i > w_{i+1}$ ;
if $FAR_i \approx FAR_{i+1} \mid FAR_i > FAR_{i+2} \mid FAR_{i+1} > FAR_{i+2}$ then $w_i = w_{i+1}$ AND $w_i < w_{i+2}$ ;
if $FAR_i > FAR_{i+1} \mid FAR_i > FAR_{i+2} \mid FAR_{i+1} > FAR_{i+2}$ then $w_{i+2} > w_{i+1} > w_i$ ;
else return false
```

Algorithm 2: User-Specific FRR-Dependent Weights.

```
Compare and sort the FRR performance rates.
if $FRR_i < FRR_{i+1} \mid FRR_i < FRR_{i+2} \mid FRR_{i+1} < FRR_{i+2}$ then $w_{i+2} > w_{i+1} > w_i$ ;
if $FRR_i \approx FRR_{i+1} \mid FRR_i < FRR_{i+2} \mid FRR_{i+1} < FRR_{i+2}$ then $w_i = w_{i+1}$ AND $w_i < w_{i+2}$ ;
if $FRR_i > FRR_{i+1} \mid FRR_i < FRR_{i+2} \mid FRR_{i+1} < FRR_{i+2}$ then $w_{i+2} > w_i > w_{i+1}$ ;
if $FRR_i > FRR_{i+1} \mid FRR_i \approx FRR_{i+2} \mid FRR_{i+1} < FRR_{i+2}$ then $w_i = w_{i+2}$ AND $w_i > w_{i+1}$ ;
if $FRR_i > FRR_{i+1} \mid FRR_i > FRR_{i+2} \mid FRR_{i+1} < FRR_{i+2}$ then $w_i > w_{i+2} > w_{i+1}$ ;
if $FRR_i < FRR_{i+1} \mid FRR_i < FRR_{i+2} \mid FRR_{i+1} \approx FRR_{i+2}$ then $w_{i+1} = w_{i+2}$ AND $w_{i+1} > w_i$ ;
if $FRR_i \approx FRR_{i+1} \mid FRR_i \approx FRR_{i+2} \mid FRR_{i+1} \approx FRR_{i+2}$ then $w_i = w_{i+1} = w_{i+2}$ ; ▷ equal-weighted fusion
if $FRR_i > FRR_{i+1} \mid FRR_i > FRR_{i+2} \mid FRR_{i+1} \approx FRR_{i+2}$ then $w_{i+1} = w_{i+2}$ AND $w_{i+1} < w_i$ ;
if $FRR_i < FRR_{i+1} \mid FRR_i < FRR_{i+2} \mid FRR_{i+1} > FRR_{i+2}$ then $w_{i+1} > w_{i+2} > w_i$ ;
if $FRR_i < FRR_{i+1} \mid FRR_i \approx FRR_{i+2} \mid FRR_{i+1} > FRR_{i+2}$ then $w_i = w_{i+2}$ AND $w_i < w_{i+1}$ ;
if $FRR_i < FRR_{i+1} \mid FRR_i > FRR_{i+2} \mid FRR_{i+1} > FRR_{i+2}$ then $w_{i+1} > w_i > w_{i+2}$ ;
if $FRR_i \approx FRR_{i+1} \mid FRR_i > FRR_{i+2} \mid FRR_{i+1} > FRR_{i+2}$ then $w_i = w_{i+1}$ AND $w_i > w_{i+2}$ ;
if $FRR_i > FRR_{i+1} \mid FRR_i > FRR_{i+2} \mid FRR_{i+1} > FRR_{i+2}$ then $w_i > w_{i+1} > w_{i+2}$ ;
else return false
```

design can improve its robustness and performance even when its unibiometric systems perform inadequately. Thus, we can conclude that biometric consolidation under the studied scenario offers a higher level of reliability, without compromising overall accuracy.

5 Distributed Multimodal Authentication with MPC

In this section, we give a detailed treatment of our secure distributed protocol for the biometric authentication mechanism and analyze its complexity, security and privacy. To facilitate readability, we divide the different phases of the process into what we call "modules", such as Figure 2 presents. From MPC perspective, this is no more than a conceptual division rather than a tangible task separation. It is important to stress that they together form a unique and uninterrupted arithmetic circuit, with a single output point. The protocol does not suffer from the typical composability related security weaknesses presented by Canetti [11]. Instead, our protocol is designed following the composable hybrid model for MPC introduced in [10] by Canetti as well. To maintain privacy and adhere to the security definition, the modules are adapted such that any leakage of information is avoided, commonly referred as data-obliviousness.

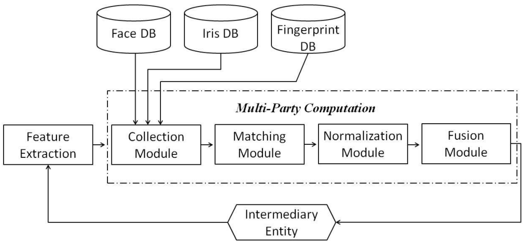

Fig. 2: Flow chart of the mechanism.

5.1 MPC Protocols

Feature Collection Module

1. ***New Template Transmission:*** The intermediary entity extracts the new template, representing the raw acquired biometrics, fixed size N^M for each modality M. The transmission of the new template occurs in shared form, using the underlying sharing mechanism, for instance the Shamir's secret sharing [31], towards the computational parties. Each bit is represented by a different share as follows: $T_i = t_1, ..., t_N$ where $t_j \in \{0, 1\}$ for all $j \in \{1, ..., N\}$.
2. ***Stored Template Transmission:*** The service providers send the binary templates in shared form and the FAR and FRR for the given template to the computational parties. We call the set of stored templates of a given modality O^M, and O_i is the i^{th} binary template where $i \in O^M$.

Matching Module

3. ***Calculate Match Scores:*** The computational parties proceed to compute the match scores between the new template, composed by the raw biometric data, and stored templates of modality M. The scores can be obtained obliviously, by utilizing the Hamming Distance algorithm to calculate distances between the new and stored template without any information leakage. As shown by Protocol 3, this can be

achieved by performing N^M multiplications, where N^M is the size of the template. The result of this phase is the vector of Hamming Distance scores H^M, where $[h]_i^M$ is new template score T versus the stored O^j, for all j delivered by the service provider.

Protocol 3: Hamming Distance Protocol.

```
Input: Vector $[T]$ of, Vector $[O]$ where $[T]$ and $[O]$ are of size $N$.
Output: Hamming Distance $[h]$
for $i \leftarrow 1$ to $N^M$ do
    $[v]_i^h \leftarrow [T]_i + [O]_i - 2 \cdot ([T]_i \cdot [O]_i)$;
end
$[h] \leftarrow \sum_{i=1}^{N^M} [v]_i^h$;
```

4. ***Select Match Scores:*** The protocol selects the best suitable score from vector H^M for every modality M. This unique value per modality is the one that corresponds to the higher/lower score in each vector H^M. We call the vector, composed of the higher/lower scores of each modality S^M, where $[s]_i^M$ represents the score of a biometric in the set of all modalities M in the i^{th} position of the vector S^M. To identify such values and to construct the vector S^M in an oblivious fashion, it suffices to follow Protocol 4.

Protocol 4: Match Score Selection Protocol.

```
Input:
Output: Vector $S^M$
for $i \leftarrow 1$ to $M$ do
    $[\delta] \leftarrow \perp$; for $j \leftarrow 1$ to $|H_i^M|$ do
        $[c] \leftarrow [\delta] \overset{?}{<} [h_{ij}^M]$;
        $[\delta] \leftarrow ([h_{ij}^M] - [\delta]) \cdot [c] + [\delta]$;
    end
    $[s]_i^M = [\delta]$;
end
```

Normalization Module

5. ***Min-Max Normalization:*** Since the set of scores S^M contains inputs in different domains, our protocol includes the *Min-Max Normalization* technique in the normalization module. To reduce the complexity of the protocol, the normalized score is expressed in fractional form and provided as a tuple $([n],[d])^{S^M}$, where $[n]$ stands for the numerator of the fraction and $[d]$ for its denominator. This value can be obliviously calculated following equations (8) and (9) respectively.

$$[n]_i^M \leftarrow [s]_i^M - [min]^M \tag{8}$$

$$[d]_i^M \leftarrow [max]_i^M - [min]_i^M \tag{9}$$

Fusion Module

6. ***Oblivious Ranking of Scores:*** The selected scores for normalization S_1^M have to be sorted in ascending order based on their FAR/FRR ($[F]$) with no information leakage. Oblivious sorting between these secretly shared scores can be achieved with

a simplified sorting network. In this case, the comparison gates use the privacy-preserving comparison functionality provided by the $\mathscr{F}_{ABB}$. Given that the mechanism considers three modalities, the sorting network described by Figure 3 suffice. Note that the sorting network should be adapted if more modalities or scores are considered.

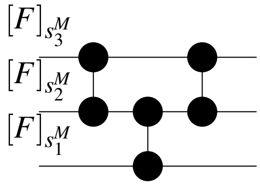

Fig. 3: A $[x] \overset{?}{<} [y]$ three-gate network for oblivious sorting

7. ***Fusion Proportions:*** To perform fusion, a set of weights is provided to the mechanism by the untrusted intermediary entity and applied to the normalized match scores. In our user-specific weighted score level fusion strategy, weights represent the performance rates for each user of the unimodal cloud-based schemes (see Section 4.3). From Algorithms 1 and 2, we discern only four possible configurations; summarized in general forms as: i) $w_i > w_{i+1} > w_{i+2}$ ii) $w_i = w_{i+1}$ AND $w_i > w_{i+2}$ iii) $w_i = w_{i+1} = w_{i+2}$ iv) $w_i = w_{i+1}$ AND $w_i < w_{i+2}$. For equal weights, the protocol has to react correctly in case two or more normalized scores have the same FAR/FRR ($[F]$) rates. In this case, the intermediary entity provides the computational parties with the matrix of weights W_{ij} in shared form, such that: each row w_i represents a different weight configuration and element $[w]_{ij}$ corresponds to the relevant weight for the normalized score $[s]_j^M$, under configuration j. Protocol 5 shows how to obliviously apply proportions for each configuration. Weights have to be given in a fractional form and in a predefined order.

Protocol 5: Fusion Proportion.

```
Input:
Output: Vector $S^M$
$[c]_1 \leftarrow [F]_{s_1^M} \overset{?}{=} [F]_{s_2^M}$;
$[c]_2 \leftarrow [F]_{s_2^M} \overset{?}{=} [F]_{s_3^M}$;
$[w]^M \leftarrow [w]_1$;
for $j \leftarrow 1$ to $M$ do
    $[w]_j^M \leftarrow ([w]_{2,j} - [w]_j^M) \cdot ([c]_1 \cdot ([c]_1 + [c]_2 - 2 \cdot ([c]_1 \cdot [c]_2))) + [w]_j^M$;
    $[w]_j^M \leftarrow ([w]_{3,j} - [w]_j^M) \cdot ([c]_2 \cdot ([c]_1 + [c]_2 - 2 \cdot ([c]_1 \cdot [c]_2))) + [w]_j^M$;
    $[w]_j^M \leftarrow ([w]_{4,j} - [w]_j^M) \cdot ([c]_1 \cdot [c]_2) + [w]_j^M$;
    $[s]_j^M \leftarrow [s]_j^M \cdot [w]_j^M$;
end
```

8. ***Fusion aggregation:*** Once the proportions are applied to the score vector S^M, they are aggregated. The result is also represented by a $([n],[d])^{\mathtt{out}}$ tuple. Given that each normalized S^M score is represented by a similar fractional, in order to be able to aggregate them, it suffices to calculate the following equations:

$$[n^{\mathtt{out}}] \leftarrow [d]_{s_2^M} \cdot [d]_{s_3^M} \cdot [n]_{s_1^M} + [d]_{s_1^M} \cdot [d]_{s_3^M} \cdot [n]_{s_2^M} + [d]_{s_1^M} \cdot [d]_{s_2^M} \cdot [n]_{s_3^M} \tag{10}$$

$$[d^{\mathtt{out}}] \leftarrow [d]_{S_2^M} \cdot [d]_{S_3^M} \cdot [d]_{S_1^M} \tag{11}$$

9. ***Result Deliverance:*** The secret shares of the fusion result are transmitted by the computational parties towards the intermediary entity. The combination of the shares is performed by the entity; this process is not computational demanding (a polynomial interpolation). The entity is the only one who access the Protocol `out`. The entity could perform the fractional division to obtain a value $\in \{0,1\}$.
10. ***Concealing Fusion Score:*** If the application requires the score of fusion to be concealed; this can be achieved as follows: the intermediary entity transmits, in shared form, the threshold of decision $[\perp]$ in fractional representation to the computational parties. The parties will be in charge of performing the comparison by cross-multiplying numerators, denominators and calling to the comparison functionality of our $\mathscr{F}_{ABB}$. The resulting shares are transmitted towards the entity, for their interpolation, yielding only $\{0,1\}$ values.

5.2 Complexity

The complexity of MPC protocols is measured in communication rounds, that is defined as a message exchange step between the computational parties. A multiplication protocol can be implemented such that it requires one computational round [16]. The same holds for sharing or reconstructing a value. On the other hand, additions have no communication cost associated and in the context of this work can be executed for "free". Although comparisons can be implemented in constant time, similar to Catrina and Hoogh [12], they are typically more expensive than multiplications, for instance they depend on parallelization, the actual number of multiplications, typically grows on the size of the input.

The *Feature Collection Module* takes place during the first two stages, there is a constant round complexity $\mathscr{O}(1)$. The *Matching Module* uses the Protocols 3 and 4; both present linear asymptotic complexities on the sides of their respective inputs: $\mathscr{O}(N^M)$ for the former, and $\mathscr{O}(|H|^M)$. Protocol 3 has to be executed at least $|O^M|$ times, yielding an overall complexity of $\mathscr{O}(|O^M| \cdot N^M)$. In addition to that, the *Normalization Module* fifth stage and *Fusion Module* 6-10 stages have constant time complexity $\mathscr{O}(1)$. This is a result of the number of biometric modalities that is fixed. In our protocol, inequality tests are only used when is strictly necessary; and they can be executed in constant rounds [12], but they are more expensive in practice.

5.3 Security and Privacy Analysis

Our protocol offers perfect security against active and passive adversaries under the information-theoretic model. We proceed to show how our protocol provides the achievable security under MPC described in Section 3.5, *Definition* 1. The *matching*, *normalization and fusion modules* are designed in a data-oblivious fashion, from the perspective of the computational parties and dealers. In other words, there is no information leakage at any stage of the protocol. If a computational party would be corrupt, it would not receive the protocol output, nor the available intermediate values for any operation performed by our $\mathscr{F}_{ABB}$, making, in this case, the simulation trivial. This also holds for the case of a corrupted dealer. Given that our protocol can be assembled as a unitary arithmetic circuit, made of addition and multiplication gates, the simulation is achieved by invoking the simulators of the gates in the predefined order by the arithmetic circuit. To such a degree, the view of the adversary over our protocol

π would not compromise any input from the honest parties, as long as the security properties of the underlying MPC primitives hold. Composability is achieved by the properties of the hybrid model described in [10]. Given that no other information is made available to any involved party, (besides their corresponding private inputs) and the binary output to the entity, we fulfill *Definition* 1. Practically, the security depends exclusively on the MPC primitives, used for being implemented upon (schemes that implement the $\mathscr{F}_{ABB}$ functionality). We mention the perfect security against passive and active adversaries of completeness theorems [3], adhering to the corresponding set of assumptions, such as private channels. This is also true for our MPC Protocols or any related protocol that is secure under composition.

6 Efficiency

The asymptotic complexity of our protocol is relatively low, as a result of the linear complexity on the templates' size. However, in realistic cases, factors, such as the cryptological primitives and the execution environment play a roll. As previously stated, a multiplication requires a communication round, whereas a comparison requires several (constant), even when its computation is parallelized [12]). We have compatibilized the number of multiplications that are needed in total for a fixed standard template size. Additionally, we measured the average execution time for the amount of multiplications and the necessary comparisons. We use a custom implementation of the BGW protocol, taking into consideration the improvements on network flow problems [1].

***E*nvironment Setting.**

We utilize the limited RAM memory $\approx$ 500 KB per instance, where each party instance takes two separate computational threads in order to manage communication and cryptological tasks separately. On the cryptographic (MPC) background and adversarial model, we consider an honest but curious setting, using Shamir's secret sharing [31], linear addition, and BGW for multiplication [3, 16]. Comparisons were implemented according to the results introduced in [12]. We consider input sizes of 32 bits.

Execution environment: We have run our computational evaluations using a 64-bit server equipped with 2*2*10-cores Intel Xeon E5-2687 at 3.1GHz.

Parties: We assume the same scenario for the mechanism put forward by this paper, considering three computational parties, under the theoretic information model (private channels). All our tests were executed on the same server; hence network latency was not considered.

Template sizes: We used for our experiments: **i)** Face: 1024 bits, **ii)** Iris: 2048 bits and **iii)** Fingerprint: 4096 bits (see *"Encyclopedia of Biometrics"* [21]). We have chosen relatively high template sizes to be able to easily adjust the protocol to realistic biometric deployments. Finally, we consider the case where the protocol is provided with five stored templates per modality for analysis.

***C*omputational Results.**

Following the results presented in Section 5, we accounted for the total number of operations that require communication rounds, specifically, multiplications and comparisons used by our protocol, (addition, is a linear operation and it is well established that the cost is negligible [1, 3, 8, 15]). Table 1 shows the number of operations per module, where σ_{M} is equal to the templates' size in bits, and γ_{M} is the number of the available templates for the analysis.

Given that our protocol uses an arithmetic circuit approach, our tests had to account for the cost of each atomic operation. Table 2 shows the CPU times for the atomic MPC operations. The results reflect the average CPU time of $_{+}2 \times 10^7$ multiplications and 1.6×10^6 inequality tests. Given the limited number of equality tests i.e., 2, the impact of the difference in performance between a comparison and an equality test is negligible. Table 3 presents the details of the amortized computational time for our circuit size.

The overall execution time of the protocol for multimodal user authentication is less than a second. Bear in mind that for some applications, the number of templates and the size are smaller than the ones considered by our experimentation.

Table 1: Total atomic Operations

Stage	**Multiplications**	**Inequality Tests**
Feature Collection	$\sum_{i=1}^{M} \sigma_i \cdot \gamma_i = 35840$	$\sigma \cdot \gamma = 15$
Normalization	–	–
Fusion	17	6
Total:	35857	21

Table 2: CPU time for atomic operations

Operation	**CPU Time in Secs**
Multiplications	2.08×10^{-5}
Inequality test	2.5×10^{-3}

Table 3: Overall CPU time

Operation	**CPU Time in Secs**
Multiplications	0.746
Inequality tests	0.054
Total:	0.8

7 Usability and Advantages

The proposed secure user-specific FAR-dependent fusion can be used for mobile applications, for instance, in biometric-based log in to ePayment accounts. Similarly, it can be used for identification processes in surveillance oriented architectures. The mechanism of Section 4 can be adapted to perform without requesting the user's identity references, following (3) and setting up the FRR-dependent fusion strategy of Algorithm 2. In the context of privacy, stored templates, matching, normalized and fusion scores are inaccessible to all parties. There is no information leakage towards the service provides who can only learn the fact that a query for a given user was made, and they do not gain access to the computational result. Thus, our privacy-aware design can be the first step for biometric solutions in cloud-based architectures with high security and privacy standards.

8 Limitations

Our paper tackles the challenges of a design that links the pattern recognition area with applied cloud cryptography. However, like any other study, our work has some limitations. Regarding the fusion strategy, one clear deficiency is the assumptions about the overall accuracy that are only based on the experimental studies on user-specific fusion and equal-weighted methods being found in the literature. This is mainly happens due to the limited availability of biometric datasets and the time-consuming process of training. The privacy-preserving protocol has been built upon the requirements put in place by the use of secure Multi-Party Computation. As it stands, the protocol is designed for the authentication procedure. However, it can operate in identification mode (at a relatively high cost for database extraction); it is not practically viable for time-consuming processes on large-scale biometric databases. Finally, we have limited it in order to work with Hamming Distance algorithms. The use of more complex biometric matching processes remains an open question and can affect the complexity and efficiency.

9 Conclusion and Future Work

In this paper, we presented a simple and secure protocol for biometric-based identity authentication in an untrusted distributed environment. The operation is dynamic and it may be easily extended to adjust different classifiers, metrics, rules and update the parameters. The limitation is that by building a more sophisticated protocol; the computation and communication complexity may effect on the overall accuracy. Furthermore, it is a part of authors' future work to explore how the combination of a variety of thresholds over the range of FAR and FRR effects on the performance. This can be achieved by training the datasets and validate the user-specific performance-dependent fusion strategy, in order to technically present its usability. Further work considers the extension of the protocol to provide efficient identification (taking into account the size of the unimodal repositories), as well as statistical anonymization of queries and advanced techniques to hide the verified identities from service providers. Trade-offs between security and efficiency should be assessed as well.

References

[1] A. Aly. *Network Flow Problems with Secure Multiparty Computation.* PhD thesis, Université Catholique de Louvain, IMMAQ, 2015.

[2] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. High-throughput semi-honest secure three-party computation with an honest majority. In *ACM SIGSAC*, pages 805–817, 2016.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *STOC*, pages 1–10. ACM, 1988.

[4] R. Bendlin, I. Damgård, C. Orlandi, and S. Zakarias. Semi-homomorphic encryption and multiparty computation. In *EUROCRYPT*, volume 6632 of *LNCS*, pages 169–188. Springer, 2011.

[5] M. Blanton and M. Aliasgari. Secure outsourced computation of iris matching. *Journal of Computer Security*, 20(2-3):259–305, 2012.

[6] M. Blanton and S. Saraph. Oblivious maximum bipartite matching size algorithm with applications to secure fingerprint identification. In *Proceedings, Part I - ESORICS 2015*, pages 384–406, 2015.

[7] D. Bogdanov, S. Laur, and J. Willemson. Sharemind: A Framework for Fast Privacy-Preserving Computations. In *Proceedings of the 13th ESORICS*, volume 5283 of *LNCS*, pages 192–206. Springer, 2008.

[8] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft. Secure multiparty computation goes live. In *Financial Cryptography*. Springer, 2009.

[9] J. Bringer, H. Chabanne, and A. Patey. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends. *IEEE Signal Process. Mag.*, 30(2):42–52, 2013.

[10] R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.

[11] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS '01*, pages 136–145, 2001.

[12] O. Catrina and S. de Hoogh. Improved primitives for secure multiparty integer computation. In *SCN*, pages 182–199, 2010.

[13] I. Damgård, M. Fitzi, E. Kiltz, J. B. Nielsen, and T. Toft. Unconditionally secure constant-rounds multiparty computation for equality, comparison, bits and exponentiation. In *TCC*, pages 285–304, 2006.

[14] I. Damgård and J. B. Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. In *CRYPTO*, volume 2729 of *LNCS*, pages 247–264. Springer, 2003.

[15] I. Damgård, V. Pastro, N. P. Smart, and S. Zakarias. Multiparty computation from somewhat homomorphic encryption. In *CRYPTO*, volume 7417 of *LNCS*, pages 643–662. Springer, 2012.

[16] R. Gennaro, M. O. Rabin, and T. Rabin. Simplified vss and fast-track multiparty computations with applications to threshold cryptography. In *PODC '98*, pages 101–111. ACM, 1998.

[17] A. M. Hamad, R. S. Elhadary, and A. O. Elkhateeb. Multimodal biometric identification using fingerprint, face and iris recognition. *Intern.l Journal of Inf. Science and Intell. System*, 3(4):53–60, 2014.

[18] A. K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38(12):2270–2285, 2005.

[19] M. Keller, E. Orsini, and P. Scholl. Mascot: Faster malicious arithmetic secure computation with oblivious transfer. In *Proceedings of ACM SIGSAC*, CCS '16, pages 830–842. ACM, 2016.

[20] E. J. Kindt. *Privacy and Data Protection Issues of Biometric Applications-A Comparative Legal Analysis*. Springer NL, 2013.

[21] S. Z. Li and A. K. Jain, editors. *Encyclopedia of Biometrics, Second Edition*. Springer US, 2015.

[22] H. Lipmaa and T. Toft. Secure equality and greater-than tests with sublinear online complexity. In *ICALP (2)*, pages 645–656, 2013.

[23] T. Lorünser, T. Länger, and D. Slamanig. Cloud security and privacy by design. In *E-Democracy - Citizen Rights in the World of the New Computing Paradigms - 6th Inter. Conference, E-Democracy 2015 Proceedings, Athens, Greece*, pages 202–206, 2015.

[24] J. Malik, D. Girdhar, R. Dahiya, and G. Sainarayanan. Reference threshold calculation for biometric authentication. *Image, Graphics and Signal Processing*, 2:46–53, 2014.

[25] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT*, pages 223–238, 1999.

[26] J. Palanichamy and R. Marimuthu. A novel image alignment and a fast efficient localized euclidean distance minutia matching algorithm for fingerprint recognition system. *Int. Arab J. Inf. Technol.*, 13(3):313–319, 2016.

[27] S. Pan, S. Yan, and W. Zhu. Security analysis on privacy-preserving cloud aided biometric identification schemes. In *Information Security and Privacy - 21st Austral. Conf., Proc.*, pages 446–453, 2016.

[28] H. Rai and A. Yadav. Iris recognition using combined support vector machine and hamming distance approach. *Expert Syst. Appl.*, 41(2):588–593, 2014.

[29] A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*. Springer-Verlag NY, Secaucus, NJ, USA, 2006.

[30] A. Ross, A. Rattani, and M. Tistarelli. Exploiting the "doddington zoo" effect in biometric fusion. In *Proceedings of the 3rd IEEE International Conference on Biometrics*, BTAS'09, pages 264–270. 2009.

[31] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[32] C. Toli, A. Aly, and B. Preneel. A privacy-preserving model for biometric fusion. In *Proceedings Cryptology and Network Security - 15th Inter. Conference, CANS 2016*, pages 743–748, 2016.

[33] Q. Wang, S. Hu, K. Ren, M. He, M. Du, and Z. Wang. Cloudbi: Practical privacy-preserving outsourcing of biometric identification in the cloud. In *ESORICS*, pages 186–205, 2015.

[34] C. Xiang, C. Tang, Y. Cai, and Q. Xu. Privacy-preserving face recognition with outsourced computation. *Soft Comput.*, 20(9):3735–3744, 2016.

[35] J. Yuan and S. Yu. Efficient privacy-preserving biometric identification in cloud computing. In *INFOCOM*, pages 2652–2660, 2013.