SIPPA Approach Towards a Privacy Preserving Voice-based Identity Solution

Bon K. Sy
Computer Science Department, Queens College and University Graduate Center/CUNY, Flushing, NY 11367, U.S.A.

Abstract - *The focus of this project is the development of a privacy preserving identity solution. A traditional identity solution associates an individual with a user identity and a user credential for the purpose of authentication, authorization and accounting. One of the underlying assumptions of a traditional identity solution is the ability to secure and to prevent tampering with the association between an individual and the corresponding user information. If this assumption does not hold, one can no longer guarantee the integrity of the system for facilitating authentication, authorization and accounting. The contribution of this project is a novel approach that removes the system reliance on the assumption. Specifically, our approach employs SIPPA to achieve credential regeneration on the fly that eliminates the need for storing such information; thereby avoiding the risk inherent in the assumption.*

Keywords: Voice-based key generation; Privacy aware authentication.

1 Introduction

The objective of this project is to develop a privacy preserving identity solution based on SIPPA — Secure Information Processing with Privacy Assurance. SIPPA [1,2] is a two-party secure computation method for comparing the private data of two parties without each party disclosing their private data to each other.

In our SIPPA based solution, personal private information or credential information for authentication will not be stored in plain. Private sensitive information will be derived on demand. This eliminates the risk on information leak since no private sensitive information is stored in the first place. Therefore, information privacy is assured. Furthermore, SIPPA protocol execution produces two artifacts; the degree of similarity resulted from the comparison of the private data, which can be used for authentication purpose, and the helper data useful for the information processing needed to regenerate the credentials for authentication/authorization. Since the SIPPA protocol has been analyzed under different security models and situations, the behavior and the security of the identity solution can be derived from that of the SIPPA protocol, and formally analyzed and assessed accordingly.

In this project, a particular embodiment of the proposed identity solution utilizing biometric voice signature and mobile device will be described — although the embodiment could be based on any modalities and devices. The rest of the paper will be organized as the followings. In section 2 we will give a summary on the system architecture of the identity solution, the formulation on the system elements and the information used for authentication. In section 3 an overview on the state-of-the art, and the context under which this project is related to the state-of-the-art, will be given. In section 4 the theory of SIPPA, and the application of SIPPA to realize the SIPPA-based identity solution under real world security model will be presented. In section 5 the system implementation and the experimental result will be detailed, which is then followed by the conclusion that briefly describes our future work.

2 Formulation and System Architecture

One of the unique characteristics of SIPPA is to allow one party to reconstruct the private data of the other party when their data are "sufficiently" similar. In the SIPPA reconstruction phase, the *server* party provides helper data for the *client* party to reconstruct server data that preserve perfect accuracy, or an accuracy proportional to the similarity of the private data of both parties. This consequently allows us to realize an identity management workflow not present in a traditional solution, which can be described as below:

- Sensitive credential information for authentication/ authorization is encoded by the personal private information of an individual.
- Only the encoded information is stored. Sensitive credential information and personal private information are never stored. But the credential information can be reconstructed during the execution of the SIPPA protocol — when the personal private information presented by an individual is sufficiently similar to that used for encoding the sensitive credential information.

In this project, the identity of an individual is characterized by three facets [3]: (i) *what one knows*, referred to as a UID (Universal ID) — a unique ID generated by the system based on personal information PID such as phone number or birth date, (ii) *what one has*, referred to as a DID (Device ID) such as a personal mobile phone or a device serial number, and (iii) *what one is*, referred to as BID (biometric

ID) such as the biometric voice, face or fingerprint. More specifically, the identity of an individual is a 3-tuple composed of DID, a biometrically encoded encryption key — BID+K, and the decryption of the encrypted hash on UID; where K is a secret key. Formally, an identity is then represented by a 3-tuple: <DID, BID+K, Dec(K, Enc(K, Hash(UID))>.

The architecture of our system consists of 3 components; namely, a voice gateway (VG), an Enrollment Module (EM) comprised of SIPPA server and a local database, and an Identity Storage and Verification Module (ISVM) comprised of SIPPA client and a centralized database.

In our design, the local database of the enrollment module stores the encryption/decryption secret K. The centralized database stores the identity information. For privacy assurance, the EM and the ISVM do not directly share with each other the information in their databases. Furthermore, the two modules do not even have to treat each other as a trust worthy party. This is different from the traditional identity solution where the trustworthiness [4] between the system components similar to that of EM and ISVM is assumed.

3 Literature Review

Privacy preserving authentication is an active research topic in many different domains [5-8]. In general, the goal is to minimize disclosure on the identity information of an individual, certain content information about an identity such as phone number or birth date, the linkability of the identity information and its usage, the issuer of the identity [9], and the data matching [10].

The research in this area can broadly be classified into cryptographic based and non-cryptographic based approach. In cryptographic based approach, Public Key Infrastructure (PKI) [16] to issue X.509 certificate with private/public key pair for encryption and message signing [11], one-way hash [12], zero-knowledge proof [13], and commitment scheme are the basic building blocks for developing a privacy preserving identity management solution. Attribute Based Credential for Trust (ABC4Trust) [14] is an exemplary state-of-the-art that allows an individual to use not one public key, but possibly multiple public keys. In addition, certificate is based on the individual's secret key, attributes that may be hidden from the Certificate Authority [15], and proof of knowledge of certificate about identical secret key used in different certificates of the individual. This is different from the conventional Public Key Infrastructure in that a certificate is based on an individual's public key, and the certificate (thus the information in the certificate) is revealed. Although ABC4Trust is an improvement over the traditional approach, the implicit deployment assumption of ABC4Trust is that a secure and trustworthy issuer (typically a Certificate Authority) exists and is always available.

An interesting aspect of non-cryptographic based approach is the idea of Privacy Preserving Data Matching (PPDM) as exemplified by Scannapieco et al [10]. The key idea behind PPDM is the use of an embedding space SparseMap [20] that preserves the similarity distance between two data objects in the metric space. The embedding space is constructed by using a subset of data objects serving as a reference set, and the distance between two data objects is mapped to two distance measures in the metric space; i.e., between a data object and the reference set, and the other data object and the reference set. Through triangular inequality, a lower bound distance measure between the two data objects can be obtained; thus realizing the privacy preserving approximate matching.

Our proposed SIPPA approach towards a privacy preserving voice-based identity solution shares similar characteristics to the research just mentioned. Yet it distinguishes itself with characteristics that are unique and attractive for privacy preserving authentication. In both our approach and ABC4Trust, Public Key Infrastructure (PKI) is required. The main difference lies on the extent that the PKI is used. In ABC4Trust, a key characteristic is to issue every user multiple keys so that privacy protection can be achieved. In our proposed approach, Certificate Authority is only required for the key infrastructure; i.e., the Voice Gateway (VG), Enrollment Module (EM), and Identity Storage and Verification Module (ISVM). Especially in our specific applications of SIPPA approach, it is not clear how a trustworthy environment can be established in order for every user to securely receive the private and public keys needed as in ABC4Trust. With respect to Hash Lock [17], the main difference is the choice of cryptographic primitives. In our SIPPA approach, we require cryptographic primitive to be not only semantically secure, but also to belong to the class of homomorphic encryption [21] for computation over the encrypted domain; e.g., Paillier encryption [22] with homomorphic additive property. By definition, cryptographic primitive that has semantic security property such as Paillier encryption does not encrypt a message to the same cipher text; thus deterring Chosen-Plain text Attack (CPA) [23]. The enforcement of semantic security in Hash Lock, however, will prevent the protocol of Hash Lock to work properly.

In reference to PPDM, our approach also tackles the problem of privacy preserving data comparison through an alternative metric space. However, our approach is completely different from that of PPDM. While PPDM relies on SparseMap for the construction of the embedding space, SIPPA maps the data objects to their Eigen space through the symmetric matrices derived from the data objects. More importantly, PPDM aims at privacy preserving approximate matching. SIPPA, on the other hand, aims at utilizing the mathematical properties implicit in the Eigen space mapping that allows precise reconstruction of the private data based on sufficiently similar data objects.

4 Theory, Practice & Security Analysis

An innovation of this project is to develop an identity solution that incorporates privacy assurance with the following properties:

- ● The identity of an individual is multi-facet and is based on *what one knows* (UID), *what one has* such as a mobile phone, and *what one is* such as biometric voice signature.
- ● A system that is fail-safe; i.e., it preserves the privacy of personal information — even if the system is compromised.

Our approach towards the development of a fail-safe system is to employ cryptographic key to protect the confidentiality of the UID/DID. The cryptographic key is generated, used and discarded. It is never stored. Only the biometrically encoded encryption key K+BID is stored; where BID is a biometric ID as discussed in section 2. The key is regenerated based on the biometrics of an individual whenever it is needed. Given a biometric sample S, the pre-processing step of the regeneration is a simple cancellation operation; i.e., (K + BID) – S.

Note that the cryptographic key K can be perfectly regenerated in the pre-processing step if BID = S. However, personal biometrics can seldom be reproduced identically. Therefore, in general BID and S are different. When BID and S are from the same individual, the error incurred by BID-S is small. Otherwise BID-S is relatively large.

4.1 SIPPA Theory

SIPPA [1,2] is a 2-party secure computation protocol [24] where a client party can reconstruct <u>source data</u> of a server party under the following conditions:

1. The client party must possess some <u>client data</u> that is a "sufficiently good approximation" of the source data, in order to initiate the SIPPA process.
2. Rather than revealing the source data of the server party to the client party, only some <u>helper data</u> related to the Eigen components of the source data is provided (by the server party) to the client party for reconstructing the source data.

In our case, the SIPPA client retrieves K+BID from the centralized database, and performs the cancellation K+BID-S. K is stored in the local database of the SIPPA server. Through the execution of the SIPPA protocol, the SIPPA client will be able to reconstruct K if (K+BID-S) and K are sufficiently similar. The formulation, the key results of SIPPA summarized as two theorems, and the algorithmic steps are already reported elsewhere [1,2]. Nonetheless, they are re-introduced to make this paper self-sufficient.

Let P1 and P2 be the SIPPA server and client respectively. Let **de** and **dv** be the column vector representing private data of P1 and P2 respectively. Let $(\lambda_{de}\ \mathbf{v_{de}})$ and $(\lambda_{dv}\ \mathbf{v_{dv}})$ be the 2-tuples of the most significant Eigen value and the corresponding unity normalized Eigen vector of the matrices $\mathbf{de}\cdot\mathbf{de}^T$ and $\mathbf{dv}\cdot\mathbf{dv}^T$ respectively.

<u>**Theorem 1:**</u> Consider $(\mathbf{de}\cdot\mathbf{de}^T + \mathbf{dv}\cdot\mathbf{dv}^T)x = \lambda_{de}\mathbf{v_{de}} + \lambda_{dv}\mathbf{v_{dv}}$, the solution $\mathbf{x} = \mathbf{v}$ satisfying $(\mathbf{de}\cdot\mathbf{de}^T + \mathbf{dv}\cdot\mathbf{dv}^T)\mathbf{v} = \lambda_{de}\mathbf{v_{de}} + \lambda_{dv}\mathbf{v_{dv}}$ has a unity scalar projection onto the unity normalized $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$, and is a bisector for the interior angle between $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$.

<u>**Theorem 2:**</u> Consider $(\mathbf{de}\cdot\mathbf{de}^T + \mathbf{dv}\cdot\mathbf{dv}^T)\mathbf{x} = \lambda_{de}\mathbf{v_{de}} + \lambda_{dv}\mathbf{v_{dv}}$, **de** can be efficiently reconstructed − with an accuracy proportional to the closeness between $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$ − by a party with **dv**, $\lambda_{dv,,}$ and $\mathbf{v_{dv}}$ when (i) the interior angle between $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$ is less than 90 degree and (ii) the party is given **x** and $\lambda_{de}/\ \mathbf{de}^T\cdot\mathbf{x}$. Specifically, $\mathbf{de} = (\mathbf{est\_v_{de}}/|\ \mathbf{est\_v_{de}}\ |)(\lambda_{de}/\ \mathbf{de}^T\mathbf{x})$; where

$\mathbf{est\_v_{de}} = \mathbf{v_{dv}}+[|\mathbf{v_{dv}}|\cdot\tan(2\cos^{-1}(\mathbf{v_{dv}}\cdot\mathbf{x}/(|\mathbf{v_{dv}}|\cdot|\mathbf{x}|)\ ))]\cdot[(\mathbf{x}-\mathbf{v_{dv}})/|\mathbf{x}-\mathbf{v_{dv}}|]$

Readers interested in the proof of the two theorems above are referred to our other publication elsewhere [1].

<u>**SIPPA Protocol:**</u>

<u>**Step 1:**</u> Derive, by the respective party, the most significant eigenvalue and its corresponding unity-normalized eigenvector of $\mathbf{de}\cdot\mathbf{de}^\mathbf{T}$ and $\mathbf{dv}\cdot\mathbf{dv}^\mathbf{T}$. This step yields $(\lambda_{de}\ \mathbf{v_{de}})$ for SIPPA server and $(\lambda_{dv}\ \mathbf{v_{dv}})$ for SIPPA client.

<u>**Step 2:**</u> Compute **x** such that $(\mathbf{de}\cdot\mathbf{de}^T + \mathbf{dv}\cdot\mathbf{dv}^T)\mathbf{x} = \lambda_{de}\mathbf{v_{de}} + \lambda_{dv}\mathbf{v_{dv}}$ utilizing SLSSP. The vector **x** is known to both parties following SLSSP. The details on SLSSP are reported elsewhere [1].

<u>**Step 3:**</u> The party that wishes to determine the deviation between its eigenvector and the other party's eigenvector can do so utilizing ***x*** (derived in step 2). Suppose that the party with $\mathbf{v_{de}}$ wishes to determine the angular deviation between $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$, this can be done by obtaining the angle between $\mathbf{v_{de}}$ and ***x***. i.e. $\cos^{-1}(\mathbf{v_{de}}\cdot\mathbf{x}/(|\mathbf{v_{de}}|\cdot|\mathbf{x}|))$. The angular deviation between $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$ is then $2\cos^{-1}(\mathbf{v_{de}}\cdot\mathbf{x}/(|\mathbf{v_{de}}|\cdot|\mathbf{x}|))$ — due to theorem 1.

<u>**Step 4:**</u> If **de** and **dv** are sufficiently similar as determined by either the angular distance or the Euclidean distance between vectors $\mathbf{v_{de}}$ and $\mathbf{v_{dv}}$ as measured by some pre-defined threshold, proceed to send the helper data: $(\lambda_{de})^{0.5}$ for a perfect reconstruction.

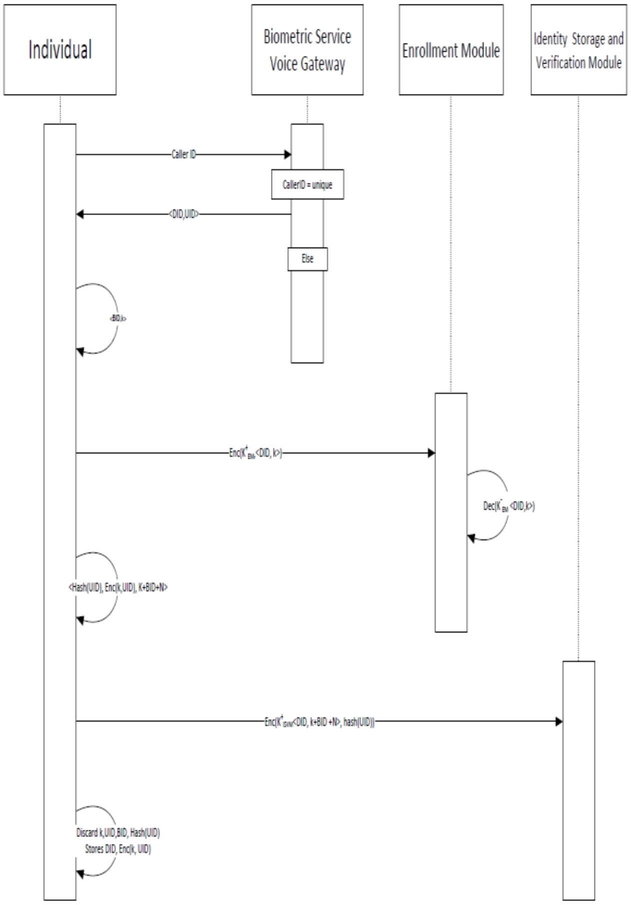
<u>**Step 5:**</u> Derive estimated $\mathbf{v_{de}}$ - $\mathbf{est\_v_{de}}$ as stated in theorem 2, and then derive $\mathbf{de} = (\mathbf{est\_v_{de}}/|\mathbf{est\_v_{de}}|)(\lambda_{de})^{0.5}$ because (1) $\lambda_{de}=\mathbf{de}^T\cdot\mathbf{de} = |\mathbf{de}|^2$ (from Theorem 1), (2) $\mathbf{de}/|\mathbf{de}| = \mathbf{v_{de}}$ or $\mathbf{de} = |\mathbf{de}|\cdot\mathbf{v_{de},}$ (from Theorem 1), and (3) $\mathbf{est\_v_{de}}/|\mathbf{est\_v_{de}}| = \mathbf{v_{de}}$ (from Theorem 2).

4.2 SIPPA-based Identity Management

In our application of SIPPA, the server data **de** is a vector of 20x1 of real numbers in the range [0,1]. The secret K stored in the local database of SIPPA server is a 20x1 vector of normalized integer values that are a fixed point representation of the real numbers. During an encryption/decryption, an AES key is generated from the MD5 hash of K. The client data **dv** is also a vector of 20x1 of real numbers derived from (K+BID)-S; where BID and S each is a normalized 20x1 vector representing a biometric voice template of cepstrum coefficient [29] in the frequency range of 0-4KHZ based on Mel scale using triangular filters.

Protocol for identity enrollment:

1. An individual established connection through a secure authenticated channel [25] to download client-side software such as applet capable of biometric voice signature extraction and cryptographic key generation.
   Note: In a secure authenticated channel, messages can be eavesdropped, relayed and replayed, but not altered.
2. The individual submits – through the downloaded client-side software – to the voice gateway his phone number that can be recognized as a caller ID for a call back.
3. If the caller ID is valid and unique, the voice gateway signs the caller ID and calls the individual back. It returns the signed version of the caller ID as the device ID – DID, as well as a token T (e.g. a random number or a timestamp). In addition, the voice gateway also sends T to ISVM.
   Note: The call back process, and the generation of T and sharing with ISVM complete the commitment scheme.
4. The individual records his/her voice sample and uses the downloaded client-side software to extract the individual's voice signature as his biometric ID – BID. The client-side software also generates a cryptographic secret key K.
5. The cryptographic secret key K and DID — <DID, K> — are encrypted (using the public key of EM Enc(K^{+}_{EM}, <DID, K>)) and sent to the Enrollment Module (EM) through a secure authenticated channel; and decrypted by EM; i.e., Dec(K^{-}_{EM}, Enc(K^{+}_{EM}, <DID, K>)); and then stored upon receiving.
6. Three pieces of information is derived by the individual using the client-side software: Generate a UID using some personally known information and the token T, and then hash UID — Hash(UID); Encrypts the hash using K— Enc(K, Hash(UID)); Computes K+BID+N where N is some noise generated by the individual.
7. Three-tuple <DID, K+BID+N, Hash(UID)> is encrypted and sent to the Identity Storage and Verification Module (ISVM) through a secure authenticated channel; and decrypted by ISVM upon receiving.
8. The downloaded client-side software is terminated and discarded. K, UID, BID, and hash(UID) are also discarded. The individual retains only DID, T, and Enc(K, Hash(UID)) (or Enc(K, UID) if UID is not deem private).


Individual
Biometric Service Voice Gateway
Enrollment Module
Identity Storage and Verification Module
Caller ID
CallerID = unique
<DID,UID>
Else
<BID,k>
Enc(K+EM,<DID, k>)
Dec(K-EM <DID,k>)
<Hash(UID), Enc(k,UID), K+BID+N>
Enc(K+ISVM<DID, k+BID +N>, hash(UID))
Discard k,UID,BID, Hash(UID)
Stores DID, Enc(k, UID)

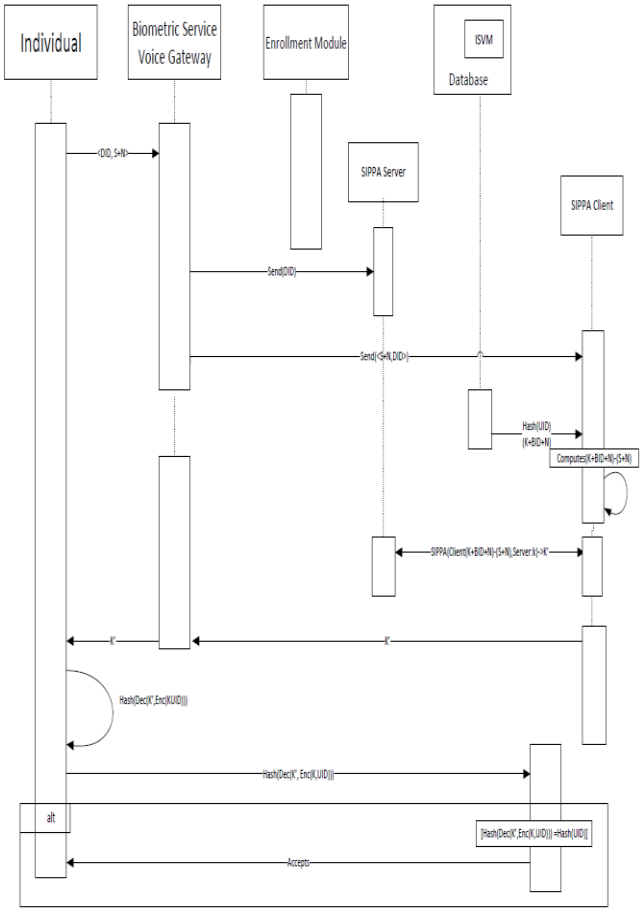
It is noteworthy that the enrollment process described above does not rely on a Certificate Authority to verify the identity of an individual. Instead, the enrollment process above allows an individual to create and self-sign an identity, whereas the process to bind an individual to a unique identity is based on what an individual has (e.g., mobile phone). It does not care the individual information that an individual may specify. It is because the individual information is not relevant to the identity verification process. As such, two individuals could have, for example, the same name but different DID and BID. They will be identified as two different entities as distinguished by different 3-tuples.

Protocol for identity verification:

1. An individual presents to voice gateway (VG) his DID and a noise-added biometric sample S+N.
2. Voice gateway relays DID to SIPPA server, and voice gateway relays S+N and DID to SIPPA client.
3. Based on DID, SIPPA client retrieves Hash(UID) from the centralized database. SIPPA client also retrieves (K+BID+N), and computes (K+BID+N)-(S+N).
4. Execute SIPPA protocol for the SIPPA client to construct a secret K'; i.e., SIPPA(client-input: (K+BID+N)-(S+N), server-inout: K) -> (client-result: K', server-result: similarity

between K and K+BID-S); where K' = K if (K+BID+N)-(S+N) is sufficiently similar to K.

5. SIPPA client returns K' through the voice gateway to the individual for the individual to derive Dec(K', Enc(k, Hash(UID))) (or Dec(K', Enc(k, UID))).
6. Compute Dec(K' Enc(k, Hash(UID))), or Hash(Dec(K' Enc(k, Hash(UID)))), depending upon whether the user stored Enc(K, UID) or Enc(K, Hash(UID)) (by the individual or SIPPA client).
7. Present the hash of the decrypted UID and the token T to ISVM for comparing against the Hash(UID) and T stored in ISVM; ISVM accepts the claimed identity if the decrypted UID is found identical to Hash(UID) of ISVM with a matching T during the authentication.



4.3 Security Analysis

The security analysis will begin with a definition of security. The definition of security is based on the composition of the identity solution in terms of the functional components, their interaction relationship, the trustworthiness of the functional components, and the behavior of adversary.

Functional components of the proposed identity solution:

1. Voice Gateway (VG) serving as an interface between a user and the system. In this research we assume the communication is through a secure authenticated channel, which is reasonable and realistic in the real world situation.
2. Enrollment Module (EM) is composed of SIPPA server and a local storage for the cryptographic secret. EM receives from a user during enrollment a DID and a cryptographic secret K for encryption/decryption. By the principle of separation of duty and need-to-know, no sensitive personal or identity information is stored.
3. Identity Storage and Verification Module (ISVM) is composed of SIPPA client and a centralized database. ISVM is responsible for cryptographic key regeneration based on the helper data provided by the SIPPA server of the Enrollment Module.

The message exchange between the SIPPA client and server during the SIPPA protocol execution is also assumed to be carried out in a secure authenticated channel. In addition, as discussed elsewhere [1] SIPPA protocol is securely usable in the following sense:

a. The correctness of protocol output on private input data is verifiable through Zero Knowledge Proof.
b. SIPPA protocol does not assume or relay on honest or semi-honest model. Under the semi-honest model, each party participating in the protocol can retain all the exchanged messages during the protocol execution and can attempt to discover new information. However, the participating parties will not abort or deviate from the protocol.
c. SIPPA employs Paillier cryptosystem, which is semantically secured, to achieve homomorphic encryption for private data comparison and reconstruction in the encrypted domain.
d. SIPPA private data comparison could serve as a means for authentication. The accuracy of authentication based on SIPPA private data is comparable to the traditional authentication approaches as measured by AUC (Area Under Curve).

Adversary model

In this research we define an adversary model that is realistic in the real world. First, an adversary is assumed to have access to the identity management environment. Therefore, the adversary can enroll himself, impersonate others, or try to influence the behavior of the VG, EM, or ISVM. Furthermore, the adversary is also assumed to possess the following capabilities:

a. Polynomial bounded computing power.

b. Privilege to initialize a SIPPA protocol execution as either a client or a server. As such, the adversary has access to protocol inputs and outputs.

Finally, the adversary can behave maliciously; i.e., the adversary can abort or deviate from the protocol, and can influence the delivery of messages (without altering them) over the authenticated communication channel. For example, the adversary can corrupt the SIPPA server/client to deliver an incorrect intermediate message (e.g., incorrect x in step 2) during the SIPPA protocol execution.

Analysis walk-through and main result

For simplicity and without the loss of generality, an adversary who can corrupt an individual user or a functional component of the identity management system is considered as a corrupted individual user or a corrupted functional component. This allows us to conduct the security analysis by considering the consequence on the privacy of the individual identity information when an individual, and/or one or more of the functional components are corrupted. The corruptible entities include: Individuals (as imposters), VG, ISVM, EM.

Key analysis result:

Claim 1: Under the assumption of one-time pre-enrollment key exchange utilizing Public Key Infrastructure among client-side software, Voice Gateway (VG), Enrollment Module (EM), and Identity Storage Verification Module (ISVM), the integrity of enrollment is guaranteed if none of the functional components in the application level is compromised.

Claim 2: SIPPA-based IDMS guarantees the privacy of the sensitive identity information — if no more than one entity is compromised; i.e., no information loss on UID and BID. In addition, it is detectable if the integrity of authentication is compromised.

Claim 3: The privacy of the sensitive identity information UID and BID is guaranteed even if all the entities are compromised.

@Claim 1:

In a secure authenticated channel, messages can be eavesdropped, relayed and replayed, but not altered. This can be achieved through message signing process using private key. In reference to client-side software download in step 1 of the enrollment process, the software may be intercepted. But the integrity of the software is guaranteed for the recipient.

In reference to step 2, if both the client-side software and the voice gateway are secure, then the only possible attack will be man-in-the-middle attack by redirecting client communication to a malicious voice gateway. Since there is a pre-enrollment key exchange among the parties, the client-side software and the end-point functional components can mutually authenticate each other in the network layer to prevent man-in-the-middle attack [27].

In reference to step 3, the call-back by the voice gateway assures the authenticity of the individual identity as characterized by the individual's device ID. This step also serves as a commitment scheme to bind an individual to his phone number, UID, and DID through the token T. Furthermore, the encryption of the identity information prior to sending over to the functional components (EM and ISVM) ensures the confidentiality over the secure authenticated channel, while the integrity is assured by the property of the secure authenticated channel. Since adversary is assumed to have only polynomial bounded computing power, the adversary will not be able to reverse engineer the encrypted information into plain text.

With trivial observation, the integrity of enrollment cannot be guaranteed if at least one functional component is comprised. For example, the 3-tuple identity information containing the hash of the UID and biometrically encoded BID will be exposed if the centralized database is compromised.

@Claim 2:

We now provide a sketch for explaining the situation where only one entity is corrupted:

Corrupted voice gateway:

Corrupted voice gateway can still communicate with the individual user and the EM as well as ISVM. However, since all end-to-end communication is under secure authenticated channel, the corrupted voice gateway can at most learn the cryptographic secret during the enrollment, but cannot modify the cryptographic secret to compromise the integrity of the system service for enrollment and authentication.

During authentication, the corrupted voice gateway can learn from the user (K+BID)-S. Since the uncorrupted EM will never share K with the corrupted voice gateway, the corrupted voice gateway cannot learn BID from (K+BID)-S. Even if the corrupted voice gateway will first record the cryptographic secret K during the enrollment phase, BID still cannot be derived BID from (K+BID)-S without knowing S, which is the biometric sample of an individual and is never shared by the individual. Therefore, the privacy if UID and BID is preserved.

Again, since the corrupted voice gateway cannot alter the message in a communication between any two-party in a secure authenticated channel, the content of the hash in steps 5 through 7 of the verification protocol remains the same, thus the integrity of the system service for authentication.

Corrupted EM:

Enrollment module is corrupted if either the SIPPA server or the local database storing the cryptographic secret is corrupted. If the local database is corrupted, the cryptographic secret may be arbitrary changed. As a consequence, authentication will always fail. However, this will be detected by test cases grounded on BID=S=N=0 injected into the centralized database of ISVM and used in the integrity test. In other words, when BID=S=N=0, SIPPA protocol will return a conclusion where an arbitrary changed K is not equal to (K+BID+N)-(S+N) for test cases where BID=S=N=0.

If SIPPA server is compromised, it can choose to ignore and not to use the K retrieved from the database. Then the consequence will be the same as before, and is detectable. On the other hand, if SIPPA server is compromised and acts like a malicious user in the SIPPA protocol execution, then the security properties of SIPPA will apply and the followings will result:

(i) Any attempt to decrypt the cipher text message without the secret key during the protocol execution will fail because the underlying cryptographic scheme Paillier cryptosystem is semantically secure and is not vulnerable to the attack by an adversary with only polynomial bounded computing resources.

(ii) Any attempt to deviate from the protocol will result in a discrepancy when Zero Knowledge Proof is applied to verify the correctness of x (derived in step 2 and used in step 3 of the SIPPA protocol).

(iii) If the help data $(\lambda_{de})^{0.5}$ is modified before sending to the SIPPA client in step 4 of the protocol, SIPPA client — with verifiable correct x and $\mathbf{v_{de}}$ (obtained in step 5 of the SIPPA protocol) —can detect the discrepancy through checking the equality $(\mathbf{de{\cdot}de}^T + \mathbf{dv{\cdot}dv}^T)\mathbf{x} = \lambda_{de}\mathbf{v_{de}} + \lambda_{dv}\mathbf{v_{dv}}$.

Corrupted ISVM:

ISVM is corrupted if either the SIPPA client or the centralized database storing is corrupted. If the centralized database is corrupted, 3-tuple identity information may be revealed and arbitrary changed. Since ISVM does not know the cryptographic secret K, it could not derive BID from K+BID. Given polynomial bounded computing power, it cannot reverse engineer UID from the one-way hash(UID/DID). However, the 3-tuple identity information may be arbitrary changed, resulting in incorrect authentication outcomes. However, this can be detected by test cases grounded on BID=S=N=0 as described before; i.e., SIPPA protocol will return a conclusion where K is not equal to (K+BID)-S for test cases where BID=S=0.

If SIPPA client is compromised, it could obtain K+BID and hash(UID) from the central database. Under the assumption on the polynomial bounded computing power, UID cannot be reverse engineered from the one-way hash. If Enc(K, UID) instead of Enc(K, hash(UID)) is stored, then UID is not deem private and exposing such information has not privacy leak.

Impersonation by individual user:

An imposter can impersonate the identity of others. However, the impostor has no knowledge of BID. Therefore, the imposter can only make a guess on the biometric sample S'. When BID and S' are not sufficiently similar, K+BID-S will be rejected by the SIPPA server as being similar to K. As such, SIPPA server will not provide helper data for SIPPA client to reconstruct K. Therefore, the privacy of UID/BID and the biometric template BID is protected.

@Claim 3

This is a restrictive case of claim 2 where only the privacy of the sensitive personal information is required and UID is deem private. Since impersonator does not have Enc(K, hash(UID)), UID cannot be uncovered even EM discloses K. In addition, UID cannot be reverse engineered from hash(UID) even if ISVM discloses it because adversaries have only polynomial bounded computing power. Similarly, impersonator does not have N, BID cannot be uncovered from K+BID+N even if EM discloses K. Therefore, UID and BID are protected even if all parties are compromised.

5 Implementation and Experimentation

For proof-of-concept, we conduct an experimental study on a prototype of the proposed identity management system. The objective of the study is to evaluate the usability of the system as measured by the verification accuracy.

The prototype is composed of an Asterisk PBX [28] for accepting up to five simultaneous incoming calls. An Asterisk to Java gateway serves as an interface for Java-based application implemented for speech processing to extract voice signature, and for SIPPA-based privacy preserving comparison.

There are two experimental trials in this study. The first trial is comprised of 90 calls from a pool of a dozen of individuals using three different phone models — with and without enabling the speaker phone mode. All enrollments and verifications were conducted in an environment where the background noise is fairly consistent. The second trial is comprised of over 400 calls from a pool of 20 individuals assuming 60 identities using 20 different phone models with two configurations — with and without headset. In average each individual assumes three different identities (i.e., enrolled three times). Furthermore, there is no restriction on the enrollment and verification in the second trial. For example, enrollments and verifications could be carried out under different noise environments, as well as different phone models and configurations.

Although it is possible to use a digital voice gateway that accepts voice signature directly from a user, in this experimental study a PBX voice gateway was used to accepts incoming calls directly from a user. The speech processing for extracting voice signatures and noise injection was handled by the voice gateway instead of the individual users. The reason for this alternation in the protocol for this study is because the list of the phones includes conventional landline phone that has no capability of processing voice in the digital form. As such, a voice gateway such as Asterisk PBX to terminate the analog PSTN calls is used in this experimentation; even though some other smart phone models such as Android based LG phones used in this study is capable of extracting voice signature and interacting with a digital voice gateway directly.

By shifting the speech processing task to the voice gateway, it exposes an additional vulnerability because a compromise in the voice gateway will leak the private information on the biometric voice signature of the sample S. However, since this experimentation is focused on the verification accuracy, a system with unrealized exploit on the additional vulnerability will result in the same behavior as one where the voice signature extraction is performed by the user.

In addition, one can also argue that there could be additional (telephone) channel noise (e.g., N') introduced into the voice sample when it is processed on the end of the voice gateway. In this case, it will cause a consistent degradation of the similarity (i.e., (K+BID+N)-(S+ N'+N)). The consequence of it is a shift in SIPPA threshold to yield the same result. But with the enrollment performed by the voice gateway, the net effect of the channel noise is roughly cancelled under the assumption of consistent channel noise (i.e., (K+BID+ N'+N)-(S+ N'+N)).

The result of this study presented as a Receiver Operating Characteristic (ROC) plot on false acceptance (FA) vs false rejection (FR) is shown below. The plots in Fig. 1 are the results of the first trial, detailing the change in the ROC with the speaker phone mode enabled/disabled. The Equal Error Rate (EER) in all cases is about 0.1. The plot in Fig. 2 is the ROC for the entire population without any restriction on the choice of the phone models, operation mode, and the background noise environment. EER is about 0.33.

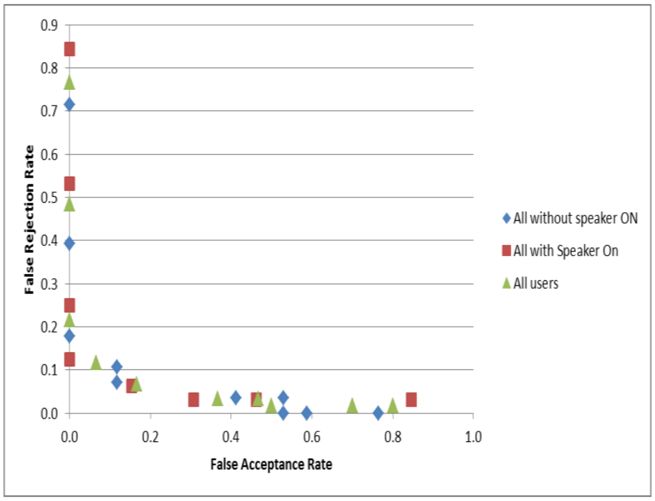


Figure 1. ROC under controlled noise environment

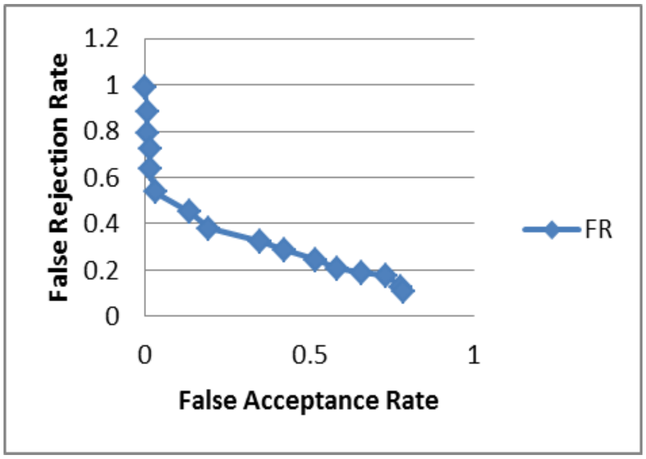


Figure 2. ROC under arbitrary noise environment

6 Conclusions

In this paper we present a privacy preserving voice-based identity solution for authentication based on our previous work on SIPPA. For proof-of-concept, we conducted a simulated experimentation to investigate the effectiveness of the prototype system in regard to its performance summarized in the ROC. Our future work will extend on the current research to investigate the effect of noise in the telephony channel on the performance, possible accuracy improvement based on indvidualized threshold, and the extensibility of its applications.

Acknowledgement : This work is supported in part from a grant by the PSC CUNY Research Award.

7 References

[1] Bon K. Sy & Arun P. Kumara Krishnan, “Generation of Cryptographic Keys from Personal Biometrics: An Illustration based on Fingerprints,” *New Trends and Developments in Biometrics*, ISBN 980-953-307-576-6, InTech, 2012.

[2] Arun P. Kumara Krishnan and Bon K. Sy “SIPPA-2.0 – Secure Information Processing with Privacy Assurance (version 2.0), ’’ *Proc. Of the 9th Conf. on PST*, Paris, France, July 2012.

[3] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus, *Electronic Authentication Guideline*; Special Publication 800-63-1; Dec 2011.

[4] Peter G. Neumann, “System and Network Trustworthiness in Perspective,” *CCS 06*, October 30–November 3, 2006, Alexandria, Virginia, USA.

[5] Kui Ren, Wenjing Lou, Kwangjo Kim, Deng, R., “A novel privacy preserving authentication and access control scheme for pervasive computing environments," *IEEE*

Transactions on Vehicular Technology, (Volume:55 , Issue: 4), July 2006.

[6] Tao Li, Wen Luo, Zhen Mo, Shigang Chen, “Privacy-preserving RFID authentication based on cryptographical encoding," *IEEE Proc. of INFOCOM*, 25-30 Mar 2012, Orlando Florida.

[7] Elli Androulaki, *A Privacy Preserving Ecommerce Oriented Identity Management Architecture*, Master Thesis, Columbia University, May 2011.

[8] Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, "Privacy-Preserving Fingercode Authentication," *MM&Sec’10*, September 9–10, 2010, Roma, Italy.

[9] Meilof Veeningen, Benne de Weger, Nicola Zannone, "Symbolic Privacy Analysis through Linkability and Detectability," *Trust Management VII: IFIP Advances in Information and Communication Technology*, Volume 401, 2013, pp 1-16.

[10] Monica Scannapieco, Ilya Figotin, Elisa Bertino, Ahmed K. Elmagarmid, "Privacy Preserving Schema and Data Matching," *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, Jun 2007, Beijing China.

[11] Ralph Merkle, "A certified digital signature", In Gilles Brassard, ed., *Advances in Cryptology – CRYPTO '89*, vol. 435 of Lecture Notes in Computer Science, pp. 218–238, Spring Verlag, 1990.

[12] Leslie Lamport, "Constructing digital signatures from a one-way function,” Technical Report CSL-98, SRI International, Oct. 1979.

[13] Jean-Jacques Quisquater, Louis C. Guillou, Thomas A. Berson, "How to Explain Zero-Knowledge Protocols to Your Children," *Advances in Cryptology - CRYPTO '89: Proceedings* 435: 628–631.

[14] Jan Camenisch, Maria Dubovitskaya, Anja Lehmann, Gregory Neven, Christian Paquin, Franz-Stefan Preiss, "Concepts and Languages for Privacy-Preserving Attribute-Based Authentication," *Policies and Research in Identity Management: IFIP Advances in Information and Communication Technology*, Volume 396, 2013, pp 34-52.

[15] Denis Trček, *Managing information systems security and privacy*, Birkhauser, p. 69. ISBN 978-3-540-28103-0, 2006.

[16] Carlisle Adams, Steve Lloyd, *Understanding PKI: concepts, standards, and deployment considerations*, Addison-Wesley Professional. pp. 11–15. ISBN 978-0-672-32391-1, 2003.

[17] Stephen August Weis, "Security and Privacy in Radio-Frequency Identification Devices," Master Thesis, MIT, May 2003.

[18] Tassos Dimitriou, “A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete,” *Proc. of IEEE PERCOM*, 2006.

[19] S. Goldwasser and S. Micali, “Probabilistic encryption,” *Journal of Computer and System Sciences*, 28:270-299, 1984.

[20] J. Bourgain, “On Lipschitz Embedding of Finite Metric Spaces in Hilbert Space,” *Israel Journal of Mathematics*, 52 (1985), no. 1-2, 46{52.

[21] Daniele Micciancio, "Technical Perspective: A First Glimpse of Cryptography's Holy Grail," *Communications of the ACM*, Vol. 53 No. 3, Page 96, March 2010.

[22] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *EUROCRYPT*, 1999.

[23] Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, Chapman & Hall/CRC, 2007.

[24] R. Cramer, I. Damgard, Jesper Buus Nielsen, (http://www.daimi.au.dk/~ivan/mpc.pdf) *Multiparty Computation: An Introduction.*

[25] M. Fitzi, D. Gottesman, M. Hirt, T. Holenstein, A. Smith, “Detectable Byzantine Agreement Secure Against Faulty Majorities,” *Proc. of the 21st ACM Symposium on Principles of Distributed Computing (PODC)*, July 2002.

[26] James A. Hanley, Barbara J. , "A method of comparing the areas under receiver operating characteristic curves derived from the same cases". *Radiology* 148 (3): 839–43. PMID 6878708.

[27] Jonathan Katz, “Efficient Cryptographic Protocols Preventing Man-in-the-Middle Attacks,” Ph.D. thesis, Columbia University, 2002.

[28] Jim Van Meggelen, Jared Smith, Leif Madsen, *Asterisk: The Future of Telephony*, ISBN-10: 0596009623, Sept 2005.

[29] Thrasyvoulou T., Benton S.: Speech Parameterization Using the Mel Scale (Part II), (2003).