내적 암호를 이용한 안전한 지문 인증 기법

김진수[1], 김정현[2], 신준범[1]
삼성전자[1], 조지아 공과대학[2]

Secure Fingerprint Authentication Using Inner Product Encryption

Jinsu Kim[1], Junghyun Kim[2], Junbum Shin[1]
Samsung Electronics[1], Georgia Institute of Technology[2]

요 약

We present a privacy preserving fingerprint authentication protocol based on minutiae points which is the most accurate and promising fingerprint matching algorithm. Our protocol provides a secure alignment and matching protocol in two-party settings between a user and a service provider using inner product encryption. We devise a new encodings to compute alignment parameters consists of shift and rotation information for minutiae points. This allows the user to align fingerprint before encrypting fingerprint sample. The implementation results over desktop takes less than 1 second in authenticating one person which shows practicality of our protocol. This results achieve at least 60 times faster than previous 2-party setting of recent work which exploits Garbled circuit.

1. Introduction

The fingerprint has widely been used to identify people since 20th century by forensic scientists. Furthermore, these days the fingerprint is the most widely used in several cases including cellphones, laptop, building entrance, and immigration. A variety of ways to authenticate fingerprints have been proposed. Among them, the minutiae points based approaches are proved that they are the most accurate and promising methods by the recent result of fingerprint matching competition [1].

The minutiae points has major characteristics of the fingerprint such as ridge ending and bifurcation. On the other hand, the minutiae extraction of the fingerprint is not reliable because of presence of noise arisen from various factors such as resolution of the scanner, noise on fingerprint (dust, water, and so forth), light, and so on. If one devises fingerprint alignment algorithm that is robust to incorrect and unreliable feature extraction of the fingerprint, the better accuracy of fingerprint authentication can be achieved. Unfortunately, it is very challenging to apply most of them to privacy preserving fingerprint authentication because operations defined over plaintext such as comparison is hard to be used in ciphertext. In fact, most works of privacy preserving outsourced fingerprint authentication protocols focus on the matching step because of the computational difficulty of finding an efficient alignment method [2,3].

In this paper, we propose a new secure fingerprint authentication protocol with pre-alignment for O2O services between two parties, a user with a built-in scanner device and a service provider. We adopt an outsourced fingerprint authentication using an inner product encryption (IPE) [6], in which an encrypted fingerprint template is stored in Service Provider (SP) and a master secret key is stored in user side.

We assume a metric for fingerprint matching such as Hamming distance and Euclidean distance could be computed using inner product computation. Let us briefly describe: 1) First, the device scans user's fingerprint and computes IPE-decryption keys of minutiae points on the fingerprint. 2) The device then registers the encrypted fingerprint as a template to the service provider. 3) When performing authentication, the device scans user's fingerprint as a sample and computes IPE-ciphertext of minutiae points on it. 4) The service provider runs decryption algorithm of IPE publicly to obtain metric between template and sample and finally determines the matching result. Unlike garbled circuit based multi-party computation, it requires only small number of interactions in the registration and authentication phases.

To reduce the number of iterations and improve the efficiency of the protocol, we propose a new privacy preserving alignment and matching protocol for fingerprint to achieve better performance. In our construction we add one more interaction between the user and the service provider for a secure fingerprint alignment. When registering a fingerprint, “reference points” are additionally used for alignment as well as minutiae points. The reason that the number of reference points are relatively small compared to minutiae points could dramatically improve the performance.

We evaluate the performance to prove the practicality of our protocol. Our implementation shows that the time for a single user authentication takes less than 1 second. This results is at least 60 times faster than two-party setting in [4] which exploits Garbled circuit for outsourced minutiae-based fingerprint authentication.

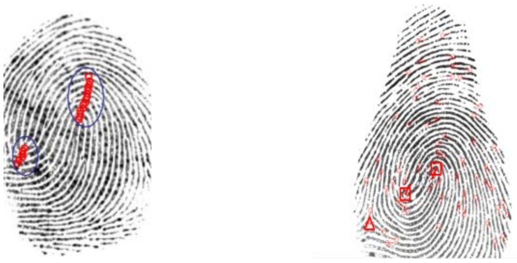

Figure 1. The illustrations of high curvature points (left) and of core point and delta point (right)

2. Protocol Description

In this section, we describe our privacy preserving protocol for secure fingerprint authentication between a user and a service provider. We use D (Device) for the user and SP for the service provider. In registration phase, D extracts a user's fingerprint template (T) and then generates and sends IPE decryption key of T to SP. In authentication phase, D first sends IPE ciphertext of reference points (such as core points and curvature points) in fingerprint sample (S) for fingerprint alignment. After receiving them, SP computes an alignment parameter Delta and sends it to without any encryption. Using Delta, D aligns S and then generates and sends IPE ciphertexts of S to SP. SP determines authentication result (pass or fail) by computing the number of matched minutiae points between IPE encrypted T and S.

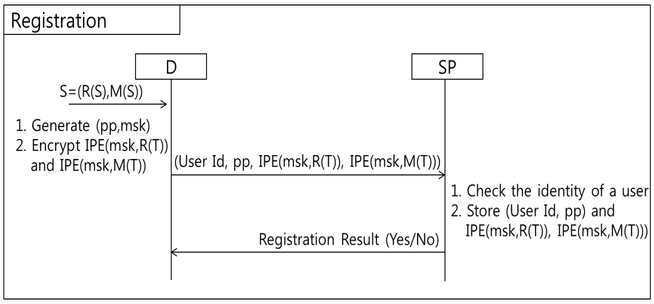
Registration
D
SP
S=(R(S),M(S))
1. Generate (pp,msk)
2. Encrypt IPE(msk,R(T)) and IPE(msk,M(T))
(User Id, pp, IPE(msk,R(T)), IPE(msk,M(T)))
1. Check the identity of a user
2. Store (User Id, pp) and IPE(msk,R(T)), IPE(msk,M(T)))
Registration Result (Yes/No)

Figure 2. Protocol description of registration phase

Registration: D first run IPE.Setup to obtain a master key and public parameter (msk, pp). Then D scans the user's fingerprint T used for template. The template T consists of a set of minutiae points M(T) and a set of reference points R(T). The reference points is essential for alignment of fingerprint and could be core/delta points or high curvature points depending on which alignment method is applied.

To generate IPE decryption key of R(T) and M(T), D applies message encodings on them. We remark that the encodings are used for computing Hamming distance and for computing difference in the (x,y)-coordinates and angles.

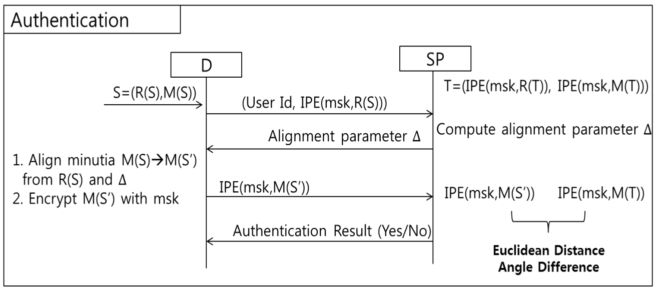
Authentication
D
SP
S=(R(S),M(S))
(User Id, IPE(msk,R(S)))
T=(IPE(msk,R(T)), IPE(msk,M(T)))
Alignment parameter Δ
Compute alignment parameter Δ
1. Align minutia M(S)→M(S') from R(S) and Δ
2. Encrypt M(S') with msk
IPE(msk,M(S'))
IPE(msk,M(S'))
IPE(msk,M(T))
Authentication Result (Yes/No)
Euclidean Distance
Angle Difference

Figure 3. Protocol description of authentication phase

Authentication: This phase consists of two procedure. The first one is a secure alignment of fingerprint and the second one is a secure fingerprint matching.

In the first procedure, SP computes the difference of (x,y) coordinates and angles of reference points (core/delta or high curvature) between the template T and the queried sample S. Thanks to specific properties of encodings and IPE, SP obtains only difference of each values without knowing any information on reference points themselves. When computing the optimal difference, we use the greedy method as in [4].

In the second procedure, D first applies alignment on plain minutiae points M(S) of S using alignment parameter given by SP. We denote it by M(S'). Then D generates and sends IPE ciphertexts of components in

M(S') to SP. For two sets of encrypted minutiae points M_T and M_{S'}, SP counts the number of matched points by computing inner product for Euclidean distance and for angle difference. When determining the matching points, we use the greedy method as in the first procedure. If the number exceeds the fixed threshold, SP could verify the identity of users.

3. Security

In this section, we show that the proposed protocol is secure in the honest-but-curious adversary model.

Proposition 1. The registration phase is secure in the honest-but-curious adversary model, if the underlying IPE satisfies simulation-based security.

The security of the registration phase immediately comes from the semantic security of IPE. Using a polynomial time simulator S.IPE for IPE scheme, we construct a polynomial time simulator S for the registration protocol.

Proposition 2. The user authentication phase is secure in the honest-but-curious adversary model, if the underlying IPE satisfies simulation-based security.

The user authentication phase consists of two sub-protocol, the alignment of fingerprint and fingerprint matching. Thus, the security of the protocol is proven by the security of sub-protocols invoking a modular composition theorem. Using a polynomial time simulator S.IPE for IPE scheme, we construct polynomial time simulators S.Ali and S.Mat for two sub-protocols, respectively.

4. Performance

In this section, we report performance of our implementation on proposed protocols for privacy preserving fingerprint authentication to prove the practicality of our protocols. Our implementation is written in C/C++ using mcl library [5], which is the most promising and reliable pairing-based library, and KKS IPE described in [6] and tested on Ubuntu 16.04 with Intel i7-6700K 4.0GHz CPU and 32GB RAM.

In the dataset, there are at most 60 minutiae points and at most 3 core/delta points. Our protocol requires the initialization phase which takes 0.007 seconds. The registration phase of our protocol takes 0.01 seconds in average. The authentication phase of our protocol takes around 0.83 seconds.

5. Conclusion

In this paper, we present a minutiae based fingerprint alignment and matching protocol. The protocol is constructed using an inner product encryption and novel message encodings. We have shown that our protocol is secure in the honest-but-curious adversary model. The implementation result shows the practicality of our protocol, which takes about 1 second. We expect that the proposed protocol could be applicable to other biometric authentication.

References

[1] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer, 2009

[2] K. Nandakumar, A.K. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. IEEE transactions on information forensics and security, 2007.

[3] H. Xu, R. NJ. Veldhuis, T. AM. Kevenaar, and T. AHM. Akkermans. A fast minutiae based fingerprint recognition system. IEEE Systems journal, 2009

[4] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, et al. Privacy-preserving fingercode authentication. The ACM workshop on Multimedia and security, 2010.

[5] MCL library: A generic and fast pairing-based cryptography library. https://github.com/herumi/mcl

[6] Sungwook Kim, Jinsu Kim, and Jae Hong Seo. A new approach for practical function-private inner product encryption. IACR Cryptology ePrint Archive, 2017.