# A Novel Identity Authentication Technique Without Trustworthy Third-Party Based on Fingerprint Verification

Liang Li, Jie Tian, and Xin Yang

Institute of Automation, Chinese Academy of Sciences, Graduate School of the Chinese Academy of Science, P.O. Box 2728, Beijing 100080, China
tian@doctor.com

## 1 Introduction

Computer networks have evolved from close local networks to open interconnected networks and the operations from data communication to online transaction. As such, identity authentication is indispensable in today's computing platform. Current identity authentication techniques primarily focus on Public Key Infrastructure (PKI) or Identity Based Encryption (IBE). However, these techniques authenticate users' identity relying on tokens or keys and one or many trustworthy third-party(s) that require databases running online, with multiple points of vulnerability and low efficiency.

A novel identity authentication technique without a trustworthy third-party based on fingerprint verification is proposed in this paper. We argue that this proposed approach is inherently more reliable than traditional authentication methods because of the incorporation of fingerprint-based biometric characteristics.

## 2 Major Research Issues

Our method is comprised of (a) the fingerprint feature coding technique, (b) the fingerprint cipher template matching technique, and (c) the fingerprint certificate technique. The fingerprint feature coding technique extracts features from fingerprint images to a digital representation. The key challenge of developing this technique is how to bridge the gap between the fuzziness of fingerprint biometric and the exactitude of cryptography. The Fourier-Mellin transformation (FMT) and discretization are applied to fingerprint images to form feature code. The FMT feature code is invariant in translation, rotation, and scaling. Experimental results have proved its power as to pattern representation. The fingerprint cipher template matching technique matches two cipher templates on terminal unit. In practical applications, fingerprint feature is ensured reliable protection in communication for its privacy and secrecy. An asymmetric encryption method protects feature templates reliably provided the availability of a trustworthy third-party. We propose a new method in which fingerprint templates are locked with a pre-defined random key to form a phase-phase product stored in a USB token. A cipher template can be unlocked by another cipher template in case two templates are from the same finger. Fingerprint certificates record personal information and fingerprint cipher templates of legitimate users, which contain the digital signature of authority as well.

H. Chen et al. (Eds.): WISI 2006, LNCS 3917, pp. 175 – 176, 2006.

These certificates can then be downloaded and accessed by other users. The cipher template of live-scan fingerprints can be matched against the one stored in certificate for identity authentication. This combination of cipher template matching and fingerprint certificate implements identity authentication without a trustworthy third-party.

The roles in this proposed system can be abstracted as the authority TA, user A and user B. TA is central to the entire system which produces and preserves the master key, computes the private key for user, and delivers the USB token. In the initialization stage of system operation, TA sets up a secure communication region and computes the master key and public parameters on a hyper-singular elliptic curve. The underlying mathematical theory is based on the bilinear Diffie-Hellman problem. In the registration stage, users show their legitimate documents to authority. Then TA sets the harden key of the USB token and stores the cipher template of the live-scan fingerprint into token. The public parameters and cryptography functions are stored in the token as well. The USB token has the function of plagiary-resistant, cryptography computation, and fingerprint verification. TA delivers the token to users face to face and produces the fingerprint certificates. In the case of secret communication between user A and user B, the message receiver must authenticate the identity of the message sender. Assuming that A sends message M to B, A computes the communication key K with a bilinear map and the ID of B and then encrypts M and the fingerprint cipher template with K. A sends the encrypted message and the cipher template to B together with the hash of the plain text. After B receives the cipher text, B matches the received cipher template with A's fingerprint certificate. This completes the first round of authentication. B then computes the communication key with B's private key and the ID of A, completing the second round of authentication.

In summary, the proposed approach uses both fingerprints and certificates to authenticate identity in a rigorous manner, combining fingerprint verification with asymmetric encryption thus avoiding the need of third-party participation.

**Acknowledgement.** This research has been supported by the National Natural Science Foundation of China (Grants 60573078 and 60334020).

## References

1. Hsinchun Chen and Fei-Yue Wang, Artificial Intelligence for Homeland Security, IEEE Intelligent Systems, Vol. 20, Issue 5, 2005, pp.12-16.
2. Y. Y. Yao, Fei-Yue Wang，J. Wang,, D. Zeng, Rule + Exception Strategies for Security Information Analysis" , IEEE Intelligent Systems, Vol. 20, Issue 5, 2005, pp. 52-57.
3. H. Chen, F.-Y. Wang, and D. Zeng, Intelligence and Security informatics for Homeland Security: Information, Communication and Transportation, IEEE Trans. Intelligent Transportation Systems, Vol. 5, No. 4, 2004, pp. 329-341.
4. Amit Sahai,Brent Waters, Fuzzy Identity-BasedEncryption, In Advances in Cryptology-Eurocrypt'05. LNCS 3494, pp. 457-473, Springer, 2005.
5. Umut Uludag, Sharath Pankanti, Salil Prabhakar,Anil K.Jain, Biometric Cryptosystems: Issues and Challenges, Proceedings of the IEEE, Special. Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92, No. 6, June. 2004.