使用指紋卡進行數位簽章及資料加密
The Use of Fingerprint-Card for Digital Signature and Encryption

Shih-Hsu Chang*(張世旭)
jang@snoopy.ee.nthu.edu.tw

Chih-Jen Huang*(黃智任)
ren@snoopy.ee.nthu.edu.tw

Fang-Hsuan Cheng†(鄭芳炫)
fhcheng@chu.edu.tw

Wen-Hsing Hsu*(許文星)
whhsu@mercury.ee.nthu.edu.tw

* Department of Electrical Engineering, National Tsing Hua University(清華大學電機系)
† Department of Computer Science, Chung-Hua University(中華大學資工系)

Abstract

We propose a system that uses minutiae points of a fingerprint as a template stored in the smart card chip (fingerprint-card) to identify users and then further uses the minutiae points as the private key to sign, encrypt, and decrypt the electronic documents.

Keywords: Digital Signature, Encryption, Fingerprint Authentication, Minutiae, Smart Card

1 Introduction

Documents in the business field carry at least one handwritten signature. More and more documents will be produced electronically and transmitted by using electronic communication. There is a strong need to use electronic signatures.

Fingerprint authentication relies on "something you are" to make personal identification and, therefore, can inherently differentiate between an authorized person and a fraudulent imposter. The x- and y-coordinates, ridge tangent, and minutiae type maybe be included as standard template elements for fingerprint authentication[5]. Hence, we propose a system that uses the minutiae points of the fingerprint as a template stored in a smart card chip(fingerprint-card) to identify users and then further uses the minutiae points as the private key in public-key cryptosystem to sign, encrypt, and decrypt electronic documents. The high level structure of the proposed system is shown in Fig. 1.

2 Digital Signature and Encryption

Based on the discrete logarithm problem[3, 2, 4], the proposed authenticated encryption system is divided into four parts: system construction, user registration, signature, and verification. The processes are stated as follows.

<***System Construction***> Assume that there is a trusted card center CC which accepts the registration of new users and publishes the public trusted parameters. CC first chooses p, a large prime number, and q, either $p-1$ or a large prime factor of $(p-1)$. Then choose $g \in [1, p-1]$ such that $1=g^q \bmod p$. The private key of CC is $x_c \in [1, q-1]$. The public key of CC is $y_c = g^{x_c} \bmod p$. The parameters $\{p, q, g, y_c\}$ are public.

<***User Registration***> Suppose that a new user U_i wants to register the system. In the enrolling process, the required minutiae points of his fingerprint are stored on his smart card(fingerprint-card). Assume that there are n minutiae points: $p_i = (x_i, y_i, \theta_i)$, where x_i, y_i, and θ_i are the x- and y-coordinates, ridge tangent of the point p_i, all x_i, y_i, and θ_i are 8 bits, for i=0 to $n-1$. His personal information is also stored on his card for certification including id number, name, parent's name, birthday, address, blood type, or other data. The private key x_i of U_i is generated by a hash function $H(\cdot)$ through combining the personal information and n minutiae points and encrypting them into a number. That is

$$info = \text{Personal Information of } U_i,$$
$$d_i = (info, p_0, p_1, \ldots, p_{n-1}), \quad (1)$$
$$x_i = H(d_i) \bmod q. \quad (2)$$

Assume that the personal information is at least 60 bytes and $n = 32$. Because the size of data d is larger than 1200 bits in Eq. (1), it is easy to generate the private key x_i in Eq. (2). We note that the private key x_i need not store on the card. The public key of U_i is $y_i = g^{x_i} \bmod p$. The user U_i submits his public key y_i and identity ID_i to CC. Then CC announces (ID_i, y_i) to all users in the system and stores them in the database. The one-way hash function H needs to be made public.

<***Signature and Encryption***> Suppose that the user U_i wants to sign and encrypt a message $M \in [1, p-1]$ and then sends the signed signature (r, s) to the user U_j. To sign and encrypt the message M, the user U_i

(1) presents himself for verification in Fig. 1, his minutiae points are extracted from his fingerprint image and compared with the minutiae points in his card. The comparison method is the fast point matching algorithm in [1]. If the matching score is less than a given threshold, the device give back an answer of "no" the user U_i is not the card owner and should be rejected by the system. If the matching score is larger than the given threshold, the device give back an answer of "yes" the user U_i is the card owner and can enter the system. This step is the fingerprint authentication.

(2) generates his private key x_i by Eq. (2) and a random number $k \in [1, q-1]$.

(3) uses his private key x_i and U_j's public key y_j to generate

$$t = g^k \bmod p. \quad (3)$$

$$r = Mt^{-1}y_j^{-k} \bmod p, r' = r \bmod q. \quad (4)$$

$$s = k - r'x_i \bmod q. \quad (5)$$

Then the user U_i sends the signature (r, s) to the user U_j. The message M is encrypted into the signature (r, s) since only who owns the private key x_j can recover the message M from the signature (r, s).

<***Verification and Decryption***> Suppose that the user U_j is the card owner(verified by the fingerprint authentication). The user U_j receives the signature (r, s) from the user U_i. He uses his private key x_j and U_i's public key y_i to verify and recover the message M by the following:

(1) Compute $r'=r \bmod q$, and $t=g^k = g^{s+r'x_i} = g^s(g^{x_i})^{r'} = g^s y_i^{r'} \bmod q$.

(2) Generate the private key x_j by Eq. (2).

(3) Because $r = Mt^{-1}y_j^{-k} \bmod p$, $M = rty_j^k \bmod p$,

$$M = rty_j^k = rt(g^k)^{x_j} = rtt^{x_j} \bmod p. \quad (6)$$

M can be recovered by Eq. (6). If the message M is meaningful, it proves that the signature is correct. We note that this scheme allows computing verification equation (6) without inverses and also gives message recovery.

3 Security

An attacker might try to recover the message M from (r, s) based on Eq. (6). Since k and x_j are unknown, it is a discrete logarithm problem to derive k and x_j. Hence M can not be recovered without k or x_j.

The attacker might try to drive the private key x_i based on the linear equation Eq. (5). For the given signature pair, Eq. (5) involves two unknown parameters, x_i and k. For any increment signature pairs, the unknown parameter is also increased by one. This attack can not work successfully.

The attacker might try to drive the private key x_i directly from the corresponding public key y_i. Since $y_i = g^{x_i} \bmod p$, it is equivalent to solving the problem of discrete logarithm. He might try to drive the random number k based on equation (4). For the given signature pair, Eq. (4) involves two unknown parameters, M and k. This attack can not work successfully. Suppose that M is known, then $r/M=g^{-k}\ y_j^{-k} \bmod p$. It is a discrete logarithm problem to derive k.

An intruder might try to forge the signature (r_1, s_1) for a given meaningful message M. He might try to randomly select an integer r_1 first and then compute the corresponding s_1 based on equation (6). Since $M=r_1(g^{s_1}\ y_i^{r_1 \bmod q})y_j^k \bmod p$, it is a discrete logarithm problem to derive r_1 and k for the given number s_1, and it is also a discrete logarithm problem to derive r_1 for the given number s_1. Suppose that the intruder collects two signature pairs (r_1, s_1) and (r_2, s_2) for two unknown M_1 and M_2, where $r_1=M_1 g^{-k_1} y_j^{-k_1} \bmod p$, $k_1=s_1+(r_1 \bmod q)x_i \bmod q$, $r_2=M_2 g^{-k_2} y_j^{-k_2} \bmod p$, and $k_2=s_2+(r_2 \bmod q)x_i \bmod q$. Since $r_1 r_2=M_1 M_2\ g^{-k_3}\ y_j^{-k_3} \bmod p$ and $k_3=(s_1+s_2)+(r_1+r_2 \bmod q)\ x_i \bmod q$, the pair $(r_1 r_2,\ s_1 + s_2)$ can not be the signature for $M_1 M_2$. The multiplication attack can not work successfully.

We note that the random number k can not be used twice for different message M_1 and M_2. If the number k is used to derive the signatures (r_1, s_1) and (r_2, s_2) for M_1 and M_2, respectively, then it is easy to derive the private key x_i(since $k=s_1+(r_1 \bmod q)x_i=s_2+(r_2 \bmod q)x_i \bmod q$).

4 Conclusions

We have proposed an authenticated encryption system that uses the minutiae points as a template stored in the smart card chip(fingerprint-card) to identify users and then further uses the minutiae points as the private key to sign, encrypt, and decrypt electronic documents. The system is a digital signature scheme integrated with public key cryptosystem and fingerprint authentication, so it provides secrecy, authenticity, nonrepudiation, and integrity, simultaneously.

References

[1] S.-H. Chang, F.-H. Cheng, W.-H. Hsu, and G.-Z. Wu, "Fast algorithm for point pattern matching: Invariant to translations, rotations and scale changes," *Pattern Recognition*, 30(3):311–320, 1997.

[2] S. J. Hwang, C. C. Chang, and W. P. Yang, "An encryption/signature scheme with low message expansion," *Journal of the Chinese Institute of Engineers*, 18(4):591–595, 1995.

[3] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," In *Advances in Cryptology-EUROCRYPT'94 Proceedings*. Springer-Verlag, 1995.

[4] Bruce Schneier, "*Applied Cryptography*," John Wiley & Sons, Inc., 1996.

[5] Jim Wayman, "Some thoughts regarding F-P minutiae template standardization," In *NIST/TTL and Biometric Consortium Workshop: Potential for Standardization of Fingerprint Templates For Authentication Applications*, February 21 1999.

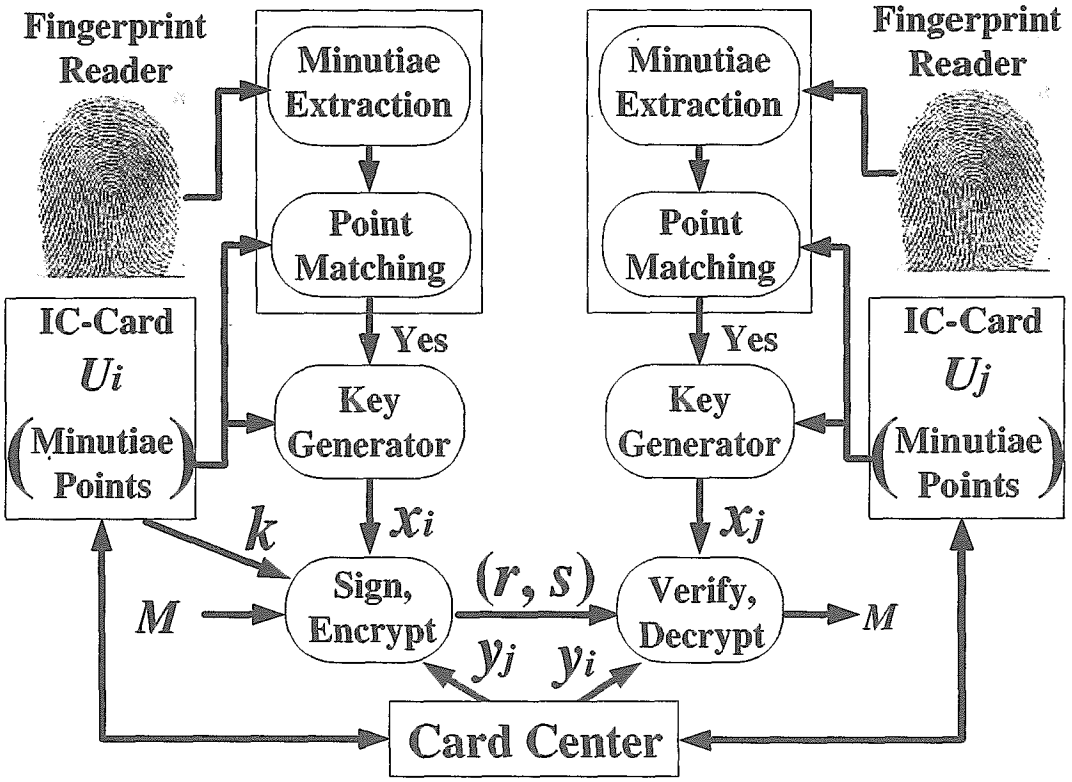

Figure 1: The flowchart of the proposed system.