以智慧卡實現門檻方法之橢圓曲線密碼系統

吳錫聰 [1] **邱炳樟** [2]

1. 國立宜蘭技術學院電子工程系講師
2. 國立台灣科技大學電子工程系教授

摘 要

在非對稱的加碼系統中，橢圓曲線密碼系統以較小的金鑰長度達成相同的安全強度，因而日受重視，橢圓曲線密碼系統的優點是其被廣泛應用於智慧卡、行動通訊之重要因素。本文應用橢圓曲線密碼系統以智慧卡來控制重要處所之門禁，如銀行金庫、實驗室等之門禁，基於一些安全考量，此重要門禁之控制須由具控制權限的一群成員來控制而非由單一成員所能控制，此涉及密秘分享之問題，解決之道乃應用所謂“門檻方法”，每個合法成員持有一機密持份 – 存於智慧卡之次密鑰，經由特定個數之智慧卡上的次密鑰正確重建門禁控制的金鑰後，即可允許正常控制門禁。為防弊不誠實成員之不當門禁控制行為，欺騙者的偵測是必須要的機制。此外，智慧卡的密碼允許其使用者自由更改以方便使用者記憶，益顯本系統之人性化。

關鍵字 : 密碼學、橢圓曲線密碼系統、智慧卡、門檻方法

Threshold Scheme with Smart Card and Elliptic Curve Cryptosystem

Shyi-Tsong Wu[1] and Bin-Chang Chieu[2]

1. Lecturer, Department of Electronic Engineering, National Ilan Institute of Technology
2. Professor, Department of Electronic Engineering, National Taiwan University of Science and Technology

Abstract

The application of Elliptic Curve Cryptosystem has gained more and more attention. ECC uses smaller key size and lower memory requirement to retain the security level and can be a crucial factor in the smart card system. An ECC based implementation of security schemes in smart card system to access coffers is proposed in this paper. For some specific safety consideration, access to coffers by a person is not permissive but a group of authorized people. It involves the problem of secret sharing. The adopted solution of sharing secret is threshold scheme. Every participant possesses a secret shadow, which will be saved in the smart card. After correct reconstructing the shared secrets, it is permissible to access the coffer's door. For resisting dishonest participants, cheating detection and cheater identification will be included. The user can change his password of smart card freely and need not to memorize his assigned lengthy password and shadow as traditional ID-based schemes makes our implementation much more user friendly.

Key Word: Cryptography; Elliptic curve cryptography; Smart card; Threshold scheme

2. Introduction

The security strength of access facilities with mechanical lock is poor for leaving no traces of identifications of persons who enter or exit the facility. Mechanical lock controlled by electronic key-card system is recommended. A user just only attaches his smart card to the card reader and keys in his password then he can access the facility after authentication procedure. If the access authority is intended to be determined by a group authorized people instead of a single member, it will involved the secret sharing cryptography. Based on the smart cards, DES encryption and shared-secret scheme, Leong and Tan [3] described an elaborate implementation to access a laboratory door. For promoting the security flexibility and the scalability of smart cards for further multi-applications, it is suggested to apply public key cryptosystem rather than symmetric DES encryption.

In the modern cryptography, public key cryptography plays an irreplaceable role. Public key cryptosystem, with the enormous growth oh the computer and communication industry, had become the cryptosystem that controls e-commerce, Internet and electronic mail. All these applications will employ encryption and authentication. Public key cryptosystem solves the problems of the key management and offers the ability to implement digital signature, etc.

Public key cryptography based on the mathematical problem is generally classified into following systems: integer factorization system, discrete logarithm system and elliptic curve discrete logarithm system. The elliptic curve discrete logarithm system is known as the Elliptic Curve Cryptography. The attraction of ECC is that it offers equal security strength for a far small bit size and fast processing computation in public cryptosystems. The properties of ECC make it well suited for some applications in constrained environments such as smart cards and mobile communications.

Recently Mohammed et al. [5] and Liu et al. [4] proposed ECC with digital certificate on smart cards. Their schemes are very novel for high security strength and the elasticity of smart cards. In this paper, we further merge ECC based system with smart cards, shared-secret scheme, cheating detection and cheater identification. The proposed scheme not only possesses the advantages as that of Mohammed et al. and Liu et al.' s schemes but also extends to the group-oriented access. In our scheme, the user need not to memorize the lengthy shared-secret code and can change his login password randomly at his will and all the access data are centralized saved at the central host for the accommodation of further analysis.

II. Some Cryptographic Background

In this section, we will describe some cryptographic schemes that will be applied further in our implementation. There are Elliptic Curve Cryptography, digital signature scheme, shared-secret scheme and cheater identification.

1. Elliptic Curve Cryptography

Here we introduce the Elliptic curve and Elliptic curve digital signature.

A. Elliptic Curve

Elliptic curves are so named because they are described by cubic equations. The cubic equation for elliptic curve takes the form:

$$y^2+\mathrm{a}xy+\mathrm{b}y = x^3+\mathrm{c}x^2+\mathrm{d}x+\mathrm{e} \qquad (1)$$

where a, b, c, d and e are real numbers that satisfy some conditions [8]. Also included in the definition of any elliptic curve is a single element denoted $\boldsymbol{O}$ and called the point at infinity or the zero point.

Addition defined for an elliptic curve is stated as follows: If three points on an elliptic curve lie on a straight line, their sum is $\boldsymbol{O}$. Fig. 1 shows example of elliptic curve addition. The addition rule of the three point (**P**, **Q**, -**R**) on the curve is $\mathbf{P}+\mathbf{Q}+(-\mathbf{R}) = \boldsymbol{O}$, $(-\mathbf{R}) + \mathbf{R} = \boldsymbol{O}$ and so $\mathbf{P}+\mathbf{Q} = \mathbf{R}$.

Multiplication of a point **P** on an elliptic curve by a positive integer s is defined as the sum of s copies of **P**. Thus $2\mathbf{P} = \mathbf{P}+\mathbf{P}$, $3\mathbf{P} = \mathbf{P}+\mathbf{P}+\mathbf{P} = 2\mathbf{P}+\mathbf{P}$, $4\mathbf{P} = 2\mathbf{P}+2\mathbf{P},\cdots$. It is very difficult to find an integer s such that $s*\mathbf{P} = \mathbf{Q}$. This is the Elliptic Curve Discrete Logarithm Problem (ECDLP).

B. Elliptic Curve Digital Signature

Firstly, an elliptic curve E defined over GF(p) or GF(2^m) with order q and a base point **P** is selected and made public to all users. Then, public and private key pairs are generated. Elliptic curve digital signature and verification primitive are used for each user' s login and described as follows.

- **Key Generation**

Each user follows thesteps for key generation:

1. Select a random number $s \in [1, q\text{-}1]$.
2. Compute $\mathbf{Q} = s^*\mathbf{P}$ on curve E.
3. The public key of the user is (E, **P**, q, **Q**) and the private key is s.

- **EC Nyberg-Rueppel Digital Signature Scheme**

The following introduction is the EC Nyberg - Rueppel digital signature scheme [6]:

1. The message needed to be sign is m.
2. Randomly generate a key pair (v, $\mathbf{V} = v^*\mathbf{P}$), where $\mathbf{V}$=($\mathbf{V}.x$, $\mathbf{V}.y$).
3. Calculate $c = \mathbf{V}.x + m$ (mod p).
4. Calculate $d = v$ - s· c (mod p).
5. Obtain the output pair (c, d) as the signature.

The signature verification procedure is as follows:

1.Calculate $\mathbf{G} = d^*\mathbf{P} + c^*\mathbf{Q}$.

2.Calcute *m*¢ = c- $\mathbf{G}.x$ (mod p)

Accept the signature for message m if and only if *m*¢ = m.

2. Shared-Secret Scheme

The solution of access to coffer of bank by a group of authorized people is threshold scheme. It divides secret data S into n pieces $S_1, S_2, \cdots, S_n$ in such a way that: (1)any k-1 or less shadows reveal no knowledge about S, (2)any k or more shadows can be used to reconstruct S. This is known as (k, n) threshold scheme.

Shamir published the threshold scheme based on a polynomial interpolation [7]. Each member was assigned a shadow associated to the interpolating polynomial, so that any k or more members together can reconstruct the secret. Shamir' s threshold scheme is an ideal threshold scheme for the reason that the domain of shadow is the same as the domain of secret [1].

Prior to using a_0= S as the secret, the shadow distributor randomly choose (k-1) number of a_is, for 1 i k-1, to establish a polynomial f(x) of degree (k-1) :

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \pmod{p} \tag{2}$$

Computing $S_i = f(X_i)$, i=1,2,$\cdots$, n, the S_i is called the shadow of S for X_i. Any k or more X_i with S_i, (X_i , S_i), can easily reconstruct $f(x)$ and obtain the secret S = $f(0)$. Given a set of two-tuples that includes at least k distinct (X_{i_1}, K_{i_1}), $(X_{i_2}, K_{i_2}), \cdots (X_{i_k}, K_{i_k}) \in$ Share $=\{(X_1,S_1), (X_2,S_2), \cdots, (X_n, S_n)\}$, we can compute the $f(x)$ of degree of (k-1) by using Lagrange interpolation [2] :

$$f(x) = \sum_{l=1}^{k} S_{i_l} \prod_{\substack{j=1 \\ j \neq l}}^{k} \frac{(x - X_{i_j})}{(X_{i_l} - X_{i_j})} \pmod{p} \tag{3}$$

To prevent obtaining S by exhaustive search, p should be relatively large and S must be relatively long in terms of bit length.

3. Cheater Detection and Cheater Identification

Tompa and Woll' s suggested a (k, n) threshold protecting policy to safeguard the secret [9]. However, their method cannot deterministically detect cheating and identify the cheater. Wu and Wu [10] applied one-way hash function for cheating and cheater identification. Their scheme is as follows:

- **Initialization**

Shadow distributor performs the following steps:

1.Use Shamir’ s (k, n) threshold scheme to distribute shadows S_i to user i, for i=1,2,‥‥,n.

2. Choose a one way function $h(\cdot)$ and a prime number$p$ such that $h(\cdot) < p$.

3. Compute

$$t = \sum_{i=1}^{n} h(S_i) \cdot p^{2(i-1)} + \sum_{i=1}^{n\text{-}1} C \cdot p^{2i-1} \tag{4}$$

where C is a positive constant randomly chosen over GF(p).

4. Publish t and p.

- **Cheater Identification**

Suppose any k participants want to pool their shadows to reconstruct the secret and let G be the set of these participants. The cheating detection and cheater identification is achieved by applying the following procedure.

1. All $U_j \in G$ present their possessed shadows S_j^*s and compute

$$t^* = \sum_{Uj \in G} h(S_j^*) \cdot p^{2(j-1)} \tag{5}$$

2. For $U_j \in G$, check the equation

$$\left\lfloor \frac{t\text{ - }t^*}{p^{2(j-1)}} \right\rfloor (\bmod\ p) \overset{?}{=} 0 \tag{6}$$

If the equation holds, U_j is honest; otherwise, U_j is a cheater. It is because that

$$\left\lfloor \frac{t\text{ - }t^*}{p^{2(j-1)}} \right\rfloor (\bmod\ p)$$

$= h(S_j)$ - $h(S_j^*)$ (mod p)

= 0 if and only if $h(S_j) = h(S_j^*)$

In our secret sharing implementation, the cheater detection and cheater identification scheme will be used as a precaution for resisting the deleted user’ s and dishonest participant’ s login.

III. The Proposed System Overview

The proposed system employs Elliptic Curve Digital Signature Algorithm (ECDSA) cryptography, shared-secret and smart card technology to control the unlocking of coffer doors. The overall system diagram is shown as Fig. 2. The Host controls the Remote Terminal Units (RTU) via the Internet since that is cheaper and has simpler communicating connection configuration compared with the leased lines.

Components of RTU are shown in Fig. 3. The main component of RTU is Personal Computer (PC_{RTU}), which communicates the microchip with RS-232 and the Host with Internet. Internal Card Reader and External Card Reader provide the interfaces for smart cards to communicate with the PC_{RTU}. Since signal level is different between microchip and RS-232, a signal level converter will be included.

Every authenticated member has his own smart card. During entry request, the members insert their smart cards to the External Card Reader and key in their passwords via keypad. The PC_{RTU} authenticates the smart cards and reconstructs the secret S. If the secret is correct, microchip unlocks the Door Access Unit under the instructions of PC_{RTU}. After unlocking the door a few predefined minutes, the door will close automatically.

The door status will be detected with an infrared detector. Finally, the data including the door status, the door open time, and the participants who access the door will all be transmitted to Host via the Internet and be recorded in the data base of Host.

IV. Implementation

1. Set-up

The Host performs the set-up procedure as follows:

1. Choose the Elliptic curve E with order q, base point $\mathbf{P}$ and private key $K_{HOST} \in [1, q\text{-}1]$.
2. Choose random number S for each RTU and $a_1, a_2, \cdots, a_{k-1} \in Zp^*$, which is corresponding to the coefficients of the polynomial of equation (2).
3. Generate random $X_1, X_2, \cdots, X_n \in Zp^*$ and compute the set share = $\{(X_i, S_i) \mid 1\leq i \leq n\}$ for each RTU.
4. Compute the t as equation (4).

Each RTU performs initial procedures respectively to apply for its certificate. The RTU sends its public key $\mathbf{Q}_{RTU}$ to Host through secure channel. Host uses its private key to sign the hash value of concatenation of private key $\mathbf{Q}_{RTU}.x$, ID of RTU ID_{RTU}, and certificate expiration date of RTU T_{RTU}. The Host then sends the signed message, i.e. certificate of RTU, through secure channel to the RTU as shown in Fig. 4, where E(m, K) is the encryption of m with the key K, D(c, K) is the decryption operation, v_{RTU} is a secret random number, K_{HOST} is the private key of HOST, S is the secret of the RTU in threshold scheme, t is the parameter of equation (4) and $h(\cdot)$ is a one way hash function.

Performing the same procedures, smart card acquires its certificate as Fig. 5, where i is the identifier of user, PWi is the password of user i, T_C is the certificate expiration date of smart card, v_C is a secret random number and S_i is the shadow of user i in threshold scheme.

2. Local Login

When a user wants to login the local RTU to access the door of coffer, he must pass the authentication procedure. The procedures are shown in Fig. 6 and described as follows.

• Local Login Phase

1. The user inserts his smart card to the exterior card reader and keys in his password PW_i^*. The smart card computes $\mathbf{Q}_C^* = PW_i^* * \mathbf{P}$. If $\mathbf{Q}_C^* \neq \mathbf{Q}_C$, it indicates the pass word PW_i^* is invalid and then abort.
2. By exchanging mutual public key, smart card and RTU compute session key $\mathbf{Q}_{CR}.x$ respectively for communication.
3. RTU generates a random number r, encrypts it with session key $\mathbf{Q}_{CR}.x$ and sends the message m_0 to smart card.
4. After decrypting m_0 and getting the random number r^*, smart card encrypts the concatenation of r^*, certificate e_C, (c_C, d_C), certificate expiration date T_C, current time T, X_i, S_i, and sends it back to RTU in terms of m_1.

• Verification Phase

Receiving the message m_1, the PC_{RTU} will perform the following steps:

1. Decrypt m_1, and get $(r^{**}, i, e_C, (c_C, d_C), T_C, T, X_i, S_i)$.
2. Check r^{**} and T_C. If either of both is invalid, the session will be aborted. And then RTU verifies the validity of the certificate and accordingly accepts the local login or not.

• Secret Reconstruction Phase

After k or more member pass the verification phase, the PC_{RTU} use the Lagrange Polynomial Interpolation to reconstruct the S^*. If S^* is correct, the PC_{RTU} will transmit an open signal and a number to the microchip. The open signal will unlock the door of coffer and the number will inform the microchip how many members will login. If the S^* is incorrect, PC_{RTU} will compute the parameter t^* of equation (5), detect the cheater and record the ID of the participant.

3. Management of Access Record

The access data including the user who logins, the access time, the status of RTU and the coffer open/close time will all be saved in PC_{RTU} for future use.

- When the door of coffer was accessed to open, the PC_{RTU} will save the entry records with the form:

  $E(\ i\quad T_{ent}\quad ENT, K_{RTU})$

  where T_{ent} is the time of the access of user *i* for entry and ENT indicates the entry access to the RTU.
- After k or more members pass the local login phase and correct reconstructing of S, the coffer’s open time and its alternative status will also be saved with the form:

  $E(\ T_o\quad Status, K_{RTU})$

  Where T_o is the time of coffer’s opening, Status indicates the status of the coffer on/off.
- Similarly, the exit records will save the exit data of user *i* with the following form:

  $E(\ i\quad T_{exit}\quad EXIT, K_{RTU}\ )$

  where T_{exit} is the access time for exit and EXIT indicates the exit access.
- The status of coffer on/off is periodically saved and transmitted to the Host with the form:

  $\{\ ID_{RTU}, E(\ i\quad T\quad Status, Q_{HR}.x)\ \}$

  where $Q_{HR}.x$ is the session key between Host and RTU, $\mathbf{Q}_{HR} = K_{RTU} * \mathbf{Q}_{HOST} = K_{HOST} * \mathbf{Q}_{RTU} = (\ Q_{HR}.x, Q_{HR}.y)$.
- The PC_{RTU} will feedback the entry record to the Host with the form: $\{\ ID_{RTU}, E(\ i\quad T_{ent}\quad ENT, Q_{HR}.x)\ \}$ and the exit record with the form: $\{\ ID_{RTU}, E(\ i\quad T_{exit}\quad EXIT, Q_{HR}.x)\ \}$.

V. Discussions and Conclusion

Smart cards offer portable storage media, a small processing unit and are not accessible to anyone but their rightful owners. Though the main barriers of smart cards are the lower processing power and constrained memory, implementation of ECC in smart card can solve the problems that the smart cards faced.

Our scheme is based on Elliptic Curve Digital Signature Algorithm. Since $\mathbf{Q}_C$ and PW_i are used for users to login the RTU, they must be tightly protected. The parameter of $\mathbf{Q}_C$ is stored in the tamper-proof smart card and cannot be retrieved directly. Even $\mathbf{Q}_C$ were compromised, PW_i remains secure because of the ECDLP. The strength of security of ECDLP is much harder than that of RSA [5].

The scheme allows users to change their passwords freely. When a user wants to change his password, he submits his smart card and chooses a new password PW_i' to the PC_{RTU} via card reader. The PC_{RTU} will perform the new $\mathbf{Q}_C'$ as $\mathbf{Q}_C' = PW_i' * \mathbf{P}$ and write the new $\mathbf{Q}_C'$ into the smart card of user *i*. After the replacement of $\mathbf{Q}_C$ in the smart card of user *i*, user *i* can use the new PW_i' to login. The bit length of PW_i is chosen freely by user *i*, it need not be 128, 256 bits or other bit length, so the password is easy to memorize for the user.

In the case of losing smart card, user *i* can use his ID to re-register a new card CID_i'. After Host checks his basic background data, the lost smart card CID_i will be invalid. The illegal holder of the lost smart card can not login because he have no password of user *i*.

Addition of new user is easier. Its procedure just likes the set-up process. Deletion of user *i* is troublesome, if the smart card of the removed user is not recovered. It requires an update of all smart cards in the dedicated RTU. The update process, that includes the changes of secret S, *t* and some other operations, will be performed friendly. It needs only to insert the smart card and key in its corresponding password of the authorized user. Although the deleted user is able to login but to open the door of the coffer in the threshold scheme will be in vain, and he will finally be detected by the cheating detection and cheater identification scheme.

References

1. Brickell, E. F, (1989), Some ideal secret sharing schemes, J. Combinatorial Mathematics Combinatorial Computing, **6**, pp. 105-113.
2. Gerald, C. F. and Wheatley, P. O. (1994), Applied numerical analysis, Harlow, UK: Addison - Wesley.
3. Leong, P. C. and E. C. Tan, (2000), Implement of smart-card access control with threshold scheme, INT. J. ELECTRONICS, **87**(6), pp. 649-657.

4. Liu, Joseph K., Vivtor K. Wei, C. Siu, Roy L. Chan, T. Choi, (2001), Multi-application smart card with elliptic curve cryptosystem certificate, EUROCON’ 2001, Trends in Communications, International Conference on, No. 2, pp. 381-384.
5. Monhammed, Elsayed, A. E. Emarah and Kh. El-shennawy, (2001),Elliptic curve cryptosystems on smart card, Security Technology, 2001 IEEE 35th International Carnahan Conference on, pp. 213-222.
6. Nyberg, K., and Rueppel, R. A. (1993), A new signature scheme based on the DSA given message recovery, Proceeding of 1st ACM Conference on Computer and Communications Security, Fairfax, pp. 58-61.
7. Shamir, A. (1979), How to share a secret, Communications of the Association for Computing Machinery, **22**, pp. 612-613.
8. Stallings William, (1999), Cryptography and Network Security: Principles and Practice, Prentice-Hall, Inc.
9. Tompa, M., Woll, H. (1988), How to sharing a secret with cheaters, J. Crytol.,**1**(2), pp. 133-138.
10. Wu, T.-C. and T.-S. Wu, (1995), Cheating detection and cheater identification in secret sharing schemes. *IEE Proc.-Comput. Digit. Tech.* 1**42(**5), pp. 367-369.

91 年 07 月 17 日投稿

91 年 08 月 10 日接受

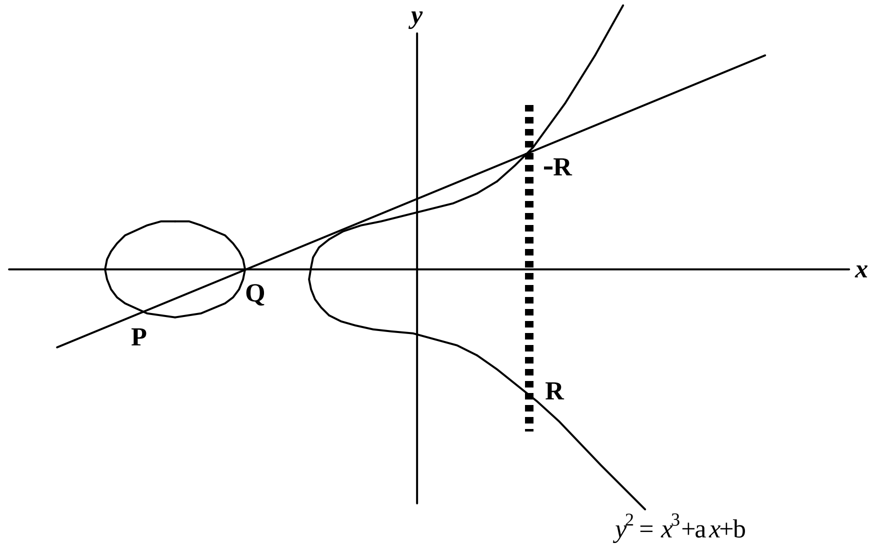

Fig 1　Elliptic Curve of Addition.

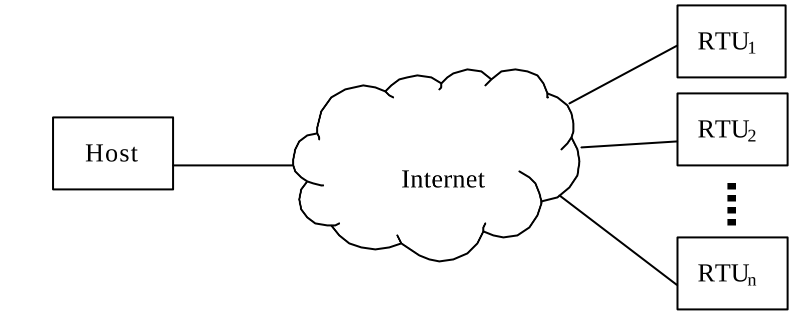

Fig 2　System block diagram.

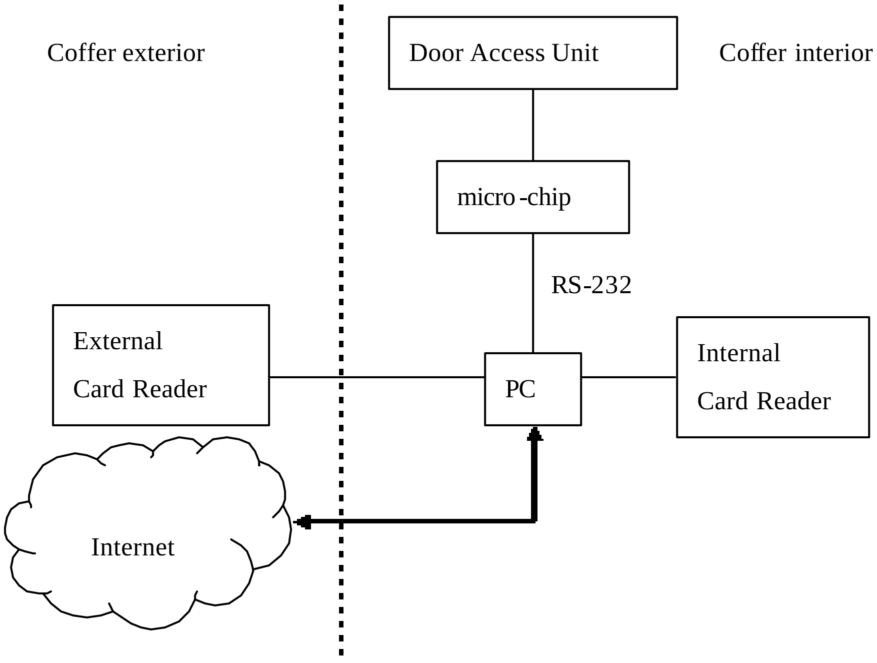

Fig 3　Remote Terminal Unit.

RTU

- Choose $K_{RTU} \in [1, q\text{-}1]$ as private key
- $\mathbf{Q}_{RTU} = K_{RTU} * \mathbf{P}$, $\mathbf{Q}_{RTU}$ is the public key of RTU
- Send $\mathbf{Q}_{RTU}$

$\mathbf{Q}_{RTU}$

Host

- Choose $v_{RTU} \in [1, q\text{-}1]$
- $\mathbf{V}_{RTU} = v_{RTU} * \mathbf{P}$
- Receive
- Select the RTU's Identifier ID_{RTU}
- $c_{RTU} = V_{RTU}.x + h(\mathbf{Q}_{RTU}.x, ID_{RTU}, T_{RTU})$
- $d_{RTU} = v_{RTU} - K_{HOST} \cdot c_{RTU}$
- Send

$\mathbf{Q}_{HOST}$, ID_{RTU}, (c_{RTU}, d_{RTU}), T_{RTU}, S, t

- Receive
- Calculate $\mathbf{G}_{RTU} = d_{RTU} * \mathbf{P} + c_{RTU} * \mathbf{Q}_{HOST}$

  $=(\mathbf{G}_{RTU}.x, \mathbf{G}_{RTU}.y)$
- $e_{RTU} = c_{RTU} - \mathbf{G}_{RTU}.x$
- Store ID_{RTU}, e_{RTU}, $\mathbf{Q}_{HOST}$, $\mathbf{Q}_{RTU}$,

  (c_{RTU}, d_{RTU}), T_{RTU}, K_{RTU}, S, t on RTU

Fig 4 Remote Terminal Unit Initialization.

Card

- Choose $PW_i \in [1, q\text{-}1]$
- $\mathbf{Q}_C = PW_i * \mathbf{P}$, $\mathbf{Q}_C$ is the public key of user i
- Send $\mathbf{Q}_C$

$\mathbf{Q}_C$

Host

- Choose $v_C \in [1, q\text{-}1]$
- $\mathbf{V}_C = v_C * \mathbf{P}$
- Receive
- $c_C = \mathbf{V}_C.x + h(\mathbf{Q}_C.x, i, T_C)$
- $d_C = v_C - K_{HOST} \cdot c_C$
- Send

$\mathbf{Q}_{HOST}$, i, (c_C, d_C), T_C, X_i, S_i

- Receive
- Calculate $\mathbf{G}_C = d_C * \mathbf{P} + c_C * \mathbf{Q}_{HOST}$

  $=(\mathbf{G}_C.x, \mathbf{G}_C.y)$
- $e_C = c_C - \mathbf{G}_C.x$
- Store i, e_C, $\mathbf{Q}_{HOST}$, $\mathbf{Q}_C$, (c_C, d_C), T_C, X_i, S_i on Smart Card

Fig 5 Card Initialization.

Card		RTU
•Receive	$\mathbf{Q}_{\mathrm{RTU}}$	•Send
•Key in PW_i^* by user		
•$\mathbf{Q}_{\mathrm{C}}^* = \mathrm{PW}_i^* * \mathbf{P}$		
•If $\mathbf{Q}_{\mathrm{C}}^* \neq \mathbf{Q}_{\mathrm{C}}$, then abort		
•Send	$\mathbf{Q}_{\mathrm{C}}$	•Receive
•$\mathbf{Q}_{\mathrm{CR}} = \mathrm{PW}_i^* * \mathbf{Q}_{\mathrm{RTU}}$		•$\mathbf{Q}_{\mathrm{CR}} = \mathrm{K}_{\mathrm{RTU}} * \mathbf{Q}_{\mathrm{C}} = (\mathrm{K}_{\mathrm{RTU}} \cdot \mathrm{PW}_i) * \mathbf{P}$
$= (\mathrm{PW}_i \cdot \mathrm{K}_{\mathrm{RTU}}) * \mathbf{P}$		•Generate random number r
		•$m_0 = \mathrm{E}(r, \mathbf{Q}_{\mathrm{CR}}.x)$
•Receive	m_0	•Send
•$\mathrm{D}[m_0, \mathbf{Q}_{\mathrm{CR}}.x] = r^*$		
•$m_1 = \mathrm{E}[(r^*, i, e_{\mathrm{C}}, (c_{\mathrm{C}}, d_{\mathrm{C}}), \mathrm{T}_{\mathrm{C}}, \mathrm{X}_i, \mathrm{S}_i, \mathrm{T}), \mathbf{Q}_{\mathrm{CR}}.x]$		
•Send	m_1	•Receive
		• $\mathrm{D}[m_1, \mathbf{Q}_{\mathrm{CR}}.x] = (r^{**}, i, e_{\mathrm{C}}, (c_{\mathrm{C}}, d_{\mathrm{C}}), \mathrm{T}_{\mathrm{C}}, \mathrm{X}_i, \mathrm{S}_i, \mathrm{T})$
		•If $r^{**} \neq r$, then abort
		•If T_{C} is not valid, then abort
		•$\mathbf{G} = d_{\mathrm{C}} * \mathbf{P} + c_{\mathrm{C}} * \mathbf{Q}_{\mathrm{HOST}} = (\mathbf{G}.x, \mathbf{G}.y)$
		•Calculate $m¢ = e_{\mathrm{C}}^* = c_{\mathrm{C}} - \mathbf{G}.x$
		• If $e_{\mathrm{C}}^* \neq e_{\mathrm{C}}$, then abort,
		• else accept the user i’ s local login

Fig 6 Authentication of Local Login.