以智慧卡與橢圓曲線密碼系統完成遠端身份鑑別

吳錫聰[1] 邱炳樟[2] 邱榮輝[3]

1. 國立宜蘭大學電子工程系講師
2. 國立台灣科技大學電子工程系教授
3. 長庚大學電機工程系副教授

摘 要

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配合智慧卡完成遠距的身份鑑別，其具有較短的金鑰長度，較快的計算及節省通信頻寬的優點。此外，本方法不需使用密碼表來比對使用者密碼，密碼也不是由系統計算出來冗長、不人性的密碼，其允許使用者自由選定及更改，以方便使用者記憶，益顯本鑑別方法之人性化。

關鍵字：遠端身份鑑別、智慧卡、橢圓曲線密碼系統

A Remote Authentication Scheme with Elliptic Curve Cryptography on Smart Cards

Shyi-Tsong Wu[1], Bin-Chang Chieu[2] and Jung-Hui Chiu[3]

1. Lecturer, Department of Electronic Engineering, National I-Lan University

2. Professor, Department of Electronic Engineering, National Taiwan University of Science and Technology

3. Associate Professor, Department of Electrical Engineering, Chang Gung University

Abstract

Elliptic Curve Cryptography (ECC) sustains equal security for a far small bit size and gains more and more attention. Based on ECC, we proposed a remote authentication scheme with smart cards. The scheme needs no password table to verify the legitimacy of the login user. It allows the users to choose and change their password freely rather than system computed un-human lengthy passwords. The scheme inherits the merits of ECC of small key size, fast computation and saving communication bandwidth.

Key Words: Remote authentication, Smart card, Elliptic curve cryptography

[2]. Introduction

In1981, Lamport [1] proposed a remote authentication with insecure communication. The scheme can resist replaying attack, but it needs a password table for verifying the legitimacy of the login user. Then ID-based scheme [2-8] are proposed to eliminate the drawback of using directory table. However in these schemes, the secret key corresponding to an ID is assigned by password generation center. It is against the user's habit. Based on discrete logarithm problem, the password authentication scheme proposed by Yang and Shieh [9], further allows the users choose and change their password freely. But, the scheme employs discrete exponential operation. It is very time-consuming and not suited for smart card systems.

Elliptic curve cryptography is one of the best cryptographic techniques because of its small key size and high security [10]. It provides the highest security strength per bit of any cryptosystem known today. ECC's properties make it especially well suited to mobile communications and smart card systems.

Integrated the elliptic curve cryptography, ID-based scheme and smart cards, we propose the remote authentication scheme on smart card system. Our scheme inherits both the merits of elliptic curve cryptography and ID-based scheme. It not only provides the same advantages as that of Yang and Shieh's scheme, but also significantly reduces the computation cost and the bandwidth of communication for remote authentication. Low communication bandwidth, low computation costs, no password table, and the permission of the random change of user's password make our scheme more user-friendly and efficient.

II. Elliptic curve cryptography

In this section, we introduce the elliptic curve cryptography. Elliptic curves are so named because they are described by cubic equations. The cubic equation for elliptic curve takes the form:

$$y^2+axy+by = x^3+cx^2+dx+e \quad (1)$$

where a, b, c, d and e are real numbers that satisfy some conditions [11]. 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 $\boldsymbol{O}$. Figure 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 $\mathbf{P}+\mathbf{Q}=\mathbf{R}$.

In the field of characteristic p and the curve equation is $y^2 = x^3+ax^2+b$. Consider adding two distinct points $\mathbf{P} = (x_1, y_1)$ and $\mathbf{Q} = (x_2, y_2)$ to give $\mathbf{R} = (x_3, y_3)$. The addition rule is defined as follows [11]:

$\mathbf{R}(x_3, y_3) = \mathbf{P}(x_1, y_1) + \mathbf{Q}(x_2, y_2)$, $\mathbf{R} \neq \boldsymbol{O}$

where $x_3 = \lambda^2 - x_1 - x_2$,

$y_3 = (x_1 - x_3)\lambda - y_1$

and $\lambda = (y_2 - y_1)/(x_2 - x_1)$ when $x_1 \neq x_2$

or $\lambda = (3x_1^2 + a)/2y_1$ when $x_1 = x_2$, $y_1 \neq 0$

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 $s*\mathbf{P} = \mathbf{G}$, where the $s*\mathbf{P}$ indicates s times multiplication of the point **P** on an elliptic curve. This is the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Table 1 compares the key sizes needed for equivalent security strength in ECC with RSA and DSA. The key sizes are considered to be equivalent strength based on MIPS years need to recover one key [10]. From this table, it is easy to see that the security strength of ECC is harder than the popular public key systems RSA and DSA.

III. Proposed scheme

In this section, we propose an ECC based remote authentication scheme with smart card. The scheme is separated into four phases: initialization, registration, login and authentication phase.

Some systematic setups will be performed in initialization phase. Prior to access remote system, a new user should submit his identity and password to the key information center for registration in the registration phase, and the key

information center will issue a smart card for the new user. In the login phase, the user attaches his smart card to the input device terminal and keys in his identifier ID_i and password PW_i. Then the terminal sends a login request message to the remote host. During the authentication phase, the remote host verifies the correctness of the submitted message and decides whether to accept the login request or not.

Initialization Phase: Firstly, an elliptic curve E with order p and a base point $\mathbf{P}$ are selected and made public to all users by key information center. The key information center is responsible for generating key information, issuing smart cards to new users and serving password-changing request for the registered users.

Registration Phase: In the registration phase, the user i submits his identifier ID_i and his choosing password $PW_i \in Zp^*$ to the key information center. That must be sent in person or over a secure channel. After receiving the registration request, the key information center performs the following steps on curve E:

1. Compute $\mathbf{A}_i = h(ID_i, s)*\mathbf{P}$. (2)
   where s is a secret key maintained by the system and $h(\cdot)$ is a collision resistant one-way hash function. The hash of the concatenation of message m_1 and m_2 is denoted as $h(m_1, m_2)$.
2. Compute $\mathbf{B}_i = PW_i * \mathbf{A}_i$. (3)
3. The key information center personalizes the smart card with the data: $\{ID_i, \mathbf{A}_i, \mathbf{B}_i, h(\cdot), E, \mathbf{P}\}$.

Login Phase: If the user i wants to login the remote system, he attaches his smart card to the input device terminal, then keys in his identifier ID_i^* and password PW_i^*. The smart card will perform the following operations.

1. Check the validity of the ID_i^*. Whether the ID_i^* is equal to the ID_i that is saved in the memory of the smart card. If they are not equal, the login process will be aborted.
2. Perform the following two following operations on curve E:
   $\mathbf{B}_i^* = PW_i^* * \mathbf{A}_i$ (4)
   $\mathbf{Z}_i = h(\mathrm{T}, \mathbf{B}_i)$ (5)
   where T is the current date and time and is used as a timestamp of the input device terminal.
3. Send a message $m = \{ ID_i^*, \mathrm{T}, \mathbf{B}_i^*, \mathbf{Z}_i \}$ to the remote system.

Authentication Phase: As receiving the message m at the time of T´, the remote system authenticates the user by using the following steps.

1. Verify the formats of ID_i^*. If the format of ID_i^* is not correct, then the system rejects the login request.
2. Verify the validity of time interval between T and T´. If (T´-T) T, where T denotes the expected valid time interval for transmission delay, then the remote system rejects the login request.
3. Compute
   $\mathbf{Z}_i^* = h(\mathrm{T}, \mathbf{B}_i^*)$. (6)
   Compare $\mathbf{Z}_i^*$ and $\mathbf{Z}_i$. If they are equal, the system accepts the request of login, otherwise rejects the request. This is because that
   $\mathbf{Z}_i^* = h(\mathrm{T}, \mathbf{B}_i^*) = h(\mathrm{T}, PW_i^* * \mathbf{A}_i)$ (7)
   and
   $\mathbf{Z}_i = h(\mathrm{T}, \mathbf{B}_i) = h(\mathrm{T}, PW_i * \mathbf{A}_i)$ (8)
   If the equation $\mathbf{Z}_i^* = \mathbf{Z}_i$ holds, it indicates that the password PW_i^* is equal to PW_i, then the system accepts the login request.

IV. Security analysis

ECC delivers the highest strength per bit of any known public-key system because of the difficulty of ECDLP. The security strength of our scheme is strong as it is based on the ECDLP. We analyze the security of our scheme as follows:

1. Replay attack (replaying an old login message $\{ID_i^*, \mathrm{T}, \mathbf{B}_i^*, \mathbf{Z}_i\}$ in Login Phase) cannot work because it will fail in the Step 2 of Authentication Phase for the time interval (T´-T) T.
2. An intruder may try to modify a message $\{ID_i^*, \mathrm{T}, \mathbf{B}_i^*, \mathbf{Z}_i\}$ into $\{ID_i^*, \mathrm{T}^*, \mathbf{B}_i^*, \mathbf{Z}_i\}$, where T^* is the current date and time, to make the Step 2 of Authentication Phase succeed. However such modification will make Step 3 of Authentication

Phase fail for that $\mathbf{Z}_i^*$ $\mathbf{Z}_i$.

3. No one can forge a valid parameter $\mathbf{B}_i^*$ or $\mathbf{B}_i$ to satisfy the equation $\mathbf{Z}_i^* = \mathbf{Z}_i$, because he will face the ECDLP o f equation (4) or the one-way hash function of equation (5).
4. Obtaining a valid message $m = \{ID_i^*, T, \mathbf{B}_i^*, \mathbf{Z}_i\}$, It is feasible to compute PW_i because of the ECDLP.
5. To acquire PW_i from the equation (3) is very difficult, because it will also face the ECDLP.

V. Discussions and conclusions

We have proposed an ECC based, user friendly, smart card remote authentication scheme without using a password file or a verification table. In this paper, we also analyze some possible attacks. Our scheme not only eliminates the drawback of traditional ID-based scheme of assigned un-human lengthy password but also reduces the bandwidth of communication. The scheme inherits the merits of ECC with small key size and high security. Because of its small key size, it has the advantages of lower computation power of processor, smaller bandwidth for communication and smaller memory needed in further applications.

When a user wants to change his password, he can submit his smart card and choose a new password PW_i' to the key information center in person or via a secure channel. The system will perform the new $\mathbf{B}_i'$ as $\mathbf{B}_i' = ID_i * \mathbf{A}_i$, then, write the new $\mathbf{B}_i'$ into the user's smart card to replace the original $\mathbf{B}_i$. After the replacement of $\mathbf{B}_i$ in the smart card of user i, user i can use the new PW_i' to login. Because that the password is chosen freely by the user, it is easy to memorize for the user.

References

[1] Lamport, L., Password authentication with insecure communication, Communication of ACM, Vol.24, 1981, pp.770-772.

[2] Sun, Hung-Min, An efficient remote use authentication scheme using smart card, IEEE transaction on Consumer Electronics, Vol. 46, November, 2000, pp.958-961.

[3] Tsujii, S., T. Itho, and K. Kurosawa, ID-based cryptosystem using discrete logarithm problem, Electronics Letters, Vol. 23, 1978, pp. 1318-1320.

[4] Okamoto, E., and K. Tanka, Identity-based information security managements system for personal computer networks, IEEE Journal on Selected Areas in Communications, Vol.7, No.2, 1989, pp. 290-294.

[5] Chang, C. C. and T. C. Wu, Remote password authentication with smart cards, IEE Proceeding-E, Vol. 138**,** No.3, 1991, pp.165-168.

[6] Chang, C. C. and S. J. Hwang, Using smart cards to authenticate remote passwords, Computers and Mathematical Applications, Vol. 26, No.7, 1993, pp.19-27.

[7] Hwang, Min-Shiang and Li-Hua Li, A new remote user authentication scheme using cards, IEEE Transactions on Consumer Electronics, Vol. 46, February, 2000, pp.28-30.

[8] Sun, Hung-Min, An efficient remote use authentication scheme using smart card, IEEE Transactions on Consumer Electronics, Vol. 46, November, 2000, pp.958-961.

[9] Yang, Wen-Her and Shiuh-Pyng Shieh, Password Authentication Scheme with Smart Cards, Computer & Security, Vol. 18, 1999, pp.727-733.

[10] Monhammed, Elsayed, A. E. Emarah and Kh. El-Shennawy, Elliptic curve cryptosystems on smart card, IEEE 35th International Carnahan Conference on Security Technology, 2001, pp. 213-222.

[11] Stallings, William, Cryptography and Network Security: Principles and Practice, Prentice-Hall, Inc., 1999.

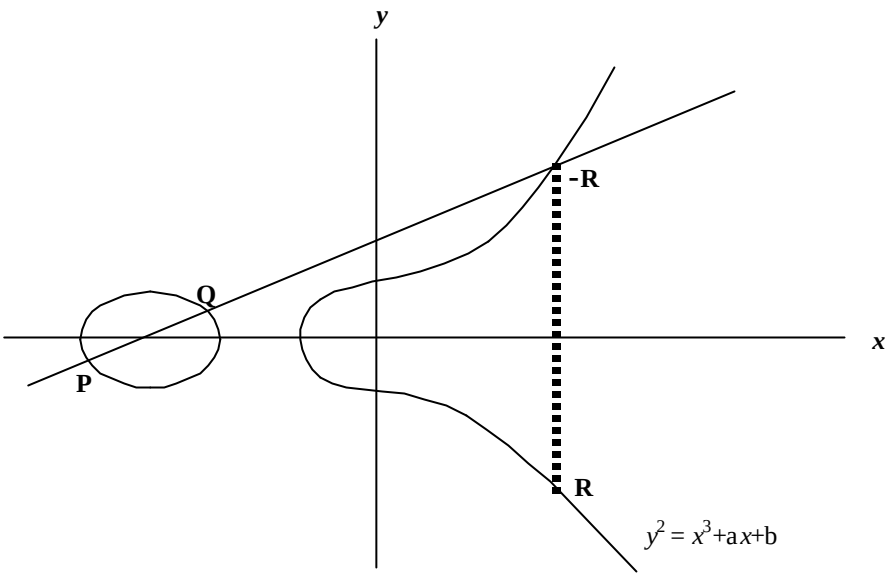

Fig 1 Elliptic Curve of Addition

Time to break in MIPS years	RSA/DSA key size	ECC key size
10^4	512	106
10^8	768	132
10^{11}	1,024	160
10^{20}	2,048	210
10^{78}	21,000	600

Table 1 Key Size Equivalent Strength Comparison