使用封簽的金匙分配法
A Seal-Based Key Distribution Scheme

張真誠和祖善明
Chang, C.C. and Tsu, S. M.

國立中正大學資訊工程系
Department of Computer Science and Information Engineering,
National Chang Cheng University, Chiayi, Taiwan 621, R.O.C
E-mail: ccc@cs.ccu.edu.tw

摘要

在本篇論文中，我們提出一個結合認証公開金匙方法的公開金匙分配法。公開金匙由於其"公開"之特性，使得它非常容易受到各式各樣的攻擊，而我們的方法可以証明每把金匙之正確性。我們的方法主要的貢獻在於公開金匙仍舊為使用者自己決定之條件下減少整個記憶體需求量及計算所需的時間。我們的方法更進一步地使每次通訊所使用的"會議"金匙都不同，以提高相同的二團體在經常互相通訊的情形下之安全層級。
開鍵字：公開金匙認證法，值基於身份碼的方法，自身驗證法，二次剩餘理論。

Abstract

In this paper, we present a public key distribution scheme combined with the public-key authentication. It is essential to certify public keys because the "publicity" makes them vulnerable to active attacks. Without the public-key authentication, many tricks will be easily derived, such as the well-known switching-in attack or substitution of a "forged" public key to a "real" one. Our seal-based key distribution scheme contributes to reduce the amount of storage used and the load of computations required in public key distribution schemes while secret keys can still be determined by the user himself and remain unknown to the authority. Further, our scheme will make the session key different from one time to the next time, it increases the security level when two fixed parties always communicates with each other.

Keywords: pubic-key authentication, identity-based scheme, certificate-based scheme, self-certified public key, quadratic residue theory.

1. Introduction

Public keys, according to their definition, do not need to be protected for confidentiality; on the contrary, they have to be as public as possible. But this "publicity" makes them particularly vulnerable to active attacks, such as the well-known switching-in attack on the Diffe-Hellman public key distribution system[2], where the intruder can result in two keys, one between the sender and the intruder and the other between the intruder and the receiver; in other words, the intruder plays two roles, "forged receiver" and "forged sender"; such an attack will succeed by means of intercepting and forging the transmitted public message in the public channel. Another weakness on the "publicity" of public keys is the substitution of a "forged" public key for a "real" one in a directory.

Shamir[13] suggested a simple but intelligent method to solve the authentication problem in public-key cryptography by making each user's public key be his identification information. The identity-based approach is very attractive, since no public keys need storing and checking. Yet it has a crucial drawback; in such a scheme, it is infeasible for users to compute their secret keys corresponding to a given identity, the secret trapdoor information; in the other words, the authority who knows some secret trapdoor information; in other words, the authority can impersonate any user at any moment since secret keys are calculated by it.

For the purpose of preventing an adversary from fraudulently impersonating another user, it appears to be essential that public-key authentication and public key usage are inseparably combined. There are two solutions proposed for this purpose. One is certificate-based; in such a scheme like[4], each user has a public key and a signature, which is made by a trusted authority and is often called certificate; the authority stores the certificate along with its corresponding public key. Since they are stored in a public directory, the impersonation by substituting public key and the certificate of the public key still works. The other is self-certified public keys[3], the public key itself in such scheme is a certificate, this is why it is called "self-certified"; there is no separate certificate and the public key is not restricted to the identity; but it's drawback is the secret key is always unchanged in such scheme; therefore, it is not appropriate to the application in communications because the shared session key between two fixed users is always the same from one time to the next time.

Maurer and Yacobi [6] introduced a non-interactive public key distribution system, although it is a real non-interactive key exchange scheme embedded with the public key authentication, but the secret keys are still calculated by a trusted authority, and the session key between two parties is always fixed from one time to the next time. Both of them decrease the security level of communication.

Recently, Harn and Yang[5] proposed two identity-based key distribution schemes, one is with direct authentication, and the other is with indirect authentication; the session key, in the former, is always unchanged between two fixed parties; although the later conquers this problem, but the secret keys in such a scheme can not be determined by the user himself; the same drawbacks occurred in [7,8], too.

In this paper, a seal-based method to combine the concepts of public-key authentication and key exchange is presented. It has the following features.

(1)The secret keys are still chosen by the user himself and remain unknown to the authority.
(2) The session key between two fixed parties is always different from one time to the next time.
(3)The public-key authentication can be performed by the user himself, not by the authority.

Our seal-based scheme is neither identity-based nor self-certified since the identity is not the public key and it is used for a "seal" on the public key, that is the reason why we call it "seal-based". The only difference between certificate-based scheme and seal-based is the former does not need to store the seal in the public directory while the later needs.

Since our scheme is based on the Shimada's crytposystem [14], we will first review the scheme in the next section. Our key exchange scheme is presented in Section 3. An improvement is given in Section 4, the security analysis and some conclusions are given in Section 5 and Section 6, respectively.

2. Shimada's Cryptosystem

We review the public-key cryptosystem proposed by Shimada in 1992. This scheme was based on Rabin's enciphering function [10]. In the cryptosystem, two prime numbers p and q are selected with $p \equiv 7 \bmod 8$ and $q \equiv 3 \bmod 8$, respectively; N=pq is used as the public key in this scheme. For a given message $M \in \{0,1,2,\ldots,N-1\}$, T and C are calculated by

$$T = M^2 \bmod N,$$

and $C = T \times E_1(M) \times E_2(M) \bmod N$, where $E_1(M)$ and $E_2(M)$ are defined as follows.

$$E_1(M) = \begin{cases} 1 \text{ if } 0 \le M \le (N-1)/2 \\ -1 \text{ if } (N+1)/2 \le M \le N-1, \end{cases}$$

$$E_2(M) = \begin{cases} 1 \text{ if } J\left(\frac{M}{N}\right) = 1 \text{ or } 0 \\ 2 \text{ if } J\left(\frac{M}{N}\right) = -1, \end{cases}$$

and $J\left(\frac{M}{N}\right)$ is the Jacobi symbol.

Here we give a brief introduction to the **Legendre Symbol** and **Jacobi symbol**.

Definition 2.1

Let Y be an odd prime and X an integer. The Legendre Symbol $L\left(\frac{X}{Y}\right)$ is defined by

$$L\left(\frac{X}{Y}\right) = \begin{cases} 0 \text{ if } Y \mid X \\ 1 \text{ if } X^{(Y-1)/2} \equiv 1 \pmod Y \\ -1 \text{ if } X^{(Y-1)/2} \equiv -1 \pmod Y. \end{cases}$$

Definition 2.2

Let Q be an odd positive integer with prime factorization $Q = Y_1^{t_1} Y_2^{t_2} \ldots Y_m^{t_m}$ and let X be an integer. Then the Jacobi symbol is defined by

$$J\left(\frac{X}{Q}\right) = L\left(\frac{X}{Y_1}\right)^{t_1} L\left(\frac{X}{Y_2}\right)^{t_2} \ldots L\left(\frac{X}{Y_m}\right)^{t_m}.$$

Here we have to note that Jacobi symbol $J\left(\frac{M}{N}\right)$ can be evaluated without knowing the factorization of integer N for complexity $O((\log_2 N)^3)$, the details are shown in Rosen [12].

For a given ciphertext $C \in \{0,1,2,\ldots,N-1\}$, the decipherment is processed below.

Step 1: Calculate T by

$$T = C/[D_1(C)D_2(C)] \bmod N,$$

Where $D_1(C)$ and $D_2(C)$ are defined as follows.

$$D_1(C) = \begin{cases} 1 \text{ if } L\left(\frac{C}{p}\right) = L\left(\frac{C}{q}\right) = 0 \\ L\left(\frac{C}{q}\right) \text{ if } L\left(\frac{C}{p}\right) = 0 \text{ and } L\left(\frac{C}{q}\right) \ne 0, \\ L\left(\frac{C}{p}\right) \text{ if } L\left(\frac{C}{p}\right) \ne 0 \end{cases}$$

$$D_2(C) = \begin{cases} 1 \text{ if } L\left(\frac{C}{p}\right)L\left(\frac{C}{q}\right) = 0 \text{ or } 1 \\ 2 \text{ if } L\left(\frac{C}{p}\right)L\left(\frac{C}{q}\right) = -1 \end{cases},$$

Step 2: Find the solution of $X^2 = T \bmod N$, the plaintext M is one of them satisfying $E_1(X)=D_1(C)$ and $E_2(X)=D_2(C)$.

3. Our Key Exchange Scheme

Similar to other key exchange schemes, our key exchange scheme also needs an authority. The authority may be a government agency, a credit card center or a financial institution, a military command center, a centralized computer facility, etc. In our scheme, the authority is merely used to issue a seal for the public-key registration, it does not participate in the key exchange processing.

There are two phases in our presented scheme; one is the registration phase, and the other is the key exchange phase. Registration is merely performed one time in the register phase when a user joins into the system. During the key exchange phase, if the sender's public key is certified correctly by the other receiver himself, then the common session key is shared by both communicated parties. We assume that there is a trusted authority, called public-key seal issuing center(PSIC), whose duty is to issue a seal for the corresponding user's submitted public key. The secret key and public keys for the PSIC is d and (e, n), which are obtained from the RSA scheme [11]. PSIC also publishes two values: a large prime number P and a primitive element g of GF(P); Pohlig and Hellman [9] suggested that P should be selected such that $P=2P'+1$, where P' is a large prime number, too. Each user U_i can choose his own secret key pair (p_i, q_i), where p_i and q_i are two large relative prime numbers, $p_i = 7 \bmod 8$ and $q_i = 3 \bmod 8$, and there is at least a large prime factor for each of them. Then U_i calculates $n_i=p_iq_i$ as his public key.

Registration Phase

When a user U_i wants to join into the system, he has to submit his identification number ID_i and public key n_i to PSIC, where $n_i=p_iq_i$ and ID_i must be unique and identical to himself. Then the PSIC performs the following steps.

Step 1: Check whether the user U_i's identification is correct or not. If ID_i is false then PSIC rejects the registration.

Step 2: Issue a seal S_i for the user U_i, where
$S_i = (n_i + ID_i)^d \bmod n$.

Step 3: Send the seal S_i back to the user U_i.

Here we have to note that PSIC stores only the public key n_i for each user U_i, not the seal S_i.

Key Exchange Phase

Assume that there are two legal users, user U_A and user U_B. Suppose that U_A and U_B want to communicate in the same session key. This phase provides the authentication of public keys before the session key is constructed. Let each legal user U_i in our scheme have the values:

the secret keys p_i and q_i.

the public key n_i, and the corresponding public-key seal S_i.

Four values e, n, P and g, which are published by the authority PSIC, are known to all legal users in the system. Before two communicated parties construct their common session key, the public-key authentication is performed as follows.

Step 1: User U_A sends his seal S_A to the receiver U_B for requesting a communication.

Step 2: User U_B accesses user U_A's public key n_A, and checks if n_A is correct by the following equation.

$$(S_A)^e - n_A \equiv ID_A \pmod n.$$

If the equation is not true, the communication request from the user U_A is rejected.

Step 3: User U_B sends his seal S_B to the sender U_A for constructing the connection between them.

Step 4: User U_A accesses user U_B's public key n_B, and checks if n_B is correct by the following equation.

$$(S_B)^e - n_B \equiv ID_B \pmod n.$$

If the equation is not true, the communication request is rejected.

After the public-key authentication is successfully completed, the common session key is constructed and shown below.

Step 1: User U_A randomly chooses a number X_A, with $\gcd(X_A, P-1) = 1$, and then calculates K_A by

$$K_A = g^{X_A} \bmod P.$$

Once X_A is obtained, he needs to compute C_A and C_A' as following:

$C_A = K_A^{\ 2} \bmod n_B.$

$C_A' = C_A \times E_1(K_A) \times E_2(K_A) \bmod n_B.$

where $E_1(M)$ and $E_2(M)$are computed by

$$E_1(M) = \begin{cases} 1 \text{ if } 0 \le M \le (n_B - 1)/2 \\ -1 \text{ if } (n_B - 1)/2 \le M \le n_B - 1, \end{cases}$$

and $$E_2(M) = \begin{cases} 1 \text{ if } J\left(\frac{M}{n_B}\right) = 1 \text{ or } 0 \\ 2 \text{ if } J\left(\frac{M}{n_B}\right) = -1. \end{cases}$$

Send C_A' to the receiver U_B.

Step 2: For a given $C_A' \in \{0,1,2...,n_B-1\}$, the receiver U_B calculates C_A by

$$C_A = C_A'/[D_1(C_A')D_2(C_A')] \bmod n_B.$$

where $D_1(C)$ and $D_2(C)$ are computed by

$$D_1(C) = \begin{cases} 1 & \text{if } L\left(\frac{C}{p_B}\right) = L\left(\frac{C}{q_B}\right) = 0 \\ L\left(\frac{C}{q_B}\right) & \text{if } L\left(\frac{C}{p_B}\right) = 0 \text{ and } L\left(\frac{C}{q_B}\right) \ne 0, \\ L\left(\frac{C}{p_B}\right) & \text{if } L\left(\frac{C}{p_B}\right) \ne 0 \end{cases}$$

and $$D_2(C) = \begin{cases} 1 & \text{if } L\left(\frac{C}{p_B}\right)L\left(\frac{C}{q_B}\right) = 0 \text{ or } 1 \\ 2 & \text{if } L\left(\frac{C}{p_B}\right)L\left(\frac{C}{q_B}\right) = -1 \end{cases}$$

Then the receiver U_B finds the solution of $X^2 \equiv C_A \pmod{n_B}$ for which $E_1(X)=D_1(C_A')$, and $E_2(X)=D_2(C_A')$. The solution can be obtained by $K_A = g^{X_A} \bmod P$.

Similarly, the user U_B performs this protocol as the user U_A does. He chooses a random number X_B in this communication. He also sends the value of $C_B' = C_A \times E_1(K_B) \times E_2(K_B) \bmod n_A$ to the user U_A, where $K_B = g^{X_B} \bmod P$ and $C_A = K_A^{\ 2} \bmod n_B$. At least, the user U_A finds the value of K_B.

Since the user U_A can construct

$$K_{AB} \equiv (K_B)^{X_A} \equiv (g^{X_B})^{X_A} \equiv g^{X_A X_B} \pmod P,$$

and the user U_B constructs

$$K_{BA} \equiv (K_A)^{X_B} \equiv (g^{X_A})^{X_B} \equiv g^{X_A X_B} \pmod P,$$

they can construct the same session key $K_{AB} \equiv K_{BA} \equiv g^{X_A X_B} \pmod P$.

The following figures are given to illustrate how these phases work. Figure 1 shows that how the registration phase works, while Figure 2 and Figure 3 demonstrate how the shared session key is constructed.

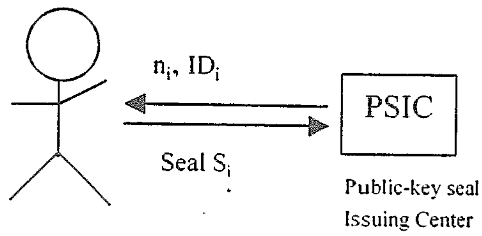

Figure 1: Registration Phase

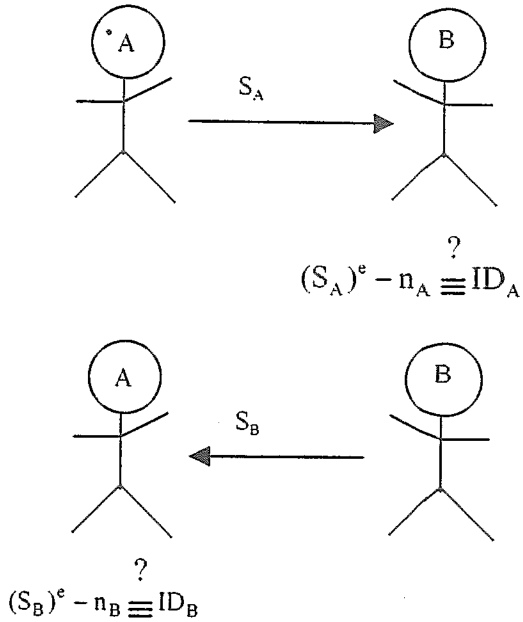

Figure 2: Public-key authentication by seals

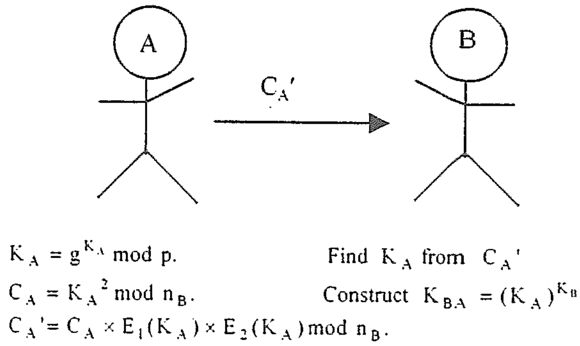

Figure 3: Common session key construction

In the following, we will use an example to illustrate how these phase work.

Example 3.1

Assume that the user U_A wants to communicate with the user U_A. The environment is set up as follows.

PSIC: $n=47 \times 59=2773$, $e=113$, $d=425$, $P=229$, and $g=6$.

User U_A: ID_A =52, p_A =31, q_A =19, n_A =31×19 = 589, and a random number X_A =47.

User U_B: ID_B =79, p_B =23, q_B =11, n_B =23×11 = 253, and a random number X_B =53.

Registration phase

The PSIC computes
$S_A = (ID_A+n_A)^d \bmod n = (52+837)^{425} \bmod 2773 = 963$, for the user U_A, and then computes
$S_B = (ID_B+n_B)^d \bmod n = (79+253)^{425} \bmod 2773 = 474$, for the user U_B,

Key Exchange phase

First, the user U_A sends his seal S_A to the user U_B for requesting a communication. The public-key authentication by the user U_B is performed below.

$$(S_A)^e - n_A \equiv (963)^{113} - 837 \equiv 889 - 837$$
$$\equiv 52 (\mathrm{mod}\ 2773) \equiv ID_A$$

Similarly, the user U_B sends his seal S_B to the user U_A. The verification is computed by the user U_A in the following.

$$(S_B)^e - n_B \equiv (474)^{113} - 253 \equiv 332 - 253$$
$$\equiv 79 (\mathrm{mod}\ 2773) = ID_B$$

After the verifications are completed successfully, the key exchange starts his job as follows.

Step 1: the user U_A chooses a random number X_A = 47, ans calculates K_A by

$K_A = g^{X_A} \bmod P = 6^{47} \bmod 229 = 189$. Next the user U_A computes $C_A = (189)^2 \bmod 253 = 48$, and

$$C_A' \equiv 48 \times E_1(189) \times E_2(189) \equiv 48 \times (-1) \times (1)$$
$$\equiv 205 (\mathrm{mod}\ 253)$$

Then he sends C_A' to the user U_B.

Step 2: After C_A' = 205 is received by the user U_B, the user U_B calculates C_A by

$$C_A \equiv 205/[D_1(205)D_2(205)] \equiv 205/[(-1)(1)]$$
$$\equiv 48 (\mathrm{mod}\ 253)$$

The solutions of $X^2 = 48 \bmod 253$ are 64, 97, 156, and 189. Since

$$E_1(189) = D_1(205) = -1 \text{ and}$$
$$E_2(189) = D_2(205) = -1,$$

So the user U_B can easily conclude that K_A = 189 is the exact solution.

Step 3: the user U_B calculates the common session key K_{BA} by

$$K_{AB} = (K_A)^{X_B} \bmod P = (189)^{53} \bmod 229 = 190.$$

Similarly, the user U_B sends C_B'=320 to the user U_A; the user U_A can find K_B mod P=110, then the common session key K_{AB} can be calculated by

$$K_{AB} = (K_B)^{X_A} \bmod P = (110)^{47} \bmod 229 = 190.$$

4. An Improvement on Shimada's Scheme

Here, we find an efficient way to evaluate the specified solution K_A instead of calculating all solution of X^2 =C mod n; take the above equation $X^2 = 48 \bmod 253$ as the example, the straightforwardly finding of K_A = 189 is given as below.

Step 1: Calculate X_{p_B}, X_{q_B} by

$$X_{p_B} = (48)^{(p_B+1)/4} \bmod p_B = (48)^6 \bmod 23 = 18.$$
$$X_{q_B} = (48)^{(q_B+1)/4} \bmod q_B = (48)^3 \bmod 11 = 9.$$

Step 2: Find an appropriate (α, β) pair by the following table.

Range	$D_1(C)$	$D_2(C)$	(α,β)
$0 < M \le \frac{N-1}{2}$	1	1	(X_{pB}, X_{qB})
$0 < M \le \frac{N-1}{2}$	1	2	$(X_{pB}, q_B - X_{qB})$
$\frac{N}{2} < M \le N-1$	-1	2	$(p_B - X_{pB}, X_{qB})$
$\frac{N}{2} < M \le N-1$	-1	1	$(p_B - X_{pB}, q_B - X_{qB})$

Table 3.1 Relations among the (α,β) pairs, $D_1(C)$ and $D_2(C)$, where $C = M^2 \times E_1(M) \times E_2(M) \bmod n_B$.

For convenience, here we assume that the evaluated values X_{pB} and X_{qB} are quadratic residue module p_B and q_B, respectively. Therefore, from the above example, we can find $\alpha = 23 - 18 = 5$ and β = 11-9 =2

Step 3: Calculate a K_A satisfying that

$$K_A = \alpha \bmod p_B = 5 \bmod 23 \text{, and}$$
$$K_A = \beta \bmod q_B = 2 \bmod 11.$$

Hence $K_A = 189$ is obtained by employing the Chinese Remainder Theorem[1].

5. Security Analysis

We propose several possible attacks to analyze the security of the above scheme. It can be easily seen that none of them can break our scheme.

Attack 1: Assume that a user U_c is an intruder, and he attempts to perform the switching–in attack as it is done in Diffie-Hellman key exchange scheme. He can intercept the information transmitted from the user

U_A to user U_B, i.e. n_A and S_A. Then U_c substitutes n_C and S_C for them. When the user U_B received these values, he can find that $(S_c)^e - n_c \neq ID_A$ in GF(n), then this communication request is rejected. Therefore the intruder U_c can not serve as a "switcher" between any two users in our scheme.

Attack 2: Assume that a user U_c wants to impersonate the user U_A to communicate with the user U_B. He intercepts user U_A's public values, n_A and S_A, and sends them to the user U_B.When the user U_B passes the public-key authentication, he sends back his returned information, C_B', to the intruder U_c, but the impersonater U_c can not recover the value of g^{X_B} mod P since he does not know the factorization of n_A. Hence this impersonation attack can not succeed.

Attack 3: Assume that the user U_c has not the right to communicate with any legal user in the system, i.e. the user U_c is an unauthorized user. Suppose U_c attempts to communicate with a registered user U_B. He create his own public key n_C and its corresponding unauthorized seal S_C, which satisfies $(S_C)^e - n_c \equiv ID_C(\bmod n)$, then sends them to the user U_B; since he did not register in the PSIC, the user U_B can not find his identification number ID_C in the PSIC electronic declaration board. The verification for the public key can not succeed; hence, an unauthorized user can not share the same session key with a registered user.

Attack 4: Assume that the user U_c and the user U_A own the same public key. When U_c registers to the PSIC, he submits user U_A's public key n_A instead of his own's, n_C. If U_c attempts to impersonate user U_A to communicate with another user U_B, since $n_A = n_C$, then $ID_C = S_C{}^e - n_C = S_C{}^e - n_A \neq S_A{}^e - n_A$. That is $ID_C \neq ID_A$, the user U_B will find the sender is the user U_c, not the user U_A. Hence the impersonation can not succeed.

6. Conclusions

We present a seal-based key distribution scheme in this paper. Our scheme is much more different and flexible than the identity-based scheme since the secret keys are selected by each user himself. Besides, our scheme also provides mutual identification with key distribution, which can prevent any intruder's attemption to do switching-in attack. The storage needed is less (= 1/2 times) than that of the certificate-based scheme since no seal is necessary to be stored. Further, the common session key between two communicating users is always different from one time to the next, which is an essential point for the security of communication.

References

[1] Denning, D. E., Cryptography and Data Security, Addison-Wesley, Reading, Massachusetts, 1982.

[2] Diffie, W. and Hellman, M. E., "New directions in cryptography", IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[3] Girault, M., "Self-certified public keys", Proc. Eurocrypt'91, pp. 490-497, 1991

[4] Gunther, C. G., "An identity-based key-exchange protocol", Proc. Eurocrypt'89, pp.29-37,1989.

[5] Lein, H. and Schoubao, Y., "ID-Based cryptographic schemes for user identification, digital signature, and key distribution", IEEE Tournal on Selected Areas in Communications, vol. 11, no. 5, pp. 757-760, June 1993.

[6] Maurer, U. M. and Yacobi, Y.. "Non-interactive public key cryptography", Proc.Eurocrypt'91, pp. 290-294, Feb. 1989.

[7] Okamoto, E. and Tanaka, K., "Identity-based information security management system for personal computer networks", IEEE Journal on Selected Areas in Communications, vol. 7, no. 2, pp. 290-294, Feb. 1989.

[8] Okamoto, E. and Tanaka, K. "Key distribution based on identification information", IEEE Journal on Selected Areas in Communications, vol. 7, no.4, pp. 481-485, May 1989.

[9] Pohling, S. and Hellman, M., "An improved algorithm for computing logarithms over GE(p) and its cryptographic significance", IEEE Trans. Inform. Theory, vol. IT-24, pp. 106-110, 1978.

[10] Rabin, M. O., "Digitalized Signatures and Public Key Functions as Intracrable as Factorization", MIT/LCS/TR-212, Jan. 1979.

[11] Rivest, R. L., Shamir, A. and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM. Vol. 21, no. 2, pp. 120-126, Feb. 1978.

[12] Rosen, K. H., Elementary number theory and its application, Addison-Weslsy, Reading, 1988.

[13] Shamir, A., "Identity-based cryptosystems and signature schemes", Proc. Crypto'84, pp. 47-53, 1984.

[14] Shimada, M., "another Practical Public-key Cryptosystem", Electronics Letters, November 1992, Vol. 28, No. 23, pp. 2146-2147.