中正嶺學報 第三十三卷 第一期 民國 93.11.
JOURNAL OF C.C.I.T., VOL.33, NO.1, NOV., 2004.

Cryptographic Identification of Users Based on Inter-mixed Approach

Pin-Chang Su[*], Erl-Huei Lu[*], and Henry Ker-Chang Chang[**]

Department of Electrical Engineering[*] Department of Business Administration[**]
Chang Gung University, Tao-Yuan, Taiwan, ROC

ABSTRACT

This study presents three identity-based cryptographic schemes, based on two-known assumptions. Most existing cryptosystem designs incorporate just one cryptographic assumption, such as factoring or discrete logarithms. These assumptions appear secure today; but, it is possible that efficient algorithms will be developed in the future to break one or more of these assumptions. The security of the proposed scheme follows from the difficulties in simultaneously solving the factoring (FAC) and discrete logarithms (DL) problems with arithmetic modulo of almost the same size. Each user in the system uses common arithmetic modulo and only requires one public key and one private key. The proposed schemes support user identification, digital signature, and key distribution.

Keywords: id-based, factoring, discrete logarithms, digital signature, key distribution

植基於混合式技術的身分識別密碼機制

蘇品長[*] 盧而輝[*] 張克章[**]

長庚大學電機工程學系[*] 長庚大學企業管理研究所[**]

摘　要

本文提出了三種植基於大家所熟悉的混合式困難度的身分識別密碼技術。現行大多數的密碼學演算法的安全性取決於計算因式分解或離散對數的單一困難度問題，在強調資訊安全的現實生活中，能提供強化演算法的安全性且不影響演算法執行效率，一直是本研究領域首要積極追求的目標。本研究提出植基於同時解因式分解及離散對數困難度的密碼機制，且計算模數等同於一般因式分解模數位數，任一使用者在本架構下僅需一對身分證別碼及私秘金鑰即可。本文架構可適用於使用者身分認證、加解密、數位簽章、金鑰交換及分配等應用機制。

關鍵字：身分基底, 因式分解, 解散對數, 數位簽章, 金鑰分配

文稿收件日期 92.3.21; 文稿修正後接受日期 93.5.26.
Manuscript received Mar. 21, 2003; revised May 26, 2004.

I. INTRODUCTION

Most existing cryptosystem designs incorporate just one cryptographic assumption, such as factoring or discrete logarithms [1-4]. These assumptions appear secure today; but it is possible that efficient algorithms will be developed in the future to break one or more of these assumptions. In 1994, K.S. McCurley proposed the first key distribution system based on two dissimilar assumptions, both of which appear to be hard. In his design, the sizes of the security parameters for these two assumptions are quite different. The modulus to satisfy the proper security requirement for one assumption is too large for the other assumption. The paper proposes a cryptographic system design based on the two popular assumptions: factoring and discrete logarithms. Breaking this system is computationally infeasible because it requires solving the Diffie-Hellman discrete logarithm problem in a subgroup. Thus, in the proposed system it is possible to choose the same size of security parameter for these two assumptions and, therefore, to maintain the efficiency of the implementation. In practice, these types of schemes are not usually implemented in a secure way [5].

In 1985, Shamir [6] introduced the concept of an identity-based cryptosystem, in which each user must visit a key authentication center (KAC) and identify him before participating in a communication. Since then, several ID-based cryptographic algorithms [7-9] based on one hard problem, such as the factorization problem or the discrete logarithm problem, have been proposed. In 1994, Harn and Yang [10] presented a digital signature based on multiple cryptographic assumptions. Unfortunately, Lee and Hwang [11] pointed out that the adversary could forge the signatures of Harn's scheme. However, the performance of these cryptosystems is not better than those of the original El Gamal scheme and RSA. These signature schemes have one common disadvantage, i.e., each user should use his arithmetic modulo. Later, Shao [12] proposed two signature schemes and claimed the security Recently, Lee [13] pointed out that Shao's signature schemes are not sufficiently secure. To overcome weaknesses inherent in Shao's scheme, a digital signature scheme is proposed [14]. This paper is built on that of [14] but has the outstanding advantage of applications in digital signature and key distribution schemes.

In the paper, we propose three identity-based cryptographic schemes based on the FAC and the DL problems. Our schemes can provide user identification, digital signature, and key distribution. We will first review related work in the next section. User identification scheme will be discussed in Sections III. Sections IV and V discuss the digital signature scheme and key distribution schemes. Security and performance analysis are shown in sections VI. At the end, we will make the notable conclusion.

II. RELATED WORK ON INTER-MIXED APPROACH

2.1 Description of Identification schemes

This section describes the ID-DL proposed identification schemes [15]. This scheme is specified by (G, (A, B)), where G is the key generation operation, (A, B) is the three-move interactive protocol between A (prover) and B (verifier).

2.1.1 *Key Generation: G*

The input and output of G are as follows:

Input: Security parameter l, which is a positive integer.

Output: A pair of public-key (p, q, g_1, g_2, t, v), and secret-key, (s_1, s_2).

The operation of G is as follows:

(a) Select primes p and q such that $q \mid p - 1$ and $|q| = l$. (e.g., $q \geq 2^{160}$, and $p \geq 2^{1024}$.)

(b) Select g_1, g_2 of order q in the group Z_p^*, and an integer $t = O(|p|)$. (e.g., $t \geq 20$.) Here, if g_2 is calculated by $g_2 = g_1^{\alpha} \bmod p$, α can be discarded after publishing g_2.

(c) Select random integers s_1, s_2 in Zq, and compute $v = g_1^{-s_1} g_2^{-s_2} \bmod p$.

Remark: (p, q, g_1, g_2, t) can be published by a system manager and used commonly by all system users as a system parameter. The system manager should then also publish some information to confirm to users that these parameters were selected honestly. For example, he publishes some witness that no trapdoor exists in p, g_1, g_2, or that these values are generated honestly. Since the primarily test for p and q is fairly easy for users, they can confirm for themselves that g_1 and g_2 are both of order q. When, as described above, the system parameter is generated and published by each user individually, he does not need to publish such information.

2.1.2 *Interactive Protocol: (A, B)*

The input and output of (A, B) are as follows:

Input: The common input between (A, B) is the public-key (p, q, g_1, g_2, t, v), and the private input of A is the secret-key (s_1, s_2).

Output: B's decision (accept or reject).

The protocol (A, B) is as follows:

(a) A picks random numbers r_1, $r_2 \in Z_q$, and computes $x = g_1^{r_1} g_2^{r_2} \bmod p$ and sends x to B.

(b) B sends a random number $e \in Z_{2^t}$ to A.

(c) A sends to B (y_1, y_2) such that

$y_1 = r_1 + es_1 \bmod q$,
and $y_2 = r_2 + es_2 \bmod q$

(d) B checks that $x = g_1^{y_1} g_2^{y_2} v^e \bmod p$

If it holds, *B* accepts, otherwise rejects.

2.2 Review of He's signature scheme

The proposed scheme [14] can be divided into three phases of initiation, signature generation, and signature verification. Details of the proposed digital signature scheme are described as follows.

2.2.1 *Initiation*

A trusted key authentication center is assumed to select the following system parameters:

(a) A prime modulo P, where $P = 4p_1 \times q_1 + 1$, and $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, and p_1, p_2, q_1, q_2 are all large prime;

(b) An element $g \in z_P^*$ of order $q_1 \times q_2$.

The system parameters P and g are made public and p_1, p_2, q_1, q_2 are all discarded. For convenience, we suppose that $R=(P-1)/4=p_1 \times q_1$. After that, each user chooses a random secret key $x \in Z_R$ such that $\gcd((x+x^{-1})^2, R)=1$ and publishes the corresponding public key $y = g^{(x+x^{-1})^2} \bmod P$.

2.2.2 *Digital signature generation*

Suppose the signer wants to sign a message m. The signer performs the following steps:

(a) Randomly select an integer $t \in Z_R$ such that $\gcd((t+t^{-1})^2, R)=1$. And compute

$r_1 = g^{(t+t^{-1})^2} \bmod P$, $r_2 = g^{(t+t^{-1})^{-2}} \bmod P$.

(b) Find s satisfying

$$(x + x^{-1}) = s(t + t^{-1}) + f(r_1, r_2, m)(t + t^{-1})^{-1} \bmod R$$

where f is a one-way hash function.

(c) Send (r_1, r_2, s) associated with m to the verifier.

2.2.3 *Digital signature verification*

The verifier uses public keys y to verify the signature by checking the following congruent equality:

$$y \overset{?}{=} r_1^{s^2} r_2^{f^2(r_1, r_2, m)} g^{2sf(r_1, r_2, m)} \bmod P.$$

III. USER IDENTIFICATION SCHEME

Generally, an identity-based cryptosystem consists of three phases: the initiation, user registration and application. The first two phases are applicable to all different applications. Since the digital signature and key distribution schemes are derived from the user identification scheme, we present the user identification scheme first. The procedure for identifying user i can be described as follows.

3.1 Initiation

The KAC selects a one-way function f, a large prime $P = 4\ p_1 \times q_1 + 1$ and a primitive element g with order $p_1 \times q_1$ in GF(P), where

$p_1 = 2\,p_2 + 1$, $q_1 = 2\,q_2 + 1$ and p_1, q_1, p_2, q_2 are all primes. The system parameters P and g are made public and p_1, q_1, p_2, q_2 are all discarded. For convenience, throughout this paper, we suppose that $R = (P - 1)/4 = p_1 \times q_1$. After that, a random number $x \in Z_R$, with $\gcd((x + x^{-1})^2, R) = 1$, is selected as KAC's secret key. KAC calculates KAC's public key as follows.

$$Y = g^{(x+x^{-1})2} \bmod P \quad (1)$$

We note that due to the property of $\gcd((x + x^{-1})^2, R) = 1$, the public key y is also a primitive element of Z_R.

3.2 User registration

Each user of the communication facility needs to visit the KAC before he can communicate with other users secretly. At this registration phase, user i will present his identity ID_i to the KAC. If user i is acceptable, the KAC computes an extended identity EID_i for user i as

$$EID_i = f(ID_i) \quad (2)$$

and the signature (r_i, s_i) of EID_i as follows.

*Step*1: Randomly select an integer $t \in Z_R$ such that $\gcd((t + t^{-1})^2, R) = 1$, and compute

$$r_{i_1} = g^{(t+t^{-1})^2} \bmod P \quad (3)$$

$$r_{i_2} = g^{(t+t^{-1})^{-2}} \bmod P \quad (4)$$

$$r_i = r_{i_1} \times r_{i_2} \bmod P \quad (5)$$

where r_{i_1}, r_{i_2} have the same order R.

*Step*2: Find s_i satisfying

$$k_i = (t + t^{-1})^2 + (t + t^{-1})^{-2} \bmod R \quad (6)$$

$$s_i = (EID_i - k_i r_i)(x + x^{-1})^2 \bmod R \quad (7)$$

*Step*3: User i send (ID_i, r_i) to the verifier.

We note that no t should be used repeatedly. Otherwise, the collusion of users can uncover the KAC secret key x. As we will see later, s_i is actually user i's secret key.

3.3 User identification

At this stage, Let us see how user i prove his identity to a verifier without revealing his secret key s_i. We use a challenge-response-type interactive protocol here. The procedure can be described as follows.

*Step*1: The verifier randomly selects an odd number $v \in Z_R$, such that $\gcd(v, R) = 1$ (i.e., $v^{-1} \bmod R$ does exist), and computes

$$W = Y^v \bmod P, \quad (8)$$

where Y is KAC's, public key. W is sent back to user i.

*Step*2: User i compute

$$Z = W^{s_i} \bmod P \quad (9)$$

and send Z back to the verifier.

*Step*3: The verifier uses Z and extended

user identity EID_i of ID_i to verify the following equation:

$$g^{EID_i} = r_i^{r_i} Z^{v^{-1}} \bmod P \qquad (10)$$

If the above equation holds, user *i* is then identified.

IV. DIGITAL SIGNATURE SCHEME

Suppose user *i* wants to sign a message *M*. Without loss of generality, the user's secret key, s_i is assumed to be obtained from user identification scheme.

4.1 Digital signature generating procedure

The digital signature generating procedure can be described as follow.

*Step*1: Find the one-way result,

$M' = f(m, Time)$, where f is the public known one-way function, Time is used as a time-stamp, and *M* is a message to be signed. The one-way function is used to compress the signing message for the identity-based cryptosystem from the replay attack.

*Step*2: User *i* randomly select a number $\alpha \in Z_R$, and computes

$$\beta_i = Y^{\alpha_i} \bmod P \qquad (11)$$

*Step*3: Since gcd(s_i, *R*) = 1, user *i* now solves the congruence

$$M' = \alpha_i \beta_i + \gamma_i s_i \bmod R$$

or

$$\gamma_i = (M' - \alpha_i \beta_i) s_i^{-1} \bmod R \qquad (12)$$

for the integer γ_i, where $0 \le \gamma_i \le R$.

The signature of message *M* is then the ordered triple(r_i, β_i, γ_i), where r_i is the public key of user *i* obtained from the KAC during the registration time.

4.2 Digital signature verification

Upon receiving the set (M, r_i, β_i, γ_i), any user can verify the signature of message M as

$$Y^{M'} = \beta_i^{B_i} \{g^{EID_i} (r_i^{r_i})^{-1}\}^{r_i} \bmod P \qquad (13)$$

where *Y* is KAC's public key, $M' = f(M, Time)$, and $EID_i = f(ID_i)$.

V. KEY DISTRIBUTION SCHEME

Two key distribution schemes are presented. The one provides only direct key authentication, and the common secret session key shared by a pair of users. The other provides a secret session shared key, if the number of users is more than two.

5.1 Scheme 1

All users have registered in KAC. Users *i* and *j* want to share a common secret session key, k_c.

*Step*1: User *i* randomly chooses a random number $v_i \in Z_R$, such that gcd(v_i, *R*)

= 1(i.e., $v_i^{-1} \bmod R$ does exist), then computes

$$W_i = Y^{v_i} \bmod P. \quad (14)$$

By using the signature scheme described in the previous section, user i generates the signature pair (W_i, γ_i) for W_i and sends (ID$_i$, r_i, W_i, γ_i) to user j. W_i is used as both user $_i$'s public key and as part of the signature of itself.

*Step*2: user j chooses $v_j \in Z_R$, and computes

$$W_j = Y^{v_j} \bmod P \; W_j = Y^{v_j} \bmod P. \quad (15)$$

in the same way. Then the signature pair (W_j, γ_j) of W_j is computed, and sends (ID$_j$, r_j, W_j, γ_j) to user i.

*Step*3: Upon receiving (ID$_j$, r_j, W_j, γ_j), user i computes whether the following j congruence hold:

$$k_c = W_j^{v_i} \bmod P. \quad (16)$$

*Step*4: User j verifies the signature of W_i. If the signature is verified, W_i from user i is authenticated by user j. Consequently, user j computes the conference key

$$k_c = W_i^{v_j} \bmod P. \quad (17)$$

5.2 Scheme 2

User 1 is assumed to be the chairman, and he collects and delivers messages between him and user j $(2 \le j \le n)$. Furthermore, all n users share a conventional encryption algorithm, $E_K(.)$, where K is their shared key. k_c will differ each time since the conference key depends on the random number, δ.

*Step*1: User 1 randomly chooses a random number $v_1 \in Z_R$, such that gcd(v_1 , R) = 1(i.e., $v_1^{-1} \bmod R$ does exist), then computes

$$W_1 = Y^{v_1} \bmod P \quad (18)$$

By using the signature scheme described in the previous section, user 1 generates the signature pair (W_1, γ_1) for W_1 and sends (ID$_1$, r_1, W_1, γ_1) to user j $(2 \le j \le n)$. W_1 is used as both user 1's public key and as part of the signature of itself.

*Step*2: Upon receiving (ID$_1$, r_1, W_1, γ_1), user j checks whether the following congruence hold:

$$Y^{M'} = W_1^{W_1} \{g^{EID_1} r_1^{-r_1}\}^{\gamma_1} \bmod P. \quad (19)$$

If holds, user j chooses $v_j \in Z_R$, and computes

$$W_j = Y^{v_j} \bmod P. \quad (20)$$

$$N_j = W_j^{v_j} \bmod P \quad (21)$$

$$\gamma_j = (N_j - W_j v_j) s_j^{-1} \bmod R \quad (22)$$

Then user j sends (ID$_j$, r_j, W_j, γ_j, N_j) to user 1.

*Step*3: Upon receiving (ID$_j$, r_j, W_j, γ_j, N_j),

user 1 checks whether the following *n*-1 congruence hold:

$$Y^{N_j} = W_j^{W_j}(g^{EID_j} r_j^{-r_j})^{\gamma_j} \bmod P. \quad (23)$$

If all the congruence holds, user 1 generates a random number $\delta \in Z_R$, and computes k_c as follows.

$$k_c = Y^{\delta} \bmod P. \quad (24)$$

Also, user 1 computes

$$\eta_j = N_j^{v_1^{-1}\delta} \bmod P, \quad (25)$$

And sends $(\eta_j, E_{k_c}(ID_1))$ to all other user.

*Step*4: User *j* computes the conference key

$$k_c = (\eta_j)^{v_j^{-1}} \bmod P, \quad (26)$$

and verifies it through decryption of $E_{k_c}(ID_1)$.

Since the conference key depends on the random number δ, k_c will be different from one time to the next.

VI. SECURITY AND PERFORMANCE ANALYSIS

In order to analyze the security of the above scheme, we propose five possible forms of attack to analyze the security. None can break the scheme presented here.

6.1 Security analysis

Attack 1: An adversary tries to reveal the private key from the public key for any user.

Analysis of attack 1: First, any adversary needs to solve the DL problem from $Y = g^{(x+x^{-1})^2} \bmod P$ to obtain $(x + x^{-1})^2 \bmod R$. The adversary musts solve the FAC problem to derive x from $(x + x^{-1})^2 \bmod R$. Given (ID_i, r_i, Y) as public known information and $g^{EID_i} = r_i^{r_i} Y^{s_i} \bmod P$, deriving s_i is unfeasible.

Attack 2: An adversary attempts an attack by revealing or forging the private key from a valid signature $\{\mathrm{ID}_i, r_i, \beta_i, \gamma_i, W_i\}$.

Analysis of attack 2: To derive s_i from $(EID_i - k_i r_i)(x + x^{-1})^2 \bmod R$, the adversary must know *t* to derive *x*. However, given *Y*, *g* and *r* deriving *t* from $r_i = g^{(t+t^{-1})^2} g^{(t+t^{-1})^{-2}} \bmod P$ is also under the FAC and DL assumptions.

Attack 3: An intruder might try to impersonate user *i* by determining a relationship between two challenged questions, *v* and *v'*.

Analysis of attack 3: The intruder can derive *Z'* as $Z' = Z^{v^{-1}v'} \bmod P$ without knowing s_i since $Z = Y^{v's_i} \bmod P$, by knowing *Z*, *v*, and *v'*. However, obtaining *v* from *W* is equivalent to

computing the FAC and DL assumptions.

Attack 4: An adversary attempts an attack by revealing the conference key from the public key for any user.

Analysis of attack 4: Accordingly, to derive k_c from $(g^{(x+x^{-1})^2})^{\delta} \bmod R$, the adversary must know x to derive δ. However, the adversary must solve the DL and FAC problems.

Attack 5: Suppose n conspirators are present among the users and try to derive the KAC's secret key x.

Analysis of attack 5: For each signature pair (r_i, s_i), the conspirators can construct the following equation.

$$s_i = (EID_i - k_i r_i)(x + x^{-1})^2 \bmod R.$$

x cannot be uniquely determined since k_i and x are unknown parameters, and k_i is different for each pair of signatures.

6.2 Performance analysis

In the following, let us consider the time complexity of our schemes. The computational cost heavily depends on the time of performing modular exponentiation, denoted as T_{exp}, the time for computing the modular inverse, denoted as T_{inv}, and the time for performing the one-way hash function f, denoted as T_f. Suppose that the times for performing modular multiplication and addition could be ignored. The time complexities for the user identification scheme, it requires $5T_{exp} + T_{inv} + T_f$ in total. For the signer and the verifier are $T_{exp} + T_{inv} + T_f$ and $5T_{exp} + T_{inv} + T_f$. Two key distribution schemes require $4T_{exp} + T_{inv} + T_f$ and $7(j + 1)T_{exp} + 2(2j + 1)\ T_{inv} + (j + 1)\ T_f$, $2 \le j \le n$, respectively.

Since γ_i and $s_i^{-1} \bmod R$ can be pre-computed offline, the computational time for a designer is almost the same as for the RSA scheme. The computational time for a verifier is almost the same as for the original ElGamal scheme [16]. Thus, the computational time of our proposed schemes are upper bounded by the worst case of the RSA and ElGamal schemes.

VII. CONCLUSION

In this paper, we modified the Harn and Yang's identity-based cryptographic schemes. Two cryptographic schemes based on the modified scheme have also been successfully generated. The security of the presented scheme is based on difficulties in simultaneously solving the factoring and discrete logarithms problems with arithmetic modulo of almost the same magnitude; we have shown that the proposed schemes are secure against these attacks.

REFERENCES

[1] Su, P. C., Lu, E. H., and Chang, K. C., "ID-Based Cryptographic Schemes based on Factoring and Discrete Logarithms," 37TH Annual IEEE International Carnahan

Conference on Security Technology, Taipei, Taiwan, ROC, pp. 556–563, 2003.

[2] Su, P. C., Lu, E. H., and Chang, K. C., "Cryptographic Identification of Users over Ad hoc Networks", ISCOM, Tao-Yuan, Taiwan, ROC, 2003.

[3] ISO 9735 Part1-Part6, 1997.

[4] Stadler, M., "Publicly Verifiable Secret Sharing," Adv. In Cryptology EUROCRYPT'96, pp. 190-199, 1996.

[5] Stinson, D. R., CRYPTOGRAPHY: Theory and Practice, Florida: CRC Press, 1995.

[6] Su, P. C., Lu, E. H., and Chang, K. C., "Security system with Embedded Traceable Cell," Information Security Conference, Tao-Yuan, Taiwan, ROC, pp.241-247, 2003.

[7] Beth, T., "Efficient zero knowledge identification scheme for smart cards", Proc. Of EUROCRYPT'88, Vol. 330, pp. 77-86, 1988.

[8] Chikazawa, T. and Inoue, T., "Improved identity-based key sharing system for multiaddress communication," Electronics Letters, Vol.28, No. 11, pp. 1015-1017, 1992.

[9] Hwang, T. and Chen, J. L., "Identity-based conference key broadcast systems," IEE Proc. Comput. Digit. Tech., pp. 57-60, 1994.

[10] Harn, L., "Public-key cryptosystem design based on factoring and discrete logarithms," IEE Proc. Comput. Digit. Tech., vol.141, No.3, pp. 193-195, 1994.

[11] Lee, N. Y. and Hwang, T., "Modified Harn signature scheme based on factoring and discrete logarithms," IEE Proc. Comput. Digit. Tech., Vol.143, No.3, pp. 196-198, 1996.

[12] Shao, Z., "Signature schemes based on factoring and discrete logarithms," IEE Proc. Comput. Digit. Tech., Vol.145, No.1, pp. 33-36, 1998.

[13] Lee, N. Y., "Security of Shao's signature schemes based on factoring and discrete logarithms," IEE Proc. Comput. Digit. Tech., vol.146, No.2, pp. 119-121, 1999.

[14] He, W. H., "Digital signature scheme based on factoring and discrete logarithms," Electronics Letters, Vol. 37, No.4, pp. 220-222, 2001.

[15] Okamoto, T., "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," Proc. CRYPTO'92, LNCS 740, pp. 31-53, 1993.