International Journal of Pure and Applied Mathematics
Volume 81 No. 1 2012, 65-79
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

NEW IDENTITY-BASED CRYPTOGRAPHIC SCHEME FOR IFP AND DLP BASED CRYPTOSYSTEM

Chandrashekhar Meshram[1] §, Xiaopeng Huang[2], S.A. Meshram[3]

[1]Department of Applied Mathematics
Shri Shankaracharya Engineering College
Junwani, Bhilai (C.G.), INDIA

[2]Department of Electrical and Computer Engineering
Stevens Institute of Technology Hoboken
New Jersey, 07030, USA

[3]Department of Mathematics
R.T.M. Nagpur University
Nagpur (M.S.), INDIA

Abstract: In 1984, Shamir proposed the concept of the identity-based cryptosystem. Instead of generating and publishing a public key for each user, the identity-based scheme permits each user to choose his name or network address as his public key. This is advantageous to public-key cryptosystems because the public-key verification is so easy and direct. This paper proposes a new identity-based cryptographic scheme for implementing public-key cryptosystem under the security assumptions of integer factorization problem(IFP) and discrete logarithm problem(DLP). The major advantage of the identity-based cryptosystem based on our scheme over other published identity-based cryptosystems is that the number of users can be extended to $a * L$ users without degrading the system's security even when users cospire, where L is the number of the system's secrets and a is the number of factors in $N - 1$.

AMS Subject Classification: 94A60
Key Words: public key cryptosystem, identity based cryptosystem, discrete logarithm problem and integer factorization problem

Received: July 9, 2012

© 2012 Academic Publications, Ltd.
url: www.acadpubl.eu

§Correspondence author

1. Introduction

In an open network environment, secret session key needs to be shared between two users before it establishes a secret communication. While the number of users in the network is increasing, key distribution will become a serious problem. In 1976, Diffie and Hellman [4] introduced the concept of the public key distribution system (PKDS). In the PKDS, each user needs to select a secret key and compute a corresponding public key and store in the public directory. The common secrete session key, which will be shared between two users can then be determined by either user, based on his own secret key and the partner's public key. Although the PKDS provides an elegant way to solve the key distribution problem, the major concern is the authentication of the public keys used in the cryptographic algorithm.

Many attempts have been made to deal with the public key authentication issue. Kohnfelder [5] used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modulo p, where p is a large prime number; the other is in modulo N, where $N = p \star q$, and p and q are large primes. Blom [7] proposed a symmetric key generation system (SKGS) based on secret sharing schemes. The problems of SKGS however, are the difficulty of choosing a suitable threshold value and the requirement of large memory space for storing the secret shadow of each user.

In 1984, Shamir [1] introduced the concept of an identity. In this system, each user needs to visit a Key authentication center (KAC) and identify him self before joining the network. Once a user's identity is accepted, the KAC will provide him with a secret key. In this way, a user needs only to know the "identity" of his communication partner and the public key of the KAC, together with his secret key, to communicate with others. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of identity-based cryptographic schemes. Okamoto et al. [6] proposed an identity-based key distribution system in 1988, and later, Ohta [10] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [15] for operations in modular N, where N is a product of two large primes, and the security of these schemes is based on the computational difficulty of factoring this large composite number N. Tsujii and Itoh [2] have also proposed an identity-based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the ElGamal

public key cryptosystem.

In 1991, Maurer and Yacobi [26] developed a non-interactive identity-based public-key distribution system. In their scheme, the public keys are self-authenticated and require no further authentication by certificates. However, some problems with this scheme were found, the scheme was modified and the final version was presented [27]. In 1998, Tseng and Jan [28] improved the scheme proposed by Maurer and Yacobi, and provided a non-interactive identity-based public-key distribution system with multi-objectives such as an identity-based signature scheme, an identification scheme, and a conference key distribution system. In their scheme, the computational complexity of the system is heavy. Therefore, it is necessary to have a powerful computational capability. Harn [14] proposed public key cryptosystem design based on factoring and discrete logarithm whose security is based factoring and discrete logarithm. In 2001, Cocks [29] used a variant of integer factorization problem to construct his identity-based encryption scheme. However, the scheme is inefficient in that a plain-text message is encrypted bit-by-bit and hence the length of the output ciphertext becomes long.

In 2004, Lee and Liao [8] design a transformation process that can transfer all of the discrete logarithm based cryptosystems into the identity-based systems rather than reinvent a new system. After 2004 several identity-based cryptosystems [9,17,22, 23, 24, 25] have been proposed. But in these schemes, the public key of each entity is not only an identity, but also some random number selected either by the entity or by the trusted authority. In 2009, Bellare et al. [11] provides security proof or attacks for a large number of identity-based identification and signature schemes. Underlying these is a framework that on the one hand helps explain how these schemes are derived and on the other hand enables modular security analysis, thereby helping to understand, simplify, and unify previous work. In 2010, Meshram [16] has also proposed cryptosystem based on double generalized discrete logarithm problem whose security is based on double generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields. After some time Meshram presented the modification of identity-based cryptosystem based on the double discrete logarithm problem [17,30] and also proposed an identity-based beta cryptosystem, whose security is based on generalized discrete logarithm problem and integer logarithm problem [31]. In 2012, Meshram et al.[32] presented the identity-based cryptographic mechanics based on generalized discrete logarithm problem and integer logarithm problem.

In this study, we design identity-based cryptosystem for discrete logarithm problem with distinct discrete exponent and integer factorization (the basic idea

of the proposed system comes on the public key cryptosystem based on discrete logarithm problem and integer factorization) because we face the problem of solving integer factorization and distinct discrete logarithm problem simultaneously in the multiplicative group of finite fields as compared to the other public key cryptosystem, where we face the difficulty of solving simultaneously the integer factoring and discrete logarithm problem in the common group. Here we describe further considerations such as the security of the system, the identification for senders, etc. Our scheme does not require any interactive preliminary communications in each message transmission and any assumption except the intractability of the discrete logarithm problem and integer factorization problem.(this assumption seems to be quite reasonable) Thus the proposed scheme is a concrete example of an identity-based cryptosystem which satisfies Shamir's original concept [1] in a strict sense.

2. The Public Key Encryption Based on IFP and DLP

In this section, we introduce some notation and parameters, which will be used throughout this paper:
Two large prime numbers p and q are safe primes and set $N = p \star q$. one may use method in [15] to generate strong random primes. A function $\varphi(N) = (p-1)(q-1)$ is a phi Euler function and an integers g is primitive element in $Z^*_{\varphi(N)}$ with order n satisfying $g^{n-1} \equiv 1(mod\ N)$.

The algorithm consists of three subalgorithm, key generation, encryption and decryption.

2.1. Key Generation

The key generation algorithm runs as follows (user 1 should do the following)

1. Pick random an integer $e < N$from $Z^*_{\varphi(N)}$ such that $\gcd(e, N) = 1$.

2. Select a random integer $0 \leq x \leq N-1$ and Compute $y_1 = g^x(mod\ N)$.

3. Use the extended Euclidean algorithm to compute the unique integer d,$1 \leq d \leq \varphi(N)$ such that $ed \equiv 1(mod\ \varphi(N))$.

The public key is formed by (e, y) and the corresponding private key is given by (d, x).

2.2. Encryption

A user 2 to encrypt a message m to user 1 should do the first, randamly choose an integer $0 \leq r \leq \varphi(N) - 1$ plaintext m, is encrypted as

$$C_1 = g^r (mod\ N) \tag{1}$$

$$C_2 = (my_1^{-r})^e (mod\ N) \tag{2}$$

The cipher text is given by $C = (C_1, C_2)$

2.3. Decryption

To decrypt a given ciphertext (C_1, C_2) one does the following:

$$C_1^x C_2^d = m(mod\ N) \tag{3}$$

3. Consistency of the Algorithm

From equation (1) and equation (2) we know that equation (3) is satisfies, note that

$$\begin{aligned} C_1^x C_2^d = [(my^{-r})^e]^d (g^r)^x (mod\ N) &= (my^{-r})(g^{rx})(mod\ N) \\ &= (mg^{-rx} g^{rx})(mod\ N) = m(mod\ N). \end{aligned}$$

4. An Identity-Based Cryptographic Scheme

The ID-based system assumes the existence of a trusted key generation center whose purpose is to provide secrets to each user when he first joins the network. Each user has a q-bits number as his ID number (e. g., $r = 100$). The ID number can be a combination of name, social security number, office number or telephone number. When each user registers his ID number with the trusted center, the center stores it in a public file. Then each user generates a t-dimensional binary vector for his ID. We denoted user k's ID by ID_k as follows:

$$ID_k = (x_{k1}, x_{k2}, x_{k3}, \ldots, x_{kt}), x_{kt} \in \{0, 1\} (1 \leq j \leq t) \tag{4}$$

The center generates two random prime numbers p and q, compute

$$N = p \star q \tag{5}$$

Then the center chooses an arbitrary random number e, $1 \leq e \leq \varphi(N)$ such that $\gcd(e, \varphi(N)) = 1$ where $\varphi(N) = (p-1)(q-1)$ is the Euler function of N. Then the center publishes (e, N) as the public key. Any users can compute the user k's extended ID, EID_k by the following:

$$EID_k = (ID_k)^e = (y_{k1}, y_{k2}, y_{k3}, \ldots, y_{kr}) \qquad (r < t). \tag{6}$$

Here $y_{ki} \in (0,1)$, $(1 \leq i \leq t-1)$, and $y_{kt} = 0$ for $\sum_{i=1}^{t-1} x_{k1}$ is odd number,$y_{kt} = 1$ for $\sum_{i=1}^{t-1} x_{k1}$ is even number. The EID likes a long pseudo-random number which prevents a countermeasure against conspiracy among some users. The center generates two vectors B and C satisfying

$$B = (b_1, b_2, b_3, \ldots, b_r)(1 \leq b_i \leq \varphi(N))(1 \leq i \leq r) \tag{7}$$

where b_i are odd numbers

$$C = (c_1, c_2, c_3, \ldots, c_t)(1 \leq c_i \leq \varphi(N))(1 \leq i \leq t) \tag{8}$$

$$BEID_i \neq BEID_j mod(\varphi(N) - 1) if EID_i \neq EID_j \tag{9}$$

$$CID_i \neq CID_j mod(\varphi(N) - 1) if ID_i \neq ID_j \tag{10}$$

where EID_i and EID_j are the expanded ID_k of user i and j. As defined in equation (6), since EID has odd number of $1k$, if we choose $b_i k$ to be all odd numbers then $BEID(mod\varphi(N) - 1)$ is almost relatively prime to $(\varphi(N) - 1)$ when the number of users is small compared to $(\varphi(N) - 1)$. The center chooses an unique integer d $1 \leq d \leq \varphi(N)$ such that

$$ed \equiv 1(mod\varphi(N)) \tag{11}$$

Now, the center chooses an integer which is a primitive element mod N and then the center computes two vectors U and V by

$$U = (u_1, u_2, u_3, \ldots, u_t) \tag{12}$$

$$V = (v_1, v_2, v_3, \ldots, v_r) \tag{13}$$

$$u_i = \beta^{c_i} mod N, i = 1, 2, \ldots, t \tag{14}$$

$$v_i = \beta^{b_i} mod N, i = 1, 2, \ldots, r \tag{15}$$

Then the center divides all users into k groups, where s is the number of factors in $(\varphi(N)-1)$ which is defined in Section 2. Each group has $L = t+r$ users. Each user knows that all the other users belong to L. If user k registers to the system, the center, issues a smart card to user k after properly verifies his physical identity. The smart card includes the set of integers $(N, N_i, 1 \le i \le s, U, V, s_k)$, where $(N, N_i, 1 \le i \le s, U, V)$ are common to all users while s_k is known only to user k. Numbers $c_j, (1 \le j \le r), b_i, (1 \le i \le t)$, can be aborted after all cards has been issued. If there is no more new user, the center can be closed. Hence $c_j, (1 \le j \le r), b_i, (1 \le i \le t)$, are kept secret from all users. The user k ' s secret, s_k can be calculated by

$$s_k^{'} = s_k mod N_j = \beta N_j + s_k \tag{16}$$

where β is an integer and j is the group to which user k belong s and s_k can be computed by

$$CID_k = (BEID_k)s_k^{'} mod(\varphi(N) - 1) \tag{17}$$

.

$$\sum_{i=1}^{t} c_i x_{ki} = (\sum_{i=1}^{r} b_i y_{ki}) s_k^{'} mod(\varphi(N) - 1) \tag{18}$$

Since $(BEID_k)$ is almost relatively prime to $(\varphi(N) - 1)$, s_k can be uniquely determined. Every user can obtain user k's public key u_k and base β_k from common public information N, N_i, U, and V by

$$u_k = (\prod_{i=1}^{t} (u_i)^{x_{ki}})^{N-1/N_j} = (\beta^{C.ID})^{N-1/N_j} mod N \tag{19}$$

$$\beta_k = (\prod_{i=1}^{r} (v_i)^{x_{ki}})^{N-1/N_j} = (\beta^{B.EID})^{N-1/N_j} mod N \tag{20}$$

where x_{ki}, y_{ki} are defined by Eqs.(4) and (6). From Eqs. $(12) - (20)$, we obtain

$$u_k = (\prod_{i=1}^{t} (u_i)^{x_{ki}})^{N-1/N_j} = (\prod_{i=1}^{r} (v_i)^{x_{ki} s_k^{'}})^{N-1/N_j} = (\beta^{(\sum b_i y_{ki}) s_k^{'}})^{N-1/N_j}$$
$$= \beta_k^{s_k} mod N \tag{21}$$

Note that although β_k is not a primitive root over $Z^*_{\varphi(N)}$, it is infeasible to compute s_k from $u_k = \beta_k^{s_k} mod N$ if N_j is a large prime number from equation (5). In our scheme, for each user k using different base β_k, the security can be increased without increasing the memory size of public file as suggested by Section 2.

5. An Identity-Based Cryptographic Scheme for IFP and DLP based Cryptosystem

Let $m(0 \leq m \leq N-1)$ be the message that user T wants to transmit to user S. User T first computes user k's public key u_k and base g_k from ID_k and the public information in his smart card. He then generates a random number $l(0 \leq l \leq N-1)$ and computes the ciphertext C as follows:

$$C = (C_1, C_2) \tag{22}$$

$$C_1 = g_k^l mod N \tag{23}$$

$$C_2 = m(u_k)^l mod N \tag{24}$$

User T sends the ciphertext C to user k via an insecure channel. When user S receives the ciphertext C, he computes

$$(C_1)^{s_k} = (g_k^l)^{s_k} mod N \tag{25}$$

Then user k recovers the message m by computing

$$\begin{aligned} C_1^{s_k} C_2^d &= [(mu_k^{-l})^e]^d (g_k^l)^{s_k} (mod\ N) = (mu_k^{-l})(g_k^{ls_k})(mod\ N) \\ &= (mg_k^{-ls_k} g_k^{ls_k})(mod\ N) = m(mod\ N). \end{aligned} \tag{26}$$

6. Security Analysis of Proposed Scheme

The security of identity-based cryptosystem based on the index problem in the multiplicative cyclic group $\mathbf{Z}^{\star}_{\varphi(\mathbf{N})}$, where $N = p \star q$ (The factorization of N is known only to the center.) where $\varphi(N)$ is Euler function of N. In this system Coppersmith showed an attacking method [33] such that $(n+1)$ users conspiracy can derive the center's secret information.

Theorem 1. ***Attack*** *1:[33] The $(n+1)$ users $k, (1 \leq k \leq n+1)$ can derive an n-dimensional vector a' over $\mathbf{Z}^{\star}_{\varphi(\mathbf{N})}$ which is equivalent (not necessarily identical) to the original center's secret information.*

Proof. When $(n+1)$ users $k, (1 \leq k \leq n+1)$ conspire, they have the

following system of linear congruences:

$$\begin{pmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{pmatrix} (mod\varphi(N)) \tag{27}$$

Since each EID_k is an n-dimensional binary vector, there exists an $(n+1)$-dimensional vector c over the integer ring such that

$$\sum_{1\leq k\leq n+1} c_k EID_k = 0 \tag{28}$$

Thus we have

$$\sum_{1\leq k\leq n+1} c_k s_k = 0(mod\varphi(N)) \tag{29}$$

And then

$$\sum_{1\leq k\leq n+1} c_k s_k = A(\varphi(N)) \tag{30}$$

If $A \neq 0$, then the $(n+1)$ users can have an integer multiple of $(\varphi(N))$, and they can find out the factorization of N. Then, a similar method with attack (1) is applicable; hence, the center's secret information can be derived by $(n+1)$ users conspiracy. □

Furthermore, Shamir developed a more general attacking method [34] for the modified system such that $(n+2)$ users conspiracy can derive the center's secret information with high probability.

Theorem 2. ***Attack*** *2[34] The $(n+2)$ users $k, (1 \leq k \leq n+2)$ can derive the center's secret information a with high probability.*

Proof. When $(n+1)$ users $k, (1 \leq k \leq n+1)$ conspire, they have the following system of linear congruences: defied by equation (31)

$$\begin{pmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{pmatrix} (mod\varphi(N)) \tag{31}$$

$$= Da(mod\varphi(N)) \tag{32}$$

Assuming that the matrix D includes n linearly independent column vectors over the integer ring, there exist some positive integers $c_k(1 \leq k \leq n+1)$ such that

$$\begin{pmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{pmatrix} - \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{pmatrix} \varphi(N) \tag{33}$$

Thus equation (33) can be rewritten by the following:

$$\begin{pmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ . \\ . \\ a_n \\ -1 \end{pmatrix} = - \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{pmatrix} \varphi(N) \tag{34}$$

$$= D'a' \tag{35}$$

From the assumption that the matrix D in equation (32) includes n linearly independent column vectors over the integer ring, it follows that the matrix D' is nonsingular over the integer ring (i. e., det $D' \neq 0$) with overwhelming probability, and thus, we have $a' \neq (mod\varphi(N))$. On the other hand, we have the following system of linear congruencefs:

$$D'a' = 0(mod\varphi(N)) \tag{36}$$

If the matrix D' is nonsingular over $\mathbf{Z}^{\star}_{\varphi(\mathbf{N})}$, then $a' = (mod\varphi(N))$, and this contradicts the above results. Thus, the matrix D' is singular over $\mathbf{Z}^{\star}_{\varphi(\mathbf{N})}$, and we have det $D' = 0(mod\varphi(N))$ with high probability. Hence, det (D') is divisible by $\varphi(N)$ with high probability. Furthermore, consider the case where the other $(n+1)$ users among $(n+2)$ conspire, and define the matrix D'' in a way similar to the above. Also, det (D'') is divisible by $\varphi(N)$ with high probability. Hence, GCD (det D', det D'') gives $e\varphi(N)$ where e is a small positive integer. By the above procedure, we can evaluate $\varphi(N)$ efficiently. An additional procedure to find the center's secret information is completely the same as attack (Theorem 1). □

Attack 3: L users in the same group j may conspire to derive the center's secret $c_k, 1 \le k \le t$,$b_k, 1 \le i \le r$ by solving L equations of the form of Eqs.(18). They are listed as follows: logarithms.

$$\begin{aligned}
&[(x_{11}c_1+x_{12}c_2+\cdots+x_{1r}c_r) = (y_{11}b_1+y_{12}b_2+\cdots+y_{1t}b_t)s_1 mod(\varphi(N)-1)] mod N_j\\
&[(x_{21}c_1+x_{22}c_2+\cdots+x_{2r}c_r) = (y_{21}b_1+y_{22}b_2+\cdots+y_{2t}b_t)s_2 mod(\varphi(N)-1)] mod N_j\\
&\qquad\qquad\vdots\\
&[(x_{L1}c_1+x_{L2}c_2+\cdots+x_{Lr}c_r) = (y_{L1}b_1+y_{L2}b_2+\cdots+y_{Lt}b_t)s_L mod(\varphi(N)-1)] mod N_j
\end{aligned} \tag{37}$$

Since $N_j \mid (N-1)$ equation (37) can be reformulated as the following form :

$$\begin{aligned}
x_{11}c_1 + x_{12}c_2 + \cdots + x_{1r}c_r &= (y_{11}b_1 + y_{12}b_2 + \cdots + y_{1t}b_t)s_1 mod\ N_j\\
x_{21}c_1 + x_{22}c_2 + \cdots + x_{2r}c_r &= (y_{21}b_1 + y_{22}b_2 + \cdots + y_{2t}b_t)s_2 mod N_j\\
&\vdots\\
x_{L1}c_1 + x_{L2}c_2 + \cdots + x_{Lr}c_r &= (y_{L1}b_1 + y_{L2}b_2 + \cdots + y_{Lt}b_t)s_L mod N_j
\end{aligned} \tag{38}$$

If $GCD(b_t mod N_j, N_j) = 1$ (the probability that $GCD(b_t mod N_j, N_j) \neq 1$ is very small), then there exists $b_r^{-1}(mod N_j)$. Multiplying both sides of equation (38) by b_r^1 we have

$$\begin{aligned}
x_{11}c_1^{'} + x_{12}c_2^{'} + \cdots + x_{1r}c_r^{'} &= (y_{11}b_1^{'} + y_{12}b_2^{'} + \cdots + y_{1t}b_t^{'})s_1 mod\ N_j\\
x_{21}c_1^{'} + x_{22}c_2^{'} + \cdots + x_{2r}c_r^{'} &= (y_{21}b_1^{'} + y_{22}b_2^{'} + \cdots + y_{2t}b_t^{'})s_2 mod N_j\\
&\vdots\\
x_{L1}c_1^{'} + x_{L2}c_2^{'} + \cdots + x_{Lr}c_r^{'} &= (y_{L1}b_1^{'} + y_{L2}b_2^{'} + \cdots + y_{Lt}b_t^{'})s_L mod N_j
\end{aligned} \tag{39}$$

where $c_k^{'} = c_k b_r^{-1}(mod N_j), (1 \le i \le t)$ and $b_s^{'} = b_s b_r^{-1}(mod N_j), (1 \le s \le r-1)$ the reformulation of equation (39) yields

$$\begin{pmatrix}
x_{11} & x_{12} & . & . & . & x_{1t} & -x_{11}s_1 & -x_{12}s_1 & . & . & . & -x_{1,r-1}s_1\\
x_{21} & x_{22} & . & . & . & x_{2t} & -x_{21}s_2 & -x_{22}s_2 & . & . & . & -x_{2,r-1}s_2\\
. & . & . & . & . & . & . & . & . & . & . & .\\
. & . & . & . & . & . & . & . & . & . & . & .\\
. & . & . & . & . & . & . & . & . & . & . & .\\
x_{L1} & x_{L2} & . & . & . & x_{Lt} & -x_{L1}s_L & -x_{L2}s_L & . & . & . & -x_{L,r-1}s_L
\end{pmatrix}$$

$$\begin{pmatrix} C'^T \\ B'^T \end{pmatrix} = \begin{pmatrix} y_{1r}s_1 \\ y_{2r}s_2 \\ \vdots \\ y_{Lr}s_L \end{pmatrix} = \begin{pmatrix} Y \end{pmatrix} * \begin{pmatrix} C' & B' \end{pmatrix} mod N_j \tag{40}$$

If $GCD(\mid Y \mid, N_j) = 1$, then we can uniquely calculate C' and B'. Then all conspirators $k(1 \leq k \leq L)$ in the same group j can find user h's secret-key $s_h(h > L)$ by

$$s_h = (x_{h1}c'_1 + x_{h2}c'_2 + \cdots + x_{hr}c'_r) \star (y_{h1}b'_1 + y_{h2}b'_2 + \cdots + y_{ht}b'_t)^{-1} mod N_j \tag{41}$$

This implies that L users in the same group j can recover message from user h in the same group j. However, they cannot derive any user's secret key which is in another group since the modulo is different.

7. Conclusion

In this present paper an identity-based cryptosystem for integer factorization problem and discrete logarithm problem in the multiplicative group of finite fields. The proposed scheme satisfies Shamir's original concepts in a strict sense, i. e. it does not require any interactive preliminary communications in each data transmission and has no assumption that tamper free modules are available. This kind of scheme definitely provides a new scheme with a longer and higher level of security than that based on a factoring and discrete logarithm problem. The proposed scheme does not need a large public-file or the exchange of private/ public keys. Instead, each user has a personal smart card storing the public information and his private keys. The number of users can be extened to $a * L$ users without the threatening of forming conspiracy where L is the number of system's secret key and a is the number of factors of $N - 1$. The major difficulty of implementing an identity-based cryptosystem is to design a system which can prevent conspiracy from its users whose number is much large than the number of the system's secrets. Our proposed cryptosystem cannot satisfy the above general requirement. However, the users can be partitioned into different groups instead and the system's security can be improved by using our scheme. The partition strategy needs to be further studied.

References

[1] A. Shamir, Identity-based cryptosystems and signature schemes, *In Proc. of CRYPTO'84* , **196** of LNCS (1984), 47-53.

[2] S. Tsujii, and T. Itoh, An ID-Based Cryptosystem based on the Discrete Logarithm Problem, *IEEE Jounral on selected areas in communications*, **7** (1989), 467-473.

[3] T. ElGmal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Trans. Inform. Theory*, **31** (1995), 469-472.

[4] W. Diffie and M. E. Hellman, New direction in Cryptography, *IEEE Trans. Inform. Theory*, **22** (1976), 644-654.

[5] L. M. Kohnfelder, *A method for certification*, Lab. Comput. Sci. Mass. Inst. Technol. Cambridge, MA, May (1978).

[6] E. Okamoto and K. Tanaka, Key distribution system based on identification information, *IEEE J. Sel. Areas Commun.*, **7** (1989), 481-485.

[7] R. Blom, An optimal class of symmetric key generation systems, *In Proc. Eurocryp '84, Pans, France* (1984), 335-338.

[8] Wei-Bin Lee and Kuan-Chieh Liao, Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, *Journal of Network and Computer Applications*, **22** (2004), 191-199.

[9] Min-Shiang Hwang, Jung-Wen Lo and Shu-Chen Lin, efficient user identification scheme based on ID-based cryptosystem, *Journal of Network and Computer Applications*, **26** (2004), 565-569.

[10] K. Ohta, Efficient identification and signature schemes, *Electron. Lett.*, **24(2)** (1988), 115-116.

[11] Mihir Bellare, Chanathip Namprempre and Gregory Neven, Security Proofs for Identity-Based Identification and Signature Schemes, *Journal of Cryptology*, **22** (2009), 1-61.

[12] R. C. Merkle and M. E. Hellman, Hiding information and signatures in trapdoor knapsacks, *IEEE Trans. Inform. Theory*, **IT-24** (1978), 525-530.

[13] S. Tsujii, J. Chao and K. Araki, A Simple ID-Based Scheme for Key Sharing, *IEEE Jounral on Selected Area in Communication*, **11**, No. 5 (1993), 730-734.

[14] L. Harn, Public key cryptosystem design based on factoring and discrete logarithm, *IEE Pro. Comput. Digit. Tech*, **141**, No. 3 (1994), 193-195.

[15] J. Gordon, Strong RSA keys, *Electron. Letter*, **20**, No. 12 (1984), 514-516.

[16] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz, Chosen-ciphertext security from identity-based encryption, *Electron. Letter*, **36**, No. 5 (2007), 1301-1328.

[17] Eike Kiltz and Yevgeniy Vahlis, CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption, *In CT-RSA*, **4964** of LNCS (2008), 221-239.

[18] Chandrashekhar Meshram, A Cryptosystem based on Double Generalized Discrete Logarithm Problem, *Int. J. Contemp. Math. Sciences*, **6**, No. 6 (2011), 285-297.

[19] Chandrashekhar Meshram, Modified ID-Based Public key Cryptosystem using Double Discrete Logarithm Problem, *International Journal of Advanced Computer Science and Applications*, **1**, No. 6 (2010), 30-34.

[20] Eun-Kyung Ryu and Kee-Young Yoo, On the security of efficient user identification scheme, *Applied Mathematics and Computation*, **171** (2005), 1201-1205.

[21] Chandrashekhar Meshram and Shyam Sundar Agrawal, An ID-Based Public Key Cryptosystem based on Integer Factoring and Double Discrete Logarithm Problem, *Information Assurance and Security Letters*, **1** (2010), 29-34.

[22] Raju Gangishetti, M. Choudary Gorantla, Manik Lal Das, Ashutosh Saxena, Threshold key issuing in identity-based cryptosystems, *Computer Standards and Interfaces*, **29** (2007), 260-264.

[23] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks,*IEEE Tran. On Parall. and Distributed Systems*, **27**, No. 9 (2010), 1227-1239.

[24] Dan Boneh and Matthew K. Franklin, Identity based encryption from the Weil pairing,*SIAM Journal on Computing*, **32**, No. 3 (2003), 586-615.

[25] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz, Chosen-ciphertext security from identity-based encryption, *SIAM Journal on Computing*, **36**, No. 5 (2003), 1301-1328.

[26] U. M. Maurer and Y. Yacobi, Non-interactive public key cryptography, *Cryptology-Eurocrypt'91*, New York: Springer (1991), 498-507.

[27] U. M. Maurer and Y. Yacobi, A non-interactive public-key distribution system, *Des. Codes. and Cryptology*, **9**, No. 3 (1996), 305-316.

[28] Y. M. Tseng, J. K. Jan, ID-based cryptographic schemes using a non-interactive public-key distribution system, *The 14th Annual Computer Security Applications Conference* (1998), 237-243.

[29] C. Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues, *International Conference on Cryptography and Coding (Proceedings of IMA)*, **2260** of LNCS, Springer-Verlag (2001), 360-363.

[30] Chandrashekhar Meshram and S. A. Meshram, Some Modification in ID-Based Cryptosystem using IFP and DDLP, *International Journal of Advanced Computer Science and Applications*, **2**, No. 8 (2011), 25-29.

[31] Chandrashekhar Meshram and S. A. Meshram, An Identity based Beta Cryptosystem, *IEEE Proceedings of 7th International Conference on Information Assurance and Security (IAS 2011)*, (2011), 298-303.

[32] Chandrashekhar Meshram, S. A. Meshram and Mingwu Zhang, An ID-based cryptographic mechanisms based on GDLP and IFP, *Information Processing Letters*, **112** (2012), 753-758.

[33] D. Coppersmith, *Private Communication* (Nov. 1987).

[34] A. Shamir, *Private Communication* (June 1988).