Asian Journal of Information Technology 10 (2): 32-35, 2011
ISSN: 1682-3915

Modified ID-Based Public Key Cryptosystem Using Double Discrete Logarithm Problem

Chandrashekhar Meshram
Department of Applied Mathematics, Shri Shankaracharya Engineering College,
Junwani, Bhilai (C.G), India

Abstract: In 1984, Shamir introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a Key Authentication Center (KAC) and identify him self before joining a communication network. Once a user is accepted, the KAC will provide him with a secret key. In this way if a user wants to communicate with others he only needs to know the identity of his communication partner and the public key of the KAC. 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. Meshram and Agrawal have proposed an id-based cryptosystem based on double discrete logarithm problem which uses the public key cryptosystem based on double discrete logarithm problem. In this study, we propose the modification in an id based cryptosystem based on the double discrete logarithm problem and we consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.

Key words: Public key cryptosystem, identity based cryptosystem, discrete logarithm problem, double discrete logarithm problem, establish, India

INTRODUCTION

In a network environment, secret session key needs to be shared between two users to establish a secret communication. While the number of users in the network is increasing, key distribution will become a serious problem. In Diffie and Hellman (1976) 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 stored 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 (1978) used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modular p where p is a large prime number; the other is in modular n where n = p q and p and q are large primes. Blom (1985) 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 Shamir (1985) introduced the concept of an identity. In this system; each user needs to visit a based cryptosystem. Key Authentication Center (KAC) and identify him self before joining the network. Once a user 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 ID-based cryptographic schemes. Okamoto and Tanaka (1989) proposed an identity-based key distribution system in 1988 and later (Ohta, 1988) extended their scheme for user identification. These schemes use the RSA public key cryptosystem (Rivest *et al*., 1978) 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 (1989) have proposed an ID-based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the El-Gamal (1985) public key cryptosystem. Meshram and Agrawal (2010a) have proposed an ID-based cryptosystem based

on the integer factoring and double discrete logarithm problem which uses the public key cryptosystem based on integer factoring and double discrete logarithm problem. Meshram and Agrawal (2010a, b) have also proposed an ID-based cryptosystem based on double discrete logarithm problem which uses the public key cryptosystem based on double discrete logarithm problem.

Now we modified this cryptosystem for discrete logarithm problem with distinct double discrete exponent because we face the problem of solving double and triple distinct discrete logarithm problem at the same time in the multiplicative group of finite fields as compared to the other public key cryptosystem where we face the difficulty of solving the traditional discrete logarithm problem in the common group.

In this study, we present modification in an ID based cryptosystem based on the double discrete logarithm problem with distinct discrete exponent (the basic idea of the proposed system comes on the public key cryptosystem based on double discrete logarithm problem) here researchers describe further considerations such as the security of the system, the identification for senders etc.

The scheme does not require any interactive preliminary communications in each message transmission and any assumption except the intractability of the discrete logarithm problem (this assumption seems to be quite reasonable) thus the proposed scheme is a concrete example of an ID-based cryptosystem which satisfies (Shamir, 1985) original concept in a strict sence.

MODIFIED ID-BASED PUBLIC KEY CRYPTOSYSTEM

Implementation of the ID-Based cryptosystem
Preparation for the enter and each entity:

Step 1: Each entity generates a k-dimensional binary vector for his ID. We denote entity A's ID by ID_A as follows:

$$ID_A = (x_{A1}, x_{A2}, x_{A3}, x_{A4}, \ldots\ldots\ldots, x_{Ak}), x_{Aj} \in \{0,1\}, (1 \le j \le k) \quad (1)$$

Each entity registers his ID with the center and the center stores it in a public file.

Step 2: The center generate two random prime number p and q and compute:

$$N = pq \quad (2)$$

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

$$EID_A = (ID_A)^e \pmod N = (y_{A1}, y_{A2}, y_{A3}, y_{A4}, \ldots\ldots\ldots, x_{At}), y_{Aj} \in \{0,1\}, (1 \le j \le t) \quad (3)$$

Where $t = |N|$ is the numbers of bits of N.

Step 3: Center's secrete information: The center chooses an arbitrary large prime p and q bit and also generated n-dimensional vector. and m-dimensional vector b over Z_p^* which satisfies:

$$a = (a_1, a_2, a_3, \ldots\ldots, a_n), b = (b_1, b_2, b_3, \ldots\ldots, b_m)$$
$$2 \le a_i b_l \le \varphi(N) - 1, (1 \le i \le n), (1 \le l \le m), (m \le n) \quad (4)$$

$$abl \ne abJ \pmod{\varphi(N)}, I \ne J \quad (5)$$

where, I and J are n-dimensional binary vector and stores it as the centers secret information. The condition of Eq. 5 is necessary to avoid the accidental coincidence of some entities secrete key. A simple ways to generate the vectors a and b is to use (Merkle and Hellman, 1978).

Step 4: The center also chooses w which satisfies gcd (w, $\varphi(N)$) = 1 and $w < \lfloor \varphi(N)/n \rfloor$ where [x] also denote the floor function which implies the largest integer smaller than compute x.

The center chooses a super increasing sequences corresponding to a and b as a_i' $(1 \le i \le n)$ and b_l' $(1 \le l \le m)$ satisfies:

$$\sum_{j=1}^{i-1, l-1} a_j' b_j' + v < \varphi(N) \text{ where } v = [\varphi(N)/w] \quad (6)$$

$$\sum_{j=1}^{n} a_j' b_j' < \varphi(N), (m \le n) \quad (7)$$

Then the centre computes:

$$a_i b_l = a_i' b_l' \, w \pmod{\varphi(N)}, \; c_i = a_i b_l \pmod w$$
$$(1 \le i \le n), (1 \le l \le m), (m \le n) \quad (8)$$

Where:

$$a = (a_1, a_2, a_3, \ldots\ldots, a_n), b = (b_1, b_2, b_3, \ldots\ldots, b_m) \quad (9)$$

Remark 1: It is clear that the vector and defined by Eq. 9 satisfies Eq. 4 and 5 the above scheme is one method of

generating an n and m dimensional vectors a and b satisfies (4) (5). In this study, we adopt the above scheme. However, another method might be possible.

Step 5: The center also choose t arbitrary integers (e_1, e_2, e_3, ..., e_t), satisfying gcd (e_i, $\varphi(N)$) = 1, (1<i<t) and compute n-dimensional and m-dimensional vectors D^j and D^k, respectively:

$$D^J = (d_1^j, d_2^j, ..., d_n^j)(1 \le j \le n)$$
$$d_1^j = e_1 a_1 \left(\text{mod}\,\varphi(N)\right)(1 \le 1 \le n) \quad (10)$$

$$D^k = (d_1^k, d_2^k, ..., d_m^k)(1 \le k \le m)$$
$$d_1^k = e_1 b_1 \left(\text{mod}\,\varphi(N)\right)(1 \le 1 \le m)(m \le n) \quad (11)$$

Since, D^j and D^k are one to one system.

Step 5; Center public information: The center chooses two arbitrary generators a and β of Z_p^* and computes n-dimensional vector h using generator a and m-dimensional vector g using generator β corresponding to the vector a and b.

$$h = (h_1, h_2, h_3, ..., h_n), g = (g_1, g_2, g_3, ..., g_m) \quad (12)$$

$$h_i = \alpha^{ai} \bmod N (1 \le i \le n), g_1 = \beta^{bl} \bmod N (1 \le 1 \le m) \quad (13)$$

The center informs each entity (N, a, β, h, g) as public information.

Step 6; Each entity secrete key: Entity A's secrete keys s_a and s_b are given by inner product of a and b (the centre's secret information) and EID_A (entity A's extended ID, Eq. 3):

$$S_a = d_1^j EID_A \left((\text{mod}\,\varphi(N)\right) = \sum_{1 \le j \le n} d_1^j y_{Aj} \left((\text{mod}\,\varphi(N)\right) \quad (14)$$

$$S_b = d_1^k EID_A \left((\text{mod}\,\varphi(N)\right) = \sum_{1 \le j \le n} d_1^k y_{Aj} \left((\text{mod}\,\varphi(N)\right) \quad (15)$$

System initialization parameters

Center ecrete information: a: n-dimensional vector and b: m-dimensional vector (Eq. 8 and 9).

Center public information: h: n-dimensional vector and g: m-dimensional vector (Eq. 12 and 13), p: a large prime number, e: an integer, two generator α and β of Z_p^*. Entity A's secrete keys s_a and s_b = entity A's public information = ID_A: k-dimensional vector.

Protocol of the proposed cryptosystem: Without loss of generality suppose that entity B wishes to send message M to entity A.

Encryption: Entity B generates EID_A (Entity A's extended ID, (Eq. 3) from ID_A. It then computes γ_1 and γ_2 from corresponding public information h and g and EID_A.

$$\gamma_1 = \left(\prod_{1 \le i \le n} h_1^{y_{Ai}}\right)^{e_1} (\text{mod}\,N)$$
$$= \left(\prod_{1 \le i \le n} (\alpha^{a_1})^{y_{Ai}}\right)^{e_1} (\text{mod}\,N)$$
$$= \alpha^{\sum_{1 \le i \le n} e_1 a_1 y_{Ai} \bmod \varphi(N)} (\text{mod}\,N)$$
$$= \alpha^{\sum_{1 \le i \le n} d_1^j y_{Ai} \bmod \varphi(N)} (\text{mod}\,N) = \alpha^{sa\,(\text{mod}\,N)}$$
$$\gamma_2 = \left(\prod_{1 \le i \le m} g_1^{y_{Ai}}\right)^{e_1} (\text{mod}\,N)$$
$$= \left(\prod_{1 \le i \le m} (\beta^{bl})^{yAl}\right)^{el} (\text{mod}\,N)$$
$$= \beta^{\sum_{1 \le i \le n} e_1 b_1 y_{Ai} \bmod \varphi(N)} (\text{mod}\,N)$$
$$= \beta^{\sum_{1 \le i \le n} d_1^k y_{Ai} \bmod \varphi(N)} (\text{mod}\,N)\, \beta^{sa\,(\text{mod}\,N)}$$

Entity B use γ_1 and γ_2 in Public key cryptosystem based on double discrete logarithm problem. Let M ($1 \le M \le N$) be entity B's message to be transmitted Entity B select two random integer u and v such that ($2 \le uv \le \varphi(N)-1$) and computes:

$$C_1 = \alpha^u \bmod N$$
$$C_2 = \beta^v \bmod N$$
$$E = M(\gamma_1)^u (\gamma_2)^v \bmod N$$
$$= M(C_1^{sa} C_2^{sb}) \bmod N$$

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

Decryption: To recover the plaintext M from the cipher text Entity A should do the following:

Compute:

$$C_1^{(p-1)-sa} \bmod N = C_1^{-sa} \bmod N$$

And

$$C_2^{(p-1)-sb} \bmod N = C_2^{-sb} \bmod N$$

Recover the plaintext:

$$M = (C_1^{-sa} C_2^{-sb} E) \bmod N$$

SECURITY ANALYSIS

The security of the proposed I based cryptosystem is based on the intractability of the discrete logarithm problem. It is very difficult to give formal proofs for the security of a cryptosystem in the following; we analyze some possible attacks against the above schemes and show that the security of these attacks is based on the LP assumption.

An intruder should solve a discrete logarithm problem twice to obtain the private key given the public as following: In this encryption the public key is given by (N, e, α, β, γ_1, γ_2) and the corresponding secret key is given by (S_a, s_b). To obtain the private key (s_a) he should solve the DLP:

$$S_a = \log_\alpha(\alpha^{sa}) \bmod(p)$$

To obtain the private key (s_b) he should solve the DLP:

$$S_b = \log_\beta(\beta^{sb}) \bmod(p)$$

This information is equivalent to computing the discrete logarithm problem over multiplicative cyclic group Z^*_p and corresponding secrete key S_a and S_b will never be revealed to the public.

An intruder might try to impersonate user A by developing some relation between w and w' since $\gamma_1 = Y^{wsa} \pmod N$ and $\gamma'_1\ Y^{w'sa} \pmod N$. Similarly $\gamma_2 = y^{wsb} \pmod N$ and $\gamma'_2\ Y^{w'sb} \pmod N$ by knowing γ_1, γ_2, w, w' the intruder can derive γ'_1 and γ'_2 as $\gamma'_1 = \gamma'^{\,w^{-1}w'}_1 \pmod N$ and $\gamma'_2 = \gamma'^{\,w^{-1}w'}_2 \pmod N$ without knowing S_a and S_b however trying to obtain w from α and β is equivalent to compute the discrete logarithm problem.

CONCLUSION

In this study present the modification in an I-based cryptosystem based on double discrete logarithm problem with distinct discrete exponents 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 double discrete logarithm problem with distinct discrete exponents. The proposed scheme also requires minimal operations in encryption and decryption algorithms and thus makes it is very efficient. The present study provides the special result from the security point of view, because we face the problem of solving double and triple distinct discrete logarithm problem at the same time in the multiplicative group of finite fields as compared to the other public key cryptosystem, where we face the difficulty of solving the traditional discrete logarithm problem in the common groups.

REFERENCES

Blorn, R., 1985. An optimal class of symmetric key generation systems. Proceedings of the EUROCRYPT 84 workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, April 9-11, Pans, France, pp: 335-338.

Diffie, W. and M. Hellman, 1976. New direction in Cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

El-Gamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472.

Kohnfelder, L.M., 1978. A Method for Certification. Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Merkle, R. and M. Hellman, 1978. Hiding information and signatures in trapdoor knapsacks. IEEE Trans. Inform. Theory, 24: 525-530.

Meshram, C.S. and S.S. Agrawal, 2010a. An ID-Based public key cryptosystem based on the double discrete logarithm problem. Int. J. Comput. Sci. Network Security, 10: 8-13.

Meshram, C. and S.S. Agrawal, 2010b. An ID-based public key cryptosystem based on integer factoring and double discrete logarithm problem. Inform. Assurance Security Lett., 1: 29-34.

Ohta, K., 1988. Efficient identification and signature schemes. Electron. Lett., 24: 115-116.

Okarnoto, E. and K. Tanaka, 1989. Key distribution system based on identification information. IEEE J. Selected Areas Commun., 7: 481-485.

Rivest, R.L., A. Shamir and L. Adelman, 1978. A method for obtaining digital signatures and public-key cryptosystem. Comrnun. ACM., 21: 120-126.

Shamir, A., 1985. Identity-based cryptosystem and signature scheme. Adv. Cryptol., 196: 47-53.

Tsujii, S. and T. Itoh, 1989. An ID-based cryptosystem based on the discrete logarithm problem. IEEE J. Selected Areas Commun., 7: 467-473.