An ID-Based Public key Cryptosystem based on the Double Discrete Logarithm Problem

Chandrashekhar Meshram†, Shyam Sundar Agrawal††,

† Faculty of Engineering Mathematics, Disha Institute of Management & Technology, Raipur, India
††Faculty of Engineering Mathematics, Disha Institute of Management & Technology, Raipur, India

Summary
In 1984, Shamir [1] 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. In this paper, we propose 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 and Hash function.

1. 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 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 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 [5] 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 [11] 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 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 et al. [10] proposed an identity-based key distribution system in 1988, and later, Ohta [12] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [20] 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 ID- based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the ElGamal public key cryptosystem. Now we generalized 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

Manuscript received July 5, 2010
Manuscript revised July 20, 2010

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 paper , we present 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 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.(this assumption seems to be quite reasonable)thus the proposed scheme is a concrete example of an ID –based cryptosystem which satisfies Shamir's original concept [1] in a strict sense.

2. The Public key Cryptosystem based on Double Discrete Logarithm Problem

The algorithm consists of three sub algorithms: key generation, encryption and decryption.

1. Key Generation:-
   The key generation algorithm runs as follows:
   1.1 Pick randomly a large prime p and two generators α and β of Z_p^* .
   1.2 Select two random integer a and b such that $1 \le ab \le p-2$.
   1.3 Compute $y_1 = \alpha^a \pmod p$ and $y_2 = \beta^b \pmod p$.

The public key is formed by $(p, \alpha, \beta, y_1, y_2)$ and the corresponding secret key is given by (a, b) .

2. Encryption:-
   An entity B to encrypt a message M to another entity A should do the following:
   2.1 Entity A obtain authentic public key $(p, \alpha, \beta, y_1, y_2)$
   2.2 Message $M \in [0, p-1]$.
   2.3 Select two random integer i and j such that $1 \le ij \le p-2$.
   2.4 Compute $C_1 = \alpha^i \pmod p$ and $C_2 = \beta^j \pmod p$.
   2.5 Compute $\gamma = M\left(C_1^a C_2^b\right) \pmod p$.

The cipher text is given by $C = \left(C_1, C_1, \gamma\right)$.

3. Decryption:-
   To recover the plaintext M from the cipher text Entity A should do the following:
   3.1 Compute $C_1^{(p-1)-a} \pmod p = C_1^{-a} \pmod p$ and $C_2^{(p-1)-b} \pmod p = C_2^{-b} \pmod p$.
   3.2 Recover the plaintext M by computing $\left(C_1^{-a}, C_2^{-b}, \gamma\right) \pmod p$.
   3.3 Return the plaintext M .

4. Verification of the Algorithm:-
   In Encryption

$$C_1 = \alpha^i \pmod p$$
$$C_2 = \beta^j \pmod p$$
$$\gamma = M\left(C_1^a C_2^b\right) \pmod p$$

In Decryption

$$C_1^{(p-1)-a} \pmod p = C_1^{-a} \pmod p$$
$$C_2^{(p-1)-b} \pmod p = C_2^{-b} \pmod p$$

Then

$$\left(C_1^{-a}, C_2^{-b}, \gamma\right) \pmod p = \left(C_1^{-a} C_2^{-b} M C_1^a C_2^b\right) \pmod p$$
$$= \left(C_1^{-a} C_2^{-b} C_1^a C_2^b M\right) \pmod p$$
$$= M \pmod p$$

3. Implementation of the ID –Based Cryptosystem

3.1 Preparation for the center 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:

$$ID_A = (x_{A1}, x_{A2}, x_{A3}, x_{A4}, x_{A5}, \ldots\ldots, x_{Ak})$$
$$x_{A1} \in (0,1) \quad , 1 \le j \le k \tag{1}$$

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

Step 2. Extended ID: The center publishes a one to one function $f(.)$ for example RSA. Any entity can compute entity A's extended ID, EID_A by (3)

$$EID_A = f(ID_A) \tag{2}$$

$$EID_A = (y_{A1}, y_{A2}, y_{A3}, y_{A4}, y_{A5}, \ldots\ldots, y_{An})$$
$$y_{Aj} \in (0,1), (1 \le j \le n) \text{ where } n \succ k \tag{3}$$

The extended ID plays the role of countermeasure against a conspiracy among some entities.

Step 3. Center's secrete information: - The center chooses an arbitrary large prime p so that for example $|p| = 512$ bit and also generated n-dimensional vector a and m-dimensional vector b over Z_p^* which satisfies

$$a = (a_1, a_2, a_3, a_4, \ldots, a_n),$$
$$b = (b_1, b_2, b_3, b_4, \ldots, b_m) \tag{4}$$
$$1 \le a_i b_l \le p-2, (1 \le i \le n), (1 \le l \le m), (m \le n)$$

$$abI \ne abJ (\text{mod } p), I \ne J \tag{5}$$

Where I and J are n-dimensional binary vector and stores it as the centers secret information. The condition of equation (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 Hellmans scheme [21].

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

$$\sum_{1 \le il \le n} a_i^{'} b_l^{'} \prec p-1, (m \le n) \tag{6}$$

Step 4: The center also chooses a w which satisfies $\gcd(w, p-1) = 1$, also compute n-dimensional vector a and m-dimensional vector b as follows

$$a_i = a_i^{'} w (\text{mod } p)(1 \le i \le n),$$
$$b_l = b_l^{'} w (\text{mod } p)(1 \le l \le m) \tag{7}$$

Where

$$a = (a_1, a_2, a_3, a_4, \ldots, a_n),$$
$$b = (b_1, b_2, b_3, b_4, \ldots, b_m) \tag{8}$$

Remark 1: it is clear that the vector a and b defined by (8) satisfies (4)-(5) the above scheme is one method of generating an n and m dimensional vectors a and b satisfies (4)-(5). In this paper, we adopt the above scheme. However, another method might be possible.

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

$$h = (h_1, h_2, h_3, h_4, \ldots\ldots, h_n),$$
$$g = (g_1, g_2, g_3, g_4, \ldots\ldots, g_m) \tag{9}$$

$$h_i = \alpha^{a_i} (\text{mod } p)(1 \le i \le n),$$
$$g_l = \beta^{b_l} (\text{mod } p)(1 \le i \le m) \tag{10}$$

The center informs each entity (p, α, 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, see eqn.2)

$$s_a = a\,EID_A \pmod{p-1}$$

$$= \sum_{1\le j\le n} a_j y_{Aj} \pmod{p-1} \quad (11)$$

$$s_b = b\,EID_A \pmod{p-1}$$

$$= \sum_{1\le j\le n} b_j y_{Aj} \pmod{p-1} \quad (12)$$

4. System Initialization Parameters

4.1 Center Secrete information

a : n -dimensional vector and b m-dimensional vector {see (6)-(8)}

4.2 Center public information

h : n -dimensional vector and g : m-dimensional vector {see (9)-(10)} , p : a large prime number, f : one to one, one way function for example RSA, 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.

5. Protocol of the proposed cryptosystem

Without loss of generality supposes that entity B wishes to send message M to entity A.

5.1 Encryption

Entity B generates EID_A (Entity A's extended ID, see eqn.2) from ID_A. It then computes γ_1 and γ_2 from corresponding public information h and g and EID_A.

$$\gamma_1 = \prod_{1\le i\le n} h_i^{\,y_{Ai}} \pmod{p}$$

$$= \prod_{1\le i\le n} \left(\alpha^{a_i}\right)^{y_{Ai}} \pmod{p}$$

$$= \alpha^{\sum_{1\le i\le n} a_i y_{Ai} \pmod{p-1}} \pmod{p}$$

$$= \alpha^{s_a} \pmod{p}$$

$$\gamma_2 = \prod_{1\le l\le m} g_l^{\,y_{Al}} \pmod{p}$$

$$= \prod_{1\le l\le m} \left(\beta^{bl}\right)^{y_{Al}} \pmod{p}$$

$$= \beta^{\sum_{1\le l\le m} b_l y_{Al} \pmod{p-1}} \pmod{p}$$

$$= \beta^{s_b} \pmod{p}$$

Entity B use γ_1 and γ_2 in Public key cryptosystem based on double discrete logarithm problem.

Let $M(1 \le M \le p-1)$ be entity B's message to be transmitted. Entity B select two random integer u and v such that $(1 \le uv \le p-2)$ and computes

$$C_1 = \alpha^u \pmod{p}$$

$$C_2 = \beta^v \pmod{p}$$

$$E = M\left(\gamma_1\right)^u\left(\gamma_2\right)^v \pmod{p}$$

$$= M\left(C_1^{\,s_a} C_2^{\,s_b}\right) \pmod{p}$$

The cipher text is given by $C = \left(C_1, C_2, E\right)$

5.2 Decryption

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

Compute $C_1^{(p-1)-s_a} \pmod{p} = C_1^{-s_a} \pmod{p}$

And

$$C_2^{(p-1)-s_b} \pmod{p} = C_2^{-s_b} \pmod{p}$$

Recover the plaintext $M = \left(C_1^{-s_a} C_2^{-s_b} E\right) \pmod{p}$

6. Security Analysis

The discrete logarithm problem is one of the hardest problems in computational theory the DLP cryptosystem assumption as follows: given a large prime p and a primitive element α. It is infeasible to compute x knowing $y = a^x \pmod{p}$.

The security of the proposed ID based cryptosystem is based on the intractability of the discrete logarithm problem, hence p

must be chosen large enough .e.g. $|p| = 512$ bits and $(p-1)$ must have at least large prime number.

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 DLP assumption.

1. 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 $(p, \alpha, \beta, \gamma_1, \gamma_2, f)$ and the corresponding secret key is given by (s_a, s_b).

To obtain the private key (s_a) he should solve the DLP

$$s_a \equiv \log_\alpha \left(\alpha^{s_a}\right) (\text{mod } p)$$

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

$$s_b \equiv \log_\beta \left(\beta^{s_b}\right) (\text{mod } p)$$

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.

2. An intruder might try to impersonate user A by developing some relation between w and w' since $\gamma_1 = Y^{w s_a} (\text{mod } p)$ and $\gamma_1' = Y^{w' s_a} (\text{mod } p)$ Similar

$\gamma_2 = Y^{w s_b} (\text{mod } p)$ and $\gamma_2' = Y^{w' s_b} (\text{mod } p)$

by knowing $\gamma_1, \gamma_2, w, w'$ the intruder can derive γ_1' and γ_2' as $\gamma_1' = \gamma_1^{w^{-1} w'} (\text{mod } p)$ and $\gamma_2' = \gamma_2^{w^{-1} w'} (\text{mod } p)$ without knowing s_a and s_b however trying to obtain w from α and β is equivalent to compute the discrete logarithm problem.

4. Conclusion

In this present paper an ID-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 paper 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

[1] A. Shamir, "Identity-based cryptosystem and signature scheme," Advances in Cryptology: Proceedings of Crypto' (Lecture Notes in Computer Science 196). Berlin, West Germany: Springer-Verlag, vol. 84, pp.47-53, 1985.

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

[3] T. ElGmal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Tran Infor Theory, vol. 31, pp. 469-472, 1995.

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

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

[6] Y. Desmedt and J. J. Quisquater, "Public-key system based on the (Is there a difference between DES and difficulty of tampering Advances in Cryptology: Proceedings of Crypto '86 (Lec- RSA?)," in lecture Notes in Computer Science 263). Berlin, West Germany: Springer-Verlag, pp. - 111-117, 1987.

[7] H. Tanaka, "A realization scheme for the identity-based cryptosystem " Advances in Cryptology: Proceedings of Crypto '87 (Lecture Springer- Notes in Computer Science 293). Berlin, West-Germany Springer Verlag, , pp. 340-349, 1988.

[8] S. Tsujii, T. Itoh, and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," Electron. Lett., vol. 23. no. 24, pp 13 18- 1320, 1987.

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

[10] E. Okarnoto and K. Tanaka, "Key distribution system based on identification information," IEEE J. SeIecr. Areas Commun.,vol. 7, pp.481485, May 1989.
[11] R. Blorn, "An optimal class of symmetric key generation systems." In Proc. Eurocryp '84, Pans, France, Apr. 9-11, pp. 335-338, 1984.
[12] K. Ohta, "Efficient identification and signature schemes." Electron. Lett., vol. 24, no. 2, pp. 115-1 16, 1988.
[13] Wei-Bin Lee and Kuan-Chieh Liao "Constructing identity-based cryptosystems for discrete logarithm based cryptosystems" Journal of Network and Computer Applications ,vol. 27, pp. 191–199, 2004.
[14] Min-Shiang Hwang , Jung-Wen Lo and Shu-Chen Lin"An efficient user identification scheme based on ID-based cryptosystem" Computer Standards & Interfaces,vol. 26,pp. 565–569, 2004.
[15] Eun-Kyung Ryu and Kee-Young Yoo "On the security of efficient user identification scheme" Applied Mathematics and Computation ,vol.171, pp. 1201–1205, 2005.
[16] Mihir Bellare , Chanathip Namprempre and Gregory Neven "Security Proofs for Identity-Based Identification and Signature Schemes" J. Cryptol.,vol. 22, pp. 1–61,2009.
[17] K. Koyama and K. Ohta, "Identity-based conference key distribution system," in *Advances in Cryptology: Proceedings* of *Crypto '87* (Lecture Notes in Computer Science 293). Berlin, West Germany: Springer- Verlag, , pp. 175-184, 1988.
[18] K. Nakamura, E. Okamoto, K. Tanaka, and S. Miura, "private communication" Aug. 1987.
[19] D. Coppersmith, "private communication" Aug. 1987.
[20] R. L. Rivest, A. Shamir And L. Adelman, "A method for obtaining digital signatures and public-key cryptosystem," Comrnun. ACM., vol. 21, no. 2, pp. 120-126, 1978.
[21] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks" IEEE Trans. Inform. Theory, vol. IT- 24, pp. 525-530,1978.

Chandrashekhar Meshram received the M.Sc and M.Phil degrees, from Pandit Ravishankar Shukla University,Raipur Chhattisgarh,India in 2007 and 2008, respectively. He is teaching as an Assistant Professor in Department of Mathematics, Disha Institute of Management and Technology Raipur, Chhattisgarh, India. He is doing his research in the field of Cryptography and its Application. He is a member of International Association of Engineers, Hong Kong and Life - time member of Indian Mathematical Society and Cryptology Research Society of India.

Shyam SundarAgrawal received the M.Sc (Maths) and Ph.D Degree from Sambalpur University, Orissa, India in 1997 and 2008, respectively. Presently he is working as an Associate Professor in the Dept. of Applied Mathematics in Disha Institute of Management & Technology, Raipur, India. His research interest includes Decision Making under Fuzzy Logic, Combinatorics and Cryptography. He is a member of IMS, ISTE India and International Association of Engineers.