General Group Oriented ID-Based Cryptosystems with Chosen Plaintext Security

Chunxiang Xu[1], Junhui Zhou[1], and Guozhen Xiao[2]

(Corresponding author: Chunxiang Xu)

School of Computer Science and Engineering, University of Electronic Science and Technology of China [1]
Chengdu, 610054, China (Email: chxxu@uestc.edu.cn)
Information Security and Privacy Institute, Xidian University, Xi'an, 710071, China[2]

(Received Nov. 4, 2005; revised and accepted Apr. 7, 2006)

Abstract

A scheme for general group oriented ID-based cryptosystems is proposed. This scheme allows an authorized subset in the general access structure to cooperatively decrypt the ciphertext of a message. It is constructed using bi-linear pairings. Its security is based on the intractability of the computational bilinear Diffie-Hellman problem. The scheme possesses chosen-plaintext security in the random oracle model.

Keywords: Chosen plaintext security, group oriented cryptosystems, general access structure, ID-based cryptography

1 Introduction

In a group oriented cryptosystem, a group of participants cooperatively decrypt the ciphertext of a message. More generally, a group oriented cryptosystem designates authorized subsets of participants. The members of an authorized subset can cooperatively decrypt the ciphertext. But those of an unauthorized subset cannot obtain any information about the message. The set of all authorized subsets is called the access structure of the participant group [14]. Let N denote the number of participants in the group. Then a (t, N) threshold cryptosystem allows any t or more out of N participants to be an authorized subset. A general group oriented cryptosystem defines an authorized subset by enumerating members. For example, there are five participants P_1, P_2, P_3, P_4 and P_5. We establish three authorized subsets by enumerating members: $\{P_1, P_2, P_3\}$, $\{P_3, P_5\}$, and $\{P_2, P_4, P_5\}$(We only consider the minimal authorized subsets). Note that these authorized subsets cannot be described as a threshold access structure. Sometimes all participants form the only authorized subset. This is a special case of general access structures. Usually so-called group oriented cryptosystems are based on this special access structure.

Group oriented cryptosystems can be certificates-based or ID-based. In certificates-based cryptography, a user chooses his private key, and the trusted authority (TA) issues a corresponding public key for the user. To assure the legal owning relation between a public key and its owner, the TA should generate a certificate for each public key. The certificate is actually the digital signature of the TA on the 2-tuple (*Public key, User's ID*). Thus certificate-based cryptography needs large amount of computation and large number of memory requirements for certificates storing, verification, and revocation. On the other hand, ID-based cryptography allows a user's ID information such as his telephone number, email address, ID card number or other ID information to serve as his public key. Such a public key is clearly bound to the user. It doesn't need a certificate any more. Hence ID-based cryptography reduces largely public keys management overhead. The application potential of ID-based cryptography has been revealed for its attractive characteristics.

Shamir [12] presented the idea of ID-based cryptography to the research society as early as in 1980s. However research on group oriented ID-based cryptosystems opened not long ago, much later than that on the certificates-based [5, 6, 7, 8, 10, 13, 15]. Additionally, It should be pointed out that Fouque et al. [7] and Shoup et al. [13] introduced the provable security approach to the research on group oriented certificates-based cryptosystems and proposed certificates-based threshold cryptosystems with provable security.

Boneh and Franklin [2] proposed the first practical, secure and efficient ID-based encryption scheme using computable bilinear maps. Liber and Quisquater [9] did a generation of Boneh-Franklin's ID-based scheme and proposed an ID-based threshold cryptosystem. Liber and Quisquater's cryptosystem is secure against chosen-plaintext attacks. Baek and Zheng [1] also proposed an ID-based threshold cryptosystem that is secure against chosen-ciphertext attacks. Recently, Z. Chai et al. [3] addressed ID-based threshold decryption without random oracles, the goal of which is to share secrets among the

authorities to remove the key escrow problem in ID-based cryptography.

ID-based group oriented cryptosystems presented in the literature are all of thresh-old schemes so far. In fact, there exist a lot of practical scenarios that cannot be described with the threshold access structure. Obviously, we can describe any scenario with the general access structure. Thus general group oriented cryptosystems have wider application potential than threshold schemes in the real world.

In this paper, we propose a scheme for general group oriented ID-based cryptosystems. The proposed scheme is constructed using bilinear pairings. Its security is based on the intractability of the computational bilinear Diffie-Hellman problem, and it is secure against chosen-plaintext attacks in the random oracle model.

The rest of the paper is organized as follows. In the following section, we discuss bilinear pairings and the bilinear Diffie-Hellman problems. In Section 3, we present our scheme for general group oriented ID-based cryptosystems. The security of our scheme is analyzed in Section 4. Finally Section 5 concludes the paper.

2 Bilinear Pairings and the Bilinear Diffie-Hellman Problems

We first review the Weil parings and the bilinear Diffie-Hellman problems. They are basis of our scheme for general group oriented ID-based cryptosystems.

2.1 The Weil Pairing

Let G_1 and G_2 denote two cyclic groups of the same prime order q, where G_1 is an additive subgroup on an elliptic curve over the finite field $GF(p)$ (p is a large prime), and G_2 is a multiplicative subgroup of the finite field $GF(p^2)$.

The Weil pairing $\hat{e}$ is a bilinear map as $\hat{e} : G_1 \times G_1 \rightarrow G_2$ that satisfies the following three conditions:

1) Non-degeneracy: $\exists P \in G_1, \hat{e}(P, P) \neq 1$;

2) Bilinearity: $\forall P, R, V \in G_1, \hat{e}(P + R, V) = \hat{e}(P, V) \cdot \hat{e}(R, V)$,and $\hat{e}(V, P + R) = \hat{e}(V, P) \cdot \hat{e}(V, R)$;

3) Computability: for any points $P, R \in G_1, \hat{e}(P, R)$ is computable.

2.2 The Bilinear Diffie-Hellman Problems

1) Discrete log problem in G_1 (DL problem):
Let P denote a generator of G_1. Given P and $Q = xP$ where $x \in Z_q^*$, compute x.

2) Computational Diffie-Hellman problem in G_1 (CDH problem):
Given a 3-tuple (P, xP, yP), where P is a generator of G_1 and $x, y \in Z_q^*$, compute xyP.

3) Decision Diffie-Hellman problem in G_1 (DDH problem):
Given a 4-tuple (P, xP, yP, zP), where P is a generator of G_1 and $x, y, z \in Z_q^*$, verify $xy = z \bmod q$.

4) Computational bilinear Diffie-Hellman problem (CBDH problem):
Given a 4-tuple (P, xP, yP, zP), where P is a generator of G_1 and $x, y, z \in Z_q^*$, compute$\hat{e}(P, P)^{xyz}$.

The DDH problem can be effectively solved by means of the properties of the Weil pairings. Compute $\xi = \hat{e}(xP, yP) = \hat{e}(P, P)^{xy}$, and $\eta = \hat{e}(zP, P) = \hat{e}(P, P)^{z}$, then check $\xi = \eta$. If it holds, the 4-tuple (P, xP, yP, zP) is a 4-tuple of the Diffie-Hellman problem, and otherwise it is not. The other three problems, the DL problem, the CDH problem and the CBDH problem are all intractable problems. However, if we could find any solution to the DL problem, that is given (P, xP, yP, zP), we could compute x, y, and z, then we could solve the CDH problem by computing xyP, and solve the CBDH problem by computing $\hat{e}(xyP, zP) = \hat{e}(P, P)^{xyz}$ accordingly. On the other hand, if we could solve the CBDH problem, whether we could solve the CDH problem and the DL problem remains unknown.

3 Scheme for General Group Oriented ID-Based Cryptosystems

The proposed scheme for general group oriented ID-based cryptosystems will be described in four phases: setup, keygen, encrypt and decrypt.

Setup: The key generation center (KGC) generates the system parameters as follows.

- Choose two cyclic groups G_1 and G_2 of the same prime order q, and a Weil map $\hat{e} : G_1 \times G_1 \longrightarrow G_2$, where G_1 is an additive group, and G_2 is a multiplicative group.
- Choose a random number $s \in Z_q^*$ as its master key. Compute its public key as P_{pub}=sP where P is a generator of G_1.
- Choose two hash functions $H_1 : \{0,1\}^* \longrightarrow G_1$ and $H_2 : G_2 \longrightarrow \{0,1\}^n$.

Then we obtain the system parameters $< n, q, G_1, G_2, P, P_{pub}, H_1, H_2, \hat{e} >$.

Keygen: The KGC computes the public key and private key corresponding to an identity $ID \in \{0,1\}^*$ as $Q_{ID} = H_1(ID)$ and $d_{ID} = sQ_{ID}$, respectively.

Encrypt: Let $M = \{P_1, P_2, \cdots, P_N\}$ denote the participants group. Their identities and corresponding private keys are denoted by $(ID_1, ID_2, \cdots, ID_N)$ and $(d_{ID_1}, d_{ID_2}, \cdots, d_{ID_N})$, respectively. The message sender

forms authorized subsets of $M : A_1, A_2, \cdots, A_f$, where $A_j = \{P_1^{A_j}, P_2^{A_j}, \cdots, P_l^{A_j}\}(j = 1, 2, \cdots, f)$. Those in an authorized subset can only be able to cooperatively decrypt the ciphertext of a message.

Suppose that a message $m \in \{0,1\}^n$needs to be sent to M. For each authorized subset $A_j(j = 1, 2, \cdots, f)$, the sender computes $g_{A_j} = \hat{e}(\sum_{P_i^{A_j} \in A_j} Q_{ID_i^{A_j}}, rP_{pub})$, where $r \in_R Z_q^*$, and the ciphertext as $C_{A_j} = (U, V_{A_j}) = (rP, m \bigoplus H_2(g_{A_j}))$.

Decrypt: The participants in any authorized subset $A_j(j = 1, 2, \cdots f)$ can cooperatively decrypt the ciphertext $C_{A_j} = (U, V_{A_j})$. Each participant $P_i^{A_j} \in A_j$ uses his private key $d_{ID_i^{A_j}}$ to calculate $\hat{e}(d_{ID_i^{A_j}}, U)$. Then the message m is calculated as: $m = V \bigoplus H_2(\prod_{P_i^{A_j} \in A_j} \hat{e}(d_{ID_i^{A_j}}, U))$.

Since $\prod_{p_i^{A_j} \in A_j} \hat{e}(d_{ID_i^{A_j}}, U) = \prod_{p_i^{A_j} \in A_j} \hat{e}(sQ_{ID_i^{A_j}}, rP)$ $= \prod_{p_i^{A_j} \in A_j} \hat{e}(Q_{ID_i^{A_j}}, rsP) = \prod_{p_i^{A_j} \in A_j} \hat{e}(Q_{ID_i^{A_j}}, rP_{pub}) = g_{A_j}$, the encrypting algorithm and the decrypting algorithm are consistent.

4 Security Analysis

Now we analyze the security of our scheme in the random oracle model, and prove that the scheme is secure against chosen-plaintext attacks.

First we introduce the notion of chosen-plaintext security [2]. An adversary E wants to attack a cryptosystem Enc. A challenger F serves as a random oracle. E chooses two plaintexts m_0 and m_1, and submits them to F. F computes a ciphertext as $C^* = Enc_{key}(m_b)$ where key is the encryption key and $b \in_R \{0,1\}$ is a random bit. F sends C^* to E, and then E guesses b.

Denote the adversary E's guess result by b'. Define the adversary's advantage as $\varepsilon = Adv(E) = |2Pr[b' = b] - 1|$ where $Pr[.]$ denotes the probability of an event. If ε is negligible, that is, if $Enc_{key}(m_0)$ and $Enc_{key}(m_1)$ are indistinguishable, the cryptosystem Enc is secure against chosen-plaintext attacks (denoted by IND-CPA).

Our scheme is an ID-based one. Suppose that an adversary makes an attack on an authorized subset of which the member number is l. We allow the adversary to possess the most advantageous conditions that he could obtain the private keys of any l-1 participants in the authorized subset, and furthermore, he could also obtain the private keys of any number of participants other than those in the authorized subset. We expect that the scheme remains secure under this worst situation.

Based on the above discussion, we define that a general group oriented ID-based cryptosystem is secure against chosen-plaintext attacks (denoted by IND-ID-ggCPA) if no polynomially bounded adversary has a non-negligible advantage against the cryptosystem in the following game. In the game, E obtains private keys by private key extraction queries.

An adversary E and a challenger F are involved in the game.

Setup: F produces the system parameters with the Setup algorithm of the cryptosystem and sends the system parameters to E.

Phase 1: E designates an authorized subset $A = \{P_1^A, P_2^A, \cdots, P_l^A\}$. The corresponding identity set is $ID_1^A, ID_2^A, \cdots, ID_l^A$. E makes private key extraction queries at any $l-1$ identities in the set. Without loss of generality, suppose that E queries at $(ID_1^A, ID_2^A, \cdots, ID_{l-1}^A)$. F responds with their corresponding private keys $(d_{ID_1{}^A}, d_{ID_2{}^A}, \cdots, d_{ID_{l-1}^A})$. Then E makes a polynomially bounded number of private key extraction queries at any identity other than $ID_1^A, ID_2^A, \cdots, ID_l^A$. The queries may be performed adaptively, that is, a query may depend on the previous answers.

Challenge: E chooses two plaintexts $m_0, m_1 \in \{0,1\}^n$ and sends m_0, m_1 and $\{ID_1^A, ID_2^A, \cdots, ID_l^A\}$ to F. F takes a random bit $b \in_R \{0,1\}$ and computes $C = Encryt(m_b, ID_1^A, ID_2^A, \cdots, ID_{l-1}^A, ID_l^A)$ with the encrypting algorithm in the cryptosystem. F sends C to E.

Phase 2: E issues a second series of private key extraction queries other than at ID_l^A.

Guess: Finally, E guesses a bit b' according to all information he obtained. If $b' = b$, E wins the game.

After receiving the ciphertext C, the adversary E may require more private key extraction queries to help himself. Thus the game adds a second series of private key extraction queries to meet his possible need.

As in IND-CPA, we also define the adversary's advantage as $\varepsilon = Adv(E) = |2Pr[b' = b] - 1|$. Then we have the following theorem.

Theorem 1. *Suppose H_1 and H_2 are random oracles. If an adversary E has a non negligible advantage ε in IND-ID-ggCPA against the proposed scheme for general group oriented ID-based cryptosystems, a challenger F can solve the bilinear Diffie-Hellman problem with an advantage no less than $\varepsilon/q_{H_1}q_{H_2}$ where q_{H_1} and q_{H_2} denote the polynomially bounded number of H_1 queries and that of H_2 queries, respectively.*

Proof. F is given a random instance (P, xP, yP, zP) of the bilinear Diffie-Hellman problem. He tries to compute $\hat{e}(P,P)^{xyz}$ by interacting with the adversary E in the following game.

Setup: F sets $P_{pub} = xP$ and generates the other system parameters $< n, q, G_1, G_2, P, H_1, H_2, \hat{e} >$with the Setup algorithm of the scheme. Then F sends the system parameters $< n, q, G_1, G_2, P, P_{pub}, H_1, H_2, \hat{e} >$ to E.

Phase 1: E queries the random oracles H_1 and H_2. F simulates H_1 and H_2. He responds to the queries and maintains two lists $List_1$ and $List_2$ (Both lists are initially empty) to store the answers for H_1 and those for H_2, respectively.

E first queries H_1 at the identities $ID_1^A, ID_2^A, \cdots, ID_{l-1}^A$ and queries for their corresponding private keys. F responds to the queries with $H_1(ID_i^A) = d_i^A P (i = 1, 2, \cdots, l-1)$where $d_i^A \in_R Z_q^*$, and the private key $d_{ID_i^A} = d_i^A P_{pub} (i = 1, 2, \cdots, l-1)$.

F chooses a random integer $a \in \{1, 2, \cdots, q_{H_1}\}$. Then E takes queries to H_1 at any q_{H_1} identities other than $ID_1^A, ID_2^A, \cdots, ID_{l-1}^A$ and takes queries for their corresponding private keys if he wants. Assume that the queries are distinct. E also issues queries to H_2. F responds to the hash queries and private key extraction queries as follows.

Response to H_1 queries: If a is queried at, then $H_1(ID_a) = yP$. Otherwise $H_1(ID) = dP$ where $d \in_R Z_q^*$, and add the entry (ID, d) to $List_1$.

Response to private key extraction queries: If ID_a is queried at, stop and output "failure". Otherwise, find out the entry (ID, d) in $List_1$ and return dP_{pub} as a private key.

Response to H_2 queries: If any $g_i (i = 1, 2, \cdots, q_{H_1})$ is queried at, search the entry (g_i, R_i) in $List_2$. If found, return R_i to E. Otherwise choose randomly $R_i \in \{0, 1\}^n$, set $H_2(g_i) = R_i$, return R_i, and add the entry (g_i, R_i) to $List_2$.

Challenge: E chooses a pair of plaintexts $\{m_0, m_1\}$ and outputs the identities $(ID_1^A, ID_2^A, \cdots, ID_l^A)$ to be challenged on. If $ID_l^A \neq ID_a$, F stops and outputs "failure". Otherwise, F chooses a random bitstring $R \in_R \{0, 1\}^n$ and sends the ciphertext $C = (zP, R)$ to E.

Phase 2: E issues a second series of queries. F handles these queries in the same way as in Phase 1.

Guess: Define $g = \hat{e}(P, P)^{xyz} \hat{e}(zP, d_{ID_1^A}) \hat{e}(zP, d_{ID_2^A}) \cdots \hat{e}(zP, d_{ID_{l-1}^A})$ and denote by Ψ the event that E makes query to H_2 at the point g during the H_2 queries. Since $Pr[b' = b|\bar{\Psi}] = \frac{1}{2}$, then $Pr[b' = b] = Pr[b' = b|\Psi]Pr[\Psi] + Pr[b' = b|\bar{\Psi}]Pr[\bar{\Psi}] \leq Pr[\Psi] + \frac{1}{2}Pr[\bar{\Psi}] = \frac{1}{2}Pr[\Psi] + \frac{1}{2}$.

We have $Pr[\Psi] \geq 2Pr[b' = b] - 1$. On the other hand, $Pr[b' = b] \geq Pr[b' = b|\bar{\Psi}]Pr[\bar{\Psi}] = \frac{1}{2} - \frac{1}{2}Pr[\Psi]$. Then $Pr[\Psi] \geq 1 - 2Pr[b' = b]$. As a result, we have $Pr[\Psi] \geq |2Pr[b' = b] - 1| = \varepsilon$. F randomly picks an entry $(h, H_2(h))$ from $List_2$, then $Pr[h = g|\Psi] = \frac{1}{q_{H_2}}$. Hence $Pr[h = g] \geq Pr[h = g|\Psi]Pr[\Psi] \geq \frac{\varepsilon}{q_{H_2}}$.

Note that in Challenge, if $ID_a = ID_l^A$, the game will not fail. The probability of the event $ID_a = ID_l^A$ is $Pr[ID_a = ID_l^A] = \frac{1}{q_{H_1}}$ (Assume that E has made H_1 query at the identity ID_l^A). The event $ID_a = ID_l^A$ and the event $h = g$ are independent. Hence $Pr[ID_a = ID_l^A, h = g] = Pr[ID_a = ID_l^A]Pr[h = g] \geq \frac{\varepsilon}{q_{H_1} q_{H_2}}$. Therefore, the probability of the event that F guesses $\frac{g}{\hat{e}(zP, d_{ID_1^A})\hat{e}(zP, d_{ID_2^A}) \cdots \hat{e}(zP, d_{ID_{l-1}^A})}$ as $\hat{e}(P, P)^{xyz}$ is non-negligible, that is, F has a non-negligible probability to find out a solution to the CBDH problem. □

5 Conclusions

We proposed a scheme for general group oriented ID-based cryptosystems using the Weil pairing and the CBDH problem. And we proved that our scheme is secure against chosen plaintext attack (IND-ID-ggCPA) in the random oracle model. Furthermore, since the message sender designates authorized subsets in our scheme, participants are known to him. Such scenarios are often seen in practice. For example, someone himself determines who can read his mail when he is absent; a person himself determines that which family members can access his testament. In most other group oriented encryption schemes, participants are anonymous to the message sender. This needs the third party to define authorized subsets.

Similarly, we can construct another scheme for general group oriented ID-based cryptosystems that possesses the security against chosen ciphertext attack. This work is under investigation.

References

[1] J. Baek and Y. Zheng, "Identity-based threshold decryption," in *Proceedings of PKC'04*, LNCS 2947, pp. 262-276, Springer, 2004.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceeding of CRYPTO 2001*, pp. 213-229, Springer-Verlag, 2001.

[3] Z. Chai, Z. Cao, and R. Lu, "ID-based threshold decryption without random oracles and its appli-cation in key escrow," in *Proceedings of the 3rd International Conference on Information Security*, pp. 119-124, ACM Press, New York, 2004.

[4] L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings," in *Proceedings of the 16th Computer Security Foundations Workshop (CSFW-16)*, pp. 219-233, 2003.

[5] Y. Desmedt, "Society and group oriented cryptography: a new concept," in *Proceeding of Crypto'87*, pp. 120-127, Springer-Verlag, 1988.

[6] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Proceeding of Crypto'89*, pp. 307-315, Springer-Verlag, 1990.

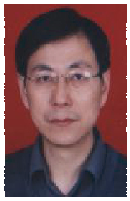
[7] P. Fouque and D. Pointcheval, "Threshold cryptosystems secure against chosen-ciphertext attacks," in *Proceedings of AsiaCryp'2001*, pp. 351-368, Springer-Verlag, 2001.

[8] T. Hwang, "Cryptosystem for group oriented cryptography," in *Proceedings of Eurocrypt'90*, pp. 352-360, Berlin, Springer-Verlag, 1991.

[9] B. Libert and J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in *Proceedings of the 22nd annual symposium on Principles of distributed computing*, pp. 163-171, ACM Press, 2003.
[10] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Proceedings of Eurocrypt'91*, pp. 522-526, Springer-Verlag, 1991.
[11] S. Saeednia and H. Ghodosi, "A self-certified group-oriented cryptosystem without a combiner," in *Proceedings of ACISP'99*, pp. 192-201, Berlin, Springer-Verlag. 1999.
[12] A. Shamir, "Identity-based cryptosystems and signature scheme," Advances in *Proceeding of Crypto'84*, LNCS 196, PP. 47-53, Springer-Verlag, 1985.
[13] V. Shoup and R. Gennaro, "Securing threshold cryptosystems against chosen ciphertext attack," *Jounal of Cryptology*, vol. 15, pp. 75-96, 2002.
[14] D. R. Stinson, *Cryptography: Theory and Practice*, pp. 343-350, Florida, CRC Press, 1995.
[15] C. C. YANG, T. Y. CHANG, J. W. LI, and M. S. HWANG, "Simple generalized group-oriented cryptosystems using elgamal cryptosystem," *Informatica*, vol. 14, no. 1, pp. 111-120, 2003.

Chunxiang Xu received her PhD degree in Cryptography, her MS degree and her BS degree in Applied Mathematics from Xidian University, in 2004, 1988 and 1985 respectively. She is currently a Professor in School of Computer Science and Engineering, University of Electronic Science and Technology of China. Her research interests include Cryptography and Information Security.

Guozhen Xiao was born in 1934. He was graduated from the Department of Mathematics, Northeast Normal University, Changchun, China, in 1954. In 1956, he received the M.S. degree in mathematics from the East China Normal University, Shanghai,China. He is now a professor and Ph.D. advisor of cryptography inCommunications Engineering School of Xidian University. His research interests include cryptography, coding and informationtheor



Junhui Zhou received his BS degree in Electronic Engineering from University of Electronic Science and Technology of China in 1982, and his MS degree in Computer Applications from Northwest Institute of Nuclear Technology in 1988. He is currently a researcher in School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include Cryptography, and Network Security.