JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 26, 1509-1523 (2010)

New Secure Broadcasting Scheme Realizing Information Granularity*

CHIN-I LEE[1], TZONG-CHEN WU[1,2], BO-YIN YANG[2] AND WEN-GUEY TZENG[3]
[1]*Department of Information Management*
National Taiwan University of Science and Technology
Taipei, 106 Taiwan
[2]*Institute of Information Science*
Academia Sinica
Taipei, 115 Taiwan
[3]*Department of Computer Science*
National Chiao Tung University
Hsinchu, 300 Taiwan

This paper proposes a new secure broadcasting scheme to realize the property of "information granularity", wherein a receiver with a higher security clearance level has the natural capability to recover a larger amount of information from the broadcasted message block. Based on the intractability of the product of the ℓ-weak Bilinear Diffie-Hellman Inversion problem and the n-modified Bilinear Diffie-Hellman problem, the proposed scheme achieves the following features: (i) the length of the enabling block is independent of the number of receivers and the number of security clearance levels; (ii) each receiver holds only one small fixed-size decryption key corresponding to his/her security clearance level; (iii) it is computationally feasible for any receiver to derive a session key of a lower but never a higher security clearance level, even taking into account collusion with other receivers; (iv) any receiver can dynamically join or leave the system without resolving the re-keying problem for the existing receivers.

Keywords: information granularity, secure broadcasting, security clearance level, ℓ-weak bilinear Diffie-Hellman inversion problem, n-modified bilinear Diffie-Hellman problem, collusion

1. INTRODUCTION

Fiat and Naor [11] introduced the concept of a secure broadcasting system, known as broadcast encryption, where a broadcaster can distribute an encrypted message block to a set of receivers via public network such that only the authorized receivers (a predefined subset of receivers) can decrypt it and recover the message block. To setup the system, each receiver is assigned a different decryption key stored in a tamper-resistant device in advance. Each broadcast session consists of two parts: the Enabling Block and the Cipher Block. The Cipher Block is simply the ciphertext of the message encrypted by a randomly chosen session key. The Enabling Block contains key management information from which each authorized receiver can use his/her decryption key to derive the session key, respectively. Nowadays many secure broadcasting systems have been developed [3, 5-7, 9-12, 14, 17-20, 23, 26-30]. These systems could be further categorized into the public-key/asymmetric and the secret-key/symmetric approaches. Any receiver

Received January 20, 2009; revised May 19, 2009; accepted June 30, 2009.
Communicated by Chin-Laung Lei.
* This work was sponsored in part by TWISC (Taiwan Information Security Center), National Science Council under the grants NSC 96-2221-E-011-148-MY1 & MY2 and NSC 97-2219-E-001-001.

can also act as the broadcaster in the public key approach, which is applicable to a distributed environment. On the other hand, only a trusted party can serve as the broadcaster in the secret key approach, and such system is usually designed to be a centralized one. In the past decade, both approaches have been successfully deployed to several practical applications, such as the pay-TV systems and the secure multicast systems for distribution of copyrighted materials.

From the viewpoint of the receiver as opposed to that of the broadcaster, we address another practical case in this paper. Let a broadcasted message block M consist of a set of disjoint message sub-blocks $M_1, M_2, \ldots, M_\omega$, for some ω, and let $U = \{u_1, u_2, \ldots, u_n\}$ be the set of receivers, for some n. Consider that each message sub-block M_j is associated with a security clearance level, denoted by $SC(M_j)$, and each receiver u_i is associated with a security clearance level, denoted by $SC(u_i)$, defined by the broadcaster in advance. It is reasonably assumed that the message sub-block M_j and its corresponding ciphertext C_j are with the same security clearance level, *i.e.*, $SC(M_j) = SC(C_j)$. Each receiver u_i can recover the message sub-block M_j from the Ciphertext Block only if $SC(u_i) \geq SC(M_j)$ (or $SC(u_i) \geq SC(C_j)$). That is, a receiver with a higher security clearance level has the capability to recover a larger amount of information from the broadcasted message block. To achieve this purpose, each receiver's decryption key should be associated with his/her security clearance level. The property of *information granularity* inherent in the broadcast encryption system is extremely useful for certain applications. The most plausible one is the conditional access of the encrypted content for granting different privileges or offering different pay-rates.

Notice that in all previously proposed broadcast encryption or multicast systems, the "entire" message block is with the same security clearance level and is encrypted by one single session key. That is, a receiver has the ability to recover either the entire message block or nothing. To achieve the property of information granularity stated above by directly employing the previously proposed systems, it should require extra amount of Enabling Blocks for distributing different session keys with different security clearance levels. This approach often results in heavy communication overhead, which is undesirable when communication capability is limited.

This paper aims to propose a novel secure broadcasting scheme realizing information granularity (SBRIG for short) for the scenario described above. Based on the hierarchical key assignment approach [1] and no re-keying procedure [10, 23], our SBRIG scheme is shown to be secure assuming the intractability of the product of the ℓ-weak Bilinear Diffie-Hellman Inversion problem [3, 8] and the n-modified Bilinear Diffie-Hellman problem [23]. Meanwhile, it preserves the merits of efficiency in computation and communication from the pairing [4, 13]. Our SBRIG scheme achieves the following features: (i) the length of the enabling block is independent of the number of receivers and the number of security clearance levels; (ii) each receiver holds only one small fixed-size decryption key corresponding to his/her security clearance level; (iii) it is computationally feasible for any receiver to derive a session key of a lower but never a higher security clearance level, even taking into account collusion with other receivers; (iv) any receiver can dynamically join or leave the system without resolving the re-keying problem for the existing receivers.

The rest of the paper is organized as follows. In section 2, we give a preliminary sketch of the pairing and the complexity assumptions that will be used in the construc-

tion of our SBRIG scheme. Then, we describe the system model of our SBRIG scheme. In section 3, we will present our SBRIG scheme. We discuss security analyses and performance evaluation of our SBRIG scheme in section 4. Finally, conclusions are given in section 5.

2. PRELIMINARIES

2.1 The Pairing and Complexity Assumptions

A bilinear pairing is defined by $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$, where G_1 is a cyclic additive group and G_2 is a cyclic multiplicative group with the same prime order q, *i.e.*, $|G_1| = |G_2| = q$. The mapping $\hat{e}$ satisfies the following properties:

(i) Bilinear: For all $P, Q \in G_1$ and all $a, b \in Z_q$, we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
(ii) Non-degenerate: $\hat{e}(P, Q) \neq 1$ for some $P, Q \in G_1$. Also if P is a generator of G_1 then $\hat{e}(P, P)$ is a generator of G_2.
(iii) Computable: Given $P, Q \in G_1$, there is an efficient algorithm to find $\hat{e}(P, Q)$.

The security of our SBRIG scheme is based on the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem, where the modified ℓ-weak Bilinear Diffie-Hellman Inversion problem (ℓ-wBDHI problem) [3, 8], referred as the ℓ-wBDHI-M problem, and the modified n-modified Bilinear Diffie-Hellman problem (n-mBDH problem) [23], referred as the n-mBDH-M problem, respectively. We introduce the definitions of these complexity assumptions below:

The ℓ-wBDHI-M hardness assumption: Let G_1, G_2, $\hat{e}$ be defined as above, P and Q be two random generators of G_1, and $b \in Z_q^*$. Given $(Q, P, bP, b^2P, \ldots, b^\ell P)$ as input, no efficient algorithms can compute $\hat{e}(P, Q)^{b^{-\lambda}} \in G_2$ with non-negligible probability for any $1 \leq \lambda \leq \ell$.

The n-mBDH-M hardness assumption: Let G_1, G_2, $\hat{e}$ be defined as above, P be a generator of G_1, $Z \in G_1$, $x \in Z_q^*$, a hash function H: $\{0, 1\}^* \rightarrow Z_q^*$, and $u_1, u_2, \ldots, u_n$ be the receivers which u_i is the receiver identifier for the ith receiver. Given $(P, \frac{1}{x+H(u_1)}P, \frac{1}{x+H(u_2)}P, \ldots, \frac{1}{x+H(u_n)}P, Z+\frac{1}{(x+H(u_1))^2}P, Z+\frac{1}{(x+H(u_2))^2}P, \ldots, Z+\frac{1}{(x+H(u_n))^2}P)$ as input, no efficient algorithms can compute $(X, \hat{e}(Z, X))$, $X \in G_1 \backslash \{0\}$ with non-negligible probability.

The product of the ℓ-wBDHI-M and the n-mBDH-M hardness assumptions: Following the definitions of the ℓ-wBDHI-M problem and the n-mBDH-M problem with the same input $(Q, P, bP, b^2P, \ldots, b^\ell P, \frac{1}{x+H(u_1)}P, \frac{1}{x+H(u_2)}P, \ldots, \frac{1}{x+H(u_n)}P, Z+\frac{1}{(x+H(u_1))^2}P, Z+\frac{1}{(x+H(u_2))^2}P, \ldots, Z+\frac{1}{(x+H(u_n))^2}P)$, no efficient algorithms can compute $(X, \hat{e}(P, Q)^{b^{-\lambda}} \cdot \hat{e}(Z, X))$, $X \in G_1 \backslash \{0\}$ with non-negligible probability for any $1 \leq \lambda \leq \ell$.

One of the important security requirements of our SBRIG scheme is to withstand the security-clearance attack where a malicious privileged receiver u_i attempts to recover the message sub-block M_j for $SC(u_i) < SC(M_j)$. We will show that the SBRIG scheme is semantically secure against a security-clearance attack under the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem in section 4.1.

2.2 The System Model

There are two types of participants: a broadcaster and a set of receivers. The proposed system model consists of four phases: *Setup*, *KeyGen*, *Encryption*, and *Decryption*. Functional specifications of these phases are stated as follows:

Setup phase: Done by the broadcaster to define the system parameters, including the security clearance levels, the authorization policy (or the rule for conditional access to the broadcasted message block) associated to each security clearance level, and the secret and public parameters. The secret parameters will be used by the broadcaster for generating the decryption keys in the *KeyGen* phase and generating the session keys in the *Encryption* phase. The public parameters will be used by the receivers for deriving the session keys in the *Decryption* phase.

KeyGen phase: Done by the broadcaster to generate the decryption keys and receivers' information for the receivers. In accordance with the predefined authorization policy, the broadcaster assigns a security clearance level, and generates the corresponding decryption key and information for each registered receiver. The receiver can use the decryption key to derive the session keys for which he/she is entitled from the Enabling Block in the *Decryption* phase. The receivers' information will be published, and the broadcaster will take into account the receivers' information of the set of authorized receivers in the *Encryption* phase. Moreover, any receiver can join or leave the system without performing re-keying for the existing receivers.

Encryption phase: Done by the broadcaster to construct the Cipher Block and the corresponding Enabling Block for each broadcast session. Recall that a broadcasted message block consists of a set of disjoint message sub-blocks. First of all, the broadcaster determines the security clearance level for each message sub-block to be broadcasted. Then, the broadcaster generates a session key associated to each security clearance level, and thereafter, each message sub-block is encrypted by the session key corresponding to its security clearance level. Note that the message sub-blocks with the same security clearance level are encrypted by the same session key. Usually, a symmetric cipher, *e.g.*, 3DES [21] or AES [22], is adopted for encrypting/decrypting the message sub-blocks in practice. After that, the broadcaster constructs the Enabling Block such that the set S of authorized receivers can derive the session keys up to his/her security clearance level, respectively. We often refer to the Enabling Block as the header and (S, the Enabling Block) as the full header. Finally, the Cipher Block is constructed directly from the encrypted message sub-blocks.

Decryption phase: Done by the receivers to recover the encrypted message sub-blocks.

Upon receiving the broadcasted message block, the receiver first uses his/her decryption key to derive the required session keys up to the corresponding security clearance levels from the Enabling Block, and then uses these session keys to recover the message sub-blocks in the Cipher Block. Note that only the authorized receivers can derive the correct session keys, while the unauthorized receivers cannot.

3. OUR SBRIG SCHEME

We are now ready to present our SBRIG scheme. Details of the *Setup*, *KeyGen*, *Encryption*, and *Decryption* phases are stated as follows.

Setup phase: To setup the system, the broadcaster does the following:

(i) Define G_1, G_2, q and $\hat{e}$ as in the previous section, where q is a prime and its bit length, *i.e.*, $|q|$, is determined for practical security consideration that will be discussed later in section 4.2.
(ii) Define ℓ security clearance levels numbered from 1, 2, …, ℓ. The security level ℓ has higher clearance than level $\ell - 1$, and higher than level $\ell - 2$, …, and so forth. In general, ℓ is not practically large. For example, the security clearance levels are classified as "top secret", "secret" and "unclassified", then $\ell = 3$.
(iii) Define the function $SC(x)$ that returns the security clearance level of receiver/message x.
(iv) Randomly choose a hash function H: $\{0, 1\}^* \rightarrow Z_q^*$, a random element $T \in G_1$ and a generator $P \in G_1$ such that $g = \hat{e}(P, P)$ is a generator of group G_2.
(v) Randomly choose $a, b, x, z \in Z_q^*$, and compute $L = (P, bP, b^2P, \ldots, b^{\ell}P)$.
(vi) Publish q, G_1, G_2, $\hat{e}$, ℓ, H, T and L, while keeping a, b, x and z secret.

KeyGen phase: First of all, the broadcaster generates the decryption key $DK_i = (d_{i,1}, D_{i,2}, D_{i,3})$ and the receiver's information for the registered receiver u_i with a dedicated security clearance level, *i.e.*, $SC(u_i) = t$ $(1 \le t \le \ell)$ as follows:

(i) Choose $\alpha_i, \beta_i \in Z_q^*$ satisfying $\alpha_i + a\beta_i \equiv z \pmod q$.
(ii) Compute $d_{i,1} = \alpha_i b^{\ell-t+1} \bmod q$, $D_{i,2} = \beta_i b^{\ell-t+1} P$ and $D_{i,3} = zP + \frac{1}{x+H(u_i)} T + \frac{1}{(x+H(u_i))^2} P$.
(iii) Compute the receiver u_i's information $\frac{1}{x+H(u_i)} P$.

Thereafter, the broadcaster publishes the receiver u_i's information, and the registered receiver u_i is assigned the decryption key DK_i.

Encryption phase: Let $Enc(k, x)$ be the adopted symmetric encryption algorithm that encrypts x using the session key k. Let $S \subseteq \{u_1, u_2, \ldots, u_n\}$ be the set of authorized receivers. The broadcaster does the following tasks to construct the Enabling Block of $M = \{M_1, M_2, \ldots, M_\omega\}$ and its corresponding Cipher Block:

(i) Randomly choose $r \in Z_q$.
(ii) Determine the security clearance level $SC(M_j) = \eta$ for M_j (for $j = 1, 2, \ldots, \omega$), and generate a corresponding session key k_η, where $\delta_\eta = rz(b^{\ell-\eta+1} + 1) \bmod q$ and $k_\eta = g^{\delta\eta}$.
(iii) Construct the Cipher Block of M, *i.e.*, CB = $\{C_1, C_2, \ldots, C_\omega\}$, where C_j =

$Enc(k_{SC(M_j)}, M_j)$ (for $j = 1, 2, \ldots, \omega$). Note that the message sub-blocks with the same security clearance level will be encrypted by the same session key.

(iv) Construct the Enabling Block of M, *i.e.*, EB = $\{Y_1, Y_2, y\}$, where $Y_1 = rP$, $Y_2 = r(T + \sum_{u_j \in S} \frac{1}{x+H(u_j)}P)$ and $y = ra \bmod q$.

(v) Broadcast (S, EB, CB) to the receivers.

Decryption phase: Let $Dec(k, x)$ be the adopted symmetric decryption algorithm that decrypts x using the session key k. Upon receiving the broadcasted (S, EB, CB), the receiver $u_i \in S$ computes the public value V for the set S from the receivers' information for all u_j ($u_j \neq u_i$) $\in S$ and then recovers M_j (for $j = 1, 2, \ldots, \omega$).

We first show that the receiver $u_i \in S$ can compute the value V from the receivers' information for all u_j ($u_j \neq u_i$) $\in S$ in the following:

$$\begin{aligned} V &= \sum_{u_j \in S, u_j \neq u_i} \frac{1}{H(u_j) - H(u_i)} \left(\frac{1}{x + H(u_i)} P - \frac{1}{x + H(u_j)} P\right) \\ &= \sum_{u_j \in S, u_j \neq u_i} \frac{1}{H(u_j) - H(u_i)} \left(\frac{x + H(u_j) - x - H(u_i)}{(x + H(u_i))(x + H(u_j))}\right) P \\ &= \sum_{u_j \in S, u_j \neq u_i} \frac{1}{(x + H(u_i))(x + H(u_j))} P. \end{aligned}$$

After that, the receiver $u_i \in S$ does the following tasks for recovering M_j (for $j = 1, 2, \ldots, \omega$):

(i) Compute $\lambda_j = SC(u_i) - SC(C_j)$.

(ii) If $\lambda_j < 0$, then do nothing; otherwise get $b^{\lambda_j}P$ from the public parameters $L = (P, bP, b^2P, \ldots, b^{\ell}P)$, compute the session key $k_{SC(C_j)}$, and recover $M_j = Dec(k_{SC(C_j)}, C_j)$, where

$$k_{SC(C_j)} = \frac{\hat{e}(d_{i,1}Y_1 + yD_{i,2}, b^{\lambda_j}P) \cdot \hat{e}(D_{i,3} + V, Y_1)}{\hat{e}(Y_2, \frac{1}{x + H(u_i)} P)}.$$

Correctness of the SBRIG scheme relies on the fact that any receiver $u_i \in S$ can use his/her own decryption key $DK_i = (d_{i,1}, D_{i,2}, D_{i,3})$ to derive the session key $k_{SC(C_j)}$ for C_j if $SC(u_i) \geq SC(C_j)$. Meanwhile, any receiver $u_i \in S$ cannot derive the session key $k_{SC(C_j)}$ for C_j if $SC(u_i) < SC(C_j)$. Next, we verify that the session key $k_{SC(C_j)}$ is computed correctly. Let $\lambda_j = SC(u_i) - SC(C_j)$. If $\lambda_j < 0$, then the receiver u_i cannot obtain $b^{\lambda j}P$ without knowing b, and hence he/she cannot compute the correct session key $k_{SC(C_j)}$ for C_j by pairing. For the case of $\lambda_j \geq 0$, derivation of the correct session key $k_{SC(C_j)}$ for C_j by the receiver $u_i \in S$ associated with a dedicated security clearance level, $SC(u_i) = t$, is shown as follows:

$$k_{SC(C_j)} = \frac{\hat{e}(d_{i,1}Y_1 + yD_{i,2}, b^{\lambda_j}P) \cdot \hat{e}(D_{i,3} + V, Y_1)}{\hat{e}(Y_2, \frac{1}{x+H(u_i)} P)}$$

$$= \hat{e}(\alpha_i b^{\ell-t+1} rP + ra\beta_i b^{\ell-t+1} P, b^{\lambda_j} P) \cdot$$
$$\frac{\hat{e}(zP + \frac{1}{x+H(u_i)} T + \frac{1}{(x+H(u_i))^2} P + \sum_{u_j \in S, u_j \neq u_i} \frac{1}{(x+H(u_i))(x+H(u_j))} P, rP)}{\hat{e}(r(T + \sum_{u_j \in S} \frac{1}{x+H(u_j)} P), \frac{1}{x+H(u_i)} P)}$$

$$= \hat{e}(P, (r\alpha_i b^{\ell-t+1+\lambda_j} + ra\beta_i b^{\ell-t+1+\lambda_j})P) \cdot$$
$$\frac{\hat{e}(rzP, P) \cdot \hat{e}(T + \sum_{u_j \in S} \frac{1}{x+H(u_j)} P, \frac{r}{x+H(u_i)} P)}{\hat{e}(T + \sum_{u_j \in S} \frac{1}{x+H(u_j)} P, \frac{r}{x+H(u_i)} P)}$$

$$= \hat{e}(P, (rzb^{\ell-t+1+\lambda_j})P) \cdot \hat{e}(rzP, P) = \hat{e}(P, P)^{(rzb^{\ell-t+1+\lambda_j})} \cdot \hat{e}(P, P)^{rz}$$

$$= g^{rz(b^{\ell-SC(C_j)+1}+1)}.$$

In the SBRIG scheme, the length of the Enabling Block is independent of the number of receivers and the number of security clearance levels. Moreover, the SBRIG scheme realizes the property of information granularity. In comparison with some previous works [28, 30] that they need to compute the session keys level by level, the SBRIG scheme uses a less number of session keys for each broadcast session. That is, a receiver who is recovering the message sub-block for a lower security clearance level does not need to compute the session keys for all intervening levels. This saves time as we do not expect every broadcast session to have message sub-blocks of each security clearance level.

4. ANALYSIS

In this section, we will analyze the security, choose parameters and then give the performance evaluation for our proposed SBRIG scheme.

4.1 Security Analysis

The security of our proposed SBRIG scheme is based on the intractability of the product of the modified versions of the ℓ-weak Bilinear Diffie-Hellman Inversion problem (ℓ-wBDHI-M problem) and the n-modified Bilinear Diffie-Hellman Problem (n-mBDH-M problem). We will show that the SBRIG scheme is semantically secure against a security-clearance attack where a malicious receiver u_i attempts to recover the broadcasted message sub-block with higher security clearance level than his/hers.

Suppose that the adversary $\mathcal{A}$ (a probabilistic Turing machine representing a malicious receiver) successfully attacks the SBRIG scheme by the definition one-way security. That is, $\mathcal{A}$ can derive the session keys associated with higher security clearance levels than his/hers. Using $\mathcal{A}$, we build an algorithm $\mathcal{B}$ that solves the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem with non-negligible advantage ε. Algorithm $\mathcal{B}$ is given as input a random product of the ℓ-wBDHI-M and the n-mBDH-M instance (Q, P,

$bP, b^2P, \ldots, b^{\ell}P, \frac{1}{x+H(u_1)}P, \frac{1}{x+H(u_2)}P, \ldots, \frac{1}{x+H(u_n)}P, Z+\frac{1}{(x+H(u_1))^2}P, Z+\frac{1}{(x+H(u_2))^2}P, \ldots, Z+\frac{1}{(x+H(u_n))^2}P$). B shall find $\hat{e}(P, Q)^{b^{-\lambda}} \cdot \hat{e}(Z, X)$ by interacting with A in the following game:

Setup: First of all, B randomly chooses $\tilde{r}_1 \in Z_q$, and sets $T = \tilde{r}_1 P - \sum_{u_j \in S} \frac{1}{x+H(u_j)} P$. After that, B gives A the public parameters

$$PK = (P, bP, b^2P, \ldots, b^{\ell}P, T, \frac{1}{x+H(u_1)}P, \frac{1}{x+H(u_2)}P, \ldots, \frac{1}{x+H(u_n)}P).$$

Query phase: The adversary A associated with a dedicated security clearance level, *i.e.*, $SC(A) = s$, $1 \le s \le \ell$, issues the decryption key query. The algorithm B randomly chooses $\tilde{\alpha}_A$, $\tilde{r}$ and $y \in Z_q$, and sets

$d_{A,1} = \tilde{\alpha}_A b^{\ell-s+1}$,
$X = \tilde{r}P$ and
$Y_1 = X$.

We can image

$y = \tilde{r}\tilde{a} \bmod q$

for some $\tilde{a} \in Z_q$. Then, B computes

$D_{A,2} = (Q - d_{A,1}Y_1)/y$ and

$$D_{A,3} = Z + \frac{1}{(x+H(u_A))^2}P + \frac{\tilde{r}_1}{x+H(u_A)}P - \sum_{u_j \in S}\frac{1}{(x+H(u_A))(x+H(u_j))}P.$$

After that, B sends the decryption key $DK_A = (d_{A,1}, D_{A,2}, D_{A,3})$ to the adversary A.

Challenge: The algorithm B constructs the ciphertext block CB* by choosing the random ciphertext $\{C_1, C_2, \ldots, C_{\omega}\}$, the security clearance levels $s + \lambda$, $1 \le \lambda \le \ell - s$. Then the algorithm B gives (Y_1, Y_2, y, CB*) as the challenge to adversary A, where

$Y_1 = \tilde{r}P$,
$Y_2 = \tilde{r}(T + \sum_{u_j \in S}\frac{1}{x+H(u_j)}P)$ and
$y = \tilde{r}\tilde{a} \bmod q$.

Break: If the adversary A returns $\{M_1', M_2', \ldots, M_{\omega}'\}$, the algorithm B randomly selects j and returns M_j' as the answer to the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem.

Theorem 1 The SBRIG scheme is semantically secure against the security-clearance attack if no polynomial-time algorithms solve the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem with non-negligible probability.

***Proof*:** In Setup, we treat $T = \tilde{r}_1 P - \sum_{u_j \in S} \frac{1}{x+H(u_j)} P$ for some $\tilde{r}_1 \in Z_q$. Then, B gives the public parameters $PK = (P, bP, b^2P, \ldots, b^\ell P, T, \frac{1}{x+H(u_1)} P, \frac{1}{x+H(u_2)} P, \ldots, \frac{1}{x+H(u_n)} P)$ to the adversary A.

In Query, we also treat

$$d_{A,1} = \tilde{\alpha}_A b^{\ell-s+1},$$
$$D_{A,2} = (Q - d_{A,1} Y_1)/y,$$
$$D_{A,3} = Z + \frac{1}{(x+H(u_A))^2} P + \frac{\tilde{r}_1}{x+H(u_A)} P - \sum_{u_j \in S} \frac{1}{(x+H(u_A))(x+H(u_j))} P,$$
$$Y_1 = \tilde{r} P \text{ and}$$
$$y = \tilde{r}\tilde{a} \bmod q$$

for some $\tilde{\alpha}_A$, $\tilde{r}$ and $\tilde{a}$. We can think that $\tilde{r}_1$, $\tilde{\alpha}_A$ and $\tilde{r}$ are randomly chosen and T, $d_{A,1}$, $D_{A,3}$, Y_1 and y are then determined. Thus, T, $d_{A,1}$, $D_{A,3}$, Y_1 and y have the identical distribution in the construction. Furthermore, we can check whether $d_{A,1}$, $D_{A,2}$ and $D_{A,3}$ satisfy the requirement of decryption key generation as follows:
Because

$$\tilde{\alpha}_A + \tilde{a}\beta_A = z \pmod{q},$$

it follows that

$$\tilde{\alpha}_A b^{\ell-s+1}\tilde{r}P + \tilde{a}\beta_A b^{\ell-s+1}\tilde{r}P = z b^{\ell-s+1}\tilde{r}P.$$

This means that

$$d_{A,1}Y_1 + y\beta_A b^{\ell-s+1}P = \tilde{r} z b^{\ell-s+1}P .$$

Since $D_{A,2}$ is set as $(Q - d_{A,1}Y_1)/y$, so

$$Q = \tilde{r} z b^{\ell-s+1}P.$$

Indeed, we have that

$$d_{A,1}Y + yD_{A,2} = Q$$

as required. Then we have that

$$\beta_A b^{\ell-s+1}P = (Q - d_{A,1}Y_1)/y = D_{A,2}.$$

On the other hand, since

$$T = \tilde{r}_1 P - \sum_{u_j \in S} \frac{1}{x+H(u_j)} P ,$$

it is easy to see that

$$\frac{1}{x+H(u_A)}T = \frac{\tilde{r}_1}{x+H(u_A)}P - \sum_{u_j \in S}\frac{1}{(x+H(u_A))(x+H(u_j))}P.$$

Then we have that

$$Z + \frac{1}{(x+H(u_A))^2}P + \frac{1}{x+H(u_A)}T = D_{A,3}.$$

Thus, the algorithm B has all the necessary values to compute the decryption key $DK_A = (d_{A,1}, D_{A,2}, D_{A,3})$.

In Challenge, B constructs the challenge (Y_1, Y_2, y, CB*) as stated above.

In Break, A returns valid $\{M_1', M_2', \ldots, M_\omega'\}$ and at least one of them is correct, say M_j'. We see that, since the adversary A can break the SBRIG scheme, for any ciphertext in the challenge (Y_1, Y_2, y, CB*), the adversary A can derive the session key whose security clearance level is $s + \lambda$ in the following: Let $Z = zP$.

$$\begin{aligned}
k_{SC(M_j')} &= g^{\tilde{r}z(b^{\ell-(s+\lambda)+1}+1)} \\
&= \hat{e}(P, \tilde{r}z(b^{\ell-s-\lambda+1}+1)P) \\
&= \hat{e}(P, \tilde{r}zb^{\ell-s+1}P)^{b^{-\lambda}} \cdot \hat{e}(P, \tilde{r}zP) \\
&= \hat{e}(P, d_{A,1}Y_1 + yD_{A,2})^{b^{-\lambda}} \cdot \frac{\hat{e}(D_{A,3} + \sum_{u_j \in S, u_j \neq u_A} \frac{1}{(x+H(u_A))(x+H(u_j))}P, Y_1)}{\hat{e}(Y_2, \frac{1}{x+H(u_A)}P)} \\
&= \hat{e}(P, Q)^{b^{-\lambda}} \cdot \hat{e}(zP, \tilde{r}P) \\
&= \hat{e}(P, Q)^{b^{-\lambda}} \cdot \hat{e}(Z, X).
\end{aligned}$$

From Theorem 1, we can see that algorithm B can solve the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem, contradicting the assumption of the product of the ℓ-wBDHI-M problem and the n-mBDH-M problem being intractible. Therefore the SBRIG scheme is semantically secure. ❑

4.2 Choices of Parameters

Since the security of our proposed SBRIG scheme depends on the cryptographic problems stated above, we should consider their security issues:

(i) The security of all elliptic curve cryptosystem assumes the intractability of the elliptic curve discrete logarithm problem (ECDLP) [2]: given an elliptic curve E defined over the finite field F_p of p elements, a point $W \in E(F_p)$ of order q, and a point $Q \in E(F_p)$, it is computationally infeasible to find an integer $x \in [0, q-1]$ such that $Q = xW$. If q is composite, the Pohlig-Hellman algorithm [24] reduces the determination of x to the determination of x modulo each of the prime factors of q. So q should have a large prime factor for assurance of a good security level. For prime q, the best known algorithm for solving the ECDLP is the Pollard Rho algorithm [25], which takes about

$\sqrt{\pi q/2}$ elliptic curve additions. To prevent the Pollard Rho attack, the number of points on the elliptic curve should be divisible by a large prime q, where $q > 2^{160}$ to reach a security level similar to that of the 1024-bit RSA [15, 16].

(ii) Meanwhile, the security of our SBRIG scheme may be reduced to a finite-field DLP given that a pairing exists. To resist up to 2^{80} time complexity of an attack based on index calculus (the most well-known and most efficient one to date being the General Number Field Sieve), a DLP must be on a group of order $\geq 2^{1024}$. The size of the field for the derived DLP is comparable to q. So the group order q of G_1 and G_2 should be at least 1024-bits, and the largest prime factor of $(q - 1)$ should also be $> 2^{160}$.

Therefore, our proposed SBRIG scheme does require 1024-bit computations for G_1 to satisfy the security requirements (like most pairing-based schemes in contrast to about 160 for straight ECDLP). If q has 1024 bits and a, b are of magnitude comparable to q, then the values of $\alpha_i b^{\ell\text{-}SC(u_i)+1} \pmod q$ (part of decryption key) and $ra \pmod q$ (part of the Enabling Block) will be random which implies computational infeasibility to obtain a and b.

4.2 Performance Evaluation

The performance of the proposed scheme heavily depends on the receiver storage, the transmission, and the computational cost. We will discuss these costs regarding to our SBRIG scheme.

(i) Receiver storage cost: the keys a receiver must store.

(ii) Transmission cost: the length of the Enabling Block sent by the broadcaster to derive the session keys for a receiver. It is common in the broadcasting systems to ignore the part S of full header that identifies the set of authorized receivers.

(iii) Computational cost: We distinguish between decryption and session key generation operations. The decryption time is how much time it takes for a receiver to derive the session keys up to his/her security clearance level. The session keys generation time is how long it takes for a broadcaster to generate the session keys for each broadcast session.

For simplicity, suppose that the broadcasted message block consists of ℓ disjoint message sub-blocks. Each message sub-block is associated with a different security clearance level from 1 to ℓ. Receiver $u_i \in S$ is associated with the highest security clearance level, *i.e.*, $SC(u_i) = \ell$. In the SBRIG scheme, we need ℓ session keys for all ℓ disjoint message sub-blocks. Let T_b be the cost of pairing computation, T_a the cost of point addition over an elliptic curve, T_{mul} the cost of scalar multiplication over an elliptic curve, $T_{\exp}$ the cost of exponentiation in G_2, T_m the cost of multiplication in finite field. Let L_{G_1} be the size of a point in G_1, $L_z \in Z_q$, $|S|$ as the number of authorized receivers. It should be noted that the computation of T_b is getting more efficient nowadays [15, 16]. To summarize the results of analysis, Table 1 shows the costs of our proposed scheme in terms of receiver storage and transmission costs and Table 2 shows the cost in terms of computational cost, respectively. Note that, at the first glance, it indeed needs $O(|S|)$ computation for the public value V in the decryption phase. However, the receiver u_i could store the current set S

and the public value V into his/her own device, then he could compute the public value V' for the new authorized set S' in the following broadcast session:

$$V' = V - \sum_{u_j \in S, u_j \notin S', u_j \neq u_i} \frac{1}{(x + H(u_i))(x + H(u_j))} P + \sum_{u_j \notin S, u_j \in S', u_j \neq u_i} \frac{1}{(x + H(u_i))(x + H(u_j))} P = \sum_{u_j \in S', u_j \neq u_i} \frac{1}{(x + H(u_i))(x + H(u_j))} P.$$

The new public value V' needs Δ computations, where Δ is equal to the number of the revoked plus newly joined receivers and $\Delta << |S|$. That is, the computing complexity could be further reduced to $O(1)$.

Table 1. The costs of the SBRIG scheme in terms of receiver storage and transmission costs.

	Receiver storage cost	Transmission cost
our SBRIG scheme	$L_Z + 2L_{G_1}$	$L_Z + 2L_{G_1}$

Table 2. The cost of the SBRIG scheme in terms of computational cost.

	Encryption phase	Decryption phase
our SBRIG scheme	$\ell(2T_{\exp} + 2T_m)$	$(\Delta + 2)(T_a + T_{mul})^* + 3\ell T_b$

* If receiver u_i cannot store the current set S and the public value V, then the computational cost is $(|S| + 1)(T_a + T_{mul}) + 3\ell T_b$.

5. CONCLUSIONS

We propose a new secure broadcasting scheme to realize the property of the information granularity. Each receiver can derive the session key corresponding to his/her own security clearance level or lower. Meanwhile, the receivers cannot construct a valid session key with higher security clearance level than theirs even in collusion with other receivers. The proposed SBRIG scheme is secure assuming the product of the modified versions of the ℓ-weak Bilinear Diffie-Hellman Inversion problem and the n-modified Bilinear Diffie-Hellman problem. It is noted that the product of the modified versions of the ℓ-weak Bilinear Diffie-Hellman Inversion problem and the n-modified Bilinear Diffie-Hellman problem may not be hard. At present, our scheme design is based on the premise that the security needs the assumption. In the future work we will loosen the assumption and prove our scheme secure under a well-known hard problem.

Furthermore, this work raises some interesting possibilities for future study. One is the security clearance levels of message sub-blocks, which are totally ordered in our proposed SBRIG scheme, but which might be in a partial order in some scenarios. The other is that we except to develop a SBRIG scheme with the traitor tracing functionality.

REFERENCES

1. S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems*, Vol. 1, 1983, pp. 239-248.
2. I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series 265, Cambridge University Press, 1999.
3. D. Boneh, X. Boyen, and E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proceedings of Advances in Cryptology – EUROCRYPT*, LNCS 3494, 2005, pp. 440-456.
4. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proceedings of Advances in Cryptology – CRYPTO*, LNCS 2139, 2001, pp. 213-229.
5. D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Proceedings of Advances in Cryptology – CRYPTO*, LNCS 3621, 2005, pp. 258-275.
6. R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," in *Proceedings of IEEE INFOCOM*, Vol. 2, 1999, pp. 708-716.
7. H. Chabanne, D. H. Ohan, and D. Pointcheval, "Public traceability in traitor tracing schemes," in *Proceedings of Advances in Cryptology – EUROCRYPT*, LNCS 3494, 2005, pp. 542-558.
8. J. H. Cheon, "Security analysis of the strong Diffie-Hellman problem," in *Proceedings of Advances in Cryptology – EUROCRYPT*, LNCS 4004, 2006, pp. 1-11.
9. J. T. Chung, C. M. Li, and T. Hwang, "All-in-one group-oriented cryptosystem based on bilinear pairing," *Information Sciences*, Vol. 177, 2007, pp. 5651-5663.
10. C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," in *Proceedings of Pairing*, 2007, pp. 39-59.
11. A. Fiat and M. Naor, "Broadcast encryption," in *Proceedings of Advances in Cryptology –CRYPTO*, LNCS 773, 1994, pp. 480-491.
12. D. Halevy and A. Shamir, "The LSD broadcast encryption scheme," in *Proceedings of Advances in Cryptology – CRYPTO*, LNCS 2442, 2002, pp. 47-60.
13. A. Joux, "A one round protocol for tripartite Diffie-Hellman," in *Proceedings of the 4th Algorithmic Number Theory Symposium*, 2000, pp. 385-394.
14. Z. Jun, Z. Yu, M. Fanyuan, G. Dawu, and B. Yingcai, "An extension of secure group communication using key graph," *Information Sciences*, Vol. 176, 2006, pp. 3060-3078.
15. A. Jurisic and A. J. Menezes, "Elliptic curves and cryptography," *Dr. Dobb's Journal*, Vol. 22, 1997, pp. 26-32.
16. N. Koblitz, A. J. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Design, Codes and Cryptography*, Vol. 19, 2000, pp. 173-193.
17. Y. R. Liu and W. G. Tzeng, "Public key broadcast encryption with low number of keys and constant decryption time," in *Proceedings of Public Key Cryptography*, 2008, pp. 380-396.
18. M. Luby and J. Staddon, "Combinatorial bounds for broadcast encryption," in *Proceedings of Advances in Cryptology – EUROCRYPT*, LNCS 1403, 1998, pp. 512-526.
19. Y. Mu and V. Varadharajan, "Robust and secure broadcast," in *Proceedings of Ad-*

vances in Cryptology – INDOCRYPT, LNCS 2247, 2001, pp. 223-231.
20. D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proceedings of Advances in Cryptology – CRYPTO*, LNCS 2139, 2001, pp. 41-62.
21. NIST FIPS 46-3, "Data encryption standard (DES) specifies the DES and triple DES algorithms," National Institute of Standards and Technology, U.S. Department of Commerce, 1999.
22. NIST FIPS 197, "Advanced encryption standard (AES)," National Institute of Standards and Technology, U.S. Department of Commerce, 2001.
23. J. H. Park, H. J. Kim, M. H. Sung, and D. H. Lee, "Public key broadcast encryption schemes with shorter transmissions," *IEEE Transactions on Broadcasting*, Vol. 54, 2008, pp. 401-411.
24. S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, Vol. 24, 1978, pp. 106-110.
25. J. Pollard, "Monte Carlo methods for index computation mod *p*," *Mathematics of Computation*, Vol. 32, 1978, pp. 918-924.
26. A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Transactions on Software Engineering*, Vol. 29, 2003, pp. 444-458.
27. R. Song and L. Korba, "Pay-TV system with strong privacy and non-repudiation protection," *IEEE Transactions on Consumer Electronics*, Vol. 49, 2003, pp. 408-413.
28. D. M. Wallner, E. J. Harder, and R. C. Agee, "Key management for multicast: Issues and architectures," Internet Request for Comments 2627, 1998, ftp://ftp.ietf.org/rfc/rfc2627.txt.
29. A. Wool, "Key management for encrypted broadcast," *ACM Transactions on Information and System Security*, Vol. 3, 2000, pp. 107-134.
30. D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, "ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, 2004, pp. 354-363.

Chin-I Lee (李靜怡) is currently a Ph.D. student in the Department of Information Management at National Taiwan University of Science and Technology, Taiwan. She received the B.S. degree in Statistics from National Cheng Kung University, Taiwan; and M.S. degree in Computer Science from the Stevens Institute of Technology, U.S.A. Her current research interests include cryptography and information security.

Tzong-Chen Wu (吳宗成) received the B.S. degree in Information Engineering from National Taiwan University in 1983, M.S. degree in Applied Mathematics from National Chung Hsing University in 1989, and Ph.D. degree in Computer Science and Information Engineering from National Chiao Tung University in 1992. From August 1992 to January 1997, he has been the associate professor in the Department of Information Management, National Taiwan University of Science and Technology (NUTST). Since February 1997, he has been the professor in the Department of Information Management, NTUST. Professor Wu is the members of IEEE, ACM, and the president of the Chinese Cryptology and Information Security Association (CCISA). He also serves as the director the Taiwan Information Security Center (TWISC) at National Taiwan University of Science and Technology (Taiwan Tech.), Taipei, Taiwan. His current research interests include data security, cryptography, network security, and data engineering.

Bo-Yin Yang (楊柏因) received his B.S. degree in Physics from National Taiwan University, Taiwan, 1987; and Ph.D. degree in Mathematics from the Massachusetts Institute of Technology, U.S.A., in 1991. He joined the Academia Sinica, Taiwan, in 2006. Dr. Yang's current research interests include algebraic cryptanalysis and multivariate public-key cryptography.

Wen-Guey Tzeng (曾文貴) received his B.S. degree in Com- puter Science and Information Engineering from National Taiwan University, Taiwan, 1985; and M.S. and Ph.D. degrees in Computer Science from the State University of New York at Stony Brook, U.S.A., in 1987 and 1991, respectively. He joined the Department of Computer and Information Science (now, Department of Computer Science), National Chiao Tung University, Taiwan, in 1991 and works there till now. Dr. Tzeng's current research interests include cryptology, information security and network security.