A New Type of ID-based Encryption System and Its Application to Pay-TV Systems

Xingwen Zhao and Fangguo Zhang
(Corresponding author: Fangguo Zhang)

School of Information Science and Technology, Sun Yat-Sen University
Guangdong Key Laboratory of Information Security Technology
No. 135, XinGang West Road, Guangzhou 510275, P.R. China (Email: isszhfg@mail.sysu.edu.cn)

(Received Sept. 1, 2009; revised and accepted Feb. 17, 2010)

Abstract

We proposed a new type of ID-based encryption scheme. Our scheme is different from other schemes on that we use tamper resistant smart card to store the private key and do the decryption job for the users. The user knows nothing about the private key. Our scheme is identical to ElGamal encryption scheme, but using RSA framework to avoid ID replacement attack. In a way, our scheme can be regarded as new application for the widely deployed RSA system. By employing the skill introduced by Dodis and Fazio for converting symmetric broadcast encryption schemes into public key ones, we extend our scheme into an efficient broadcast encryption scheme and apply it to the pay-TV system. We show that our broadcast encryption scheme is efficient in some aspects. For example, public keys of our system are of the size O(1) and decryption cost for each receiver is one modular exponentiation.

Keywords: Broadcast encryption, ID-based cryptosystem, pay-TV system

1 Introduction

Broadcast encryption (BE) provides a convenient method to distribute digital content to subscribers over an insecure broadcast channel so that only the qualified users can recover the data [27]. The receiver set can be static or dynamic. Static set means that the receivers are determined at the beginning and cannot be changed during the lifetime of the system, while the dynamic set means the system can invite new members to join or revoke undesired members when needed. Broadcast encryption is quite useful and enjoys many applications including pay-TV systems, distribution of copyrighted material, streaming audio/video and many others.

The first broadcast encryption scheme was formally proposed by Fiat and Naor in [13]. Later, Naor et al. [19] brought forward two subset-cover schemes that are suitable for the case of stateless receivers. In that case, keys for each user are fixed throughout the lifetime of the system, and receivers cannot record the operating state. After that, several schemes based on subset-cover were proposed [1, 15, 16]. Dodis and Fazio [11] extend the schemes of [16, 19] into public key broadcast encryption systems. The best known fully collusion systems are the schemes of Boneh, Gentry and Waters [7], with constant-sized ciphertexts and private keys, or with ciphertexts and public keys of size $O(\sqrt{n})$. Recently, several works with comparable efficiency were proposed [9, 10, 23].

An ID-based Encryption (IBE) system [24] is a public key system where the public key can be an arbitrary string such as an email address, IP address or telephone numbers, which will be used as a receiver's identities [26]. A central authority uses a master key to issue private keys associated to these identities. With the private key, a recipient can correctly decrypt ciphertext. The notion of IBE was introduced by Shamir in [24]. Later, Boneh and Franklin [6] gave us the first efficient IBE system by using the bilinear pairings. Since then, many efficient IBE schemes were proposed [2, 4, 5, 14, 25, 28].

Pay-TV system broadcasts the signals of TV channels to a great number of consumers. To enjoy these TV programs, each consumer needs only a television, a decoder box (a set-top box) and a smart card (possibly plugged into the decoder box). Since there is only a one-way communication channel from the service provider to the consumer, it is necessary to find ways to make sure that only those consumers who fulfill the payment are capable to recover the TV signals. Also the service provider needs to make it difficult to duplicate the decoder box and make it easy to trace out the traitors if there are any pirate decoder boxes. We notice that pay-TV system is an application just identical to broadcast encryption.

In this paper, we proposed a new type of ID-based encryption scheme. Our idea is to construct a ElGamal-like ID-based scheme [12], using RSA [22] framework to avoid ID replacement attack and using tamper resistant smart card [21] to store the private key. Our scheme is based on RSA so that, in a way, our scheme can be regarded as new application for the widely deployed RSA system. By employing the skill introduced by Dodis and Fazio [11], we extend it into an efficient broadcast encryption scheme and apply it to the pay-TV system.

The rest of this paper is organized as follows. We briefly describe the related work in Section 2. Then we introduce our new type of ID-based encryption model, describe the detailed scheme and consider its security in Section 3. In Section 4 we improve it into a efficient broadcast encryption scheme using skill introduced in [11] and apply it in pay-TV system. In Section 5, we analyze the efficiency of our BE scheme. Finally, concluding remarks will be made in Section 6.

2 Related Work

Boneh and Franklin [6] described the first secure and truly practical IBE system. Canetti et al. [8] presented an IBE system without random oracles in selective-ID model. Boneh and Boyen [5] presented a fully secure scheme with adaptive security. Waters [25] simplified the scheme described in [5], substantially improving its efficiency. Gentry [14] proposed a practical IBE scheme without random oracles.

Broadcast encryption was formally studied by Fiat and Naor in [13]. Since then, it has become a major topic in cryptography, due to various commercial applications, such as pay-TV. Later, Naor et al. [19] brought forward two subset-cover schemes that are suitable for the case of stateless receivers, namely the Complete Subtree (CS) scheme and the Subset Difference (SD) scheme. In that case, keys for each user are fixed throughout the lifetime of the system, and receivers cannot record the operating state. After that, several schemes based on subset-cover were proposed, for instance, the Layered Subset Difference (LSD) scheme [16], the flexible SD and the flexible LSD scheme [1], and the stratified Subset Difference (SSDF) scheme [15]. Dodis and Fazio [11] extend the schemes of [16, 19] into public key broadcast encryption systems. The best known fully collusion systems are the schemes of Boneh, Gentry and Waters [7], with constant-sized ciphertexts and private keys, or with ciphertexts and public keys of size $O(\sqrt{n})$. Later, Delerablée et al. proposed fully collusion resistant scheme [10], where users can join the system dynamically. They call it a dynamic broadcast encryption scheme. Its encryption key, decryption key, and header size are O(n), O(1), and $O(r)$, and the encryption and decryption cost are $O(r^2)$ and $O(r)$, respectively, where r denotes the number of revoked users. Sakai and Furukawa proposed an identity based broadcast encryption scheme [23], with encryption key, decryption key, and header size the same as [7]. Delerabl*é*e proposed a scheme similar to [9]. Kusakawa et al. [17] proposed a variant scheme of [10], achieving less computational cost and less public key. Park et al. [20] proposed a new public key broadcast encryption scheme, with shorter transmissions than [7].

3 Construction

In this section, we propose a new type of ID-based encryption scheme. We describe the models first, and then present the detailed scheme. We use tamper resistant smart card to store the private keys and conceal the weakness. When the smart card detects any tampering operation, it will wipe off all the key material. The construction is as follows.

3.1 Models

Our new type of ID-based Encryption Model consists of the following steps:

- **Setup:** A trusted party, called Private Key Generator (PKG), runs this probabilistic algorithm to generate a pair of keys SK and PK defining the scheme. It publishes PK and keeps SK secret.
- **Extract:** A deterministic algorithm that, on inputs SK and an identity string ID, outputs the trapdoor information S_{ID} associated to the identity. The S_{ID} is used as the private key and stored in a tamper resistant smart card. The user should know nothing about the private key and can decrypt message only by using the smart card.
- **Encryption:** A probabilistic algorithm that, on inputs PK, an identity string ID, a message m, outputs a ciphertext C_{ID} for the specific ID. We denote $C_{ID} = Enc(PK, ID, m)$.
- **Decryption:** A deterministic algorithm that, on inputs the ciphertext C_{ID}, the public key PK, receiver's identity string ID and its private key S_{ID}, outputs the recovered message $m = Dec(C_{ID}, ID, S_{ID})$. All these jobs are done within the smart card.

As an encryption scheme, our model must be correct, that is to say, $m = Dec(Enc(PK, ID, m), ID, S_{ID})$. As a public-key encryption scheme, basically, our model should resist chosen-plaintext attack (CPA). In addition, we also want to make sure that illegal receivers can not obtain the message from the ciphertext using ID replacement attack.

3.2 ID-based Encryption with Tamper Resistant Decryptcard

- **Setup:** A trusted center selects the security parameters as required in RSA system, $x \in_R Z_n^*$, and publishes $PK = \{n = pq,\ g,\ y = g^x \mod n,\ H_1,\ H_2\}$ and keeps $\{p, q, x\}$ secret. Here, $\varphi(n) = (p-1)(q-1)$, H_1 is a hash function from $\{0,1\}^* \rightarrow \mathcal{Z}_n^*$, H_2 is a hash function from $\mathcal{Z}_n^* \rightarrow \{0,1\}^l$. l is a security length, for instance, l=1024. Both are collision-free hash functions. The selection of them is out of scope of this paper.

- **Extract:** For an identity string ID, the center computes $id = H_1(ID)$ and $s = id \cdot x \mod \varphi(n)$. Then s is put into a tamper resistant smart card which we called decryptcard. This card will be later issued to the registered user. The user should know nothing about his private key.

- **Encryption:** For a message m and a user's identity ID , the center randomly select $k \in \mathcal{Z}_n^*$ to computes $r = g^k \mod n$, $id = H_1(ID)$, $v = m \oplus H_2(y^{id\cdot k} \mod n)$ and outputs (r, v) as the ciphertext.

- **Decryption:** Set r, v as the input of the tamper resistant decryptcard, it will return $v \oplus H_2(r^s \mod n) = m$.

If the user knows his secret key, then two users can cooperate to find the factors of n, because they can find the $\varphi(n)$. That is why we put the secret key into a tamper resistant smart card. We can see that, our scheme requires one modular exponentiation for encryption and decryption respectively. While in the IBE scheme of Boneh et al. [6], the encryption and decryption need one pairing in G_2 respectively. We also notice that our RSA framework is susceptible to side-channel attacks [18] such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA), we rely on the technology development for countermeasures against these attacks.

3.3 Security Consideration

3.3.1 Correctness

Our scheme is correct as follows,

$$y^{id\cdot k} = g^{x\cdot id\cdot k} = \left(g^k\right)^{x\cdot id} = r^s \ (\mod n)$$

so we have $m \oplus H_2(y^{id\cdot k} \mod n) \oplus H_2(r^s \mod n) = m$.

3.3.2 CPA-security

Our scheme is identical to the ElGamal public-key encryption scheme, so we can easily prove that our scheme is indistinguishable under chosen plaintext attack (abbreviated IND-CPA).

In the proof, we use the decisional Diffie-Hellman (DDH) assumption, so we describe it here in brief. DDH problem is, given $\{g,\ g^\alpha,\ g^\beta,\ z\}$, to decide $z = g^{\alpha\beta}$ or not. Then DDH assumption is, for any probabilistic polynomial time algorithm, the probability of solving DDH problem is negligible.

Theorem 1. *The proposed scheme is IND-CPA secure assuming DDH problem is hard.*

Proof. Suppose adversary $\mathcal{A}$ can (t, ϵ)-wins the IND-CPA game for the proposed scheme. We show how to construct a t'-time algorithm $\mathcal{B}$ that can solve the DDH problem with probability at least ϵ' for all t' and ϵ' satisfying

$$\epsilon' = \epsilon \cdot Pr[z = g^{\alpha\beta}] \text{ and } t' \approx t + q_E$$

where $Pr[z = g^{\alpha\beta}]$ is the probability of z equals to $g^{\alpha\beta}$ and q_E is the time $\mathcal{A}$ queries for messages encryption.

S1 Suppose $\mathcal{B}$ receives an instance of DDH problem $\{g, g^\alpha, g^\beta, z\}$. $\mathcal{B}$ carefully selects RSA parameters p, q to make sure that $n = pq$ is large enough to cover $g^{\alpha\beta}$. Then $\mathcal{B}$ set $x = \alpha$, and publishes $PK = \{n = pq, g, y = g^x \mod n, H_1, H_2\}$.

S2 When $\mathcal{A}$ queries the encryption value of message m_i on ID ID_i, $\mathcal{B}$ selects $k_i \in \mathcal{Z}_n^*$ to computes $r_i = g^{k_i} \mod n, v_i = m \oplus H_2(y^{id_i\cdot k_i} \mod n)$ and outputs (r_i, v_i) to $\mathcal{A}$, where $id_i = H_1(ID_i)$.

S3 $\mathcal{A}$ presents an new ID to attack and two messages $\{m_0, m_1\}$, both of which are not queried before. $id = H_1(ID)$. $\mathcal{B}$ flips a fair coin $b \in \{0, 1\}$, set $k = \beta$ (also unknown to $\mathcal{B}$) and calculates $v = m_b \oplus H_2(z^{id} \mod n)$, then sends $(r = g^\beta, v)$ to $\mathcal{A}$.

S4 On receiving (r, v), $\mathcal{A}$ has to decide $b' \in \{0, 1\}$. If $b' = b$, $\mathcal{B}$ decides $z = g^{\alpha\beta}$, else z is a randomly selected.

If $\mathcal{A}$ can (t, ϵ)-wins the IND-CPA game, and the probability of z equals to $g^{\alpha\beta}$ is $Pr[z = g^{\alpha\beta}]$, $\mathcal{B}$ can solve the DDH problem with probability at least $\epsilon' = \epsilon\cdot Pr[z = g^{\alpha\beta}]$ within time $t' \approx t + q_E$. □

3.3.3 Robust Confidentiality

Everyone listening to the insecure channel can receive the ciphertext (r, v). So malicious user i may want to distort the ciphertext to make it fixed for his decryptcard. If the ciphertext (r, v) is for user j, What user i has to do is to add some distortion factor to r as following, $r' = r^{id_i^{-1}\cdot id_j}$. Then (r', v) can be fed to user i's decryptcard to get the message $v \oplus H_2((r')^{s_i} \mod n)$=$v \oplus H_2((r)^{id_i^{-1}\cdot id_j\cdot id_i\cdot x} \mod n)$=$v \oplus H_2((r)^{s_j} \mod n) = m$. We call it ID replacement attack. However, user i has to solve the RSA problem in order to get id_i^{-1}.

4 New Pay-TV System

Pay-TV system is an application identical to broadcast encryption on that only subscribers who have fulfill the payment are capable to decrypt the encrypted TV signals. Any broadcast encryption scheme that is collusion resistant and with revocation ability can be used to construct a pay-TV system. A trivial way for constructing a broadcast encryption scheme (pay-TV system) is encrypting TV programs separately for each subscriber using our IBE scheme. It will be a waste of bandwidth, so we improve our scheme by using the subset-cover framework [19].

Dodis and Fazio [11] showed how to apply CS, SD [19] and LSD [16] methods to get public key broadcast encryption schemes from IBE schemes. Baek et al. [3] used the above methods to convert their IBE scheme into an efficient BE scheme. The same idea is applicable to our scheme. That is to say, pay-TV center first defines the total number of expected subscribers, says $N = 2^t$, and fits all these subscribers into a complete binary tree, says $\mathcal{T}$. Each subscriber is associated with one distinct leaf. Then pay-TV center uses one of the above methods to decide the collection of all useful subsets, says S, and generate decryption key for each subset. After that, pay-TV center decides the sub-collections each leaf belongs to, says S'_i, for $i = 1, \cdots, N$. In other words, if a subset S' contains leaf i, then $S' \in S'_i$. For a certain user i, if its corresponding sub-collection S'_i consists of m subsets, the center will store these m corresponding keys into a smart card. The smart card will be later issued to user i. If the center broadcasts a TV signal to subset S', which contains user i, user i can use the key for S' to decrypt that signal.

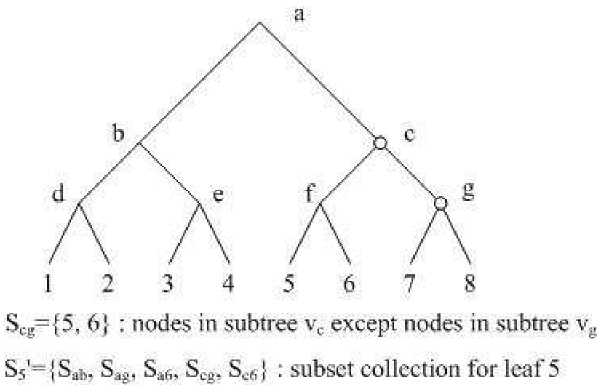
a
b
c
d
e
f
g
1
2
3
4
5
6
7
8
S_cg={5, 6} : nodes in subtree v_c except nodes in subtree v_g
S_5'={S_ab, S_ag, S_a6, S_cg, S_c6} : subset collection for leaf 5

Figure 1: Example for SD framework

Figure 1 is an example for SD framework. We show how to construct a pay-TV system based on SD method as follows. Systems that use other methods can be constructed similarly. Suppose the pay-TV system can support up to $\mathcal{N}$ users. For simplicity of applying the SD method, we have $N = |\mathcal{N}|$ be equal to some power of 2 (ie. $N = 2^j$, for some positive integer j). The set of revoked user is $\mathcal{R}$ and the number of revoked users $R = |\mathcal{R}|$. We suppose the decoder box (set-top box) is a simple one that just feeds the TV signals into the smart card and feeds the decryption output to the TV-set.

- **Setup:** A pay-TV center selects the security parameters as required in our IBE scheme, and the public key is $PK = \{n = pq, g, y = g^x \mod n, H_1, H_2\}$ and the secret key is $SK = \{p, q, x\}$.

- **Extract:** When all these N users are fit into a complete binary tree, the center can decide the sub-collection for each user according to SD method. There are totally $\frac{N}{2}(\log N + 1)$ subsets in the system. Each subset is assigned a secret key, for instance, the subset with ID S_{ij} is assigned the key $H_1(S_{ij}) \cdot x \mod \varphi(n)$, where S_{ij} denotes the subset that consists of all the leaves of the subtree rooted at node v_i except those in the subtree rooted at node v_j (with v_i ancestor of v_j). In the sub-collection for a random leaf i, there are $O(log^2 N)$ subsets that cover it. So the pay-TV center has to run $O(log^2 N)$ times the Extract algorithm of our IBE to obtain all the keys for the subsets that cover the leaf i. The secret keys for these subsets are then stored into the smart card that will be later issued to the user with the leaf i.

- **Registration:** When a subscriber applies to be a user of the pay-TV system, the center just associates the subscriber with a unused leaf and gives him/her the corresponding smart card. The information of subscriber and the associated leaf is stored into a database for audit purpose. The user plugs the smart card into the decoder box (set-top box) obtained from the center or elsewhere.

- **Encryption:** Given a set of privileged users $\mathcal{N} \setminus \mathcal{R}$, the center figures out what is the optimal partition by employing the SD method, says $\{S_1, S_2, \cdots, S_t\}$. For a message m, the center selects $k \in Z_n^*$ at random, then it computes and broadcasts $(r, \langle ID_{S_1}, v_1\rangle, \cdots, \langle ID_{S_t}, v_t\rangle)$ as the ciphertext, where $r = g^k \mod n$, $v_j = m \oplus H_2(y^{H_1(S_j) \cdot k \mod \varphi(n)} \mod n)$ for $j = 1, \cdots, t$.

- **Decryption:** Set $(r, \langle ID_{S_1}, v_1\rangle, \cdots, \langle ID_{S_t}, v_t\rangle)$ as the input of the tamper resistant smart card of certain user i. If user's identity string i belongs to one of the subsets in $\{S_1, S_2, \cdots, S_t\}$, says S_j, the smart card will return $v_j \oplus H_2(r^{H_1(S_j) \cdot x \mod \varphi(n)} \mod n) = m$. If the smart card finds no subset for itself, it will return $\perp$.

- **Revocation:** When the center detects that some users didn't pay the fee of the last month, it adds them to $\mathcal{R}$, so as to exclude them in Encryption of the coming month. After the revoked user fulfils the payment, the center removes him from $\mathcal{R}$.

5 Analysis

In this section, we evaluate our broadcast encryption scheme in terms of transmission cost (message header), storage (number of secret keys per user and public key size), as well as computational complexity (encryption and decryption cost) per user. The efficiency of our scheme is comparable to the symmetric SD scheme [19] and the asymmetric (public key) SD scheme [11]. The difference is that our scheme relies on tamper resistant smart card to achieve an efficient IBE scheme, so it is applicable to applications where smart cards are preferred. For instance, when subscribing for pay-TV service, what people need is a smart card issued by the providers, while they can buy all kinds of favorite set-top boxes from the market.

Transmission Cost. When in the case of SD method, as shown in [11], the message header length is $O(r)$, where r denotes the number of revoked users. Our scheme, as other subset-cover schemes, is efficient in applications where messages are broadcast to large sets, namely $r \ll n$, where n denotes the number of all users.

User Storage Cost. When in the case of SD method, each smart card has to store $O(log^2 n)$ secret keys, where n denotes the number of all users. If other improved methods applied [16, 15], the storage will be less.

Public Key Size. Dodis et al. [16] have shown that, if identifiers of subsets and users are mapping into a complete binary tree, public key size in our scheme can be reduced to $O(1)$.

Encryption Cost. Our scheme require $O(r)$ modular exponentiations in Z_n for encryption. Here r is the number of revoked users.

Decryption Cost. We need only one modular exponentiation in Z_n for decryption.

Collusion Resistance. Our system inherits collusion resistance from the subset-cover framework. Destination subset collections are carefully partitioned so that all the revoked users are excluded, so they don't have the right decryption key for the broadcast, even they collude together. If all the revoked users collude and some pre-assigned keys can still be used to decrypt, it raises an contradiction with Broadcast algorithm defined in [19]. Moreover, We assume the keys are protected by tamper resistant smart card, the users don't know the pre-assigned keys to create new decryption key.

Revocation. Our system performs the revocation when selecting destination subset collections before transmission. However, our scheme is less efficient when the number of revoked users becomes larger, because the transmission cost is linear to the number of revoked users.

Traitor Tracing. Since we use the tamper resistant smart card to store the private key and to do the entire decryption job, the smart card will wipe off all its data if anyone wants to read the private key maliciously. No duplicate smart card means that there is only one decoder for each user in our pay-TV system, in a way, we can consider that there is no pirate decoder in our system and there is no need for traitor tracing. However, our system does have the ability to trace traitors. As discussed in [19], the tracing cost is $O(t \log n)$ for at most t traitors in a binary tree of depth $\log n$.

6 Conclusion

In this paper, we proposed a new type of ID-based encryption scheme. Our scheme is identical to ElGamal encryption scheme, but using RSA framework to avoid ID replacement attack and using tamper resistant smart card to protect the private key. In a way, our scheme can be regarded as new application for the widely deployed RSA system. Our IBE scheme can be turned into an efficient broadcast encryption scheme and applied in pay-TV system. The efficiency of our broadcast encryption scheme is comparable to the symmetric SD scheme [19] and the asymmetric one [11]. For example, public keys of our system are of the size O(1) and decryption cost for each receiver is one modular exponentiation. Our scheme relies on tamper resistant smart card to achieve an efficient IBE scheme, so it is applicable to applications where smart cards are preferred.

References

[1] N. Attrapadung, K. Kobara, and H. Imai, "Sequential key derivation patterns for broadcast encryption and key predistribution schemes", *Asiacrypt 2003*, LNCS 2894, pp. 374-391, Springer-Verlag, 2003.

[2] A. K Awasthi and S. Lal, "ID-based ring signature and proxy ring signature schemes from bilinear pairings", *International Journal of Network Security*, vol. 4, no. 2, pp. 187-192, Mar. 2007.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption", *PKC 2005*, LNCS 3386, pp. 380-397, Springer-Verlag, Berlin, 2005.

[4] D. Boneh, and X. Boyen, "Efficient selective-ID identity based encryption without random oracles", *Eurocrypt 2004*, LNCS 3027, pp. 223-238, Springer-Verlag, Berlin, 2004.

[5] D. Boneh, and X. Boyen, "Secure identity based encryption without random oracles", *Crypto 2004*, LNCS 3152, pp. 443-459, Springer-Verlag, Berlin, 2004.

[6] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing", *Crypto 2001*, LNCS 2139, pp. 213-229, Springer-Verlag, Berlin, 2001.

[7] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys", *Crypto 2005*, LNCS 3621, pp. 258-275, Springer-Verlag, Berlin, 2005.

[8] R. Canetti, S. Halevi, and J. Katz, "A Forward-Secure Public-Key Encryption Scheme", *Eurocrypt 2003*, LNCS 2656, pp. 255-271, Springer-Verlag, Berlin, 2003.

[9] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys", *Asiacrypt 2007*, LNCS 4833, pp. 200-215, Springer-Verlag, Berlin, 2007.

[10] C. Delerablée, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys", *PAIRING 2007*, LNCS 4575, pp. 39-59, Springer-Verlag, Berlin, 2007.

[11] Y. Dodis, and N. Fazio, "Public key broadcast encryption for stateless receivers", *ACM DRM 2002*, LNCS 2696, pp. 61-80, Springer-Verlag, Berlin, 2003.

[12] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithm", *IEEE Transactions on Informtion Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[13] A. Fiat, and M. Naor, "Broadcast encryption", *Crypto 1993*, LNCS 773, pp. 480-491, Springer-Verlag, Berlin, 1994.

[14] C. Gentry, "Practical Identity-based encryption without random oracles", *Eurocrypt 2006*, LNCS 4004, pp. 445-464, Springer-Verlag, Berlin, 2006.

[15] M. T. Goodrich, J. Z. Sun, and R. Tamassia, "Efficient tree-based revocation in groups of low-state devices", *Crypto 2004*, LNCS 3152, pp. 511-527, Springer-Verlag, Berlin, 2004.

[16] D. Halevy, and A. Shamir, "The LSD broadcast encryption scheme", *Crypto 2002*, LNCS 2442, pp. 47-60, Springer-Verlag, Berlin, 2002.

[17] M. Kusakawa, H. Hiwatari, T. Asano, S. Matsuda, "Efficient dynamic broadcast encryption and its extension to authenticated dynamic broadcast encryption", *CANS 2008*, LNCS 5339, pp. 31-48, Springer-Verlag, Berlin, 2008.

[18] P. Kocher, J. Jaffe, and B. Jun, *Introduction to Differential Power Analysis and Related Attacks*, 1998. (http://www.cryptography.com/resources/whitepapers/DPA.html)

[19] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers", *Crypto 2001*, LNCS 2139, pp. 41-62, Springer-Verlag, Berlin, 2001.

[20] 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, No. 3, pp. 401-411, 2008.

[21] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper Resistance Mechanisms for Secure, Embedded Systems", *Proceedings of the 17th international Conference on VLSI Design (VLSID 2004)*, pp. 605-611, IEEE Computer Society, Washington, DC, 2004.

[22] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[23] R. Sakai, and J. Furukawa, "Identity-based broadcast encryption", Cryptology ePrint Archive: Report 2007/217, 2007. (http://eprint.iacr.org/2007/217)

[24] A. Shamir, "Identity-based cryptosystems and signature schemes", *Crypto 1984*, LNCS 196, pp. 47-53, Springer-Verlag, Berlin, 1985.

[25] B. Waters, "Efficient identity-based encryption without random oracles", *Eurocrypt 2005*, LNCS 3494, pp. 114-127, Springer-Verlag, Berlin, 2005.

[26] C. Xu, J. Zhou, and G. Xiao, "General group oriented ID-based cryptosystems with chosen plaintext security", *International Journal of Network Security*, vol. 6, no. 1, pp. 1-5, Jan. 2008.

[27] B. Yang, H. Ma, and S. Zhu, "A traitor tracing scheme based on the RSA system", *International Journal of Network Security*, vol. 5, no. 2, pp. 182-186, Sept. 2007.

[28] Z. M. Zhao, "ID-based weak blind signature from bilinear pairings", *International Journal of Network Security*, vol. 7, no. 2, pp. 265-268, Sept. 2008.

Xingwen Zhao is a doctor candidate in the School of Information Science and Technology at Sun Yat-sen University in Guangzhou, China. He was born in 1977, Guangxi, China. He received the B.S degree and M.S. degree from School of Communication Engineering, Xidian University in 1999 and 2004. His main research interests include broadcast encryption, signatures and key management.

Fangguo Zhang is a professor in the School of Information Science and Technology, at Sun Yat-sen University in Guangzhou, China. He obtained his Ph.D. degree in Cryptography from School of Communication Engineering, Xidian University in 2001. His main research interests include elliptic curve cryptography, pairing-based cryptosystem and its applications.