

# Anonymous signature scheme

Chunbo Ma and Jun Ao

*School of Information and Communication,  
Guilin University of Electronic Technology, Guilin, Guangxi, 541004, P. R. China  
[machunbo@guet.edu.cn](mailto:machunbo@guet.edu.cn)*

**Abstract.** In order to hide the identity of a signer, an anonymous signature scheme is presented in this paper. In this scheme, a signer located in a specified group produces a signature on behalf of the group. The recipient can verify whether the signature is valid and comes from the specified group, while tracing the signature to its source is impossible. The proposed anonymous signature is similarly to ring signature in some respects, for example, there is no manager, and no revocation mechanism against signer's anonymity. The most different between these two kinds of signatures is that the group in ring signature is adaptively constructed by the signer, while the group in our scheme is fixed.

**Keywords.** Anonymity, Signature, Public key, Group

## 1. Introduction

Digital signature is one of the crucial primitives in public key cryptography. It has been widely used in providing authenticity, integrity and non-repudiation. However, in many scenarios such as e-voting, e-auction, and many others, we need to protect a signer's identity from being arrested by malicious attackers. Currently, some signatures are designed to conceal the real identity of a signer. Ring-based signature and group signature are of the important two kinds of signatures which provide anonymity for the signer.

The concept of a group signature scheme introduced in 1991 by Chaum and van Heyst [1] is a well studied subject in cryptography. In such a scheme, a trusted group manager distributes specially designed keys to their members. Individual members can then use these keys to anonymously sign messages on behalf of their group. From view of the point of a verifier, the signature produced by different group members look indistinguishable, while the group manager can revoke the anonymity of misbehaving signers.

The concept of ring signatures was formally introduced in [2], and can be considered as a simplified group signature. After that, many proposals of ring signature schemes have been published [3][4][5][6]. In a ring signature scheme, an entity signs a message on behalf of a set of members. The verifier of the signature is convinced that it was produced by some member of the ring, but he does not obtain any information about which member of the ring actually signed. Ring signatures are a useful tool to provide anonymity in the scenarios that a member of a group has to leak some messages on behalf of the group while does not want to open his identity. There are some other works on anonymous signature such as [7][8].

Obviously, the most distinguish different between these two kinds of signatures is that a trusted manager is existed in group signature while it is not in ring signature. The role of the manager is a combiner, and when necessary it can act as an arbiter. The common ground of the two kinds of signatures is that they all provide anonymity for the signer. In some special scenario such as in a fixed group, in which the key of each member is well designed, providing the anonymity for a signer is much easier.

Ma et al. [9] presented a group-based encryption scheme, in which each member of the specified group has ability to decrypt a ciphertext encrypted for the group. In this paper, we present an anonymous signature from this encryption scheme. From view of the point of a verifier, the signature just comes from the specified group, and can't be traced. Similarly to the ring signature, there is no group manager in the group. What the different from ring signature is that the group is predefined and there are some underling relationship among group members.

## 2. Related works

The original group signature scheme that first proposed by Chaum and Heyst [1] is linear to the size of the group. Currently, many improved schemes have been proposed to achieve constant signature size, i.e. the signature size is independent of the size of the group. Camenisch and Groth [11] presented an efficient scheme that is secure under strong RSA assumption and the Diffie-Hellman decision

assumption. Boneh et al. [12] proposed another efficient group signature scheme under strong Diffie-Hellman and linear assumption. The signature produced in this scheme is under 200 bytes, while provides the same security level as an RSA signature of the same length.

The NS [13] achieves anonymity, but compare to BBS, its computation cost and the size of group signature are larger. Furthermore, although NS claims to be secure in BSZ security model, there are some flaws in the proof. Its security needs in-depth research.

The notion of ring signatures was first introduced in 2001 by Rivets et al. [2], after following lots of related ring signature scheme. In 2002, Abe et al. [14] proposed how to use public-keys of several different signature schemes to generate 1-out-of-n signatures. Another interesting work based on bilinear pairings and identity-based cryptography [15] was presented by Zhang and Kim.

Lee et al. [16] proposed a convertible ring signature the can withdraw the anonymity in 2005. Nguyen [17] designed a dynamic accumulator based on bilinear pairings, and presented an ID-based Ad-hoc anonymous identification scheme. He pointed out that applying the Fiat-Shamir heuristics to the ID-based Ad-hoc anonymous identification scheme results in an ID-based ring signature scheme with constant-size signatures. There are some other researches on ring signature [18] [19]. Chen et al. [20] extended the existing notion of ring signatures, and proposed the concept of identity-based anonymous designated ring signature which can be used in a Peer-to- Peer (P2P) network.

### 3. Background

#### 3.1 Bilinear Maps

Let  $G_1$  be a cyclic multiplicative group generated by  $g$ , whose order is a prime  $q$  and  $G_2$  be a cyclic multiplicative group of the same order  $q$ . Assume that the discrete logarithm in both  $G_1$  and  $G_2$  is intractable. A bilinear pairing is a map  $e: G_1 \times G_1 \rightarrow G_2$  and satisfies the following properties:

1. *Bilinear*:  $e(g^a, p^b) = e(g, p)^{ab}$ . For all  $g, p \in G_1$  and  $a, b \in \mathbb{Z}_q$ , the equation holds.
2. *Non-degenerate*: There exists  $p \in G_1$ , if  $e(g, p) = 1$ , then  $g = O$ .
3. *Computable*: For  $g, p \in G_1$ , there is an efficient algorithm to compute  $e(g, p)$ .
4. *Commutativity*:  $e(g^a, p^b) = e(g^b, p^a)$ . For all  $g, p \in G_1$  and  $a, b \in \mathbb{Z}_q$ , the equation holds.

Typically, the map  $e$  will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field. Pairings and other parameters should be selected for efficiency and security.

#### 3.2 Complexity assumptions

##### — *Computational Diffie-Hellman Assumption*

Given  $g^a$  and  $g^b$  for some  $a, b \in \mathbb{Z}_q^*$ , compute  $g^{ab} \in G_1$ . A  $(\tau, \varepsilon)$ -CDH attacker in  $G_1$  is a probabilistic machine  $\Omega$  running in time  $\tau$  such that

$$Succ_{G_1}^{cdh}(\Omega) = \Pr[\Omega(g, g^a, g^b) = g^{ab}] \geq \varepsilon$$

where the probability is taken over the random values  $a$  and  $b$ . The CDH problem is  $(\tau, \varepsilon)$ -intractable if there is no  $(\tau, \varepsilon)$ -attacker in  $G_1$ . The CDH assumption states that it is the case for all polynomial  $\tau$  and any non-negligible  $\varepsilon$ .

##### — *k-Strong Diffie-Hellman (k-SDH) Assumption[10]*

Given  $\{g, g^x, g^{x^2}, \dots, g^{x^k}\}$  for a random number  $x \in \mathbb{Z}_q^*$ , the attacker adaptively chooses random  $c \in \mathbb{Z}_q^*$  and computes  $g^{(c+x)^{-1}}$ . A  $(\tau, \varepsilon)$ -k-SDH attacker in  $G_1$  is a probabilistic machine  $\Omega$  running in time  $\tau$  such that

$$Succ_{G_1}^{k-sdh}(\Omega) = \Pr[\Omega(g, g^x, g^{x^2}, \dots, g^{x^k}, c) = g^{(c+x)^{-1}}] \geq \varepsilon$$

We say the k-SDH problem is  $(\tau, \varepsilon)$ -intractable if there is no  $(\tau, \varepsilon)$ -attacker in  $G_1$ .

— **T- Diffie-Hellman (TDH) Assumption**

Given  $\{g, g^a, g^{a^2}, \dots, g^{a^l}, g^{ak}, g^{a^2k}, \dots, g^{a^lk}\}$  for random numbers  $a, k \in \mathbb{Z}_q^*$ , compute  $g^{a^{l+1}k} \cdot g^r$  and  $g^{ar}$ , where  $r \in \mathbb{Z}_q^*$ . A  $(\tau, \varepsilon)$ -TDH attacker in  $G_1$  is a probabilistic machine  $\Omega$  running in time  $\tau$  such that

$$Succ_{G_1}^{tdh}(\Omega) = \Pr[\Omega(g, g^a, g^{a^2}, \dots, g^{a^l}, g^{ak}, g^{a^2k}, \dots, g^{a^lk}) = (g^{a^{l+1}k} \cdot g^r, g^{ar})] \geq \varepsilon$$

We say the TDH problem is  $(\tau, \varepsilon)$ -intractable if there is no  $(\tau, \varepsilon)$ -attacker in  $G_1$ .

### 3.3 Security notions

The accepted definition of security for signature schemes is *existential unforgeability under adaptive chosen message attack*, which is described in [21][22]. We say that a signature scheme is secure against an existential forgery under adaptive chosen messages attack in random oracle model if no polynomial bounded adversary has a non-negligible advantage in the following game:

1. **Setup:** the *Challenger* runs the **Initialize** algorithm and gives the system parameters to the *Attacker*.
2. **Attack phase:** the *Attacker* performs a polynomial bounded number of requests as follows.
  - 1). **H** queries: The *Attacker* queries the *Challenger* on a random chosen triple  $(m_i, R_{1i}, R_{2i})$ , and the *Challenger* responds with  $\mathbf{H}(m_i, R_{1i}, R_{2i})$ .
  - 2). **Sign** queries: The *Attacker* produces a query on  $m_i$ . The *Challenger* simulates **Sign** oracle and outputs  $(m_i, U_{1i}, U_{2i}, V_{1i}, V_{2i})$  to the *Attacker* as the answer.
3. **Forge phase:** the *Attacker* gives a new signature  $(m, U_1, U_2, V_1, V_2)$  and wins the game if the signature can be verified correctly.

We define the advantage of the *Attacker* to be  $Adv(Attack) = \Pr[Attack \text{ WIN}]$ . We say that a signature is secure if no polynomial bounded *Attacker* has non-negligible advantage in the game described above.

## 4. The proposed signature scheme

### 4.1 Initialize

Let  $G_1$  be a cyclic multiplicative group generated by  $g$ , whose order is a prime  $q$  and  $G_2$  be a cyclic multiplicative group of the same order  $q$ . A bilinear pairing is a map:  $e: G_2 \times G_1 \rightarrow G_2$  that can be efficiently computed. Define one cryptographic hash function:

$$H: \{0,1\}^* \rightarrow \mathbb{Z}_q$$

PKG chooses  $a \in \mathbb{Z}_q^*$  uniformly at random, and computes  $g_1 = g^a$ . The master private key is  $a$ , and the master public keys are  $(g_1, g^{a^2})$ .

### 4.2 Key Generation

PKG chooses  $k \in \mathbb{Z}_q^*$  uniformly at random as the tag of the group A. Using  $PK_A = g^k$  as group A's public key. The member  $p_i$ 's private keys can be generated as follows:

1. PKG chooses  $r_i \in \mathbb{Z}_q^*$  uniformly at random.
  2. Compute and output  $d_{i1} = g^{ar_i}$  and  $d_{i2} = g^{ak} g^{r_i}$ .
- The member  $p_i$ 's private key is  $d_i = \{d_{i1}, d_{i2}\}$ .

### 4.3 Signature

Signer chooses a random number  $t \in \mathbb{Z}_q^*$ , and computes following two values

$$U_1 = g^{a^2 \cdot t} \quad U_2 = g^{a \cdot r_i \cdot t}$$

We have  $V_1 = d_{i_2}^{(t+h)}$  and  $V_2 = d_{i_1}^h$ , and the signature of  $m$  is  $(m, V_1, V_2, U_1, U_2)$ , where  $h = H(m, U_1, U_2)$ .

We say the signature is valid, since

$$\begin{aligned} e(V_1, g^a) &= e((g^{ak} \cdot g^{r_i})^{(t+h)}, g^a) \\ &= e(g^{ak(t+h)}, g^a) e(g^{r_i(t+h)}, g^a) \\ &= e(g^{akt}, g^a) e(g^{akh}, g^a) e(g^{r_i t}, g^a) e(g^{r_i h}, g^a) \\ &= e(g^k, g^{a^2 t}) e(g^{kh}, g^{a^2}) e(g^{ar_i t}, g) e(g^{ar_i h}, g) \\ &= e(PK_A, U_1) e(PK_A^h, g^{a^2}) e(U_2, g) e(V_2, g) \end{aligned}$$

Obviously, any recipient can verify the validity of the signature and accept that the signature comes from the specified group, however, he can't distinguish who signed the message since  $t \in \mathbb{Z}_q^*$  is a random number.

## 5. Security

In this section, we will discuss the security of the proposed anonymous signature scheme. Firstly, we give following lemma.

**Lemma.** *Suppose the **CDH** assumption holds. Then given  $g^b, g^{br_i} \in G_1$ , computing  $g^{r_i}$  is intractable.*

**Proof.** Assume that given  $g^b, g^{br_i} \in G_1$ , the attacker Alice has ability to compute  $g^{r_i}$ . Then we can design an algorithm to solve **k-SDH** problem. In other words, given  $g^m, g^{m^2} \in G_1$ , the challenger Bob can compute  $g^{m^{-1}}$  by running Alice as a subroutine. Bob Inputs  $g^{m^2}, g^m \in G_1$  to Alice. As we have assumed above, Alice outputs  $g^{m/m^2}$  as a feedback. In other words, given  $g^m, g^{m^2} \in G_1$ , Bob can solve **k-SDH** via Alice. □

For a person Carol outside the group, she can't forge a valid signature without the help of malicious members. As we have mentioned above, since Carol can't forge a valid  $d_{c_2}$ , she can't produce a valid  $V_1$ . We have following theorem.

**Theorem.** *If there exists an attacker Alice, who is allowed to request at most  $q_0$  Hash queries and  $q_d$  signature queries, can break the proposed signature scheme with probability  $\varepsilon$  and within a time bound  $t$ , assume that  $\varepsilon \geq 10(q_{d_s} + 1)(q_{d_s} + q_0) / 2^k$ , then there exists another attacker Bob, who can solve **TDH** problem by recalling Alice as a subroutine in expected time  $t' \leq 120686q_0 t / \varepsilon$ .*

**Proof.** Assume that if the attacker Alice has ability to break the proposed signature scheme with non-negligible probability  $\varepsilon$ , then we will show how Bob can solve **TDH** problem. In other words, given  $g^a, g^{a^{-k}}, g^{a^2 k}, g^{a^2} \in G_1$ , Bob can compute  $g^{ak} \cdot g^r$  and  $g^{ar}$  with non-negligible probability by running Alice as a subroutine, where  $g^r \in G_1$  and random number  $r \in \mathbb{Z}_q^*$ . The challenger Bob interacts with Alice by simulating **H** and **Sign** oracles.

Bob initializes the system and gives  $g^a, g^{a^2} \in G_1$  as the public keys.

**H hash queries.** In this phase, attacker Alice is allowed to request at most  $q_0$  hash queries. Bob maintains an empty  $\Delta$ -list. For each query  $(m_i, R_{i_1}, R_{i_2})$ , Bob first checks the list:

- 1). If there exists an item  $(m_i, R_{i_1}, R_{i_2}, h_i)$  in  $\Delta$  list, then Bob return  $h_i$  to Alice.
- 2). If there is no such record in  $\Delta$  list, i.e., the item  $(m_i, R_{i_1}, R_{i_2})$  has not been queried to H oracle. Challenger Bob chooses a random number  $h_i \in \mathbb{Z}_q^*$ , and then preserves the item  $(m_i, R_{i_1}, R_{i_2}, h_i)$  in  $\Delta$ -list. Finally, he returns  $h_i$  to Alice as the answer.

**Signature queries.** In this phase, Alice is allowed to query at most  $q_d$  signature queries. For each query on  $m_i$ , Bob performs following step to return an answer.

- 1). Choose two random numbers  $c_i, d_i \in \mathbb{Z}_q^*$ , and then computes  $U_{i_1} = g^{kd_i}$  and  $U_{i_2} = g^{kc_i d_i - k^2 d_i}$ .

- 2). Choose a random number  $h_i \in \mathbb{Z}_q^*$ , and then preserves  $(m_i, U_{i1}, U_{i2}, h_i)$  in  $\Delta$ -list.
- 3). Compute  $V_{i1} = g^{a^{-1}k_i d_i} g^{ac_i h_i}$  and  $V_{i2} = g^{a^2 c_i h_i - a^2 k_i h_i}$ , and then Bob returns  $(m_i, U_{i1}, U_{i2}, V_{i1}, V_{i2})$  to Alice as the answer.

Actually, challenger Bob sets  $g^{r_i} = g^{ac_i - ak}$  and  $t = a^{-2} k d_i$  in above process. Then  $U_{i1}, U_{i2}, V_{i1}$  and  $V_{i2}$  can be expressed as follows.

$$\begin{aligned} U_{i1} &= g^{a^2 t} = g^{a^2 a^{-2} k d_i} = g^{k d_i} \\ U_{i2} &= g^{ar_i t} = g^{a(ac_i - ak)a^{-2} k d_i} = g^{k c_i d_i - k^2 d_i} \\ V_{i1} &= (g^{ak} g^{r_i})^{(t+h)} = g^{ac_i(a^{-2} k d_i + h)} = g^{a^{-1} k c_i d_i} g^{ac_i h_i} = g^{a^{-1} k c_i d_i} g^{ac_i h_i} \\ V_{i2} &= g^{ar_i h_i} = g^{a(ac_i - ak)h_i} = g^{(a^2 c_i - a^2 k)h_i} = g^{(a^2 c_i - a^2 k)h_i} \end{aligned}$$

The simulation is perfect in the random oracle. After all the queries, Alice outputs a fresh signature  $\sigma_0 = (m^*, U_{j1}, U_{j2}, V_{j1}, V_{j2})$ , where warrant  $m^*$  has never been queried to the **Sign** oracle. According to the forking lemma [20][21], if  $\epsilon \geq 10(q_{d_s} + 1)(q_{d_s} + q_0)/2^k$ , then Bob has ability to produce two valid signatures  $\sigma_0 = (m^*, U_{j1}, U_{j2}, V_{j1}, V_{j2})$  and  $\sigma_1 = (m^*, U_{j1}, U_{j2}, V'_{j1}, V'_{j2})$  on the same warrant  $m^*$  such that  $H(m^*, U_{j1}, U_{j2}) \neq H(m^*, U_{j1}, U_{j2})$ . Thus means, Bob can compute  $d_{j2}$  and  $d_{j1}$  as follows

$$d_{j2} = g^{ak} g^{r_j} = (V'_{j1} / V_{j1})^{(h_j - h_j)^{-1}} \quad d_{j1} = g^{ar_j} = (V'_{j2} / V_{j2})^{(h_j - h_j)^{-1}}$$

Since we have

$$\begin{aligned} V'_{j1} / V_{j2} &= (g^{ak} g^{r_j})^{(t+h'_j)} / (g^{ak} g^{r_j})^{(t+h_j)} & V'_{j2} / V_{j1} &= (g^{ar_j h'_j} / g^{ar_j h_j}) \\ &= (g^{ak} g^{r_j})^{(h'_j - h_j)} & &= g^{ar_j (h'_j - h_j)}. \end{aligned}$$

According to the forking lemma, Bob can solve the **TDH** problem in expected time  $t' \leq 120686q_0 t / \epsilon$ . □

For a person Carol who is not a member of the group, without the help of inner members she can't produce valid private keys. Carol chooses a random number  $r_c \in \mathbb{Z}_q^*$ , then she can compute  $d_{c1} = g^{ar_c}$  since  $g^a$  is a public value. However, it is impossible for her to draw  $d_{c2}$  from public information. Given  $g^a$  and  $g^k$ , Carol can't compute  $g^{ak}$  under the assumption that **CDH** is intractable. This means that Carol can't forge a valid  $d_{c2}$ .

For a person David who is a member of the specified group, he can't forge valid private keys without help of other members. Given  $d_{i1} = g^{ar_i}$ , according to the **Lemma** that has been mentioned above, he can't compute  $g^{r_i}$  under **k-SDH** assumption. Thus means drawing  $g^{ak}$  from his private keys is intractable. It also indicates that a member can't forge valid private keys via his known information.

## 6. Conclusions

The anonymity is crucial in some scenarios where a signer doesn't want to disclose his identity. The signers in both ring signature and group signature achieve anonymity by hiding themselves in a specified group. In this paper, we present another method that hides the signer in a group. From view of the point of verifier, the signature just comes from a specified group, and no one can be traced. The difference between the proposed anonymous signature and the ring signature is that the group used in ring signature is adaptively constructed by the signer, however the group used in our scheme is fixed, i.e., the signer can't choose the group as he want.

## References

- [1] D. Chaum, V. E. Heyst. Group signature. In Proceedings of EUROCRYPT'91. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1991, 547:257-265.

- [2] R. L. Rivest, A. Shamir, Y. Tauman. How to leak a secret. In Proceedings of ASIACRYPT'01. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2001, 2248: 552-565.
- [3] E. Bresson, J. Stern, M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In Proceedings of CRYPTO'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2442: 465-480.
- [4] J. Herranz, G. Saez. New identity-based ring signature scheme. In Proceedings of ICICS 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3269: 27-39.
- [5] J. K. Liu, D. S. Wong. On the security models of (threshold) ring signature schemes. In Proceedings of ICISC 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3506: 204-217.
- [6] M. H. Au, S. S. Chow, W. Susilo, et al.. Short linkable ring signatures revisited. In Proceedings of EuroPKI 2006. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 4043: 101-115.
- [7] G. Fuchsbaauer and D. Pointcheval. Anonymous proxy signatures. In Proceedings of SCN 2008, Lecture Notes in Computer Science, 2008, 5229: 201-217.
- [8] X. Boyen and B. Waters. Full-domain subgroup hiding and constant-size group signatures. In Proceedings of PKC 2007, Lecture Notes in Computer Science 2007, 4450: 1-15.
- [9] C. B. Ma, J. Ao, and J. H. Li. Broadcast Group-oriented Encryption Secure against Chosen Ciphertext attack. Journal of Systems Engineering and Electronics. 18(4) (2007): 811-817.
- [10] F. Zhang, R. Safavi-Naini, W. Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Applications. Practice and Theory in Public Key Cryptography-PKC 2004, Lecture Notes in Computer Science, Springer-Verlag, 2004, 2947: 277-290.
- [11] J. Camenisch and J. Groth. Group signatures: Better efficiency and new theoretical aspects. In Security in communication Networks 2004, Berlin: Springer-Verlag, 2005, 3352: 120-133.
- [12] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In Proceedings of CRYPTO 2004, Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3152: 41-55.
- [13] L. Nguyen and R. Safavi-Naini. Efficient and Provably Secure Trapdoor-free Group Signature Schemes from Bilinear Pairings. In Proceedings of Asiacrypt'04. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3329: 372-386.
- [14] M. Abe, M. Ohkubo, K. Suzuki. 1-out-of-n signatures from a variety of keys. In Proceedings of ASIACRYPT'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2501: 415-432.
- [15] F. G. Zhang, K. Kim. ID-based blind signature and ring signature from pairings. In Proceedings of ASIACRYPT'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2501: 533-547.
- [16] K. C. Lee, H. Wei, T. Hwang. Convertible ring signature. IEE Proceedings of Communications, 2005, 152(4): 411-414.
- [17] L. Nguyen. Accumulator from bilinear pairings and application to ID-based ring signatures and group membership revocation. In Proceedings of CT-RSA 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3376: 275-292.
- [18] T. Ishiki, K. Tanaka. An (n-t)-out-of-n threshold ring signature scheme. In Proceedings of ACISP 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3574: 406-416.
- [19] P. P. Tsang, V. K. Wei. Short linkable ring signatures for E-voting, E-cash and attestation. In Proceedings of ISPEC 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3439: 48-60.
- [20] Y. Q. Chen, W. Susilo, Y. Mu. Identity-based anonymous designated ring signatures. In Proceedings of IWCMC 2006. USA: ACM Press, 2006, 189-194.
- [21] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures[A]. J. of Cryptology, 2000, 13(3):361-396.
- [22] E. Brickell, D. Pointcheval, S. Vaudenay, Yung M. Design validations for discrete logarithm based signature schemes. In PKC'2000, Lecture Notes in Computer Science, Vol. 1751. Springer-Verlag (2000) 276-292.