Self-Certified Ring Signatures

Nan Li, Yi Mu, Willy Susilo, Fuchun Guo
Centre for Computer and Information Security
School of Computer Science and Software Engineering
University of Wollongong Wollongong, NSW 2522, Australia
{nl864,ymu,wsusilo,fg278}@uow.edu.au

ABSTRACT

We present a new notion, *Self-certified Ring Signature* (SCRS), to provide an alternative solution to the certificate management problem in ring signatures and eliminate private key escrow problem in identity based ring signatures. Our scheme captures all features of ring signatures and exhibits the advantages such as low storage, communication and computation cost. The main contribution of this paper is a precise definition of self-certified ring signatures along with a concrete construction. We also provide a security model of SCRS and a security proof of our scheme.

1. INTRODUCTION

The notion of ring signature was first proposed by Rivest, Shamir, and Tauman in 2001 [13]. Ring signatures are group-oriented digital signatures, which achieve signer anonymity as a major feature. It differs to a group signature as there is no anonymity revocation provided and no group setup stage. Ring signatures allow the user to sign on behalf of a group which is not predefined. Hence, any user can freely choose a set of users that include himself as a group and generate a ring signature. Verifiers believe that someone in the group signed the message, but cannot know who is the actual signer.

In traditional public key infrastructure (PKI), a signer's public key is certified with a signature of the certificate authority. Although the public key certificates can be used to authenticate user public keys, they increase the computation and communication cost, especially for a large group. This issue has been a concern for the application of ring signatures (e.g., [3, 7]). Furthermore, the complexity of certificates management is also a drawback.

Shamir [15] introduced the notion of identity-based signature (IBS) in 1984. The idea of the IBS is to eliminate the certificate verification and management problems by using the signer's identity as the public key. This idea was later applied to ring singatures (e.g., [17, 5, 4]). The identity-based ring signatures (IBRS) exhibit a better applicability. Unfortunately, the main disadvantage of IBS and IBRS are user private keys are known by the trusted authority (TA) who generates the private keys for users. Therefore, TA can impersonate any user to generate his/her signatures. This problem is referred to as *private key escrow*.

Girault [9] introduced the concept of self-certified public keys as a solution to certificate management and private key escrow. The main feature of self-certified model (SCM) is that the user public key is computable through the witness and the public key of the trusted third party (TTP). As the public key is compressed into the witness, there is no need to verify the user's public key. Hence, compared with PKI, the self-certified model presents advantages about the amount of storage, communication and computation. SCM captures the level-3 security defined by Girault as the private key escrow problem is also eliminated, while a normal IBS only reaches the level-1.

However, Saeednia [14] found a problem in the Girault's algorithm in that the TTP could still compromise the user private key via the selected composite modular of RSA (a product of two special primes that helps to solve discrete log problem). A potential solution given in [14] is to increase the size of primes, but the size of witness will also be increased. Although it is not a problem in [20], the public key recovery must be separated from the signature verification and an additional computation is necessary.

1.1 Our Contribution

In this paper, we propose the first self-certified ring signature (SCRS) scheme, which reaches the level-3 security and fixes a problem in the original SCM. Our scheme captures all the features of self-certified model and ring signature schemes. Intuitively, in our scheme, the user's public key is embedded in a witness. The user only has to provide the identity and the witness. The verifier can compute the public key during the signature verification. We present the precise definition of self-certified ring signatures. We also present a concrete scheme where the ring is formed with the three-move model introduced in [1].

Our scheme achieves the level-3 security defined by Girault [9]. We provide a security model of self-certified ring signatures and prove that our SCRS is secure under this model. Different from the Girault's algorithm, our scheme does not rely on the RSA assumption. Therefore, the private key leakage problem is eliminated.

1.2 Related work

Different but similar approach to the self-certificate cryptography is certificateless public key cryptography (CL-PKC),

ASIACCS '11, March 22–24, 2011, Hong Kong, China.

	Escrow Free	Secure Channel*	Public Key Recovery	Components of Private key
SCRS	Yes	No	Yes	1
CLRS	Yes	Yes	No	2
CBRS	Yes	No	No	2

Table 1: Properties of related paradigms. (*A secure channel is required during the certificate/PPK transmission.)

which was introduced by Al-Riyami and Paterson [2] in 2003. It can also eliminate the key escrow and certificate management problems. In CL-PKC, the user gets a certificate from the key generation center (KGC). It is seen as a partial private key (PPK). Then, the actual private key is composed of the PPK and a secret value chosen by the user. The user then generates the public key and it can be verified without a certificate. In 2007, the notion of ring signatures was applied to CL-PKC by Zhang, Zhang and Wu [19]. Independently, another certificateless ring signature scheme is proposed in [6].

Another related paradigm "certificate-based cryptography" (CBC) [8] was introduced to solve the same problems in P-KI and IBS. In CBC, the private key and the corresponding public key are decided before getting a certificate. But, the same as in CL-PKC, the certificate is used to sign. CBC is very close to CL-PKC and Wu *et al.* [16] present a generic construction to convert a certificateless signature to a certificate-based signature. CBC is also applied to ring signatures. Au *et al.* [3] proposed the first certificate-based (linkable) ring signature. We compare some features of certificateless ring signature (CLRS), certificate-based ring signature (CBRS) and SCRS in Table 1. We can find their similarities and differences.

1.3 Organization

The rest of this paper is organized as follows. In section 2, we give the definitions of self-certified ring signature schemes, the security model, and some mathematical definitions. The concrete scheme was presented in section 3. The security analysis of our scheme is given in section 4. Finally, we conclude the paper in section 5.

2. DEFINITIONS

We give a definition of self-certified ring signatures. As introduced in [9], our SCRS scheme has a special registration phase where each user gets a witness form the TTP. The SCRS security model and complexity definitions are also given in this section.

2.1 Self-Certified Ring Signature

A self-certified ring signature is composed of the five algorithms: **SysSetup, KeyGen, WitReg, Sign** and **Verify**.

- **SysSetup**(λ_1)**:** Taking as input a security parameter λ_1, the algorithm returns public parameters Params and a master secret key msk.
- **KeyGen**(λ_2)**:** Taking as input a security parameter λ_2, the algorithm returns the public and private keys (PK, SK).
- **WitReg**(ID, PK, Q)**:** Taking as input the identity ID, public key PK and the proof of knowledge of private key Q, the algorithm returns the witness W if the Q is valid, otherwise rejects.
- **Sign**$(m, \bigcup_{i=0}^{n-1}\{ID_i\}, \bigcup_{i=0,i\neq k}^{n-1}\{W_i\}, SK_k)$**:** Taking as input a set of identities $\bigcup_{i=0}^{n-1}\{ID_i\}$, a set of witnesses $\bigcup_{i=0,i\neq k}^{n-1}\{W_i\}$, a private key SK_k, $k \in \{0, 1, \ldots, n-1\}$ and the message m, the algorithm outputs a self-certified ring signature σ.
- **Verify**$(m, \sigma, \bigcup_{i=0}^{n-1}\{ID_i\}, \bigcup_{i=0}^{n-1}\{W_i\})$**:** Taking as input a signature σ, the message m and a set of identities $\bigcup_{i=0}^{n-1}\{ID_i\}$ with the corresponding witnesses $\bigcup_{i=0}^{n-1}\{W_i\}$, the algorithm returns *true* if it is valid, otherwise returns *false*.

2.2 SCRS Unforgeability

According to [9], the security of a self-certified signature scheme is defined as three levels: 1) the TTP knows the user's private key; 2) the attacker cannot know user's private key, but it can forge a false witness without being detected by users; 3) anyone cannot know the user's private key and cannot generate a false witness without being detected. Level 3 is the highest security level of self-certified scheme.

We expand this notion and define a security model of self-certified ring signature schemes. In this model, the self-certified ring signature scheme must be existentially unforgeable against adaptive chosen-message attacks in two cases. For each type, a game is given to describe the related attack.

- *Type I attack***:** The *Type I attacker* is an illegal user who does not get a valid witness from the TTP. The attacker tries to forge a witness that cannot be detected in the self-certified ring signature verification phase. Let *Type I attacker* be $\mathcal{A}_I$ for short.
- *Type II attack***:** The *Type II attacker* represents a dishonest TTP who tries to compromise the user's private key in the witness registration phase. Let *Type II attacker* be $\mathcal{A}_{II}$ for short.

Game 1: In this game, we let the adversary be an uncertified user (*Type I attacker*) who tries to forge a valid self-certified ring signature with a forged witness.

Setup: The challenger $\mathcal{C}$ runs **SysSetup** to generate public parameters Params and the master secret key. Then, $\mathcal{C}$ gives Params to the adversary.

Queries: $\mathcal{A}_I$ can adaptively issue the **Wit-Query** and **Signature-Query** queries to $\mathcal{C}$. These queries are answered as follows:

- **Wit-Query:** The adversary makes a witness query on (ID, PK, Q), $\mathcal{C}$ responds a valid witness by running **WitReg** algorithm. Let q_w be the number of witness queries in this phase.
- **Signature-Query:** $\mathcal{A}_I$ can query the signature for its choice $(m, \bigcup_{i=0}^{n-1}\{ID_i\})$. $\mathcal{C}$ generates witnesses and returns a signature σ on the message m. Let q_s be the number of signature queries in this phase.

Forgery: $\mathcal{A}_I$ outputs a message m^*, a signature σ^*, a set of identities and a set of witnesses such that $(m^*, \bigcup_{i=0}^{n-1}\{ID_i^*\})$ is not used in queries and the forged witness W^* is not generated by $\mathcal{C}$. The adversary wins the game if Verify$(m^*, \sigma^*$,

$\bigcup_{i=0}^{n-1}\{ID_i^*\}, \bigcup_{i=0}^{n-1}\{W_i^*\})$ returns *true*. We denote the advantage of $\mathcal{A}_I$ as:

$$Adv_{\mathcal{A}_I} = \Pr\left[\begin{array}{l} Verify(m^*, \sigma^*, \bigcup_{i=0}^{n-1}\{ID_i^*\}, \\ \bigcup_{i=0}^{n-1}\{W_i^*\}) = true : \\ (PK_i, s_i) \xleftarrow{R} KeyGen(\lambda); \\ W_i \leftarrow WitReg(ID_i, PK_i, Q_i); \\ W^* \neq W_i \ for \ i \in \{1 \ldots, q_w\}; \\ m^* \neq m_i, \ for \ i \in \{1 \ldots, q_s\}; \\ (m^*, \sigma^*) \leftarrow \mathcal{A}_I(\bigcup\{ID^*\}, \bigcup\{W^*\}); \end{array}\right].$$

Definition 1. We say that a self-certified ring signature scheme is (t, q_w, q_s, ϵ)-secure against Type I attack if there is no Type I attacker who wins Game 1 in t-time with advantage at least ϵ after q_w, q_s queries.

Game 2: In this game, we let the adversary be a malicious TTP (*Type II attacker*) who tries to forge a self-certified ring signature using the chosen identity and the corresponding witness.

Setup: The challenger runs **SysSetup** to generate public parameters Params and master secret key msk. $\mathcal{C}$ gives Params and msk to the adversary.

Queries: $\mathcal{A}_{II}$ can adaptively issue the **Public-key-Query** and **Signature-Query** queries to $\mathcal{C}$. These queries are answered as follows:

- **Public-key-Query:** $\mathcal{A}_{II}$ makes a public key query on ID_i. $\mathcal{C}$ generates (PK_i, SK_i) and returns PK_i. Let q_p be the number of public key queries in this phase.
- **Signature-Query:** $\mathcal{A}_{II}$ makes a signature query on $(m, \bigcup_{i=0}^{n-1}\{ID_i\}, \bigcup_{i=0}^{n-1}\{W_i\})$. $\mathcal{C}$ responds a valid signature σ by running Sign algorithm. Let q_s be the number of signature queries in this phase.

Forgery: $\mathcal{A}_{II}$ forges a self-certified ring signature and wins if Verify$(m^*, \sigma^*, \bigcup_{i=0}^{n-1}\{ID_i^*\}, \bigcup_{i=0}^{n-1}\{W_i^*\})$ returns *true* where $(m^*, \bigcup_{i=0}^{n-1}\{ID_i^*\}, \bigcup_{i=0}^{n-1}\{W_i^*\})$ does not appear in Signature-Query. We denote the advantage of this adversary as:

$$Adv_{\mathcal{A}_{II}} = \Pr\left[\begin{array}{l} Verify(m^*, \sigma^*, \bigcup_{i=0}^{n-1}\{ID_i^*\}, \\ \bigcup_{i=0}^{n-1}\{W_i^*\}) = true : \\ W_i \leftarrow WitReg(ID_i, PK_i, Q_i); \\ W^* \neq W_i \ for \ i \in \{1 \ldots, q_w\}; \\ (m^*, \sigma^*) \leftarrow \mathcal{A}_{II}(ID, \bigcup_{i=0}^{n-1}\{W_i\}); \\ m^* \neq m_i, \ for \ i \in \{1 \ldots, q_s\}; \end{array}\right].$$

Definition 2. We say that a self-certified ring signature scheme is (t, q_p, q_s, ϵ)-secure against Type II attack if there is no Type II attacker who wins Game 2 in t-time with advantage at least ϵ after q_p, q_s queries.

2.3 SCRS Anonymity

Anonymity is the main feature of ring signatures. It requires that the adversary cannot tell which member in the group generates the signature in polynomial-time with the probability greater than $\frac{1}{n}$, n is the number of group members. We define a stronger security model of anonymity of self-certified ring signatures and a powerful adversary $\mathcal{A}_p$. The adversary holds all members' private keys while he/she makes a decision. The game is constructed as follows:

Game 3: In the game, we let $\mathcal{A}_p$ be an adversary who tries to guess the actual singer of a given signature with all users' keys and witnesses.

Setup: The challenger runs the **SysSetup** algorithm to generate public parameters Params and a master secret key x. $\mathcal{C}$ gives Params to the adversary.

Query: $\mathcal{A}_p$ makes a signature query of its choice $(\bigcup_{i=0}^{n-1}\{ID_i\}, \bigcup_{i=0}^{n-1}\{W_i\}, \bigcup_{i=0}^{n-1}\{SK_i\})$. $\mathcal{C}$ chooses a signer and runs the Sign algorithm to generate and return a signature σ. Let q_s be the number of signature queries in this phase.

Guess: $\mathcal{A}_p$ guesses the actual singer of a given signature and wins if $\mathcal{A}_p$ has successfully found the index of the singer in the set of identities. We denote the advantage of this adversary as:

$$Adv_{A_p} = \left| \Pr\left[\begin{array}{l} A_p^{guess}(m, \bigcup_{i=0}^{n-1} ID_i, \bigcup_{i=0}^{n-1} W_i, \\ \bigcup_{i=0}^{n-1} SK_i) = j : \\ j \in \{0, ...n-1\}; \\ (SK_i, PK_i) \xleftarrow{R} KeyGen(\lambda); \\ W_i \leftarrow WitReg(ID_i, PK_i, Q_i); \\ \sigma \xleftarrow{R'} Sign(m, \bigcup_{i=0}^{n-1} ID_i, \\ \bigcup_{i=0}^{n-1} W_i, \bigcup_{i=0}^{n-1} SK_i); \end{array}\right] - \frac{1}{n} \right|,$$

where elements in all sets are indexed as $0, \ldots, n-1$ and j is the index of the singer in the set. We define $\xleftarrow{R'}$ as "randomly select" a user to be the signer.

Definition 3. We say that a self-certified signature scheme is (t, q_s, ϵ)-anonymous if there is no adversary who wins Game 3 in t-time with advantage at least ϵ after q_s queries.

2.4 Bilinear Maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be an additive and a multiplicative cyclic group of same prime order q, respectively. P is a generator of $\mathbb{G}_1$. The map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is a bilinear mapping (pairing) and $(P, q, \mathbb{G}_1, \mathbb{G}_2, e)$ is a symmetric bilinear group. Some properties of bilinear pairing are as follows:

- **Bilinearity:** $\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_q^*$, we have the equation $e(aP, bQ) = e(P, Q)^{ab}$.
- **Non-Degeneracy:** $\forall P \in \mathbb{G}_1$, if P is a generator of $\mathbb{G}_1$, we have $e(P, P) \neq 1$ is a generator of $\mathbb{G}_2$.
- **Efficiency:** There is an efficient algorithm to calculate $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

2.5 Complexity Assumptions

Definition 4. (Discrete Logarithm assumption) The discrete logarithm problem (DLP) is (t, ϵ)-hard, if given a tuple $< P, aP >$ that P is a generator of a group $\mathbb{G}_1$ and $a \in_R \mathbb{Z}_q^*$, there is no probabilistic polynomial time (PPT) algorithm $\mathcal{A}$ to compute a in t-time with advantage at least ϵ.

Definition 5. (Computational Diffie-Hellman assumption) The CDH problem is (t, ϵ)-hard, if given a tuple $< P, aP, bP >$ that P is a generator of a group $\mathbb{G}_1$ and $a, b \in_R \mathbb{Z}_q^*$, there is no PPT algorithm $\mathcal{A}$ to compute abP in t-time with advantage at least ϵ.

In [18], Zhang, Safavi-Naini and Susilo introduced the $(k+1)$-exponent problem ($(k+1)$-EP) and proved that it is polynomial time equal to the k-wCDHP [12]. They also mentioned that the $(k+1)$-EP is no harder than the CDH problem.

Definition 6. (k+1 exponent assumption) The (k+1)-exponent problem is (t,ϵ)-hard, if given $k+1$ valus $< P, aP, a^2P, \ldots, a^kP >$ that P is a generator of a group $\mathbb{G}_1$ and $a \in_R \mathbb{Z}_q^*$, there is no PPT algorithm $\mathcal{A}$ to compute $a^{k+1}P$ in t-time with advantage at least ϵ.

3. THE PROPOSED SCHEME

In this section, we present our self-certified ring signature scheme. Like CLRS and CBRS, it contains an interactive phase where the user requests a witness from the TTP. Since the certificate (witness) is used as a PPK in CLRS, the interaction must be protected by a secure channel that increases the cost and potential security problems. Otherwise, any one gets a certificate can generate a valid signature. Although the CBRS is no need to protect the certificate transmission, it still uses the certificate as a part of private key. In most CLRS and CBRS schemes, the user must keep these two elements. However, the witness in our scheme is a public parameter. The signing algorithm only requires the private key to be chosen by user. Normally, the length of private key in SCRS is half of that in CLRS and CBRS. In addition, the signature and witness can be generated in parallel. It is useful in some potential applications. While the public key in our scheme is implicitly calculated in the verification, it can be explicitly recovered from the witness and the TTP's public key.

3.1 Construction

SysSetup: The TTP chooses a symmetric bilinear group $(P, q, \mathbb{G}_1, \mathbb{G}_2, e)$ and two collision-resistant hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. It also randomly selects $x, y \in_R \mathbb{Z}_q^*$ and sets $msk = (x, y)$, public keys $(U, V) = (xP, \frac{y}{x}P)$. Finally, the TTP gives a set of the public parameters $\mathsf{Params} = (e, \mathbb{G}_1, \mathbb{G}_2, P, q, U, V)$.

KeyGen: The user randomly chooses a private key $s \in_R \mathbb{Z}_q^*$ and let $SK = s$. It computes the corresponding public key $PK = e(P,P)^s$.

WitReg: Let $(PK, SK) = (e(P,P)^s, s)$ be the user's public and private keys and do as follows:

- The user computes the $Q = sV$ and then sends (ID, PK, Q) to the TTP.
- The TTP first verifies the user's Q. If the equation $e(Q, \frac{1}{y}U) = PK$ holds, the TTP generates a witness as:
$$W = \frac{1}{x}H_1(ID) + \frac{1}{y}Q.$$
- Upon receiving the witness, the user checks if the following equation holds. If so, the user accepts and publishes the witness; otherwise, rejects it. Remark that the user only publishes his/her identity and the witness.
$$\begin{aligned} & e(W,U)e(H_1(ID),P)^{-1} \\ &= e(x^{-1}H_1(ID) + y^{-1}Q, U)e(H_1(ID),P)^{-1} \\ &= e(x^{-1}H_1(ID) + sy^{-1}V, U)e(H_1(ID),P)^{-1} \\ &= e(x^{-1}H_1(ID), xP)e(sx^{-1}P, xP)e(H_1(ID),P)^{-1} \\ &= e(H_1(ID),P)e(sP,P)e(H_1(ID),P)^{-1} \\ &= e(sP,P) \\ &= PK. \end{aligned}$$

Sign: Let the signer be the kth of the selected set of users. The user Takes as input a message $m \in \{0,1\}^*$, $\bigcup_{i=0}^{n-1}\{ID_i\}$, $\bigcup_{i=0,i\neq k}^{n-1}\{W_i\}$ and s_k, the user generates the self-certified ring signature as follows:

- Randomly chooses a number $\alpha \in_R \mathbb{Z}_q^*$ to compute, $c_{k+1} = H_2(L||m||e(P,P)^\alpha)$, where L is the list of selected IDs (include the signer), such that $L = ID_0||ID_1 || \ldots ||ID_{n-1}$.
- Randomly selects $r_i \in_R \mathbb{Z}_q^*$, for $i = k{+}1, k{+}2, \ldots, n-1, 0, \ldots, k-1$, then compute each c_{i+1} by
$$c_{i+1} = H_2(L||m||e(r_iP - c_iH_1(ID_i), P)e(c_iW_i, U)).$$
- To form a ring, the user uses the private key (s_k) and calculates,
$$r_k = \alpha - s_kc_k \pmod q.$$
The signature of m is $\sigma = (c_0, r_0, r_1, \ldots, r_{n-1})$.

Verify: Taking as input $(m, \sigma, \bigcup_{i=0}^{n-1}\{ID_i\}, \bigcup_{i=0}^{n-1}\{W_i\})$, the user computes c_{i+1} as above, for $i = 0, 1, \ldots, n-1$. Accept the signature if $c_0 = c_n$, otherwise reject it.

3.2 Correctness

Our self-certified ring signature scheme is correct as the following equation holds:

$$\begin{aligned} c_{k+1} &= H_2(L||m||e(r_kP - c_kH_1(ID_k), P)e(c_kW_i, U)) \\ &= H_2(L||m||e(r_kP - c_kH_1(ID_k), P)e(x^{-1}H_1(ID_k) \\ &\quad + x^{-1}s_kP, xP)^{c_k}) \\ &= H_2(L||m||e((\alpha - s_kc_k)P, P)e(s_kc_kP, P) \\ &= H_2(L||m||e(P,P)^\alpha). \end{aligned}$$

4. SECURITY ANALYSIS

The security of self-certified ring signatures contains two parts, the unforgeability and the anonymity. Different from certificateless and certificate-based ring signatures, the public key replacement attack in [10] and [11] is no longer valid in self-certified signatures. Our scheme is secure if there is no adversary who wins any of the following games.

4.1 Game 1 Security

Theorem 1. Our self-certified ring signature scheme is (t, q_w, q_s, ϵ)-secure against Type I attack if the (k+1)-EP is (t', ϵ')-hard.

4.2 Game 2 Security

Theorem 2. Our SCR signature scheme is (t, q_p, q_s, ϵ)-secure against Type II attack if the DL problem is (t', ϵ')-hard.

4.3 SCR Anonymity

Theorem 3. Our self-certified ring signature scheme is (t, q_s, ϵ)-anonymous.

Because of the space limitation, the security proofs of these theorems are omitted in this paper.

5. CONCLUSION

In this paper, we proposed a new notion, *Self-Certified Ring Signature* (SCRS). It solved the private key escrow and certificate management problems. Since our scheme embedded the public key into the witness, it reduces the cost of storage, communication and computation. We compared it with two related schemes: certificateless ring signatures and certificate-based ring signatures. Our SCRS is better due to shorter key size and lower setup cost. We proposed a precise definition of self-certified ring signatures and provided a concrete scheme. Our scheme has been proven secure.

6. REFERENCES

[1] M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n signatures from a variety of keys. In *Advances in Cryptology - Asiacrypt '02, LNCS 2501*, pages 415–432. Springer-Verlag, 2002.

[2] S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In *Advances in Cryptology-Asiacrypt '03, LNCS 2894*, pages 452–473. Springer-Verlag, 2003.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Certificate based (linkable) ring signature. In *ISPEC '07, LNCS 4464*, pages 79–92. Springer-Verlag, 2007.

[4] M. H. Au, J. K. Liu, Y. H. Yuen, and D. S. Wong. Id-based ring signature scheme secure in the standard model. In *IWSEC '06, LNCS 4266*, pages 1–16. Springer-Verlag, 2006.

[5] S. S. Chow, R. W. Lui, L. C. Hui, and S. Yiu. Identity based ring signature: Why, how and what next. In *EuroPKI 2005, LNCS 3545*, pages 144–161. Springer-Verlag, 2005.

[6] S. S. Chow and W.-S. Yap. Certificateless ring signatures. In *Cryptology ePrint Archive, Report 2007/236*. http://eprint.iacr.org/2007/236/, 2007.

[7] S. S. Chow, S. Yiu, and L. C. Hui. Efficient identity based ring signature. In *ACNS '05, LNCS 3531*, pages 499–512. Springer-Verlag, 2005.

[8] C. Gentry. Certificate-based encryption and the certificate revocation problem. In *EUROCRYPT '03, LNCS 2656*, pages 272–293. Springer-Verlag, 2003.

[9] M. Girault. Self-certified public keys. In *EUROCRYPT '91, LNCS 547*, pages 490–497. Springer-Verlag, 1991.

[10] X. Huang, W. Susilo, Y. Mu, and F. Zhang. On the security of certificateless signature schemes from asiacrypt '03. In *CANS 2005, LNCS 3810*, pages 13–25. Springer-Verlag, 2005.

[11] J. Li, X. Huang, Y. Mu, W. Susilo, and Q. Wu. Certificate-based signature: Security model and efficient construction. In *EuroPKI '07, LNCS 4582*, pages 110–125. Springer-Verlag, 2007.

[12] S. Mitsunari, R. Sakai, and M. Kasahara. A new traitor tracing. *IEICE Tran.*, E85-A(2):481–484, 2002.

[13] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secre. In *ASIACRYPT '01, LNCS 2248*, pages 552–565. Springer-Verlag, 2001.

[14] S. Saeednia. A note on girault's self-certified model. In *Information Processing Letters 86*, pages 323–327, 2003.

[15] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology Crypto '84, LNCS 196*, pages 47–53. Springer-Verlag, 1985.

[16] W. Wu, Y. Mu, W. Susilo, and X. Huang. Certificate-based signatures revisited. *Journal of Universal Computer Science*, 15:1659–1684, 2009.

[17] F. Zhang and K. Kim. Id-based blind signature and ring signature from pairings. In *Advances in Cryptology - Asiacrypt' 02, LNCS 2501*, pages 533–547. Springer-Verlag, 2002.

[18] F. Zhang, R. Safavi-Naini, and W. Susilo. An efficent signature scheme from bilinear pairings and its applications. In *PKC 2004, LNCS 2947*, pages 277–290. Springer-Verlag, 2004.

[19] L. Zhang, F. Zhang, and W. Wu. A provably secure ring signature scheme in certificateless cryptography. In *ProvSec '07, LNCS 4784*, pages 103–121. Springer-Verlag, 2007.

[20] Y. Zhou, Z. Cao, and R. Lu. An efficient digital signature using self-certified public keys. In *Proceedings of the 3rd international conference on Information security*, volume 85, pages 44–47. ACM, 2004.