Online/Offline Ring Signature Scheme*

Joseph K. Liu[1], Man Ho Au[2], Willy Susilo[2], and Jianying Zhou[1]

[1] Cryptography and Security Department
Institute for Infocomm Research, Singapore
{ksliu,jyzhou}@i2r.a-star.edu.sg
[2] Centre for Computer and Information Security (CCISR)
School of Computer Science and Software Engineering
University of Wollongong, Australia
{aau,wsusilo}@uow.edu.au

Abstract. In this paper, for the first time in the literature, we introduce the notion of online/offline ring signature scheme. Our primitive enables ring signature schemes to be used in practice, since the online mechanism can be performed very efficiently and hence, it is very suitable to be used in a mobile-device environment. We provide a formal model to capture our primitive, and we proceed with a concrete construction of online/offline ring signature schemes. Finally, we show that our scheme is secure in our model.

1 Introduction

Bluetooth is a short-range exchange data enabler protocol that allows mobile devices to communicate in an ad-hoc way. It was originally motivated as the wireless alternative to the RS232 data cable. This technology enables mobile devices, such as iPhone, Windows devices or Android devices, to communicate wirelessly in an ad-hoc manner. It will enable an ad-hoc communication built among business people meeting in a conference room, since the communication can be done efficiently and in a very simple manner. This technology will allow cryptographic techniques to be embedded to it, for instance to create an authenticated message on behalf of the group. One possible solution is by incorporating the primitive put forth by Rivest, Shamir and Tauman known as the ring signature schemes [26]. In fact, this has been "implied" since the invention of ring signatures that these types of primitives can be used on top of ad-hoc technology, such as Bluetooth.

A ring signature scheme (for examples [1, 7, 8, 14, 15, 26, 33, 13, 31, 24, 22, 32, 23, 3, 20, 2, 4, 21, 25]) allows members of a group to sign messages on behalf of the group without revealing their identities, i.e. signer anonymity. In addition, it is not possible to decide whether two signatures have been issued by the same group member. Different from a group signature scheme (for examples, [11], [9] and [5]), the group formation is spontaneous and there is no group manager to

* The first and fourth author of this work are funded by the EU project SMEPP-033563.

S. Qing, C.J. Mitchell, and G. Wang (Eds.): ICICS 2009, LNCS 5927, pp. 80–90, 2009.

revoke the identity of the signer. That is, under the assumption that each user is already associated with a public key of some standard signature scheme, a user can form a group by simply collecting the public keys of all the group members including his own. These diversion group members can be totally unaware of being conscripted into the group.

Ring signature schemes could be used for whistle blowing [26], anonymous membership authentication for ad hoc groups [8] and many other applications which do not want complicated group formation stage but require signer anonymity. For example, in the whistle blowing scenario, a whistleblower gives out a secret as well as a ring signature of the secret to the public. From the signature, the public can be sure that the secret is indeed given out by a group member while cannot figure out who the whistleblower is. At the same time, the whistleblower does not need any collaboration of other users who have been conscripted by him into the group of members associated with the ring signature. Hence the anonymity of the whistleblower is ensured and the public is also certain that the secret is indeed leaked by one of the group members associated with the ring signature.

Ring signature scheme can be used to derive other primitives as well. It had been utilized to construct non-interactive deniable ring authentication [29], perfect concurrent signature [30] and multi-designated verifiers signature [19].

Nevertheless, the existing ring signature schemes requires very heavy computations. Usually the number of exponentiations required during the signing stage is proportional to the number of users included in the ring signature. Say, if the signature includes 10000 users, the signing stage requires at least 10000 exponentiations. This may not be a big problem for personal computers. However, the schemes will not be suitable in practice to be used in mobile devices as these computations will drain the battery quickly.

In this paper, we address the above problem specifically by introducing the notion of "online/offline ring signatures". In our primitive, the signing stage is divided into two phases. Similar to other online/offline signatures [16, 28, 18, 12, 17, 6], the offline mechanism can be quite computationally heavy, but the online mechanism should be very efficient. This way, we can achieve an ad-hoc communication among mobile devices using the available technology, such as Bluetooth. Our primitive has enabled the use of ring signature schemes in a more practical way.

However, there is one major difference between normal online/offline signatures and online/offline ring signatures. For a normal signature, there is only 1 user. For a ring signature, there are n different users included. The crux of constructing such a scheme relies on the fact that during the offline phase, *the signers are not known* in advance. The group of signers will only be known during the online phase, and therefore this creates some subtleties in the scheme. Otherwise, by using some generic construction of normal online/offline signature schemes such as [28], it is quite trivial to construct one from a normal ring signature scheme.

In the practical point of view, if we need to fix the possible signers in the offline phase, it is not useful. Suppose we need to create a ring signature during a meeting using a mobile device. The offline phase should be done before the meeting. However, it maybe impossible to know who are going to attend the meeting at this moment yet. We are not interested in this model as it is not practical to be used in many applications. Instead, we do not need to know any possible signers in the offline phase. Furthermore, we even allow any third party to generate the offline phase. That is, no secret key is needed and no secret information is generated in the offline phase. This creates even more flexibility for different kinds of scenarios. Therefore it is quite challenging to design and construct such a scheme with these nice properties.

1.1 Contribution

In this paper, we propose a new notion called online/offline ring signature scheme. It is the "online/offline" version of ring signature scheme, with the following additional properties:

1. Most of the heavy computations are done in the offline phase, while the online phase just requires relatively light computation.
2. The online computation requirement is independent to the number of possible signers included in the ring signature. In our construction we just require 2 exponentiations in this phase, no matter how many possible signers are included in the signature.
3. The offline phase does not require the public keys of the possible signers. That is, the public keys are not needed to be fixed at this phase yet.
4. The offline phase can be done by any third party. All information produced or generated during this phase is publicly known. There is no secret information included or required in this phase.

Our scheme is proven secure in the random oracle model, under the standard RSA assumption.

2 Definitions

2.1 Mathematical Assumption

The security of our scheme relies on the RSA assumption with safe prime, which is defined as follow:

Definition 1 (Safe Prime). *p is a safe prime if it can be expressed as $2p'+1$ where p' is also a prime.*

Definition 2 (RSA Assumption with Safe Prime). *Let $N = pq$ where p and q are k-bits length safe primes. Let e be a number such that e and $\phi(N)$ are co-prime. Given an element $r \in \mathbb{Z}_N$ chosen at random, find an integer x such that $x^e = r \bmod N$. An adversary $\mathcal{A}$ has at least an ϵ advantage if*

$$\Pr[\mathcal{A}(N, e, r) = x \mid x^e = r \bmod N] \geq \epsilon$$

We say that the (ϵ, τ, k)-RSA assumption holds if no algorithm running in time at most τ can solve that RSA problem with advantage at least ϵ, where the modulus is a product of two safe primes with k-bits length.

2.2 Security Definition

Definition 3. *A online/offline ring signature scheme is defined by the following algorithms:*

- Key-Gen is a probabilistic algorithm taking as input a security parameter. It returns the user secret key sk and public key pk.
- Offline-Sign is a probabilistic algorithm taking n' as input, where n' is the maximum number of users to be included in the ring signature. Optionally, it may also take the actual signer's secret key sk and public key pk as input. It returns an offline signature $\bar{\sigma}$.
- On-Sign is a probabilistic algorithm taking $(L, m, sk, \bar{\sigma})$ as input, where L is the list of n public keys to be included in the ring signature and $n \leq n'$ and m is the message to be signed. It returns a signature σ.
- Verify is a deterministic algorithm taking (L, m, σ) as input. It outputs either Accept or Reject.

The security of a ring signature scheme consists of two requirements, namely *Signer Ambiguity* and *Existential Unforgeability*. They are defined as follows.

Definition 4 (Signer Ambiguity). *Let $L = \{pk_1, \cdots, pk_n\}$ be the list of public keys and $L_{sk} = \{sk_1, \cdots, sk_n\}$ be the corresponding secret keys. Each key is generated by Key-Gen. A ring signature scheme is said to be unconditionally signer ambiguous if, for any L, any message m, and any signature $\sigma \leftarrow$ On-Sign$(L, m, sk_\pi,$ Offline-Sign$(|L|))$ where $sk_\pi \in L_{sk}$, any unbound adversary $\mathcal{A}$ accepts as inputs L, m and σ, outputs π with probability $1/n$.*

It means that even all the private keys are known, it remains uncertain that which signer out of n possible signers actually generates a ring signature.

Definition 5 (Existential Unforgeability). *For a ring signature scheme with n public keys, the existential unforgeability is defined as the following game between a challenger and an adversary $\mathcal{A}$:*

1. The challenger runs algorithm Key-Gen. Let $L = \{pk_1, \cdots, pk_n\}$ be the set of n public keys and $L_{sk} = \{sk_1, \cdots, sk_n\}$ be the corresponding secret keys. $\mathcal{A}$ is given L.
2. $\mathcal{A}$ can adaptively queries the signing oracle q_S times: On input any message m and L' where $L' \subseteq L$ (the corresponding secret keys are denoted by L'_{sk}) returns a ring signature $\sigma \leftarrow$ On-Sign$(L', m, sk_\pi,$ Offline-Sign$(|L'|))$, where $sk_\pi \in L'_{sk}$ and Verify$(L', m, \sigma) =$ Accept.
3. Finally $\mathcal{A}$ outputs a tuple (L^*, m^*, σ^*).

$\mathcal{A}$ wins the game if:

1. $L^* \subseteq L$.
2. (L^*, m^*) has not been submitted to the signing oracle.
3. $\mathsf{Verify}(L^*, m^*, \sigma^*) = \mathsf{Accept}$

We define $\mathcal{A}$'s advantage in this game to be $Adv(\mathcal{A}) = \Pr[\mathcal{A} \text{ wins }]$.

3 The Proposed Scheme

3.1 Construction

Let k_1, k_2, k_3 be security parameters such that $k_1 \leq k_2 - 1$. Assume G is a hash function that maps any arbitrary string into k_1-bits odd integer.

Key-Gen: Each user selects two safe primes p, q of length k_2-bits, such that $p = 2p' + 1, q = 2q' + 1$ where p', q' are also primes. His secret key is (p, q) and public key is $N = pq$.

Offline-Sign: Assume there are maximum n' users to be included in the ring signature (their public keys are not yet known in this stage, except the real signer). For $i = 1, \ldots, n' - 1$, randomly selects integers $x_i \in_R \{0,1\}^{2k_2 - 1}$, $e_i \in_R \{0,1\}^{k_3}$ and computes $y_i = x_i^{G(e_i)}$ (without modulus). Stores the offline signature $\bar{\sigma} = (x_1, e_1, y_1, \ldots, x_{n'-1}, e_{n'-1}, y_{n'-1})$.

Online-Sign: Let $L = \{N_1, \ldots, N_n\}$ be a list of n public keys to be included in the ring signature, where $n \leq n'$. Let $H_i : \{0,1\}^* \rightarrow \mathbb{Z}_{N_i}$ be some hash functions for $i = 1, \ldots, n$. W.l.o.g., we assume user n is the actual signer. The actual signer executes the following steps:

1. Randomly generates an integer $e_n \in_R \{0,1\}^{k_3}$ and computes $d_n = 1/G(e_n) \bmod \phi(N_n)$.
2. Randomly generates $r_n \in_R \mathbb{Z}_{N_n}$, computes $c_1 = H_1(L, m, r_n)$.
3. For $i = 1, \ldots, n-1$, computes $c_{i+1} = H_{i+1}(L, m, c_i + y_i \bmod N_i)$.
4. Computes $x_n = (r_n - c_n)^{d_n} \bmod N_n$.

If $|x_n| = 2k_2$ bits, repeats step 2 - 4 until getting another x_n which is strictly less than $2k_2$ bits. Outputs the signature $\sigma = (x_1, e_1, \ldots, x_n, e_n, c_1)$.

Verify: To verify a signature for message m and public keys $L = \{N_1, \ldots, N_n\}$, For $i = 1, \ldots, n$ computes $r_i = c_i + x_i^{G(e_i)} \bmod N_i$ and $c_{i+1} = H_{i+1}(L, m, r_i)$ if $i \neq n$. Accept if $c_1 = H_1(L, m, r_n)$. Otherwise reject.

Remarks

1. The offline signing phase can be executed by any third party. We do not require the secret key of the actual signer. There is neither any secret information (such as secret randomness) produced at this stage. All data generated here are publicly known. The tradeoff is, we require a modulus inverse

$1/G(e_n)$ in the online part. To further improve efficiency, this part (step 1 of the online signing stage) can be put into the offline signing phase. However, since this step requires the knowledge of the secret key (factorization of N_n), by doing so, the offline signing phase also requires the secret key as the input and (e_n, d_n) are stored as part of the offline signature.

2. The expected running time of step 2 - 4 in Online-Sign is 2. It is calculated as follow: For each time,

$$\Pr[|x_n| = 2k_2] \leq 0.5$$

as $|N_n| = 2k_2$. That means at least with probability 0.5 the computation of step 4 is successful ($|x_n| < 2k_2$). The expected running time S should be:

$$S = 1 \times \frac{1}{2} + 2 \times \frac{1}{2^2} + 3 \times \frac{1}{2^3} + 4 \times \frac{1}{2^4} + \cdots \tag{1}$$

From (1), multiply both sides by $\frac{1}{2}$, we get

$$\frac{1}{2}S = \frac{1}{2^2} + \frac{2}{2^3} + \frac{3}{2^4} + \frac{4}{2^5} + \cdots \tag{2}$$

(1) - (2), we get

$$\frac{1}{2}S = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots = \frac{\frac{1}{2}}{1 - \frac{1}{2}} = 1 \tag{3}$$

From (3), we can get the result $S = 2$.

3.2 Security Analysis

Theorem 1. *Our ring signature scheme is unconditionally signer ambiguous.*

Proof. All e_i are taken randomly from $\{0,1\}^{k_3}$ and all x_i except x_n are also taken randomly from $\{0,1\}^{2k_2-1}$. At the closing point, $x_n \in \{0,1\}^{2k_2-1}$ also distributes randomly as r_n is randomly chosen, c_n depends on previous x_i and e_i which are all random numbers. The remaining c_1 is uniquely determined from L, m and r_n.

Note that the reason why we need to restrict x_n to be at most $2k_2 - 1$ bits is that, as other x_i are all at most $2k_2 - 1$ bits, if x_n is $2k_2$ bits, one may know that user n is the actual signer. □

Theorem 2. *Suppose the (τ', ϵ', k_2)-RSA assumption with safe prime holds. Then our ring signature scheme with n users is $(\tau, q_s, q_h, q_g, \epsilon)$-secure against existential forgery under an adaptive chosen message attack provided that:*

$$\epsilon' \geq \frac{2\left(1 - \frac{q_h q_s}{N_{min}}\right)\left(1 - \frac{1}{N_{min}}\right)\left(1 - \frac{1}{2^{k_2-1}}\right)\epsilon}{q_h(q_h+1)q_g n} \qquad \tau' = \tau$$

where N_{min} is the smallest modulus among n public keys, q_s is the maximum number of signing oracle queries allowed, q_h is the maximum number of H_i random oracle queries allowed, q_g is the maximum number of G random oracle queries allowed.

Proof. Setup: The proof uses the approach described in [1]. Suppose the adversary $\mathcal{A}$ can forge the ring signature scheme with n users. We construct an algorithm $\mathcal{S}$ that uses $\mathcal{A}$ to solve the (τ', ϵ', k_2)-RSA problem.

$\mathcal{S}$ receives the problem instance (N, e, r), where N is the product of two safe prime numbers of length k_2-bits, e is coprime to $\phi(N)$, $2 < e < N$ and $0 \leq r < N$. $\mathcal{S}$ is asked to output an integer x such that $x^e = r \bmod N$. For simplicity, we let $k_1 = k_2 - 1$ to be the length of the output string of G random oracle.

$\mathcal{S}$ randomly chooses $\pi \in_R [1, n]$ and assigns the public key of user π to be N (the problem instance). For the other $n-1$ users' public keys, $\mathcal{S}$ generates them according to the algorithm.

$\mathcal{S}$ also chooses three integers u, v, w such that $1 \leq u \leq v \leq q_h$ and $1 \leq w \leq q_g$.

Oracle Simulation:

- *H_i Random Oracle:* For simplicity, the H_i random oracles are treated as single oracle that takes $Q_j = (i, L_j, m_j, r_j)$ as the j-th query and returns a random value that corresponds to $H_i(L_j, m_j, r_j)$ maintaining consistency against duplicated queries.
- *G Random Oracle:* $\mathcal{S}$ assigns e (the problem instance) to be the output of the w-th query. For the other queries, it just returns a random value and maintaining consistency against duplicated queries.
- *Signing Oracle:* Upon receiving the signing query for (L_j, m_j), $\mathcal{S}$ simulates the signing oracle in the following way.
  1. Randomly choose $c_1 \in_R \mathbb{Z}_{N_1}$.
  2. For $i = 1, \ldots, |L_j|$, randomly select integers $x_i \in_R \{0,1\}^{2k_2-1}$ and $e_i \in_R \{0,1\}^{k_3}$, compute $r_i = x_i^{G(e_i)} + c_i \bmod N_i$, and then compute $c_{i+1} = H_{i+1}(L_j, m_j, r_j)$ if $i \neq |L_j|$.
  3. Assign c_1 to the value of $H_1(L_j, m_j, r_{|L_j|})$.

Output Calculation: Since the queries form a ring, there exists at least one index, say κ, in $\{1, \ldots, n\}$ such that $Q_u = (\kappa+1, L, m, r_\kappa)$ and $Q_v(\kappa, L, m, r_{\kappa-1})$ satisfy $u \leq v$. Namely, κ is in between the gap of query order. We call such (u, v) a gap index. Note that $u = v$ happens only if $n = 1$, which means that the resulting L contains only one public-key. If there are two or more gap indices with regard to a signature, only the smallest one is considered.

At the beginning of the simulation, $\mathcal{S}$ has chosen a pair of index (u, v) randomly such that $1 \leq u \leq v \leq q_h$. If the guess is correct, $\mathcal{S}$ receives $Q_u = (\kappa + 1, L, m, r_\kappa)$ and $Q_v = (\kappa, L, m, r_{\kappa-1})$ so that (u, v) is a gap index. When query Q_v is made (u-th query has been already made by this moment), $\mathcal{S}$ returns $c_\kappa = r_\kappa - r \bmod N_\kappa$ (r is the problem instance) as the value of $H_\kappa(L, m, r_{\kappa-1})$. If $\mathcal{A}$ is successful in forgery, it outputs x_κ that satisfies $r_\kappa = c_\kappa + x_\kappa^{G(e_\kappa)} \bmod N_\kappa$. Since $r_\kappa = c_\kappa + r \bmod N_\kappa$, we obtain x_κ as the inverse of r with regard to N, if e_κ is the w-th G-query. That is, the output of that particular query is e (the problem instance).

Probability Analysis: $\mathcal{S}$ is successful if

1. $\mathcal{A}$ outputs a valid forged signature;
2. There is no abortion or failure in any oracle simulation; and
3. All guesses are correct.

$\mathcal{A}$ outputs a valid forged signature with probability ϵ.

$\mathcal{S}$ fails if Step 3 in the signing oracle simulation causes inconsistency in H_1. It happens with probability at most q_h/N_{min} where N_{min} is the smallest N_i in L. Hence, the simulation is successful q_s times with probability at least

$$\left(1 - \frac{q_h}{N_{min}}\right)^{q_s} \geq 1 - \frac{q_h q_s}{N_{min}}$$

For H_i random oracle, with probability at least $1 - 1/N_{min}$, there exist queries $Q_j = (i+1, L, m, r_i)$ for all $i = 1, \ldots, n$ due to the ideal randomness of H. Similarly, for G random oracle, with probability at least $1 - 1/2^{k_2-1}$, there will be no collision occur.

At the beginning of the simulation, $\mathcal{B}$ selects a pair of index (u, v). With probability $2/q_h(q_h+1)$, the guess is correct. $\mathcal{B}$ also selects an index w for the G random oracle query, whose output is assigned to the problem instance. With probability $1/q_g$, the guess is correct. $\mathcal{B}$ needs to guess the index of the user corresponding to the (u, v) gap. $\mathcal{B}$ is correct if $\pi = \kappa$. This happens with probability $1/n$.

Combining all cases, overall successful probability of $\mathcal{B}$ is at least

$$\frac{2\left(1 - \frac{q_h q_s}{N_{min}}\right)\left(1 - \frac{1}{N_{min}}\right)\left(1 - \frac{1}{2^{k_2-1}}\right)\epsilon}{q_h(q_h+1)q_g n}$$

The running time of $\mathcal{S}$ is almost the same as τ as $\mathcal{S}$ runs $\mathcal{A}$ only once and the simulation cost for the signing oracle and the random oracles are assumed to be sufficiently smaller than τ. □

4 Efficiency of Existing Ring Signatures

The following table (Table 1) summarizes the time complexities of existing ring signatures. We breakdown the time complexity of the protocol into the number of multi-exponentiations (multi-EXPs). A multi-EXP computes the product

Table 1. Time Complexities of Existing Ring Signatures

Scheme	Number of Multi-EXP
Rivest-Shamir-Tauman [26]	$n+1$
Abe-Ohkubo-Suzuki [1]	$n+1$
Dodis-Kiayias-Nicolosi-Shoup [15]	14
Chow-Wei-Liu-Yuen [13]	n
Shacham-Waters [27]	$2n+2$
Chandran-Groth-Sahai [10]	$5 + 6\sqrt{n} + \frac{n+1}{3}$
Our scheme	2

of exponentiations faster than performing the exponentiations separately. Normally, a multi-based exponentiation takes only 10% more time compared with a single-based exponentiation. We assume that one multi-EXP operation multiplies up to 3 exponentiations. Let n be the size of the ring and the number of multi-EXP is taken after the n public keys and the message are known.

5 Conclusion

In this paper, we have proposed a new notion called Online/Offline Ring Signature scheme. Under this notion, most of the heavy computations are done in the offline phase. At this phase the public keys of all users and the message to be signed are yet to be known. In the online phase, only very little computations are needed after knowing those public keys and the signing message. We provided a concrete construction of this notion. In our construction, the offline phase can be done by other third party. This allows more flexibility. We believe the online/offline ring signature scheme can be used in many different applications such as authentication or whistle blowing using mobile devices.

There are some future improvements that can be done. One of them is to further reduce the online computation requirement. Currently we still require about 2 exponentiations during the online phase. It is better to eliminate it totally. Another open problem is to construct a constant size online/offline ring signature scheme as the signature size of our current construction is still linear with the number of users included in the ring. Finally, it would be interesting to construct an online/offline ring signatures that do not require random oracle models.

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n Signatures from a Variety of Keys. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 415–432. Springer, Heidelberg (2002)
2. Au, M.H., Liu, J.K., Susilo, W., Yuen, T.H.: Constant-size ID-based linkable and revocable-iff-linked ring signature. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 364–378. Springer, Heidelberg (2006)
3. Au, M.H., Liu, J.K., Susilo, W., Yuen, T.H.: Certificate based (linkable) ring signature. In: Dawson, E., Wong, D.S. (eds.) ISPEC 2007. LNCS, vol. 4464, pp. 79–92. Springer, Heidelberg (2007)
4. Au, M.H., Liu, J.K., Yuen, T.H., Wong, D.S.: ID-based ring signature scheme secure in the standard model. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S.-i. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 1–16. Springer, Heidelberg (2006)
5. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 614–629. Springer, Heidelberg (2003)
6. Boneh, D., Boyen, X.: Short signatures without random oracles the SDH assumption in bilinear groups. Journal of Cryptology 2, 149–177 (2008)

7. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 416–432. Springer, Heidelberg (2003)
8. Bresson, E., Stern, J., Szydlo, M.: Threshold Ring Signatures and Applications to Ad-hoc Groups. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 465–480. Springer, Heidelberg (2002)
9. Camenisch, J., Stadler, M.: Efficient Group Signature Schemes for Large Groups (Extended Abstract). In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997)
10. Chandran, N., Groth, J., Sahai, A.: Ring signatures of sub-linear size without random oracles. In: Arge, L., Cachin, C., Jurdziński, T., Tarlecki, A. (eds.) ICALP 2007. LNCS, vol. 4596, pp. 423–434. Springer, Heidelberg (2007)
11. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
12. Chen, X., Zhang, F., Susilo, W., Mu, Y.: Efficient generic online/offline signatures without key exposure. In: Katz, J., Yung, M. (eds.) ACNS 2007. LNCS, vol. 4521, pp. 18–30. Springer, Heidelberg (2007)
13. Chow, S.S., Liu, J.K., Wei, V.K., Yuen, T.H.: Ring Signatures without Random Oracles. In: ASIACCS 2006, pp. 297–302. ACM Press, New York (2006)
14. Chow, S.S.M., Yiu, S.-M., Hui, L.C.K.: Efficient Identity Based Ring Signature. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 499–512. Springer, Heidelberg (2005); Also available at Cryptology ePrint Archive, Report 2004/327
15. Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous Identification in Ad Hoc Groups. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 609–626. Springer, Heidelberg (2004)
16. Even, S., Goldreich, O., Micali, S.: On-line/Off-line digital signatures. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 263–275. Springer, Heidelberg (1990)
17. Joye, M.: An efficient on-line/off-line signature scheme without random oracles. In: Franklin, M.K., Hui, L.C.K., Wong, D.S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 98–107. Springer, Heidelberg (2008)
18. Kurosawa, K., Schmidt-Samoa, K.: New online/offline signature schemes without random oracles. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 330–346. Springer, Heidelberg (2006)
19. Laguillaumie, F., Vergnaud, D.: Multi-designated Verifiers Signatures. In: López, J., Qing, S., Okamoto, E. (eds.) ICICS 2004. LNCS, vol. 3269, pp. 495–507. Springer, Heidelberg (2004)
20. Liu, D.Y.W., Liu, J.K., Mu, Y., Susilo, W., Wong, D.S.: Revocable ring signature. J. Comput. Sci. Technol. 22(6), 785–794 (2007)
21. Liu, J.K., Susilo, W., Wong, D.S.: Ring signature with designated linkability. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S.-i. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 104–119. Springer, Heidelberg (2006)
22. Liu, J.K., Wei, V.K., Wong, D.S.: A Separable Threshold Ring Signature Scheme. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 352–369. Springer, Heidelberg (2004)
23. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 325–335. Springer, Heidelberg (2004)

24. Liu, J.K., Wong, D.S.: On the Security Models of (Threshold) Ring Signature Schemes. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 204–217. Springer, Heidelberg (2005)
25. Liu, J.K., Wong, D.S.: Enhanced security models and a generic construction approach for linkable ring signature. Int. J. Found. Comput. Sci. 17(6), 1403–1422 (2006)
26. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001)
27. Shacham, H., Waters, B.: Efficient ring signatures without random oracles. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 166–180. Springer, Heidelberg (2007)
28. Shamir, A., Tauman, Y.: Improved online/offline signature schemes. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 355–367. Springer, Heidelberg (2001)
29. Susilo, W., Mu, Y.: Non-Interactive Deniable Ring Authentication. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 386–401. Springer, Heidelberg (2004)
30. Susilo, W., Mu, Y., Zhang, F.: Perfect Concurrent Signature Schemes. In: López, J., Qing, S., Okamoto, E. (eds.) ICICS 2004. LNCS, vol. 3269, pp. 14–26. Springer, Heidelberg (2004)
31. Tsang, P.P., Wei, V.K., Chan, T.K., Au, M.H., Liu, J.K., Wong, D.S.: Separable Linkable Threshold Ring Signatures. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 384–398. Springer, Heidelberg (2004)
32. Wong, D.S., Fung, K., Liu, J.K., Wei, V.K.: On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST. In: Qing, S., Gollmann, D., Zhou, J. (eds.) ICICS 2003. LNCS, vol. 2836, pp. 34–46. Springer, Heidelberg (2003)
33. Zhang, F., Kim, K.: ID-Based Blind Signature and Ring Signature from Pairings. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 533–547. Springer, Heidelberg (2002)