Lightweight Anonymous Authentication for Ad Hoc Group: A Ring Signature Approach

Xu Yang[1,2], Wei Wu[1,2](✉), Joseph K. Liu[3], and Xiaofeng Chen[4]

[1] Fujian Provincial Key Laboratory of Network Security and Cryptology,
School of Mathematics and Computer Science, Fujian Normal University,
Fuzhou 350117, Fujian, China
weiwu@fjnu.edu.cn

[2] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China

[3] Faculty of Information Technology, Monash University, Melbourne, VIC 3800,
Australia
joseph.liu@monash.edu

[4] State Key Laboratory of Integrated Service Networks (ISN),
Xidian University, Xi'an, China
xfchen@xidian.edu.cn

Abstract. Anonymous authentication protocol allows the system to authenticate a user anonymously. That is, the system knows that the requester is eligible to access, yet does not know his/her actual identity. Anonymous authentication is useful in many privacy-preserving applications such as wireless sensor networks and roaming. However, most of the anonymous authentication protocols are not lightweight. They all require a number of exponentiations or pairings which cannot be executed by lightweight devices such as sensors or RFID. In this paper, we propose a lightweight anonymous authentication protocol for *Ad Hoc* group. Our protocol contains only lightweight calculations such as hashing or modulus square but *not* exponentiation or pairing in both prover and verifier sides. The core primitive of our mechanism is a lightweight ring signature scheme. The security of our scheme can be reduced to the classic integer factorization assumption in the random oracle model.

1 Introduction

Privacy is an important factor in many areas. For example, no one wants his/her own daily behaviours, either location information in the physical world or web-browsing history in the cyber world, to be known by others. There exist various kinds of anonymization technologies that can help one become "anonymous" and protect user privacy. However, this will raise another security concern. There are many services that are designated for a particular group of users, for example, those who have paid and subscribed for the service. Being totally anonymous prevents the service provider telling whether a user belongs to the subscribed group or not. Thus we need a kind of *anonymous authentication* mechanism to ensure the authenticity of users while privacy is preserved simultaneously.

M.-H. Au and A. Miyaji (Eds.): ProvSec 2015, LNCS 9451, pp. 215–226, 2015.
DOI: 10.1007/978-3-319-26059-4_12

Ring signature is a good candidate to provide anonymous authentication, especially to ad hoc group. A ring signature scheme (for examples [1–6,8,9,13,16,18,22,24,27–36,38,42–47]) 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, [7,10,12]), the group formation is spontaneous and there is no group manager to 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/her own. These diversion group members can be totally unaware of being conscripted into the group.

Ring signature schemes could be used for whistle blowing [38], anonymous membership authentication for ad hoc groups [9], anonymous data sharing [19], E-voting [14] 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 schemes can be used to derive other primitives as well. It had been utilized to construct non-interactive deniable ring authentication [40], perfect concurrent signature [41] and multi-designated verifiers signature [20].

Nevertheless, existing ring signature schemes need very heavy computations. *All* existing ring signature schemes require exponentiations, at least on the verification stage. (Some may require the execution of pairings, which is even computationally expensive) 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.

1.1 Our Contributions

In this paper, we address the problem specifically. Our solution does not require the signer or the verifier to execute any exponentiation or pairing. Both algorithms are considered heavy and not suitable for lightweight device (e.g. wireless sensor and RFID) to execute. Only hashing, modulus square and addition operations are needed in both stages. For a setting of n users, on average our new scheme requires $n + 4$ hashing, square and addition operations and one square-root operation for the signature generation. The verifier only requires n hashing, square and addition operations.

Note that our scheme is different from another primitive called online/offline ring signature [23]. Online/offline ring signature together with online/offline (identity-based) encryption [15,17,37], signcryption [25] and signature [26] belong to the paradigm of online/offline cryptogrpahy.

In an online/offline ring signature scheme, the signing part is splitted into two parts while some offline computations have to be completed before knowing the message and the set of public keys. While this will speed up the (online) signature generation, the verification cost of online/offline (ring) signature is not reduced. The scheme of [23] requires n exponentiations for verifying a ring signature containing n users. Nonetheless, despite the efficiency differences, both schemes are the same in terms of functionality. Thus we can regard our scheme is a further improvement of online/offline signature scheme in two ways: (1) We do not require any offline stage in the signing part; and (2) The verification is lightweight.

Paper Organisation. The remainder of this paper is organised as follows. Section 2 reviews the mathematical preliminaries and the syntax of ring signature. Our scheme is proposed in Sect. 3. Section 4 analyzes the performance of our scheme. We conclude the paper in Sect. 5.

2 Definitions

This section reviews the complexity assumption and definitions of ring signature.

2.1 Complexity Assumption

The security of our scheme relies on the factorization assumption with safe primes, which is defined as follows:

Definition 1 (Safe Prime). *p is a safe prime if it is of the form $2p'+1$, where p' is also a prime.*

Definition 2 (Factorization Assumption with Safe Prime). *Let $N = pq$ where p and q are k-bit length safe primes. Given N as the input, the goal of an algorithm of $\mathcal{A}$ is to output an unordered pair (p, q). $\mathcal{A}$ has at least an advantage of ϵ if*

$$\Pr[\mathcal{A}(N) = p, q \mid N = pq] \geq \epsilon.$$

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

Definition 3 (Quadratic Residues). *An integer $y \in Z_N^*$ is called a quadratic residue modulo N if there exists an integer $x \in Z_N^*$ such that: $x^2 = y \pmod N$. Let $QR(N)$ denote the set of quadratic residues modulo N.*

2.2 Security Model

Definition 4. *A ring signature scheme consists of three algorithms:*

- $\mathsf{Key\text{-}Gen}(k) \rightarrow (sk, pk)$: $\mathsf{Key\text{-}Gen}$ is a probabilistic algorithm taking as input a security parameter k. It returns the user secret key sk and public key pk.
- $\mathsf{Sign}(L, sk, m) \rightarrow \sigma$: Sign is a probabilistic algorithm taking (L, m, sk) as input, where L is the list of n public keys to be included in the ring signature, sk is the secret key of the actual signer (such that the corresponding public key is included in L) and m is the message to be signed. It returns a signature σ.
- $\mathsf{Verify}(L, m, \sigma) \rightarrow \{\mathsf{Accept}, \mathsf{Reject}\}$. Verify is a deterministic algorithm taking (L, m, σ) as input, where L is the list of n public keys of the ring members and $m, \sigma)$ is the message/ring-signature pair. 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 5 (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 $\mathsf{Key\text{-}Gen}$. A ring signature scheme is said to be unconditionally signer ambiguous if, for any L, any message m, and any signature $\sigma \leftarrow \mathsf{Sign}(L, m, sk_\pi)$ 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 who, out of n possible signers, actually produced the ring signature. Note that we do not allow $\mathcal{A}$ to know the random coins used to generate the signature.

Definition 6 (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 $\mathsf{Key\text{-}Gen}$. 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}), the challenger returns a ring signature $\sigma \leftarrow \mathsf{Sign}(L', m, sk_\pi)$, where $sk_\pi \in L'_{sk}$ and $\mathsf{Verify}(L', m, \sigma) = \mathsf{Accept}$.
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, and
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

This section describes our proposal and its security analysis.

3.1 Construction

The details of our design are given as follows.

Key-Gen: Let κ be security parameters. Each user selects two safe primes p, q of length k-bit, such that $p = 2p' + 1, q = 2q' + 1$ where p', q' are also primes. The private key is (p, q) and public key is $N = pq$.

Sign: Let $L = \{N_1, \ldots, N_n\}$ be a list of n public keys to be included in the ring signature. Let $H_i : \{0,1\}^* \to \mathbb{Z}_{N_i}$ be some hash functions for $i = 1, \ldots, n$. H_i is a random oracle. W.l.o.g., we assume user n is the actual signer and thus the signer knows sk_n but not sk_i where $i = 1, \ldots, n-1$. The actual signer executes the following steps:

1. Randomly generate $r_n \in_R \mathbb{Z}_{N_n}$, compute $c_1 = H_1(L, m, r_n)$.
2. (For $n > 1$ only) For $i = 1, \ldots, n-1$, randomly generate $x_i \in_R Z_{N_i}$ and compute $c_{i+1} = H_{i+1}(L, m, c_i + x_i^2 \mod N_i)$.
3. Compute $t_n = r_n - c_n \mod N_n$. If $t_n \notin QR(N)$, repeat the following steps until $t_n \in QR(N)$.
   - (For $n > 1$) choose another random $x_{n-1} \in_R Z_{N_{n-1}}$ and compute $c_n = H_n(L, m, c_{n-1} + x_{n-1}^2 \mod N_{n-1})$.
   - (For $n = 1$) choose another random $r_1 \in_R \mathbb{Z}_{N_1}$ and compute $c_1 = H_1(L, m, r_1)$.
4. Compute $x_n = {t_n}^{1/2} \mod N_n$ using the knowledge of the factorization of N_n.

Output the signature $\sigma = (x_1, \ldots, x_n, c_1)$.

Verify: To verify a signature $\sigma = (x_1, \ldots, x_n, c_1)$ for message m and public keys $L = \{N_1, \ldots, N_n\}$, computes $r_i = c_i + x_i^2 \mod N_i$ for $i = 1, \ldots, n$ and $c_{i+1} = H_{i+1}(L, m, r_i)$ for $i \neq n$. The Verify algorithm accepts the signature if $c_1 = H_1(L, m, r_n)$. Otherwise, it rejects.

The correctness of our scheme is obvious and thus omitted.

3.2 Security Analysis

We will show that the proposed scheme is unconditionally signer ambiguous and existentially unforgeable.

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

Proof. All x_i except x_n are taken randomly from $\mathbb{Z}_{N_i}$. At the closing point, $x_n \in \mathbb{Z}_{N_n}$ also distributes randomly as r_n is randomly chosen, c_n depends on previous x_{n-1} which is also a random number. Therefore, for fixed (L, m), $(x_1, \ldots, x_n)$ has $\prod_{i=1}^{n} N_i$ variation that are equally likely regardless of the closing point. The remaining c_1 is uniquely determined from L, m and x_i's and thus reveals no information of the actual signer. □

Theorem 2. *Suppose the (ϵ', τ', k)-Factorization assumption holds, then our ring signature scheme with n users is $(\tau, q_s, q_h, \epsilon)$-secure against existential forgery under adaptive chosen message attacks in the random oracle model provided that:*

$$\epsilon' \leq \frac{\left(1 - \frac{q_h q_s}{N_{min}}\right)\left(1 - \frac{1}{N_{min}}\right)\epsilon}{q_h(q_h+1)n}, \qquad \tau' = \tau$$

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

Proof. The proof uses the approach described in [1]. (Readers may refer to [1] for some preliminary understanding.) 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 factorization problem.

Setup: $\mathcal{S}$ receives the problem instance N, which is the product of two safe prime numbers of length k-bit. $\mathcal{S}$ is asked to output a non-trivial factor of N.

$\mathcal{S}$ 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 two integers u, v such that $1 \leq u \leq v \leq q_h$.

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.
- *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 $x_i \in_R \mathbb{Z}_{N_i}$, compute $r_i = x_i^2 + c_i \mod N_i$, 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 $c_\kappa = r_\kappa - R \mod N_\kappa$ (where $R = r^2 \mod N_\kappa$ and $r \in_R N_\kappa$ is chosen by $\mathcal{S}$) as the value of $H_\kappa(L, m, r_{\kappa-1})$. If $\mathcal{A}$ is successful in forgery, it outputs x_κ that satisfies $r_\kappa = c_\kappa + x_\kappa^2 \mod N_\kappa$. Since $r_\kappa = c_\kappa + R \mod N_\kappa$, we obtain x_κ as the square root of R with regard to N_κ. That is, $x_\kappa^2 = R \mod N_\kappa$ or $x_\kappa^2 = r^2 \mod N_\kappa$. With half probability, $x_\kappa \neq r$. That is, $x_\kappa - r$ and $x_\kappa + r$ are two non-trivial factors of N_κ.

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.

Suppose $\mathcal{A}$ outputs a valid forged signature with probability at least 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 hash function.

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. $\mathcal{B}$ 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 $1/n$. Finally, with probability $1/2$, $x \neq r$ for the square root of R.

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

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

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. This contradicts the assumption that the (ϵ', τ', k)-Factorization assumption holds where

$$\epsilon' \leq \frac{\left(1 - \frac{q_h q_s}{N_{min}}\right)\left(1 - \frac{1}{N_{min}}\right)\epsilon}{q_h(q_h + 1)n}, \qquad \tau' = \tau$$

This completes our proof. □

4 Efficiency Analysis

4.1 Comparison 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 exponentiations (EXP) and pairings (PAIR) (the other operation such as hashing or multiplication is relatively small when compared to exponentiation and pairing)[1]. The running time of a pairing operation is about 2 to 3 times of an exponentiation. Let n be the size of the ring. We split the analysis into signing and verification. Note that no scheme in the comparison requires any pairing opeartions in the signing stage.

Table 1. Time complexities of existing ring signatures.

Scheme	# of EXP (sign)	# of EXP (verify)	# of PAIR (verify)
Rivest-Shamir-Tauman [38]	n	n	0
Abe-Ohkubo-Suzuki [1]	n	n	0
Dodis-Kiayias-Nicolosi-Shoup [18]	14	14	0
Chow-Wei-Liu-Yuen [13]	n	n	0
Shacham-Waters [39]	$4n + 3$	0	$2n + 3$
Chandran-Groth-Sahai [11]	$5 + 6\sqrt{n} + \frac{n+1}{3}$	3	$6 + 6\sqrt{n}$
Liu-Au-Susilo-Zhou [23]	2	n	0
Our Scheme	0	0	0

4.2 Running Time

We also implement our scheme to analyze the running time. Details are as follows:

- Equipment: Thinkpad x201s, Intel(R) Core™ I7 processor I7-640LM (2.13 GHz) with dual-core, 2.8 GB RAM running on 32 bits ubuntu 12.04
- Key length: 1024 bits

[1] Note that our scheme requires $n - 1$ square operations and 1 square root operation in the signing stage and n square operations in the verification stage. But since the running time of square and square root is far less than EXP and PAIR, we do not include these two operations in the comparison table.

- Number of running times: average by 80,000,000 times
- Library used: openSSL linux
- Running time: It takes 0.000568101266 ms for an additional operation over modulus (1024 bits), 0.003478101266 ms for a square operation over modulus (1024 bits), 12.877974683544 ms for an exponentiation operation over modulus (1024 bits). Suppose there are n users included in the signature. Our scheme takes around ($0.0040462 \times n$) ms for signing and verification.

5 Conclusion

In this paper, we have proposed a lightweight anonymous authentication protocol, the essential of which is actually a lightweight ring signature scheme. It is lightweight in the sense that it does not contain any exponentiation or pairing in both prover and verifier sides. Instead, it only requires a few hashing and modulus square operations. We believe it is particular suitable for lightweight devices such as sensors and RFID and those applications that require authentication and privacy simultaneously. In the future, we may incorporate the technique from lattices [21] to further improve the efficiency while keeping all desired features.

Acknowledgement. The authors would like to thank anonymous reviewers for their helpful comments. This work is supported by National Natural Science Foundation of China (61472083, U1405255, 61402110), Fok Ying Tung Education Foundation (141065), Fujian Normal University Innovative Research Team (IRTL1207), the State Key Laboratory of Cryptology Research Fund (China), China 111 Project (No. B08038), Doctoral Fund of Ministry of Education of China (No. 20130203110004), Program for New Century Excellent Talents in University (No. NCET-13-0946), the Fundamental Research Funds for the Central Universities (Nos. BDY151402 and JB142001-14)

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., Susilo, W., Yuen, T.H.: Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. Theor. Comput. Sci. **469**, 1–14 (2013)
5. Au, M.H., Liu, J.K., Susilo, W., Zhou, J.: Realizing fully secure unrestricted id-based ring signature in the standard model based on HIBE. IEEE Trans. Inf. Forensics Secur. **8**(12), 1909–1922 (2013)

6. 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. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 1–16. Springer, Heidelberg (2006)
7. 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)
8. 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)
9. 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)
10. Camenisch, J.L., Stadler, M.A.: Efficient group signature schemes for large groups. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997)
11. 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)
12. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
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 (2006)
14. Chow, S.S.M., Liu, J.K., Wong, D.S.: Robust receipt-free election system with ballot secrecy and verifiability. In: Proceedings of the Network and Distributed System Security Symposium, NDSS 2008, San Diego, California, USA, 10th February - 13th February 2008. The Internet Society (2008)
15. Chow, S.S.M., Liu, J.K., Zhou, J.: Identity-based online/offline key encapsulation and encryption. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, pp. 52–60. Hong Kong, China, 22–24 March 2011
16. 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)
17. Chu, C., Liu, J.K., Zhou, J., Bao, F., Deng, R.H.: Practical id-based encryption for wireless sensor network. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010, Beijing, China, April 13–16, 2010, pp. 337–340. ACM (2010)
18. 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)
19. Huang, X., Liu, J.K., Tang, S., Xiang, Y., Liang, K., Xu, L., Zhou, J.: Cost-effective authentic and anonymous data sharing with forward security. IEEE Trans. Comput. **64**(4), 971–983 (2015)
20. 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)
21. Ling, S., Nguyen, K., Wang, H.: Group signatures from lattices: simpler, tighter, shorter, ring-based. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 427–449. Springer, Heidelberg (2015)

22. 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)
23. Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Online/offline ring signature scheme. In: Qing, S., Mitchell, C.J., Wang, G. (eds.) ICICS 2009. LNCS, vol. 5927, pp. 80–90. Springer, Heidelberg (2009)
24. Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Linkable ring signature with unconditional anonymity. IEEE Trans. Knowl. Data Eng. **26**(1), 157–165 (2014)
25. Liu, J.K., Baek, J., Zhou, J.: Online/offline identity-based signcryption revisited. In: Lai, X., Yung, M., Lin, D. (eds.) Inscrypt 2010. LNCS, vol. 6584, pp. 36–51. Springer, Heidelberg (2011)
26. Liu, J.K., Baek, J., Zhou, J., Yang, Y., Wong, J.W.: Efficient online/offline identity-based signature for wireless sensor network. Int. J. Inf. Sec. **9**(4), 287–296 (2010)
27. Liu, J.K., Susilo, W., Wong, D.S.: Ring signature with designated linkability. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 104–119. Springer, Heidelberg (2006)
28. Liu, J.K., Tsang, P.P., Wong, D.S.: Efficient verifiable ring encryption for Ad Hoc groups. In: Molva, R., Tsudik, G., Westhoff, D. (eds.) ESAS 2005. LNCS, vol. 3813, pp. 1–13. Springer, Heidelberg (2005)
29. 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. Springer, Heidelberg (2004)
30. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for Ad Hoc groups. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 325–335. Springer, Heidelberg (2004)
31. Liu, J.K., Wong, D.S.: On the security models of (threshold) ring signature schemes. In: Park, C., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 204–217. Springer, Heidelberg (2005)
32. Liu, J.K., Wong, D.S.: Linkable ring signatures: security models and new schemes. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3481, pp. 614–623. Springer, Heidelberg (2005)
33. 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)
34. Liu, J.K., Wong, D.S.: A more efficient instantiation of witness-indistinguishable signature. I. J. Network Secur. **5**(2), 199–204 (2007)
35. Liu, J.K., Wong, D.S.: Solutions to key exposure problem in ring signature. I. J. Network Secur. **6**(2), 170–180 (2008)
36. Liu, J.K., Yuen, T.H., Zhou, J.: Forward secure ring signature without random oracles. In: Qing, S., Susilo, W., Wang, G., Liu, D. (eds.) ICICS 2011. LNCS, vol. 7043, pp. 1–14. Springer, Heidelberg (2011)
37. Liu, J.K., Zhou, J.: An efficient identity-based online/offline encryption scheme. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 156–167. Springer, Heidelberg (2009)
38. 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)
39. 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)
40. Susilo, W., Mu, Y.: Non-interactive deniable ring authentication. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971. Springer, Heidelberg (2004)

41. 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)
42. Tsang, P.P., Au, M.H., Liu, J.K., Susilo, W., Wong, D.S.: A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity (extended abstract). In: Heng, S.-H., Kurosawa, K. (eds.) ProvSec 2010. LNCS, vol. 6402, pp. 166–183. Springer, Heidelberg (2010)
43. 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)
44. 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)
45. Yuen, T.H., Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Threshold ring signature without random oracles. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, Hong Kong, China, March 22–24, 2011, pp. 261–267. ACM (2011)
46. Yuen, T.H., Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Efficient linkable and/or threshold ring signature without random oracles. Comput. J. **56**(4), 407–421 (2013)
47. 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)