Identity Based Threshold Ring Signature

Sherman S.M. Chow*, Lucas C.K. Hui, and S.M. Yiu

Department of Computer Science
The University of Hong Kong
Pokfulam, Hong Kong
`{smchow, hui, smyiu}@cs.hku.hk`

Abstract. In threshold ring signature schemes, any group of t entities spontaneously conscripting arbitrarily $n-t$ entities to generate a publicly verifiable t-out-of-n signature on behalf of the whole group, yet the actual signers remain anonymous. The spontaneity of these schemes is desirable for ad-hoc groups such as mobile ad-hoc networks [7]. In this paper, we present an identity based (ID-based) threshold ring signature scheme. The scheme is provably secure in the random oracle model [4] and provides trusted authority compatibility [25]. To the best of authors' knowledge, our scheme is the first ID-based threshold ring signature scheme and the most efficient (in terms of number of pairing operations required) ID-based ring signature scheme (when $t = 1$).

Key words: Threshold ring signature, identity-based signature, bilinear pairings, anonymity

1 Introduction

1.1 Background

Anonymity is becoming a major concern in many multi-user electronic commerce applications such as e-lotteries, e-cash and online games. Group-oriented signature schemes [9] enable an entity of a group to produce a signature on behalf of the group. There are two major paradigms in anonymous group-oriented signature schemes: group signature and ring signature. In a group signature scheme, the group is predefined and there is a group manager that can revoke this anonymity. Ring signature scheme provides a similar feature. It does not support anonymity revocation mechanism, but no setup stage is needed to produce and distribute a group secret explicitly. Hence it enables any individual spontaneously conscripting arbitrarily $n - 1$ entities to generate a publicly verifiable 1-out-of-n signature on behalf of the whole group, yet the actual signer

---

* corresponding author

remains unconditionally anonymous. Threshold ring signature is the t-out-of-n threshold version where t or more entities can jointly generate a valid signature but $t-1$ or fewer entities cannot. These schemes are getting more and more popular due to the increasing prevalence of pervasive computing applications and mobile ad-hoc networks, where ad-hoc groups are very common [7].

1.2 Motivation of ID-based Threshold Ring Signature

In traditional public key infrastructure (PKI), a user must pre-enroll the PKI or he/she cannot enjoy the cryptographic services provided by the PKI, e.g. no one can send them any encrypted message. Identity-based (ID-based) cryptography [5, 21] solves this problem: all users already have their corresponding public key before their enrollment since the public key can be derived via a public algorithm with input of a string that can uniquely identify each of them, such as an email address.

All previous threshold ring signature constructions are non ID-based, hence *real spontaneity* is not always possible: the public key of each member of the group is required to be published by the underlying PKI before it can be used to generate the signature. Removing this prerequisite requirement motivates the construction of ID-based threshold ring signature scheme, which provide a better alternative than non-ID based solutions[1].

1.3 Related Work

Ring signature scheme was first formalized by Rivest *et. al.* in [19]. After that, several other ring signature schemes [1, 29] were proposed. Bresson *et. al.* extended [19] into a threshold ring signature using the concept of partitioning [7]. Later, Wong *et. al.* proposed another threshold ring signature using tandem construction method [24].

Recently there are some threshold ring signature schemes with special properties, Liu *et. al.* introduced separability to a threshold ring signature [17], which enables the use of various flavours of public keys in a single threshold ring signature; while Chan *et. al.* constructed CDS-type [12] t-out-of-n blind threshold ring signature [8].

In [17], a generic construction of threshold ring signature from any trapdoor-one-way type signature scheme and three-move type signature

---

[1] Under the assumption that the trusted authority (the Private Key Generator) will not reveal any information about who has requested for his/her private key and who has not.

scheme is given. Yet, the authors have not illustrated the correctness and security of this construction except the specific instantiations from RSA [18] and Schnorr signature [20].

Using bilinear pairing to construct ring signature is not a new idea. [6] proposed a ring signature and [27] proposed a proxy ring signature from bilinear pairing. In [28], a ring signature is derived from the short signature proposed. ID-based ring signature was introduced in [26] and a more efficient version was proposed in [16]. Small inconsistency in [26] and [16] were fixed by [2], together with a new proxy ring signature scheme. Another ring signature with formally proven security was proposed in [14]. In [23], a bilinear threshold ring signature was proposed; but the scheme is not ID-based and has not addressed the TA (trusted authority) compatibility issue [25] in which not all the users join the same TA.

1.4 Our Contributions

In this paper, we present an ID-based threshold ring signature scheme. The scheme is provably secure in the random oracle model [4] and provides TA compatibility [25]. To the best of authors' knowledge, our scheme is the first ID-based threshold ring signature scheme. Pairing operation is usually the most computational intensive operation in pairing-based cryptography. Our scheme is also the most efficient (in terms of number of pairing operations required) ID-based ring signature scheme (when $t = 1$).

1.5 Organization

The rest of the paper is organized as follows. The next section contains some preliminaries about the formal definitions of an ID-based threshold ring signature scheme, bilinear pairing as well as the Gap Diffie-Hellman group. Formal security definitions describing the adversary's capabilities and goal are presented in Section 3. In Section 4, we describe the proposed ID-based threshold ring signature scheme. The security and efficiency analysis of our scheme are given in Section 5. Finally, Section 6 concludes the paper.

2 Preliminaries

2.1 Framework of ID-Based Threshold Ring Signature

An ID-based threshold ring signature scheme consists of four algorithms: `Setup`, `KeyGen`, `Sign`, and `Verify`.

- `Setup`: On an unary string input 1^k where k is a security parameter, it produces the common public parameters *params*, which include a description of a finite signature space and a description of a finite message space.
- `KeyGen`: On an input of signer's identity $ID \in \{0,1\}^*$, it outputs the signer's secret signing key S_{ID}. (The corresponding public verification key Q_{ID} can be computed easily by everyone.)
- `Sign`: On input of a message m, a group of n users' identities $\{ID_j\}$, where $1 \leq j \leq n$, and the secret keys of t members $\{S_{ID_{i_j}}\}$, where $1 \leq i_j \leq n$, $1 \leq j \leq t$ and $t \leq n$; it outputs a (t,n) ID-based threshold ring signature σ on the message m.
- `Verify`: On a threshold ring signature σ, a message m, the threshold t and the group of signers' identities $\{ID_j\}$ as the input, it outputs $\top$ for "true" or $\perp$ for "false", depending on whether σ is a valid signature signed by at least t members in the group $\{ID_j\}$ on a message m.

These algorithms must satisfy the standard consistency constraint of ID-based threshold ring signature scheme, i.e. if $\sigma = \texttt{Sign}(m, \{ID_j\}, \{S_{ID_{i_j}}\})$, we must have $\texttt{Verify}(\sigma, \{ID_j\}, m, t) = \top$. Security requirements will be described in Section 3.

2.2 Bilinear Pairing and Gap Diffie-Hellman Groups

Bilinear pairing is an important cryptographic primitive (for examples, [6, 11, 14, 16, 23, 26–28]). Here, we describe some of its key properties.

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \cdot)$ be two cyclic groups of prime order q. The bilinear pairing is given as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, which satisfies the following properties:

1. *Bilinearity*: For all $P, Q, R \in \mathbb{G}_1$, $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$.
2. *Non-degeneracy*: There exists $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ $\forall P, Q \in \mathbb{G}_1$.

Definition 1. *Given a generator P of a group $\mathbb{G}$ and a 3-tuple (aP, bP, cP), the Decisional Diffie-Hellman problem (DDH problem) is to decide whether $c = ab$.*

Definition 2. *Given a generator P of a group $\mathbb{G}$, (P, aP, bP, cP) is defined as a valid Diffie-Hellman tuple if $c = ab$.*

Definition 3. *Given a generator P of a group $\mathbb{G}$ and a 2-tuple (aP, bP), the Computational Diffie-Hellman problem (CDH problem) is to compute abP.*

Definition 4. *If $\mathbb{G}$ is a group such that DDH problem can be solved in polynomial time but no probabilistic algorithm can solve CDH problem with non-negligible advantage within polynomial time, then we call $\mathbb{G}$ a Gap Diffie-Hellman (GDH) group.*

We assume the existence of a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ that one can solve Decisional Diffie-Hellman Problem in polynomial time.

3 Formal Security Model

Let $\mathbb{G}_1$ be a GDH group, $H(\cdot)$ and $H_0(\cdot)$ are two cryptographic hash functions where $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

3.1 Unforgeability of ID-Based Threshold Ring Signature

The following EUF-IDTR-CMIA2 game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ formally defines the *existential unforgeability of ID-based threshold ring signature under adaptive chosen-message-and-identity attack*.

EUF-IDTR-CMIA2 Game:

Setup: The challenger $\mathcal{C}$ takes a security parameter k and runs the `Setup` to generate common public parameters *params* and also the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries). The types of queries allowed are described below.

- Hash functions queries: $\mathcal{A}$ can ask for the values of the hash functions (e.g. $H(\cdot)$ and $H_0(\cdot)$ in our proposed scheme) for any input.
- `KeyGen`: $\mathcal{A}$ chooses an identity ID. $\mathcal{C}$ computes $\texttt{Extract}(ID) = S_{ID}$ and sends the result to $\mathcal{A}$.
- `Sign`: $\mathcal{A}$ chooses a group of n users' identities $\{ID_j\}$, any t' signers indexed by $\{i_j\}$, where $1 \leq i_j \leq n$, $1 \leq j \leq t'$ and $t' \leq n$ and any message m. On input of $(m, \{ID_j\}, \{S_{ID_{i_j}}\})$, $\mathcal{C}$ outputs a (t', n) ID-based threshold ring signature σ.

Forgery: The adversary $\mathcal{A}$ outputs (t', n) ID-based threshold ring signature σ, $\{ID_j\}$, a group of n users' identities $\{ID_j\}$, and any t' signers indexed by $i_1, \cdots, i_{t'}$, where $1 \leq i_j \leq n$, $1 \leq j \leq t'$ and $t' \leq n$. The only restriction is that $(m, \{ID_j\}, \{S_{ID_{i_j}}\})$ does not appear in the set of previous `Sign` queries and there is at least one secret key in $\{S_{ID_{i_j}}\}$ that is never returned by any `KeyGen` query. i.e. less than t' private keys of $\{S_{ID_{i_j}}\})$ are known. It wins the game if the `Verify`$(\sigma, \{ID_j\}, m, , t)$ is equal to $\top$. The advantage of $\mathcal{A}$ is defined as the probability that it wins.

Definition 5. *An ID-based threshold ring signature scheme is said to have the existential unforgeability against adaptive chosen-message-and-identity attacks property (EUF-IDTR-CMIA2 secure) if no adversary has a non-negligible advantage in the EUF-IDTR-CMIA2 game.*

3.2 Signer Ambiguity of ID-Based Threshold Ring Signature

Definition 6. *An ID-based threshold ring signature scheme is said to have the unconditional signer ambiguity if for any group of n users' identities $\{ID_j\}$, any t' signers indexed by $\{i_j\}$, where $1 \leq i_j \leq n$, $1 \leq j \leq t'$ and $t' \leq n$, any message m and any signature σ, where $\sigma = \mathtt{Sign}(m, \{ID_j\}, \{S_{ID_{i_j}}\})$, any verifier $\mathcal{A}$ (i.e. not the signer in the group $\{ID_{i_j}\}$, even with unbounded computing resources, cannot identify any of the signer with probability better than a random guess. That is, $\mathcal{A}$ can only output any member of $\{i_j\}$ with probability no better than $\frac{t'}{n}$.*

4 Our Proposed Scheme

In this section, we show how to adopt the techniques introduced in [17] with the elegancy of bilinear mapping to spawn an efficient ID-based threshold ring signature scheme with reasonable signature size.

4.1 Basic Construction

Define $\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot)$ as in the previous section where $\mathbb{G}_1$ is a GDH group. $H(\cdot)$ and $H_0(\cdot)$ are two cryptographic hash functions where $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

`Setup`: TA randomly chooses $s \in_R \mathbb{Z}_q^*$, keeps it as the master secret key and computes the corresponding public key $P_{pub} = sP$. The system parameters are:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}(\cdot,\cdot), q, P, P_{pub}, H(\cdot), H_0(\cdot)\}.$$

`KeyGen`: The signer with identity $ID \in \{0,1\}^*$ submits ID to TA. TA sets the signer's public key Q_{ID} to be $H(ID) \in \mathbb{G}_1$, computes the signer's private signing key S_{ID} by $S_{ID} = sQ_{ID}$. Then TA sends the private signing key to the signer.

`Sign`: Let L be the set of all identities of the n users, the t participating signers carry out the following steps.

1. An arbitrary entity in the group of t participating signers "prepares the signature on behalf of" other entities in the group by performing the following computations: For $i = t+1, \cdots, n$, choose x_i and $h_i \in_R \mathbb{Z}_q^*$ and compute $U_i = x_i P - h_i P_{pub}$ and $V_i = x_i Q_{ID_i}$.
2. For $j = 1, \cdots, t$, choose $r_j \in_R \mathbb{Z}_q^*$ and compute $U_j = r_j P$.
3. Compute $h_0 = H_0(L, t, m, \cup_{k=1}^{n}\{U_k\})$ and construct a polynomial f of degree $n-t$ over $\mathbb{Z}_q$ such that $f(0) = h_0$ and $f(i) = h_i$ for $t+1 \leq i \leq n$.
4. For $j = 1, \cdots, t$, compute $h_j = f(j)$ and $V_j = r_j Q_{ID_j} + h_j S_{ID_j}$.
5. Compute $V = \sum_{k=1}^{n} V_k$.
6. Output the signature for m and L as $\sigma = \{\cup_{k=1}^{n}\{U_k\}, V, f\}$.
   (Note that the polynomial f only contain information for the hash values used and its inclusion will not compromise the unforgeability and the anonymity of the scheme.)

`Verify`: A verifier checks a signature $\sigma = \{\cup_{k=1}^{n}\{U_k\}, V, f\}$ for the message m and a set of identities L as follows.

1. Check if the degree of polynomial f is $n-t$ and $H_0(L, t, m, \cup_{k=1}^{n}\{U_k\})$ is the constant term of f. Proceed if both conditions are true, reject otherwise.
2. For $k = 1, \cdots, n$, compute $h_k = f(k)$.
3. Check whether $\prod_{k=1}^{n} \hat{e}(Q_{ID_k}, U_k + h_k P_{pub}) = \hat{e}(P, V)$. If the equality holds, return $\top$. Otherwise, return $\perp$.

4.2 Trusted Authority Compatibility

In the reality, it is quite often that different user joined different trusted authorities (TAs). In [25], the notion of TA compatibility is introduced in the ID-based signcryption [11, 25] scenario. We extend their notion into TA compatibility in ID-based threshold ring signature. In ID-based threshold ring signature, spontaneity will be affected if the intended group of signers joined different TAs. However, our scheme can be easily extended to handle this situation without compromising the spontaneity. We just need to change the equality to be checked in the verification algorithm to $\prod_{k=1}^{n} \hat{e}(Q_{ID_k}, U_k + h_k P_{pub_k}) = \hat{e}(P, V)$, where P_{pub_k} is the public key of the TA of the k-th user.

4.3 Robustness

Robustness is often desirable in group-oriented signature scheme. For a threshold ring signature scheme that does not support robustness, the misbehavior of any participating signer cannot be detected, and the final signature generated by the group of signers will be invalid even there is only one misbehaving signer. In our scheme, the partial signature $\sigma_j = \{h_j, U_j, V_j\}$ generated by the signer ID_j can be verified easily by checking whether $\hat{e}(Q_{ID_j}, U_j + h_j P_{pub}) = \hat{e}(P, V_j)$ holds.

5 Analysis of the Proposed Scheme

5.1 Consistency

The consistency of our basic construction can be easily verified by the following equations.

$$\begin{aligned}
\hat{e}(P, V) &= \hat{e}(P, \sum_{k=1}^{n} V_k) \\
&= \prod_{i=1}^{t} \hat{e}(P, V_i) \prod_{j=t+1}^{n} \hat{e}(P, V_j) \\
&= \prod_{j=1}^{t} \hat{e}(P, r_j Q_{ID_j} + h_j S_{ID_j}) \prod_{i=t+1}^{n} \hat{e}(P, x_i Q_{ID_i}) \\
&= \prod_{j=1}^{t} \hat{e}(P, (r_j + h_j s) Q_{ID_j}) \prod_{i=t+1}^{n} \hat{e}(x_i P, Q_{ID_i}) \\
&= \prod_{j=1}^{t} \hat{e}(Q_{ID_j}, (r_j + h_j s) P) \prod_{i=t+1}^{n} \hat{e}(Q_{ID_i}, x_i P - h_i P_{pub} + h_i P_{pub}) \\
&= \prod_{j=1}^{t} \hat{e}(Q_{ID_j}, U_j + h_j P_{pub}) \prod_{i=t+1}^{n} \hat{e}(Q_{ID_i}, U_i + h_i P_{pub}) \\
&= \prod_{k=1}^{n} \hat{e}(Q_{ID_k}, U_k + h_k P_{pub})
\end{aligned}$$

The consistency of the checking for the sake of robustness and that of our extended scheme with TA compatibility can be verified easily in a similar manner.

5.2 Efficiency Analysis

Although some research has been done in analyzing the complexity and speeding up the computation of pairing function (for examples, [3], [10], [13] and [15]), pairing operations are still rather expensive. Our scheme is the most efficient (in terms of number of pairing operations required) ID-based ring signature scheme (when $t = 1$). Taken into account the computational costs for signature generation and verification, [26] uses $4n - 1$ pairing operations while both of [2] and [16] use $2n + 1$ of them. While the most efficient scheme before the birth of our scheme is [14], which uses $n + 3$ pairings in total (i.e. signing and verification), our scheme only uses $n + 1$ pairing operations. Although the difference is not great, our scheme can be further optimized while [14] cannot, since the multiplication of a series of pairings in `Verify` can be optimized by using the concept of "Miller lite" of Tate pairing presented in [22].

Compared with the previous threshold ring signature from bilinear pairings [23], which is not ID-based and provides no TA compatibility, our scheme achieved the same efficiency in terms of the number of pairing operations required.

Considering the signature size, our scheme is also up to the state-of-the-art. Signature sizes in [7] and [24] are $O(n \lg n)$ and $O(n^t)$, respectively. We share the same order of space complexities as in [17] and [23]. However, due to the elegancy of elliptic curve, our scheme should achieve shorter signature size than [17].

5.3 Existential Unforgeability and Signer Ambiguity

Theorem 1 *In the random oracle model (the hash functions are modeled as random oracles), if there is an algorithm $\mathcal{A}$ that can win the EUF-IDTR-CMIA2 game in polynomial time, then CDHP can be solved with non-negligible probability in polynomial time.*

Proof. See the appendix. □

Theorem 2 *Our ID-based threshold ring signature scheme satisfies the unconditional signer ambiguity property.*

Proof. See the appendix. □

6 Conclusion

In this paper, we present an ID-based threshold ring signature scheme. We prove the security of our scheme in the random oracle model [4]. Moreover, our scheme provides trusted authority compatibility [25]. To the best of authors' knowledge, our scheme is the first ID-based threshold ring signature scheme and the most efficient ID-based ring signature scheme (when $t = 1$) in terms of the number of pairing operations. Due to the elegancy of bilinear pairing, signatures generated by our scheme are much shorter and simpler than signatures from other previous threshold ring signature schemes. Future research directions include making a constant-size ID-based threshold ring signature scheme.

References

1. Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n Signatures from a Variety of Keys. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2002.
2. Amit K Awasthi and Sunder Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2004/184, 2004. Available at http://eprint.iacr.org.
3. Paulo S.L.M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. Efficient Algorithms for Pairing-Based Cryptosystems. In Moti Yung, editor, *Advances in Cryptology: Proceedings of CRYPTO 2002 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–368. Springer-Verlag Heidelberg, 2002.
4. Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *The First ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
5. Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag Heidelberg, 2001.
6. Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.
7. Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold Ring Signatures and Applications to Ad-hoc Groups. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 465–480. Springer, 2002.
8. Tony K. Chan, Karyin Fung, Joseph K. Liu, and Victor K. Wei. Blind Spontaneous Anonymous Group Signatures for Ad Hoc Groups. In *1st European Workshop*

on Security in Ad-Hoc and Sensor Networks (ESAS 2004), Heidelberg, Germany, August 5-6, 2004, Lecture Notes in Computer Science. Springer, 2004. To Appear.

9. David Chaum and Eugène van Heyst. Group Signatures. In Donald W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, 1991.
10. YoungJu Choie and Eunjeong Lee. Implementation of Tate Pairing of Hyperelliptic Curves of Genus 2. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 97–111. Springer, 2003.
11. Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 352–369. Springer, 2003.
12. Ronald Cramer, Ivan Damgard, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer, 1994.
13. Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the Tate Pairing. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer, 2002.
14. Javier Herranz and Germán Sáez. A Provably Secure ID-based Ring Signature Scheme. Cryptology ePrint Archive, Report 2003/261, 2003. Available at http://eprint.iacr.org.
15. Tetsuya Izu and Tsuyoshi Takagi. Efficient Computations of the Tate Pairing for the Large MOV Degrees. In Pil Joong Lee and Chae Hoon Lim, editors, *Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 283–297. Springer-Verlag Heidelberg, 2003.
16. Chih-Yin Lin and Tzong-Chen Wu. An Identity-based Ring Signature Scheme from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/117, 2003. Available at http://eprint.iacr.org.
17. Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. A Separable Threshold Ring Signature Scheme. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 352–369. Springer, 2003.
18. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 26(1):96–99, January 1983.
19. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International*

Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

20. Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology: The Journal of the International Association for Cryptologic Research*, 4(3):161–174, 1991.
21. Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO 1984, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 19–22 August 1985.
22. Jerome A. Solinas. ID-based digital signature algorithms. Slide Show presented at 7th Workshop on Elliptic Curve Cryptography (ECC 2003), August 2003.
23. Victor K. Wei. A Bilinear Spontaneous Anonymous Threshold Signature for Ad Hoc Groups. Cryptology ePrint Archive, Report 2004/039, 2004. Available at http://eprint.iacr.org.
24. Duncan S. Wong, Karyin Fung, Joseph K. Liu, and Victor K. Wei. On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST. In Sihan Qing, Dieter Gollmann, and Jianying Zhou, editors, *Information and Communications Security, 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13, 2003, Proceedings*, volume 2836 of *Lecture Notes in Computer Science*, pages 34–46. Springer, 2003.
25. Tsz Hon Yuen and Victor K. Wei. Fast and Proven Secure Blind Identity-Based Signcryption from Pairings. In *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005 (CTRSA05)*, Lecture Notes in Computer Science, San Francisco, CA, USA, February 2005. Springer. To Appear. Also available at Cryptology ePrint Archive, Report 2004/121.
26. Fangguo Zhang and Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer, 2002.
27. Fangguo Zhang, Reihaneh Safavi-Naini, and Chih-Yin Lin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/104, 2003. Available at http://eprint.iacr.org.
28. Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Applications. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.
29. Chong zhi Gao, Zheng an Yao, and Lei Li. A Ring Signature Scheme Based on the Nyberg-Rueppel Signature Scheme. In Jianying Zhou, Moti Yung, and Yongfei Han, editors, *Applied Cryptography and Network Security, First International Conference, ACNS 2003, Kunming, China, October 16-19, 2003 Proceedings*, volume 2846 of *Lecture Notes in Computer Science*, pages 169–175. Springer, 2003.

Appendix

Proof of Theorem 1
Suppose the challenger $\mathcal{C}$ receives a random instance (P, aP, bP) of the CDHP and has to compute the value of abP. $\mathcal{C}$ will run $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the EUF-IDTR-CMIA2 game. During the game, $\mathcal{A}$ will consult $\mathcal{C}$ for answers to the random oracles H and H_0. Roughly speaking, these answers are randomly generated, but to maintain the consistency and to avoid collision, $\mathcal{C}$ keeps three lists to store the answers used. We assume $\mathcal{A}$ will ask for $H(ID)$ before ID is used in any other queries.

$\mathcal{C}$ gives $\mathcal{A}$ the system parameters with $P_{pub} = bP$. Note that b is unknown to $\mathcal{C}$. This value simulates the master key value for the TA in the game.

H requests: When $\mathcal{A}$ asks queries on the hash values of identities, $\mathcal{C}$ checks the list L_1, If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a value d_i from $\mathbb{Z}_q^*$ will be randomly generated and d_iP will be used as the answer, the query and the answer will then be stored in the list. Note that the associated private key is d_ibP which $\mathcal{C}$ knows how to compute.

The only exception is that $\mathcal{C}$ has to randomly choose one of the H queries from $\mathcal{A}$, say the i-th query, and answers $H(ID_i) = aP$ for this query. Since aP is a value in a random instance of the CDHP, it does not affect the randomness of the hash function H. Since both a and b are unknown to $\mathcal{C}$, a `KeyGen` request on this identity will make $\mathcal{C}$ fails.

H_0 requests: When $\mathcal{A}$ asks queries on these hash values, $\mathcal{C}$ checks the corresponding list L_2. If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a randomly generated value will be used as an answer to $\mathcal{A}$, the query and the answer will then be stored in the list.

`Sign` requests: $\mathcal{A}$ chooses a group of n users' identities $L = \{ID_j\}$, any t' signers indexed by $\{i_j\}$, where $1 \leq i_j \leq n$, $1 \leq j \leq t'$ and $t' \leq n$ and any message m. On input of $(L, \{i_j\}, m)$, $\mathcal{C}$ outputs a (t', n) ID-based threshold ring signature σ as follows.

1. For $i = 0, t', t'+1, \cdots, n$, randomly choose $h_i \in_R \mathbb{Z}_q^*$.
2. Construct a polynomial f over $\mathbb{Z}_q$ such that the degree of f is $n - t'$ and $f(i) = h_i$ for $i = 0, t', t'+1, \cdots, n$.
3. For $j = 1, \cdots, t$, compute $h_j = f(j)$.
4. For $k = 1, \cdots, n$, randomly choose h_k and compute $U_k = x_kP - h_kP_{pub}$
5. Compute $V = \sum_{k=1}^{n} x_kQ_{ID_k}$.

6. Randomly generate a value h_0 from $\mathbb{Z}_q$, assign h_0 as the value of $H_0(L, t, m, \cup_{k=1}^{n}\{U_k\})$, if collision occurs, generate another h_0 and repeat.
7. Output the signature for m and L as $\sigma = \{\cup_{k=1}^{n}\{U_k\}, V, f\}$.

Finally, $\mathcal{A}$ outputs a forged signature $\sigma = \{U, V, f\}$ that is pretended to be signed by some t' members in the group $\{ID_j\}$, $Q_{ID_i} = H(ID_i) = aP \in \{ID_j\}$ and $\mathcal{A}$ only requested for the private key of some $t' - 1$ members in the group. It follows from the forking lemma that if $\mathcal{A}$ is a sufficiently efficient forger in the above interaction, then we can construct a Las Vegas machine $\mathcal{A}'$ that outputs two signed messages (U, V, f) and (U, V', f'). To do so we keep all the random tapes in two invocations of $\mathcal{A}$ the same except h_0 returned by H_0 query of the forged message.

Now we consider the probability that Q_{ID_i} is the chosen target of forgery. Let π be the index of $Q_{ID_i} = aP$ in L, to solve for CDHP, we need $f(\pi) \neq f'(\pi)$. Since $f(0) \neq f'(0)$ and the degrees of f and f' are both $n - t'$, there is at least one value $1 \leq j \leq n$ such that $f'(j) \neq f(j)$, and the probability having $j = \pi$ is at least $\frac{1}{n}$

Given the machine $\mathcal{A}'$ derived from $\mathcal{A}$, we can solve the CDHP by computing $abP = (h_\pi - h'_\pi)^{-1}(V - V')$.

We calculate the probability of success of $\mathcal{C}$ as follows. For $\mathcal{C}$ to succeed, $\mathcal{A}$ did not ask a `KeyGen` query on ID_i. And the corresponding probability is at least $\frac{1}{q_H}$, as there are at most q_H entries in H. The probability of having a faithful simulation is at least $\frac{1}{nq_H}$.

$\square$

Proof of Theorem 2
The polynomial f with degree $n-t$ can be considered as a function chosen randomly from the collection of all polynomials over $\mathbb{Z}_q$ with degree $n-t$ since $h_{t+1}, \cdots, h_n$ are randomly generated and h_0 is the output of the random oracle H_0.

For $i = t+1, \cdots, n$, and for $j = 1, \cdots, t$, $\{x_i\}$ and $\{r_j\}$ are chosen independently and distributed uniformly over $\mathbb{Z}_q^*$. So $\{U_i\} \cup \{U_j\}$ and hence $\cup_{k=1}^{n} \{U_k\}$ are also uniformly distributed.

The polynomial f is determined by $h_{t+1}, \cdots, h_n$ and h_0, then the distributions of $h_1, \cdots, h_t$ are also uniform over the underlying range, with the fact that $\{S_{ID_j}\}$ is independent of $\{r_j\}$ and $\{h_j\}$, we say that $\{V_i\} \cup \{V_j\}$ and hence V are also uniformly distributed.

To conclude, for any fixed message m and fixed set of identities L, the distribution of $\{U, V, f\}$ are independent and uniformly distributed no matter which t participating signers are. So we conclude that even an adversary with all the private keys corresponding to the set of identities L and unbounded computing resources has no advantage in identifying any one of the participating signers over random guessing. $\square$