Goldberg and Reyzin (March 2017) discovered that if one does not hash the unique identifier when computing the challenge of the proof system, the uniqueness of the VRF from DDH assumption is violated. Therefore, when using the VRF, it is important to hash the unique identifier as well. The problem has been fixed in the current version.

Moreover, they also identified an important flaw on proving the unforgeability of our unique ring signature in the random oracle model (ROM). In the new version, we can only prove a more loose bound on the unforgeability for our unique ring signature in the ROM. Still, this appears to be the most tight reduction for unique ring signatures. Please refer to our full paper for details: Cryptology ePrint Archive: Report 2012/577.

Unique Ring Signatures: A Practical Construction

Matthew Franklin and Haibin Zhang

Dept. of Computer Science, University of California, Davis, California 95616, USA
{franklin,hbzhang}@cs.ucdavis.edu

Abstract. We propose unique ring signatures that simplify and capture the spirit of linkable ring signatures. We provide an instantiation which can be more tightly related to the CDH problem and DDH problem in the random oracle model, leading to the most efficient linkable/unique ring signature.

Keywords: anonymity, authentication, e-voting system, provable security, ring signature, tight reduction, unique signature, verifiable random function.

1 Introduction

Ring signatures [25] are very useful tools for many privacy-preserving applications. However, they are not adequate in settings where some degree of privacy for users must be balanced against limited access. For example, a service provider might have the list of public keys that correspond to all users that have purchased a single access to some confidential service for that day (requiring anonymous authentication). For this kind of application, a number of restricted-use ring signatures are proposed. Notable examples include *linkable ring signatures* [1, 8, 21, 22, 27, 28] and *traceable ring signatures* [15, 16].

Linkable ring signature asks that if a user signs any two messages (same or different) with respect to the same ring, then an efficient public procedure can verify that the signer was the same (although the user's identity is not revealed).

Traceable ring signature is a ring signature scheme where each message is signed not only with respect to a list of ring members, but also with respect to an *issue* (e.g., identifying label of a specific election or survey). If a user signs any two different messages with respect to the same list of ring members *and* the same issue label, then the user's identity is revealed by an efficient public procedure. If a user signs the same message twice with respect to the same list of ring members *and* the same issue label, then the two signed messages can be determined to have come from the same signer by an efficient public procedure (although the signer's identity remains concealed).

Both linkable ring signatures and traceable ring signatures admit interesting applications such as various *e-voting systems* and *e-token systems*, and so on. Notably, the e-voting schemes *directly* from linkable or traceable ring signatures do *not* need any central authorities, a unique and desirable property in sharp contrast to all the schemes from other methods.

Unique ring signatures. We define *unique ring signatures* that capture the essence of linkable ring signatures and traceable ring signatures without identity revelation. We may say a ring signature scheme *unique* if whenever a signer produces two different ring signatures of the *same message* with respect to the same ring, such that both will pass the verification procedure, then these two ring signatures will always have a large common component (hereinafter *unique identifier*). For all the applications introduced in this paper, we further need a *non-colliding* property for a unique ring signature. Call a unique ring signature non-colliding if two different signers of the same message, almost never produce ring signatures with the same unique identifier.

Our contributions. We provide an efficient instantiation of unique ring signature in the random oracle model (ROM). Compared to prior linkable ring signatures, security of the scheme can be more tightly reduced to the CDH problem and the DDH problem (where, by "tight," it means that the success probability of some adversary in some time is roughly equal to the probability of solving some hard problem within almost the same period of time). Despite the similarities with the linkable ring signature due to Liu, Wei, and Wong [21], our scheme also exploits the *algebraic* property of the CDH and DDH problems, namely, the random self-reducibility (RSR) property (see, e.g., [2]) and uses Coron's technique [9].

2 Unique Ring Signature Model

We begin by recalling the definition of a *ring signature* scheme $\mathcal{RS} = (\mathsf{RK}, \mathsf{RS}, \mathsf{RV})$ that consists of three algorithms:

- $\mathsf{RK}(1^\lambda)$. The randomized *user key generation* algorithm takes as input the security parameter λ and outputs a public key pk and a secret key sk.
- $\mathsf{RS}(sk, R, m)$. The probabilistic *ring signing* algorithm takes as input a user secret key sk, a ring R that is a set of public keys (such that $pk \in R$), and a message m to return a signature σ on m with respect to the ring R.

- $\mathsf{RV}(R, m, \sigma)$. The deterministic *ring verification* algorithm takes as input a ring R, a message m, and a signature σ for m to return a single bit b.

The following correctness condition is required: for any security parameter λ, any integer n, any $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \mathsf{RK}(1^\lambda)$ (where now $R = \{pk_i\}_1^n$), any $i \in [n]$, and any m, it holds that $\mathsf{RV}(R, m, \mathsf{RS}(R, sk_i, m)) = 1$.

We consider *unique ring signature* where the signature should have the form of $(R, m, \sigma) = (R, m, \tau, \pi)$ where τ is the *unique identifier* for some message m and some signer i, and π is the rest of the signature. For our constructions, one may simply consider that τ is *the* signature, and π is the corresponding (maybe probabilistic) proof of correctness. Following the recent formulation for ring signature due to Bender, Katz, and Morselli [4], we define for unique ring signature three security requirements: uniqueness, anonymity, and unforgeability. The way we define uniqueness property largely follows from that for unique group signature [13], where the uniqueness security is coupled to a non-colliding property. The formalization of the definitions of security can be found in [14].

3 Unique Ring Signature in Random Oracle Model

We start by describing our basic underlying signature/VRF scheme, and then give the construction of unique ring signature. Notice that our proof techniques do not require *proof of knowledge* but heavily rely on zero-knowledge proof of *membership*, which is one of the main reasons our signature enjoys tight security reductions and admits an improvement in efficiency for a given level of security.

The Underlying VRF Scheme. The signature we shall describe is first predicated on a (well-known) observation that given a random public group element $y = g^x$, the function $F(m) := H(m)^x$ is a PRF, if we model the hash function $H(\cdot)$ as a random oracle.

Our scheme is furthermore based on a well-known zero-knowledge proof system for equality of discrete logarithm due to Chaum and Pederson [6]:

A prover and a verifier both know (g, h, y_1, y_2) with $g, h \neq 1$ and $y_1 = g^x$ and $y_2 = h^x$ for an exponent $x \in \mathbb{Z}_q$. A prover also knows the exponent x. They run the following protocol:

1. The prover chooses $r \xleftarrow{\$} \mathbb{Z}_q$ and sends $a \leftarrow g^r$, $b \leftarrow h^r$ to the verifier.
2. The verifier sends a challenge $c \xleftarrow{\$} \mathbb{Z}_q$ to the prover.
3. The prover sends $t \leftarrow r - cx \bmod q$ to the verifier.
4. The verifier accepts iff $a = g^t y_1^c$ and $b = h^t y_2^c$.

The above protocol is a *sound* proof system but also *honest-verifier zero-knowledge* (HVZK). By using Fiat-Shamir transformation [11], it becomes a NIZK proof system if we model the hash function as a random oracle. Given the above PRF and NIZK proof system, we apply the Bellare-Goldwasser (BG) paradigm [3] to obtain a VRF scheme depicted in Figure 1. (The scheme is in fact a PRF with a NIZK proof and of course a secure signature scheme.) Note that the function that maps x to g^x is not a commitment scheme: the binding property is satisfied while the hiding property is not. This prevents us from following the general BG construction's proof strategy exactly. However, under the DDH assumption, this can be proven secure with a similar proof to that of BG signature.

$\mathsf{Setup}(1^\lambda)$.

The setup algorithm takes as input the security parameter λ and outputs a multiplicative group $\mathbb{G}$ of prime order q and a randomly chosen generator g of $\mathbb{G}$. It also provides two hash functions $H\colon \{0,1\}^* \rightarrow \mathbb{G}$ and $H'\colon \{0,1\}^* \rightarrow \mathbb{Z}_q$. It outputs the public parameters as

$$\mathsf{pp} = (\lambda, q, \mathbb{G}, H, H').$$

$\mathsf{Gen}(1^\lambda, \mathsf{pp})$.

The key generation algorithm takes as input the parameter pp and chooses $x \overset{\$}{\leftarrow} \mathbb{Z}_q$ and sets $y \leftarrow g^x$. It outputs the public key as $pk = y$ and the secret key as $sk = x$.

$\mathsf{Sig}(sk, m)$.

To sign the message m, the signer selects $r \overset{\$}{\leftarrow} \mathbb{Z}_q$ and computes

$$(m, H(m)^x, c, t),$$

where $c \leftarrow H'(g, m, H(m)^x, g^r, H(m)^r)$ and $t \leftarrow r - cx \bmod q$.

$\mathsf{Vrf}(sk, m, \sigma)$.

The verification algorithm first parses σ as (m, τ, c, t) and checks if $\tau \in \mathbb{G}$ and

$$c = H'(g, m, y, \tau, g^t y^c, H(m)^t \tau^c).$$

Fig. 1. Efficient Signature/VRF from the DDH assumption in the random oracle model. The algorithms are described in the context of digital signature. It is also a VRF scheme, where $\mathcal{VRF}.\mathsf{Eva}(sk, m) = H(m)^x$, $\mathcal{VRF}.\mathsf{Prove}(sk, m) = (c, t)$, and $\mathcal{VRF}.\mathsf{Ver}(m, \sigma) = \mathcal{DS}.\mathsf{Vrf}(m, \sigma)$.

Extending the underlying proof system. We now extend the underlying NIZK proof to an "or" language—a proof system that a unique identifier τ (for a message m and a ring R) has the same logarithm with respect to base $H(m||R)$ as one of the public keys $y_j := g^{x_j}$ $(j \in [n])$ with respect to base g. Assume, without loss of generality, $\log_{H(m||R)} \tau = \log_g y_i$ and the prover knows x_i. In particular, we use the proof system between a prover and a verifier.

1. For $j \in [n]$ and $j \neq i$, the prover selects $c_j, t_j \overset{\$}{\leftarrow} \mathbb{Z}_q$ and computes $a_j \leftarrow g^{t_j} y_j^{c_j}$ and $b_j \leftarrow H(m)^{t_j} (H(m)^{x_i})^{c_j}$; for $j = i$, the prover selects $r_i \overset{\$}{\leftarrow} \mathbb{Z}_q$ and computes $a_i \leftarrow g^{r_i}$ and $b_i \leftarrow H(m)^{r_i}$. It sends $\{a_j, b_j\}_1^n$ to the verifier.
2. The verifier sends a challenge $c \overset{\$}{\leftarrow} \mathbb{Z}_q$ to the prover.
3. The prover computes $c_i \leftarrow c - \sum_{j \neq i} c_j$ and $t \leftarrow r - c_i x_i \bmod q$, and sends $c_1, t_1, \cdots, c_n, t_n$ to the verifier.
4. The verifier accepts iff $a_j = g^{t_j} y_j^{c_j}$ and $b_j = H(m)^{t_j} \tau^{c_j}$ for every $j \in [n]$.

The above protocol combines the Chaum-Pederson (CP) technique for proving the equality of two discrete logarithms of [6] and Cramer-Damgård-Schoenmakers (CDS) transformation [10]. Since both of the conversions "preserve" the properties of Σ-protocols, the above system is a sound proof system,[1] and also an interactive honest-verifier zero-knowledge of membership. However, as far as we are concerned, its soundness property has never been used in any signature schemes related to the above proof system. (This is perhaps due to the fact no one needs this property in these schemes anyway.) We now prove that the above proof system is sound;[2] in particular, even an arbitrarily malicious prover P^* cannot convince the verifier to accept a false statement.

Proof. The goal is to show that if $\log_{H(m)} \tau \neq \log_g y_j$ for every $j \in [n]$, then given any $\{a_j, b_j\}_1^n$ sent by P^* there is at most one value c for which P^* can respond correctly. Recall above that we let x_0 denote $\log_{H(m)} \tau$ and x_j denote $\log_g y_j$ for every $j \in [n]$. In this case, we have that $x_0 \neq x_j$ $(j \in [n])$. Given any $\{a_j, b_j\}_1^n$ (where we assume $a_j = g^{r_j}$ and $b_j = H(m)^{r'_j}$) sent to the verifier by a cheating prover, we have the following: if the verifier is to accept, then we must have that

$$c = \sum_1^n c_j, \tag{1}$$

and for every $j \in [n]$,

$$a_j = g^{t_1} y_j^{c_j}, \tag{2}$$

$$b_j = H(m)^{t_j} \tau^{c_j}. \tag{3}$$

By (2) and (3) we obtain that for every $j \in [n]$,

$$r_j = t_j + x_j c_j, \tag{4}$$

$$r'_j = t_j + x_0 c_j. \tag{5}$$

Noting that $x_0 \neq x_j$ for every $j \in [n]$, we have $c_j \leftarrow (r_j - r'_j)(x_o - x_j)^{-1} \bmod q$. According to equation (1), we can now conclude that there is at most one challenge which the cheating prover can respond to. Therefore, the verifier generates this challenge with probability $1/q$ and the proof now follows.

If we turn the above system into a NIZK proof system by following Fiat-Shamir transformation through a hash function H' then one can check that the soundness property is bounded by q_h/q, where q_h denotes the number of times the adversary makes to the random oracle H'. Indeed, in this case, for any $\{a_j, b_j\}_1^n$

[1] Strictly speaking, Σ-protocols can be divided into two categories: Σ-protocols for proof of knowledge, and Σ-protocols for proof of membership. In particular, we can formally show, in the setting of proof of membership, the special soundness property implies that a Σ-protocol is always an interactive proof system.

[2] This is needed, since we shall be providing the exact bound on the soundness property in the random oracle model which appears in our full paper [14].

and any query $H(m, \{a_j, b_j\}_1^n)$ made by an adversary P^*, it follows from the above proof that there is at most one possible value of c satisfying the verification equations. The unique ring signature (from the DDH assumption in the ROM) is described in Figure 2.

$\mathsf{Setup}(1^\lambda)$.

The setup algorithm takes as input the security parameter λ and outputs a multiplicative group $\mathbb{G}$ of prime order q and a randomly chosen generator g of $\mathbb{G}$. It also provides two hash functions $H\colon \{0,1\}^* \to \mathbb{G}$ and $H'\colon \{0,1\}^* \to \mathbb{Z}_q$. It outputs the public parameters as

$$\mathsf{pp} = (\lambda, q, \mathbb{G}, H, H').$$

$\mathsf{RG}(1^\lambda, \mathsf{pp})$.

The key generation algorithm for user i takes as input the parameter pp and selects an element $x_i \xleftarrow{\$} \mathbb{Z}_q$ and computes $y_i \leftarrow g^{x_i}$. It outputs the public key as $pk_i = (\mathsf{pp}, y_i)$ and the secret key as $sk_i = (\mathsf{pp}, x_i)$.

$\mathsf{RS}(sk_i, R, m)$.

To sign the message m in the ring $R = (pk_1, ..., pk_n)$, the signer i with the secret key $sk_i = x_i$ generates the signature in the following way:

1. (Simulation step.) For $j \in [n]$ and $j \neq i$, select $c_j, t_j \xleftarrow{\$} \mathbb{Z}_q$ and compute $a_j \leftarrow g^{t_j} y_j^{c_j}$ and $b_j \leftarrow H(m||R)^{t_j} (H(m||R)^{x_i})^{c_j}$.
2. For $j = i$, select $r_i \xleftarrow{\$} \mathbb{Z}_q$ and compute $a_i \leftarrow g^{r_i}$ and $b_i \leftarrow H(m||R)^{r_i}$.
3. Let $c_i \leftarrow H'(m, R, H(m||R)^{x_i}, \{a_j, b_j\}_1^n) - \sum_{j \neq i} c_j \bmod q$ and $t_i \leftarrow r_i - c_i x_i \bmod q$.
4. Return $(R, m, H(m||R)^{x_i}, c_1, t_1, \cdots, c_n, t_n)$.

$\mathsf{RV}(R, m, \sigma)$.

On receiving the signature (R, m, σ), the verification algorithm first parses σ as $(\tau, c_1, t_1, \cdots, c_n, t_n)$ and checks if $\tau \in \mathbb{G}$ and

$$\textstyle\sum_1^n c_j = H'(m, R, \tau, \{g^{t_j} y_j^{c_j}, H(m||R)^{t_j} \tau^{c_j}\}_1^n).$$

Fig. 2. Unique ring signature from the DDH assumption in the ROM.

The following theorem establishes the security of the above scheme (with proof and exact security bounds in our full paper [14]).

Theorem 1. *The scheme presented in this section is a unique ring signature in the random oracle model under the DDH assumption.* ▮

Acknowledgments

The authors thank Tsz Hon Yuen and anonymous reviewers for comments. Matthew Franklin was sponsored by NSF grant CNS 0831547. Haibin Zhang received support for this project under NSF grant CNS 0831547, CNS 0904380, and CNS 1228828. Many thanks to the NSF for their kind support.

References

1. M. Au, S. Chow, W. Susilo, and P. Tsang. Short linkable ring signatures revisited. *EUROPKI 2006*, LNCS vol. 4043, Springer, pp. 101–115, 2006.
2. M. Bellare, A. Boldyreva, and S. Micali. Public-key encryption in a multi-user setting: security proofs and improvements. *EUROCRYPT 2000*, LNCS vol. 1807, Springer, pp. 259–274, 2000.
3. M. Bellare and S. Goldwasser. New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. *CRYPTO '89*, LNCS vol. 435, Springer, pp. 194–211, 1990.
4. A. Bender, J. Katz, and R. Morselli. Ring signatures: stronger definitions, and constructions without random oracles. *Journal of Cryptology* 22(1): 114–138, 2009.
5. D. Chaum and H. Antwerpen. Undeniable signatures. In *CRYPTO '89*, LNCS vol. 435, Springer, pp. 212–216, 1990.
6. D. Chaum and T. Pedersen. Wallet databases with observers. *CRYPTO '92*, LNCS vol. 740, Springer, pp. 89–105, 1993.
7. B. Chevallier-Mames. An efficient CDH-based signature scheme with a tight security reduction. *CRYPTO 2005*, LNCS vol. 3621, Springer, pp. 511–526, 2005.
8. S. Chow, W. Susilo, and T.H. Yuen. Escrowed linkability of ring signatures and its applications. *VIETCRYPT 2006*, LNCS vol. 4341, pp. 172–192, Springer, 2006.
9. J. Coron. On the exact security of full-domain hash. In *CRYPTO 2000*, LNCS vol. 1880, Springer, pp. 229–235, 2000.
10. R. Cramer, I. Damgård, and B. Schoemakers. Proofs of partial knowledge and simplified design of witness hiding protocols. *CRYPTO '94*, LNCS vol. 839, Springer, pp. 174–187, 1994.
11. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. *CRYPTO '86*, LNCS vol. 263, pp. 186–194, 1987.
12. M. Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. *CRYPTO 2005*, LNCS vol. 3621, Springer, pp. 152–168, 2005.
13. M. Franklin and H. Zhang. Unique group signatures. *ESORICS 2012*, LNCS vol. 7459, Springer, pp. 643–660. Full version in Cryptology ePrint Archive: Report 2012/204. http://eprint.iacr.org
14. M. Franklin and H. Zhang. A Framework for Unique Ring Signatures. Cryptology ePrint Archive: Report 2012/577. http://eprint.iacr.org
15. E. Fujisaki and K. Suzuki. Traceable ring signature. *IEICE Transactions 91-A(1)*: 83–93 (2008).
16. E. Fujisaki. Sub-linear size traceable ring signatures without random oracles. *CT-RSA '11*, LNCS vol. 6558, Springer, pp. 393–415, 2011.
17. E. Goh, S. Jarecki, J. Katz, and N. Wang. Efficient signature schemes with tight security reductions to the Diffie-Hellman problems. *J. of Cryptology* 20(4): 493–514, 2007.
18. E. Goh and S. Jarecki. A signature scheme as secure as the Diffie-Hellman problem. *EUROCRYPT 2003*, LNCS vol. 2656, Springer, pp. 401–415, 2003.
19. J. Herranz and G. Sáez. Forking lemmas for ring signature schemes. *INDOCRYPT 2003*, LNCS vol. 2904, Springer, pp. 266–279, 2003.
20. J. Katz and N. Wang. Efficiency improvements for signature schemes with tight security reductions. *CCS 2003*, ACM press, pp. 155–164, 2003.
21. J. Liu, V. Wei, and D. Wong. Linkable spontaneous anonymous group signatures for ad hoc groups. *ACISP 2004*, LNCS vol. 3108, Springer, pp. 325–335, 2004.
22. J. Liu and D. Wong. Linkable ring signatures: Security models and new schemes. *ICCSA 2005*, LNCS vol. 3481, Springer, pp. 614–623, 2005.

23. S. Micali and L. Reyzin. Improving the exact security of digital signature schemes. *J. Cryptology*, 15(1): 1–18, 2002.
24. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3): 361–396, 2000.
25. R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret: Theory and applications of ring signatures. *Theoretical Computer Science, Essays in Memory of Shimon Even*, LNCS vol. 3895, Springer, pp. 164–186, 2006.
26. C.-P. Schnorr. Efficient identification and signatures for smart cards. *CRYPTO '89*, LNCS vol. 435, Springer, pp. 239–252, 1990.
27. P. Tsang and V. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. *IPSEC 2005*, LNCS vol. 3439, Springer, pp. 48–60, 2005.
28. P. Tsang, V. Wei, T. Chan, M. Au, J. Liu, and D. Wong. Separable linkable threshold ring signatures. *INDOCRYPT 2004*, LNCS vol. 3348, pp. 389–398, 2004.