Ring Signatures of Sub-linear Size without Random Oracles

Nishanth Chandran, Jens Groth*, and Amit Sahai**

UCLA Computer Science Department
4732 Boelter Hall, Los Angeles CA 90095, USA
E-mail: {nishanth,jg,sahai}@cs.ucla.edu

Abstract. Ring signatures, introduced by Rivest, Shamir and Tauman, enable a user to sign a message anonymously on behalf of a "ring". A ring is a group of users, which includes the signer. We propose a ring signature scheme that has size $\mathcal{O}(\sqrt{N})$ where N is the number of users in the ring. An additional feature of our scheme is that it has perfect anonymity.
Our ring signature like most other schemes uses the common reference string model. We offer a variation of our scheme, where the signer is guaranteed anonymity even if the common reference string is maliciously generated.

1 Introduction

Ring signatures, introduced by Rivest, Shamir and Tauman [RST06], enable a user to sign a message anonymously on behalf of a "ring" with the only condition that the user is a member of the ring. A ring is a collection of users chosen by the signer. The signer has to be a member of the ring but the other users do not need to cooperate and may be unaware that they are included in a ring signature.

A variety of applications have been suggested for ring signatures in previous works (see for example [RST06,Nao02,DKNS04]). The original application given was the anonymous leaking of secrets. For example, a high-ranking official in the government wishes to leak some important information to the media. The media want to verify that the source of information is valid, at the same time the official leaking it desires anonymity. Ring signatures give us a way to achieve this task, wherein the media can verify that some high-ranking government official signed the message but cannot ascertain which member actually leaked the secret. Another application is that of designated-verifier signatures [JSI96]. Ring signatures enable Alice to sign an email and send it to Bob with the property that Bob cannot convince a third party that Alice actually sent him this message.

The description of the ring itself is in general linear in the number of members because it is necessary to specify the users included in the ring. Yet, one might face a situation wherein we would like to verify many different signatures on the same ring.

* Supported by NSF ITR/Cybertrust grant No. 0456717.
** Supported by grant No. 0456717 from the NSF ITR and Cybertrust programs, an equipment grant from Intel, and an Alfred P. Sloan Foundation Research Fellowship.

In this case, the size of the ring-signature being sub-linear is quite useful.[1] Most ring signature schemes known today are of linear size in the number of ring members, the only exception being the scheme in [DKNS04], which is independent of the size of the ring. Apart from [CWLY06,BKM06,SW06,Boy07], to the best of our knowledge, all other constructions (including [DKNS04]) are in the random oracle model. The scheme in [CWLY06] is based on a strong new assumption, while in [BKM06], the scheme uses generic ZAPs for NP, thus making it impractical. Shacham and Waters [SW06] give a construction of linear size that is secure under the computational setting of the definitions in [BKM06]. Boyen [Boy07] gives a linear size ring signature in the common random string model with perfect anonymity. Our goal is to construct a sub-linear size ring-signature scheme with perfect anonymity without random oracles.

1.1 Our Contribution

We give the first ring signature of sub-linear size without random oracles. Our scheme is based on composite order groups with a bilinear map. Security is based on the strong Diffie-Hellman assumption [BB04] and the subgroup decision assumption [BGN05]. Our scheme has perfect anonymity in the common reference string model. To reduce the amount of trust in the common reference string, we also offer a variant of our scheme that gives an unconditional guarantee of anonymity even if the common reference string is generated maliciously. Both schemes have ring signatures of size $\mathcal{O}(k\sqrt{N})$ bits, where N is the number of users in the ring and k is a security parameter.

TECHNIQUE. The broad idea behind the scheme is as follows: Let the number of members in the ring be N. To compute a ring signature, the signer first chooses a random one-time signature key and issues a signature on the message using this one-time signing key. Both the public key of the one-time signature and the signature are published. Next, the signer validates the one-time signature key. In other words, she signs the one-time signature key with her own signing key. This validation signature has to be hidden for anonymity. The signer, hence makes two perfectly hiding commitments to her verification key and the validation signature and publishes these values. She then makes non-interactive witness-indistinguishable (NIWI) proofs using techniques from [GOS06,BW06,GS06] that the commitments indeed contain a verification key and a signature on the one-time signature verification key respectively. Finally, the signer will prove that the committed verification key belongs to the ring. The main novelty in our scheme is a sub-linear size proof for a commitment containing one out of N verification keys. This proof relies on a technique akin to one-round private information retrieval (PIR) with $\mathcal{O}(\sqrt{N})$ communication complexity, which is used to get a commitment to the verification key.

2 Ring Signatures – Definitions

[BKM06] contains a comprehensive classification of ring signature definitions. We achieve security under the strongest of these definitions. In the following, we will mod-

[1] Generally speaking, sub-linear size ring signatures are useful when we can amortize the cost of describing the ring itself over many signatures.

ify their definitions in order to include a common reference string and to define information theoretical anonymity.

Definition 1 (Ring signature). *A ring signature scheme consists of a quadruple of PPT algorithms* $(\mathrm{CRSGen}, \mathrm{Gen}, \mathrm{Sign}, \mathrm{Verify})$ *that respectively, generate the common reference string, generate keys for a user, sign a message, and verify the signature of a message.*

- $\mathrm{CRSGen}(1^k)$*, where* k *is a security parameter, outputs the common reference string* ρ*.*
- $\mathrm{Gen}(\rho)$ *is run by the user. It outputs a public verification key* vk *and a private signing key* sk*.*
- $\mathrm{Sign}_{\rho,sk}(M, R)$ *outputs a signature* σ *on the message* M *with respect to the ring* $R = (vk_1, \ldots, vk_N)$*. We require that* (vk, sk) *is a valid key-pair output by* Gen *and that* $vk \in R$*.*
- $\mathrm{Verify}_{\rho,R}(M, \sigma)$ *verifies a purported signature* σ *on a message* M *with respect to the ring of public keys* R*.*

The quadruple $(\mathrm{CRSGen}, \mathrm{Gen}, \mathrm{Sign}, \mathrm{Verify})$ *is a ring signature with perfect anonymity if it has perfect correctness, computational unforgeability and perfect anonymity as defined below.*

Definition 2 (Perfect correctness). *We require that a user can sign any message on behalf of a ring where she is a member. A ring signature* $(\mathrm{CRSGen}, \mathrm{Gen}, \mathrm{Sign}, \mathrm{Verify})$ *has perfect correctness if for all adversaries* $\mathcal{A}$ *we have:*

$$\Pr\Big[\rho \leftarrow \mathrm{CRSGen}(1^k); (vk, sk) \leftarrow \mathrm{Gen}(\rho); (M, R) \leftarrow \mathcal{A}(\rho, vk, sk); \\ \sigma \leftarrow \mathrm{Sign}_{sk}(M, R) : \ \mathrm{Verify}_{\rho,R}(M, \sigma) = 1 \ \vee \ vk \notin R\Big] = 1.$$

Definition 3 (Unforgeability). *A ring signature scheme* $(\mathrm{CRSGen}, \mathrm{Gen}, \mathrm{Sign}, \mathrm{Verify})$ *is unforgeable (with respect to insider corruption) if it is infeasible to forge a ring signature on a message without controlling one of the members in the ring. Formally, it is unforgeable when there is a negligible function* ϵ *so for any non-uniform polynomial time adversaries* $\mathcal{A}$ *we have:*

$$\Pr\Big[\rho \leftarrow \mathrm{CRSGen}(1^k); (M, R, \sigma) \leftarrow \mathcal{A}^{\mathrm{VKGen},\mathrm{Sign},\mathrm{Corrupt}}(\rho) : \\ \mathrm{Verify}_{\rho,R}(M, \sigma) = 1\Big] < \epsilon(k),$$

- VKGen *on query number* i *selects a randomizer* w_i*, runs* $(vk_i, sk_i) \leftarrow \mathrm{Gen}(\rho; w_i)$ *and returns* vk_i*.*
- $\mathrm{Sign}(\alpha, M, R)$ *returns* $\sigma \leftarrow \mathrm{Sign}_{\rho,sk_\alpha}(M, R)$*, provided* (vk_α, sk_α) *has been generated by* VKGen *and* $vk_\alpha \in R$*.*
- $\mathrm{Corrupt}(i)$ *returns* w_i *(from which* sk_i *can be computed) provided* (vk_i, sk_i) *has been generated by* VKGen*.*
- $\mathcal{A}$ *outputs* (M, R, σ) *such that* Sign *has not been queried with* $(*, M, R)$ *and* R *only contains keys* vk_i *generated by* VKGen *where* i *has not been corrupted.*

Definition 4 (Perfect anonymity). *A ring signature scheme* $(\mathrm{CRSGen}, \mathrm{Gen}, \mathrm{Sign}, \mathrm{Verify})$ *has perfect anonymity, if a signature on a message* M *under a ring* R *and key* vk_{i_0} *looks exactly the same as a signature on the message* M *under the ring* R *and key* vk_{i_1}*. This means that the signer's key is hidden among all the honestly generated keys in the ring. Formally, we require that for any adversary* $\mathcal{A}$*:*

$$\begin{aligned}
&\Pr\Big[\rho \leftarrow \mathrm{CRSGen}(1^k); (M, i_0, i_1, R) \leftarrow \mathcal{A}^{\mathrm{Gen}(\rho)}(\rho); \\
&\qquad\qquad \sigma \leftarrow \mathrm{Sign}_{\rho, sk_{i_0}}(M, R) : \mathcal{A}(\sigma) = 1\Big] \\
&= \Pr\Big[\rho \leftarrow \mathrm{CRSGen}(1^k); (M, i_0, i_1, R) \leftarrow \mathcal{A}^{\mathrm{Gen}(\rho)}(\rho); \\
&\qquad\qquad \sigma \leftarrow \mathrm{Sign}_{\rho, sk_{i_1}}(M, R) : \mathcal{A}(\sigma) = 1\Big],
\end{aligned}$$

where $\mathcal{A}$ *chooses* i_0, i_1 *such that* $(vk_{i_0}, sk_{i_0}), (vk_{i_1}, sk_{i_1})$ *have been generated by the oracle* $\mathrm{Gen}(\rho)$*.*

We remark that perfect anonymity implies anonymity against full key exposure which is the strongest definition of anonymity in [BKM06].

3 Preliminaries

We make use of bilinear groups of composite order. These were introduced by Boneh, Goh and Nissim [BGN05] and can for instance be based on elliptic curves and the modified Weil-pairing from Boneh and Franklin [BF03]. Let $\mathrm{Gen}_{\mathrm{BGN}}$ be a randomized algorithm that outputs (p, q, G, G_T, e, g) so we have:

- G is a multiplicative cyclic group of order $n := pq$
- g is a generator of G
- G_T is a multiplicative group of order n
- $e : G \times G \rightarrow G_T$ is an efficiently computable map with the following properties:
  - Bilinear: $\forall\ u, v\ \in G$ and $a, b \in \mathbb{Z}_n :\ e(u^a, v^b) = e(u, v)^{ab}$
  - Non-degenerate: $e(g, g)$ is a generator of G_T whenever g is a generator of G
- The group operations on G and G_T can be performed efficiently

We will write G_p and G_q for the unique subgroups of G that have respectively order p and order q. Observe, $u \mapsto u^q$ maps u into the subgroup G_p.

We base our ring signature scheme on two assumptions - namely, the strong Diffie-Hellman Assumption [BB04] in G_p and the subgroup decision assumption [BGN05].

SUBGROUP DECISION ASSUMPTION. Informally, in the above setting of composite order groups, the subgroup decision assumption holds if random elements from G and G_q are computationally indistinguishable. Formally, for generator $\mathrm{Gen}_{\mathrm{BGN}}$, the subgroup decision assumption holds if there is a negligible function ϵ so for any non-uniform

polynomial time adversary $\mathcal{A}$:

$$\begin{aligned}&\Pr\Big[(p,q,G,G_T,e,g) \leftarrow \mathrm{Gen}_{\mathrm{BGN}}(1^k); n := pq; r \leftarrow \mathbb{Z}_n^*; h := g^r : \\ &\qquad\qquad \mathcal{A}(n,G,G_T,e,g,h) = 1\Big] \\ -&\Pr\Big[(p,q,G,G_T,e,g) \leftarrow \mathrm{Gen}_{\mathrm{BGN}}(1^k); n := pq; r \leftarrow \mathbb{Z}_q^*; h := g^{pr} : \\ &\qquad\qquad \mathcal{A}(n,G,G_T,e,g,h) = 1\Big] \leq \epsilon(k).\end{aligned}$$

STRONG DIFFIE-HELLMAN ASSUMPTION IN G_p. The strong Diffie-Hellman assumption holds in G_p if there is a negligible function ϵ so for all non-uniform adversaries that run in polynomial time in the security parameter:

$$\begin{aligned}&\Pr\Big[(p,q,G,G_T,e,g) \leftarrow \mathrm{Gen}_{\mathrm{BGN}}(1^k); x \leftarrow \mathbb{Z}_p^* : \\ &\qquad \mathcal{A}(p,q,G,G_T,e,g^q,g^{qx},g^{qx^2},\ldots) = (c, g^{\frac{q}{x+c}}) \in \mathbb{Z}_p \times G_p\Big] < \epsilon(k).\end{aligned}$$

UNDERLYING SIGNATURE SCHEME. Boneh and Boyen [BB04] suggest two signature schemes. One that is secure against weak chosen message attack, see below, and one which is secure against adaptive chosen message attack. We will use the scheme that is secure against weak chosen message attack, since it has a shorter public key and this leads to a simpler and more efficient ring signature.

We define the scheme to be secure against weak message attack if there is a negligible function ϵ so for all non-uniform polynomial time interactive adversaries $\mathcal{A}$:

$$\begin{aligned}&\Pr\Big[(M_1,\ldots,M_q) \leftarrow \mathcal{A}(1^k); (vk,sk) \leftarrow \mathrm{KeyGen}(1^k); \sigma_i \leftarrow \mathrm{Sign}_{sk}(M_i); \\ &(M,\sigma) \leftarrow \mathcal{A}(vk,\sigma,\ldots,\sigma_q) : \mathrm{Verify}_{vk}(M,\sigma) = 1 \text{ and } M \notin \{M_1,\ldots,M_q\}\Big] < \epsilon(k).\end{aligned}$$

The Boneh-Boyen signature scheme adapted to the composite order bilinear group model is weak message attack secure under the strong Diffie-Hellman assumption.

- **Key generation:** Given a group (p,q,G,G_T,e,g) we pick a random $sk \leftarrow \mathbb{Z}_n^*$ and compute $vk := g^{sk}$. The key pair is (vk,sk).
- **Signing:** Given a secret key $sk \in \mathbb{Z}_n^*$ and a message $M \in \{0,1\}^\ell$, output the signature $\sigma := g^{\frac{1}{sk+M}}$. By convention, $1/0$ is defined to be 0 so that in the unlikely event that $sk+M=0$, we have $\sigma := 1$. We require $\ell < |p|$, this is quite reasonable since we can always use a cryptographic hash-function to shorten the message we sign.
- **Verification:** Given a public key vk, a message $M \in \{0,1\}^\ell$ and a signature $\sigma \in G$, verify that
$$e(\sigma, vk \cdot g^M) = e(g,g).$$
If equality holds output "Accept". Otherwise, output "Reject".

Boneh and Boyen [BB04] prove that their signature scheme is existentially unforgeable under weak chosen message attack provided the strong Diffie-Hellman assumption holds in prime order groups. This proof translates directly to the composite group order model. Our concern is only whether a signature is forged in the order p subgroup G_p, i.e., an adversary that knows p and q finds (M, σ) so $e(vkg^M, \sigma)^q = e(g, g)^q$. As in [BB04] it can be shown to be infeasible to forge a signature in G_p under a weak chosen message attack assuming the strong Diffie-Hellman assumption holds in G_p.

A COMMITMENT/ENCRYPTION SCHEME. We use a commitment/encryption scheme based on the subgroup decision assumption from [BGN05]. The public key will be a description of the composite order group as well as an element h. The element h is a random element, chosen to have order n (perfect hiding commitment) or order q (encryption). The subgroup decision assumption implies that perfect hiding commitment keys and encryption keys are indistinguishable.

To commit to a message $m \in G$, we pick $r \leftarrow \mathbb{Z}_n$ at random and compute the commitment $c := mh^r$. When h has order n, this is a perfectly hiding commitment to m. However, if h has order q, the commitment uniquely determines m's projection on G_p. Let λ be chosen so $\lambda = 1 \bmod p$ and $\lambda = 0 \bmod q$. Given the factorization of n, we can compute

$$m_p = c^\lambda = m^\lambda h^{\lambda r} = m^\lambda.$$

We can also commit to a message $m \in \mathbb{Z}_n$ by computing $g^m h^r$. If h has order n, then this is a perfectly hiding Pedersen commitment. If h has order q, then the commitment uniquely determines $m \bmod p$.

NON-INTERACTIVE WITNESS-INDISTINGUISHABLE PROOFS. A non-interactive proof enables us to prove that a statement is true. The proof should be complete, meaning that if we know a witness for the statement being true, then we can construct a proof. The proof should be sound, meaning that it is impossible to construct a proof for a false statement. We will use non-interactive proofs that have perfect witness-indistinguishability. This means that given two different witnesses for the statement being true, the proof reveals no information about which witness we used when we constructed the proof.

We will use the public key for the perfectly hiding commitment scheme described above as a common reference string for our NIWI proofs. When h has order n we get perfect witness-indistinguishability. However, if h has order q, then the proof has perfect soundness in G_p.

One type of statement that we will need to prove is that a commitment c is of the form $c = g^m h^r$ for $m \in \{0, 1\}$. Boyen and Waters [BW06], building on [GOS06], give a non-interactive witness-indistinguishable proof for this kind of statement, $\pi = (g^{2m-1} h^r)^r$, which is verified by checking $e(c, cg^{-1}) = e(h, \pi)$. When h has order n, this proof has perfect witness-indistinguishability, because π is uniquely determined from the verification equation so all witnesses must give the same proof. On the other hand, if h has order q, then the verification shows that $e(c, cg^{-1})$ has order q. This implies $m = 0 \bmod p$ or $m = 1 \bmod p$.

We will also need non-interactive witness-indistinguishable proofs for more advanced statements. Groth and Sahai [GS06] show that there exist very small non-interactive witness-indistinguishable proofs for a wide range of statements. These

proofs have perfect completeness on both types of public key for the commitment scheme, perfect soundness in G_p, when h has order q, and perfect witness-indistinguishability when h has order n.

4 Sub-linear Size Ring Signature Scheme Construction

We will give a high level description of the ring signature. We have a signer that knows sk_α corresponding to one of the verification keys in the ring $R = \{vk_1, \ldots, vk_N\}$ and wants to sign a message M. The verification keys are for the Boneh-Boyen signature scheme. There are three steps in creating a signature:

1. The signer picks one-time signature keys, $(otvk, otsk) \leftarrow \mathrm{KeyGen}_{\mathrm{one-time}}(1^k)$. The message M will be signed with the one-time signature scheme. The verification key $otvk$ and the one-time signature will both be public. The signer will certify $otvk$ by signing it with a Boneh-Boyen signature under vk_α.
2. The signer needs to hide vk_α and the certifying signature on $otvk$. She will therefore make two perfectly hiding commitments to respectively vk_α and the signature. Using techniques from [GS06] she makes a non-interactive witness-indistinguishable proof that the commitments contain a verification key and a signature on $otvk$.
3. Finally, the signer will prove that the committed verification key belongs to the ring. The main novelty in our scheme is this sub-linear size proof. She arranges R in an $\nu \times \nu$ matrix, where $\nu = \sqrt{N}$. She commits to the row of the matrix that contains vk_α and makes a non-interactive witness-indistinguishable proof for having done this. She then makes a non-interactive witness-indistinguishable proof that the committed verification key appears in this row.

We now present a detailed description of the ring signature scheme. CRSGen generates a common reference that contains the description of a composite order group and a public key for the perfectly hiding commitment scheme.

$\underline{\mathrm{CRSGen}(1^k)}$

1. $(p, q, G, G_T, e, g) \leftarrow \mathrm{Gen}_{\mathrm{BGN}}(1^k)$
2. $n := pq$; $x \leftarrow \mathbb{Z}_n^*$; $h := g^x$
3. Output (n, G, G_T, e, g, h) /* Perfectly hiding commitment scheme

The users' key generation algorithm Gen takes as input a common reference string and outputs a signing public-private key pair (vk, sk). In our case, it will output keys for the Boneh-Boyen signature scheme that is secure against weak message attack.

$\underline{\mathrm{Gen}(n, G, G_T, e, g, h)}$

1. $sk \leftarrow \mathbb{Z}_n^*$; $vk := g^{sk}$
2. Output (vk, sk) /* Boneh-Boyen signature scheme with public key (g, vk)

A user with keys (vk_α, sk_α) wants to sign a message M under the ring $R = \{vk_1, \ldots, vk_N\}$ of size N. Let i, j be values such that $\alpha = (i-1)\nu + j$, where $\nu = \sqrt{N}$.[2] It is useful to think of R as a $\nu \times \nu$ matrix. Then $vk_\alpha = vk_{(i-1)\nu+j}$ is the entry in row i and column j.

$\underline{\mathrm{Sign}_{(n,G,G_T,e,g,h,sk_\alpha)}(M,R)}$

1. $(otvk, otsk) \leftarrow \mathrm{KeyGen}_{\mathrm{one-time}}(1^k)$; $\sigma_{\mathrm{one-time}} \leftarrow \mathrm{Sign}_{otsk}(M,R)$

   /* This was step 1 in the high level description: a one-time signature on the message and the ring. The pair $(otvk, \sigma_{\mathrm{one-time}})$ will be public.
2. $r \leftarrow \mathbb{Z}_n$; $C := vk_\alpha h^r$; $\sigma_\alpha := g^{\frac{1}{sk_\alpha + otvk}}$; $s \leftarrow \mathbb{Z}_n$; $L := \sigma_\alpha h^s$; $\pi_L := g^{\frac{r}{sk_\alpha+otvk}+(sk_\alpha+otvk)s} \cdot h^{rs}$

   /* This was step 2 in the high level description. σ_α is the signer's certifying signature on $otvk$. C, L are perfectly hiding commitments to respectively vk_α and σ_α. π_L is a NIWI proof [GS06] that C, L contain respectively a verification key and a signature on $otvk$. All that remains is to make a NIWI proof that C contains some $vk_\alpha \in R$ without revealing which one. The rest of the protocol is this NIWI proof.
3. $r_l \leftarrow \mathbb{Z}_n$; $C_l := h^{r_l}$; $\pi_l^C := (g^{-1}h^{r_l})^{r_l}$ for $0 \le l < \nu$, $l \ne i-1$;
   $r_{i-1} := -\sum_{l \ne i-1} r_l$; $C_{i-1} := gh^{r_{i-1}}$; $\pi_{i-1}^C := (gh^{r_{i-1}})^{r_{i-1}}$

   /* The commitments $C_0, \ldots, C_{\nu-1}$ are chosen so C_{i-1} is a commitment to g, whereas the others are commitments to 1. The proofs $\pi_0, \ldots, \pi_{\nu-1}$ are NIWI proofs [GOS06,BW06] that each $C_0, \ldots, C_{\nu-1}$ contains either 1 or g. Since the commitments have been chosen such that $\prod_{l=0}^{\nu-1} C_l = g$, this tells the verifier that there is exactly one C_{i-1} that contains g, while the other commitments contain 1. We will use this in a PIR-like fashion to pick out row i in the $\nu \times \nu$ matrix R. Observe, for all $1 \le m \le \nu$ we have $A_m := \prod_{l=0}^{\nu-1} e(C_l, vk_{l\nu+m}) = e(g, vk_{(i-1)\nu+m}) e(h, \prod_{l=0}^{\nu-1} vk_{l\nu+m}^{r_l})$, which is a commitment to $e(g, vk_{(i-1)\nu+m})$.
4. $s_m \leftarrow \mathbb{Z}_n$; $B_m := vk_{\nu(i-1)+m} h^{s_m}$; $\pi_m^B := g^{-s_m} \cdot \prod_{l=0}^{\nu-1} vk_{l\nu+m}^{r_l}$ for $1 \le m \le \nu$

   /* $B_1, \ldots, B_\nu$ are commitments to the verification keys in row i of R. Recall $A_1, \ldots, A_\nu$ contain row i of R paired with g. $\pi_1^B, \ldots, \pi_\nu^B$ are NIWI proofs [GS06] that $B_1, \ldots, B_\nu$ contain elements that paired with g give the contents of $A_1, \ldots, A_\nu$. This demonstrates to the verifier that $B_1, \ldots, B_\nu$ indeed does contain row i of R.
5. $t_m \leftarrow \mathbb{Z}_n$; $D_m := h^{t_m}$; $\pi_m^D := (g^{-1}h^{t_m})^{t_m}$ for $1 \le m \le \nu$, $m \ne j$
   $t_j := -\sum_{m \ne j} t_m$; $D_j := gh^{t_j}$, $\pi_j^D := (gh^{t_j})^{t_j}$

[2] Without loss of generality we assume N is a square. If N is not a square, we can simply copy vk_1 sufficiently many times to make N a square.

/* $D_1, \ldots, D_\nu$ are commitments so D_j contains g, and the other commitments contain 1. The NIWI proofs [GOS06,BW06] $\pi_1^D, \ldots, \pi_\nu^D$ convince the verifier that $D_1, \ldots, D_\nu$ contain 1 or g. Combining this with $\prod_{m=1}^{\nu} D_m = g$ shows that exactly one D_j is a commitment to g, while the others contain 1.

6. $\pi_C := g^{s_j - r} \prod_{m=1}^{\nu} vk_{(i-1)\nu+m}^{t_m} h^{s_m t_m}$

   /* $A := \prod_{m=1}^{\nu} e(B_m, D_m) = e(g, vk_{(i-1)\nu+j}) e(h, g^{s_j} \prod_{m=1}^{\nu} vk_{(i-1)\nu+m}^{t_m} h^{s_m t_m})$ is a commitment to $e(g, vk_\alpha)$. π_C is a NIWI proof [GS06] that the content of C paired with g corresponds to the content in A.
7. Output the signature $\sigma := \Big(otvk, \sigma_{\mathrm{one-time}}, C, L, \pi_L, \{C_0, \ldots, C_{\nu-1}\}, \{\pi_0^C, \ldots, \pi_{\nu-1}^C\}, \{B_1, \ldots, B_\nu\}, \{\pi_1^B, \ldots, \pi_\nu^B\}, \{D_1, \ldots, D_\nu\}, \{\pi_1^D, \ldots, \pi_\nu^D\}, \pi_C\Big)$.

$\mathrm{Verify}_{(n,G,G_T,e,g,h,R)}(M, \sigma)$

1. Verify that $\sigma_{\mathrm{one-time}}$ is a one-time signature of M, R under $otvk$.
2. Verify that $e(L, C g^{otvk}) = e(g, g) e(h, \pi_L)$.
3. Verify that $e(C_l, C_l g^{-1}) = e(h, \pi_l^C)$ for all $0 \leq l < \nu$ and $\prod_{l=1}^{\nu} C_l = g$.
4. Compute $A_m := \prod_{l=1}^{\nu} e(C_l, vk_{(l-1)\nu+m})$ and verify $A_m = e(g, B_m) e(h, \pi_m^B)$ for all $1 \leq m \leq \nu$.
5. Verify that $e(D_m, D_m g^{-1}) = e(h, \pi_m^D)$ for all $1 \leq m \leq \nu$ and $\prod_{m=1}^{\nu} D_m = g$.
6. Compute $A := \prod_{m=1}^{\nu} e(B_m, D_m)$ and verify $A = e(C, g) e(h, \pi_C)$.
7. "Accept" if all the above steps verify correctly, otherwise "Reject".

Theorem 1. *The scheme presented in the previous section is a ring signature scheme with perfect correctness, perfect anonymity and computational unforgeability under the subgroup decision assumption, the strong Diffie-Hellman assumption and the assumption that the one-time signature is unforgeable.*

Sketch of Proof. Perfect correctness follows by inspection. Perfect anonymity follows from the fact that $otvk$ and $\sigma_{\mathrm{one-time}}$ are generated the same way, no matter which signing key we use, and the fact that when h has order n, then all the commitments are perfectly hiding and the proofs are perfectly witness-indistinguishable [GOS06,BW06,GS06].

Computational unforgeability can be proven in three steps. By the subgroup decision assumption it is possible to switch from using h of order n in the common reference string to use h of order q with only negligible change in the probability of a forgery happening. The commitments are now perfectly binding in G_p and the NIWI proofs are perfectly sound in G_p [GOS06,BW06,GS06], so C contains some uncorrupt $vk_\alpha \in R$ and L contains a signature σ_α on $otvk$ under vk_α. By the properties of the one-time signature scheme, $otvk$ has not been used in any other signature, and thus σ_α is a forged Boneh-Boyen signature on $otvk$. By the strong Diffie-Hellman assumption this probability is negligible. □

5 Untrusted Common Reference String Model

Suppose we do not trust the common reference string. There are two possible problems: maybe it is possible to forge signatures, or maybe the ring signatures are not

anonymous. The possibility of forgery can in many cases be viewed as an extended ring signature, we know that one of the N ring-members or the key generator signed the message. This may not be so problematic, if for instance one of the ring members was the key generator this is not a problem since that member can sign anyway. A breach of anonymity seems more problematic. If we consider the example from the introduction, where a high-ranking official wants to leak a secret to the media, she needs to have strong guarantees of her anonymity. We will modify our scheme to get a (heuristically) unconditional guarantee of anonymity.

In the scheme presented earlier the common reference string is $\rho = (n, G, G_T, e, g, h)$. If we generate the groups as described in [BGN05] it is easy to verify that we have a group of order n with a bilinear map e, where all group operations can be computed efficiently. It is also easy to find a way to represent the group elements, so we can check that $g, h \in G$ [GOS06]. What is hard to check is how many prime factors n has and what the order of g and h is. We make the following observation, which follows from the proof of anonymity: If h has order n, then the ring signature has perfect anonymity. We will therefore not include h in the common reference string but instead provide a method for the signer to choose a full order h as she creates the ring signature.

To get anonymity, h should have order n. If we pick a random element in G there is overwhelming probability that it has order n, unless n has a small prime factor. Lenstra's ECM factorization algorithm [Len87] heuristically takes $O(e^{(1+o(1))\sqrt{(\ln p)(\ln \ln p)}})$ steps to find the prime factor p. Therefore, it is heuristically possible to verify that n only has superpolynomial prime factors and we can pick random elements that with overwhelming probability have order n.

We will modify the key generation such that a user also picks a random element $h_i \in G$ when creating her key. The signer's anonymity will be guaranteed if the element she picks has order n. When she wants to issue a signature, she picks $t \leftarrow \mathbb{Z}_n$ at random and uses $h := \prod_{i=1}^{N} h_i^{t^{i-1}}$. We will argue in the proof of Theorem 2 that with overwhelming probability over the choice of t, that element h she generates this way has order n. Using this h she then creates the ring signature as described in the previous section.

5.1 Ring Signature with Unconditional Anonymity

Our modified ring signature scheme $(\mathrm{CRSGen}', \mathrm{Gen}', \mathrm{Sign}', \mathrm{Verify}')$ works as follows:

- $\mathrm{CRSGen}'(1^k)$ outputs $\rho' := (n, G, G_T, e, g, h') \leftarrow \mathrm{CRSGen}(1^k)$
- $\mathrm{Gen}'(\rho')$ uses Lenstra's ECM factorization algorithm to check that n has no polynomial size prime factors. It runs $(vk_i, sk_i) \leftarrow \mathrm{Gen}(\rho')$ and picks h_i at random from G. It sets $vk_i' := (vk_i, h_i)$ and outputs (vk_i', sk_i).[3]

[3] For practical purposes, say with 1024-bit n and ring-size less than 10000, checking that n has no prime factors smaller than 40 bits is sufficient to guarantee that each time the user signs a message there is less than one in a million risk of the signature not being perfectly anonymous. Since Lenstra's ECM factorization algorithm is only run once during key generation and is reasonably efficient when looking for 40-bit prime factors this cost is reasonable.

– $\mathrm{Sign}'_{\rho',sk_\alpha}(M,R')$ sets $R := (vk_1,\ldots,vk_N)$ for $R' = ((vk_1,h_1),\ldots,(vk_N,h_N))$. It picks $t \leftarrow \mathbb{Z}_n$ and sets $h := \prod_{i=1}^{N} h_i^{t^{i-1}}$. It sets $\rho := (n,G,G_T,e,g,h)$ and creates a ring signature $\sigma \leftarrow \mathrm{Sign}_{\rho,sk_\alpha}(M,R)$. It outputs $\sigma' := (t,\sigma)$.
– $\mathrm{Verify}'_{\rho',R'}(M,\sigma')$ sets $R := (vk_1,\ldots,vk_N)$ and $h := \prod_{i=1}^{N} h_i^{t^{i-1}}$ as the signing algorithm. It sets $\rho := (n,G,G_T,e,g,h)$ and outputs the response of $\mathrm{Verify}_{\rho,R}(M,\sigma)$.

Theorem 2. *The quadruple* $(\mathrm{CRSGen}',\mathrm{Gen}',\mathrm{Sign}',\mathrm{Verify}')$ *is a ring signature scheme with perfect correctness, heuristic statistical anonymity and computational unforgeability under the subgroup decision and strong Diffie-Hellman assumptions.*

Sketch of proof. To prove computational unforgeability we will modify Gen' such that it picks h_i of order q. Using the groups suggested in [BGN05] we can construct convincing randomness that would lead Gen' to pick such an h_i. We can therefore answer any corruption queries the adversary makes. By the subgroup decision assumption, no non-uniform polynomial time adversary can distinguish between seeing correctly generated h_i's of order n and h_i's of order q. It must therefore have at most negligibly smaller chance of producing a forgery after our modification. Now $h = \prod_{i=1}^{N} h_i^{t^{i-1}}$ has order q for any $t \in \mathbb{Z}_n$. The proof of Theorem 1 shows that a polynomial time adversary with has negligible chance of producing a forgery on h of order q.

We will now prove heuristic statistical anonymity, even when the common reference string is maliciously generated by the adversary. Consider an honest signer with keys $(vk_\alpha,h_\alpha),sk_\alpha$. From the run of Lenstra's ECM factorization algorithm we know heuristically that n has no polynomial size prime factors. Therefore, with overwhelming probability the randomly chosen h_α has order n. We will argue that with overwhelming probability over the choice of t, the signer picks h that has order n. When h has order n all commitments will be perfectly hiding and all proofs will be perfectly witness-indistinguishable [GS06], so we will get perfect anonymity.

It remains to argue that with overwhelming probability over t the element $h = \prod_{i=1}^{N} h_i^{t^{i-1}}$ has order n. Consider a generator γ for G and let $x_1,\ldots,x_N$ be the discrete logarithms of $h_1,\ldots,h_N$ with respect to γ. We wish to argue that for any prime factor $p|n$ we have $\sum_{i=1}^{N} t^{i-1}x_i \neq 0 \bmod p$.

Given a prime $p|n$ we will show that there is at most $N-1$ choices of $t \bmod p$ so $\sum_{i=1}^{N} t^{i-1}x_i = 0 \bmod p$. To see this, consider the following system of linear equations:

$$V\boldsymbol{x} = \begin{pmatrix} 1 & t_1 & t_1^2 & \ldots & t_1^{N-1} \\ 1 & t_2 & t_2^2 & \ldots & t_2^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t_N & t_N^2 & \ldots & t_N^{N-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

V is a Vandermonde matrix and has non-zero determinant if all $t_1,\ldots,t_N$ are different. Since $x_\alpha \neq 0 \bmod p$ this implies that we cannot find N different $t_1,\ldots,t_N$ so $\sum_{i=1}^{N} t_i^{i-1}x_i = 0 \bmod p$. When choosing t at random there is at least probability $1 - \frac{N-1}{p}$ that $\sum_{i=1}^{N} t^{i-1}x_i \neq 0 \bmod p$. Since p is superpolynomial, this probability

is negligible. The same argument holds for all other prime factors in n, so with overwhelming probability h is a generator of G. □

References

[BB04] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In *EUROCRYPT'04 - Advances in Cryptology*, pages 56–73, 2004.

[BF03] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-dnf formulas on ciphertexts. In *TCC'05: Theory of Cryptography Conference*, pages 325–341, 2005.

[BKM06] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC'06: Theory of Cryptography Conference*, pages 60–79, 2006.

[Boy07] Xavier Boyen. Mesh signatures. In *Advances in Cryptology—EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 210–227. Berlin: Springer-Verlag, 2007. Available at `http://www.cs.stanford.edu/~xb/eurocrypt07b/`.

[BW06] Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In *EUROCRYPT 2006, LNCS 4004*, pages 427–444, 2006.

[CWLY06] Sherman S. M. Chow, Victor K. Wei, Joseph K. Liu, and Tsz Hon Yuen. Ring Signatures without Random Oracles. In *ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, pages 297–302, New York, NY, USA, 2006. ACM Press.

[DKNS04] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In *EUROCRYPT 2004 - Advances in Cryptology*, pages 609–626, 2004.

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero-knowledge for np. In *EUROCRYPT 2006, LNCS 4004*, pages 339–358, 2006.

[GS06] Jens Groth and Amit Sahai. Efficient non-interactive proofs for bilinear groups. Manuscript, 2006.

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In *EUROCRYPT '96 - Advances in Cryptology*, pages 143–154, 1996.

[Len87] Hendrik W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[Nao02] Moni Naor. Deniable ring authentication. In *CRYPTO 2002 - Advances in Cryptology*, pages 481–498, 2002.

[RST06] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret: Theory and applications of ring signatures. In *Essays in Memory of Shimon Even*, 2006.

[SW06] Hovav Shacham and Brent Waters. Efficient ring signatures without random oracles. Available at http://eprint.iacr.org/2006/289.pdf, 2006.