Unique Ring Signatures

Matthew Franklin **Haibin Zhang**

Department of Computer Science
University of California at Davis

April, 3, 2013

Outline

Outline

Unique Ring Signatures—Our Contributions

- **Simplified definitions.**

Unique Ring Signatures—Our Contributions

- **Simplified definitions.**
- **A simple, general, and unified framework.**

Unique Ring Signatures—Our Contributions

- **Simplified definitions.**
- **A simple, general, and unified framework.**
- **Two efficient instantiations.**

Unique Ring Signatures—Our Contributions

- **Simplified definitions.**
- **A simple, general, and unified framework.**
- **Two efficient instantiations.**
  - The most efficient construction with tight security reduction.

Unique Ring Signatures—Our Contributions

- **Simplified definitions.**
- **A simple, general, and unified framework.**
- **Two efficient instantiations.**
  - The most efficient construction with tight security reduction.
  - Simplifying the traceable ring signature of Fujisaki.

Outline

Ring Signature

- Goes back to Rivest, Shamir, and Tauman (ASIACRYPT 2001).

Ring Signature

- Goes back to Rivest, Shamir, and Tauman (ASIACRYPT 2001).

Three features of ring signatures:

Ring Signature

- Goes back to Rivest, Shamir, and Tauman (ASIACRYPT 2001).

Three features of ring signatures:

- "rings" are ad hoc;

Ring Signature

- Goes back to Rivest, Shamir, and Tauman (ASIACRYPT 2001).

Three features of ring signatures:

- "rings" are ad hoc;
- signers are *anonymous*;

Ring Signature

- Goes back to Rivest, Shamir, and Tauman (ASIACRYPT 2001).

Three features of ring signatures:

- "rings" are ad hoc;
- signers are *anonymous*;
- *no* manager; *no* opener.

Outline

Restricted-Use Ring Signatures

- **Linkable ring signature.**
  ⇒ Linking signatures by the same signer.

Restricted-Use Ring Signatures

- **Linkable ring signature.**
  $\Rightarrow$ Linking signatures by the same signer.
- **Traceable ring signature.**
  $\Rightarrow$ Further revealing the identity of the same signer.

Restricted-Use Ring Signatures

- **Linkable ring signature.**
  ⇒ Linking signatures by the same signer.
- **Traceable ring signature.**
  ⇒ Further revealing the identity of the same signer.
- **Unique ring signature.**
  ⇒ n signers can sign a message for *exactly* n times.

Outline

Unique Ring Signature—Syntax

A *ring signature* scheme $\mathcal{RS} = (\mathsf{RK}, \mathsf{RS}, \mathsf{RV})$ that consists of three algorithms:

Unique Ring Signature—Syntax

A *ring signature* scheme $\mathcal{RS} = (\text{RK}, \text{RS}, \text{RV})$ that consists of three algorithms:

- $\text{RK}(1^\lambda)$. The *user key generation* algorithm outputs a public key pk and a secret key sk.

Unique Ring Signature—Syntax

A *ring signature* scheme $\mathcal{RS} = (\mathsf{RK}, \mathsf{RS}, \mathsf{RV})$ that consists of three algorithms:

- RK(1^λ). The *user key generation* algorithm outputs a public key pk and a secret key sk.
- RS(sk, R, m). The *ring signing* algorithm takes a user secret key sk, a ring R, and a message m to return a signature σ.

Unique Ring Signature—Syntax

A *ring signature* scheme $\mathcal{RS} = (\mathsf{RK}, \mathsf{RS}, \mathsf{RV})$ that consists of three algorithms:

- $\mathsf{RK}(1^\lambda)$. The *user key generation* algorithm outputs a public key pk and a secret key sk.
- $\mathsf{RS}(sk, R, m)$. The *ring signing* algorithm takes a user secret key sk, a ring R, and a message m to return a signature σ.
- $\mathsf{RV}(R, m, \sigma)$. The *ring verification* algorithm takes a ring R, a message m, and a signature σ to return a bit b.

Unique Ring Signature—Syntax

A *ring signature* scheme $\mathcal{RS} = (\mathsf{RK}, \mathsf{RS}, \mathsf{RV})$ that consists of three algorithms:

- $\mathsf{RK}(1^\lambda)$. The *user key generation* algorithm outputs a public key pk and a secret key sk.
- $\mathsf{RS}(sk, R, m)$. The *ring signing* algorithm takes a user secret key sk, a ring R, and a message m to return a signature σ.
- $\mathsf{RV}(R, m, \sigma)$. The *ring verification* algorithm takes a ring R, a message m, and a signature σ to return a bit b.

Unique Ring Signature

Unique Ring Signature—Syntax

A *ring signature* scheme $\mathcal{RS} = (\mathsf{RK}, \mathsf{RS}, \mathsf{RV})$ that consists of three algorithms:

- RK(1^λ). The *user key generation* algorithm outputs a public key pk and a secret key sk.
- RS(sk, R, m). The *ring signing* algorithm takes a user secret key sk, a ring R, and a message m to return a signature σ.
- RV(R, m, σ). The *ring verification* algorithm takes a ring R, a message m, and a signature σ to return a bit b.

Unique Ring Signature

- $(R, m, \sigma) = (R, m, \tau, \pi)$ where τ is the unique identifier

Unique Ring Signatures—Security Definitions

Unique Ring Signature

Unique Ring Signatures—Security Definitions

Unique Ring Signature

- Three security notions

Unique Ring Signatures—Security Definitions

Unique Ring Signature

- Three security notions
  - Anonymity

Unique Ring Signatures—Security Definitions

Unique Ring Signature

- Three security notions
  - Anonymity
  - Unforgeability

Unique Ring Signatures—Security Definitions

Unique Ring Signature

- Three security notions
  - Anonymity
  - Unforgeability
  - Uniqueness

Unique Ring Signatures—Security Definitions

Unique Ring Signature

- Three security notions
  - Anonymity
  - Unforgeability
  - Uniqueness + **Non-Colliding Property**

Unique Ring Signatures—Security Definitions

Anonymity

Unique Ring Signatures—Security Definitions

Anonymity

- **Experiment** $\mathbf{Exp}^{\text{anon}}_{\mathcal{RS},n}(\mathcal{A})$

  $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \mathsf{RK}(1^\lambda);\ \mathtt{CU} \leftarrow \emptyset;\ \mathtt{RS}_{\mathbf{R},\mathbf{M}} \leftarrow \boldsymbol{\varnothing}$

  $(i_0, i_1, R, m) \xleftarrow{\$} \mathcal{A}^{\mathsf{USK}(\cdot),\mathsf{RS}(\cdot,\cdot,\cdot)}(\{pk_i\}_1^n)$

  $b \xleftarrow{\$} \{0,1\};\ \sigma \xleftarrow{\$} \mathsf{RS}(sk_{i_b}, R, m)$

  $b' \xleftarrow{\$} \mathcal{A}^{\mathsf{USK}(\cdot),\mathsf{RS}(\cdot,\cdot)}(\mathsf{guess}, \sigma, \mathsf{s})$

  if $b' \neq b$ then return 0

  return 1

where for each $d \in \{0,1\}$ we have $i_d \notin \mathtt{CU}$ and $i_d \notin \mathtt{RS}_{R,m}$. We define the advantage of $\mathcal{A}$ as

$$\mathbf{Adv}^{\text{anon}}_{\mathcal{RS},n}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{anon}}_{\mathcal{RS},n}(\mathcal{A}) = 1] - 1/2.$$

Unique Ring Signatures—Security Definitions

Unforgeability

Unique Ring Signatures—Security Definitions

Unforgeability

- **Experiment** $\mathbf{Exp}^{\mathrm{uf}}_{\mathcal{RS},n}(\mathcal{A})$

  $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \mathsf{RK}(1^\lambda)$; $\mathtt{CU} \leftarrow \emptyset$; $\mathtt{RS}_{\mathbf{R},\mathbf{M}} \leftarrow \boldsymbol{\varnothing}$

  $(m, R, \sigma) \xleftarrow{\$} \mathcal{A}^{\mathsf{USK}(\cdot),\mathsf{RS}(\cdot,\cdot,\cdot)}(\{pk_i\}_1^n)$

  if $\mathsf{RV}(R, m, \sigma) = 0$ then return 0

  return 1

where $R \subseteq \{pk_i\}_1^n \backslash \mathtt{CU}$ and $\mathcal{A}$ never queried $\mathsf{RS}(\cdot,\cdot,\cdot)$ with $(\cdot, R, m)$. We define the advantage of $\mathcal{A}$ as

$$\mathbf{Adv}^{\mathrm{uf}}_{\mathcal{RS},n}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathrm{uf}}_{\mathcal{RS},n}(\mathcal{A}) = 1].$$

Unique Ring Signatures—Security Definitions

Uniqueness

Unique Ring Signatures—Security Definitions

Uniqueness

- **Experiment** $\mathbf{Exp}^{\text{unique}}_{\mathcal{RS},n}(\mathcal{A})$

  $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \mathsf{RK}(1^\lambda);\ \mathtt{CU} \leftarrow \emptyset;\ \mathtt{RS}_{\mathbf{R},\mathbf{M}} \leftarrow \mathbf{\O}$

  $(m, \sigma_1, \cdots, \sigma_{|\mathtt{CU} \cup \mathtt{RS}_{T,m}|+1}) \xleftarrow{\$} \mathcal{A}^{\mathsf{USK}(\cdot),\mathsf{RS}(\cdot,\cdot,\cdot)}(T)$

  for $i \leftarrow 1$ to $|\mathtt{CU} \cup \mathtt{RS}_{T,m}| + 1$ do

  if $\mathsf{RV}(T, m, \sigma_i) = 0$ then return 0

  for $i, j \leftarrow 1$ to $|\mathtt{CU} \cup \mathtt{RS}_{T,m}| + 1$ do

  if $i \neq j$ and $\tau_i = \tau_j$ then return 0

  return 1

  where $T \leftarrow \{pk_i\}_1^n$ and each σ_i is of the form (τ_i, π_i). We define the advantage of $\mathcal{A}$ as

$$\mathbf{Adv}^{\text{unique}}_{\mathcal{RS},n}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{unique}}_{\mathcal{RS},n}(\mathcal{A}) = 1].$$

Unique Ring Signatures—Security Definitions

Non-colliding property

Unique Ring Signatures—Security Definitions

Non-colliding property—**Not a security definition!**

Non-colliding property—**Not a security definition!**

- Two honest signers never produce the same *unique identifier*.
- Formally, for all security parameter λ and integer n, all $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \mathsf{RK}(1^\lambda)$ with $T = \{pk_i\}_1^n$, all $i, j \in [n]$ and $i \neq j$, and all message $m \in \{0,1\}^*$, it holds that

$$\Pr[(\tau_i, \pi_i) \xleftarrow{\$} \mathsf{RS}(sk_i, T, m); (\tau_j, \psi_j) \xleftarrow{\$} \mathsf{RS}(sk_j, T, m) : \tau_i = \tau_j] \leq \epsilon(\lambda).$$

Outline

A General Framework for Unique Ring Signature

Extending Bellare-Goldwasser paradigm

A General Framework for Unique Ring Signature

Extending Bellare-Goldwasser paradigm

- $\mathsf{Setup}(1^\lambda)$ selects a common random string η, a PRF $F : \mathcal{S} \times \mathcal{X} \to \mathcal{Y}$, and a commitment scheme Com.

A General Framework for Unique Ring Signature

Extending Bellare-Goldwasser paradigm

- $\mathsf{Setup}(1^\lambda)$ selects a common random string η, a PRF $F : \mathcal{S} \times \mathcal{X} \to \mathcal{Y}$, and a commitment scheme Com.
- $\mathsf{RG}(1^\lambda)$ for user i computes $C_i = \mathsf{Com}(r_i, s_i)$ for a random s_i, and outputs the public/secret key pair (pk_i, sk_i) as $(C_i, (s_i, r_i))$.

A General Framework for Unique Ring Signature

Extending Bellare-Goldwasser paradigm

- $\mathsf{Setup}(1^\lambda)$ selects a common random string η, a PRF $F : \mathcal{S} \times \mathcal{X} \to \mathcal{Y}$, and a commitment scheme Com.
- $\mathsf{RG}(1^\lambda)$ for user i computes $C_i = \mathsf{Com}(r_i, s_i)$ for a random s_i, and outputs the public/secret key pair (pk_i, sk_i) as $(C_i, (s_i, r_i))$.
- $\mathsf{RS}(sk_i, R, m)$ outputs (R, m, τ, π), where $\sigma = (\tau, \pi)$ is the unique identifier and π is a NIZK proof that $(\{C_j\}_{j=1}^n, R, m, \tau) \in \mathcal{L}_{\mathsf{OR}}$ where $\mathcal{L}_{\mathsf{OR}} := \{(\{C_j\}_{j=1}^n, R, m, \tau) | \exists (j, s_j, r_j)[C_j = \mathsf{Com}(r_j, s_j) \text{ and } \tau = F_{s_j}(m||R)]\}$.

A General Framework for Unique Ring Signature

Extending Bellare-Goldwasser paradigm

- $\mathsf{Setup}(1^\lambda)$ selects a common random string η, a PRF $F : \mathcal{S} \times \mathcal{X} \to \mathcal{Y}$, and a commitment scheme Com.
- $\mathsf{RG}(1^\lambda)$ for user i computes $C_i = \mathsf{Com}(r_i, s_i)$ for a random s_i, and outputs the public/secret key pair (pk_i, sk_i) as $(C_i, (s_i, r_i))$.
- $\mathsf{RS}(sk_i, R, m)$ outputs (R, m, τ, π), where $\sigma = (\tau, \pi)$ is the unique identifier and π is a NIZK proof that $(\{C_j\}_{j=1}^n, R, m, \tau) \in \mathcal{L}_{\mathsf{OR}}$ where $\mathcal{L}_{\mathsf{OR}} := \{(\{C_j\}_{j=1}^n, R, m, \tau) | \exists (j, s_j, r_j)[C_j = \mathsf{Com}(r_j, s_j)$ and $\tau = F_{s_j}(m||R)]\}$.
- $\mathsf{RV}(R, m, \sigma)$ first parses σ as (τ, π) and checks if π is a correct NIZK proof for the language $\mathcal{L}_{\mathsf{OR}}$.

Security

A General Framework for Unique Ring Signature

Security

- $\mathbf{Adv}^{\mathrm{uf}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{sound}}_{(P,V)}(\mathcal{A}_1) + \mathbf{Adv}^{\mathrm{zk}}_{(P,V)}(\mathcal{A}_2) + n \cdot \mathbf{Adv}^{\mathrm{hide}}_{\mathcal{CM}}(\mathcal{A}_3) + n \cdot \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{A}_4) + n/|\mathcal{Y}|$.

A General Framework for Unique Ring Signature

Security

- $\mathbf{Adv}^{\mathrm{uf}}_{\mathcal{RS}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{sound}}_{(P,V)}(\mathcal{A}_1) + \mathbf{Adv}^{\mathrm{zk}}_{(P,V)}(\mathcal{A}_2) + n \cdot \mathbf{Adv}^{\mathrm{hide}}_{\mathcal{CM}}(\mathcal{A}_3) + n \cdot \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{A}_4) + n/|\mathcal{Y}|$.
- $\mathbf{Adv}^{\mathrm{anon}}_{\mathcal{RS}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{zk}}_{(P,V)}(\mathcal{A}_1) + n \cdot \mathbf{Adv}^{\mathrm{hide}}_{\mathcal{CM}}(\mathcal{A}_2) + n \cdot \mathbf{Adv}^{\mathrm{prf}}_{F}(\mathcal{A}_3)$.

A General Framework for Unique Ring Signature

Security

- $\mathbf{Adv}^{\text{uf}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{sound}}_{(P,V)}(\mathcal{A}_1) + \mathbf{Adv}^{\text{zk}}_{(P,V)}(\mathcal{A}_2) + n \cdot \mathbf{Adv}^{\text{hide}}_{\mathcal{CM}}(\mathcal{A}_3) + n \cdot \mathbf{Adv}^{\text{prf}}_{F}(\mathcal{A}_4) + n/|\mathcal{Y}|$.
- $\mathbf{Adv}^{\text{anon}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{zk}}_{(P,V)}(\mathcal{A}_1) + n \cdot \mathbf{Adv}^{\text{hide}}_{\mathcal{CM}}(\mathcal{A}_2) + n \cdot \mathbf{Adv}^{\text{prf}}_{F}(\mathcal{A}_3)$.
- $\mathbf{Adv}^{\text{unique}}_{\mathcal{RS}}(\mathcal{A}) \leq t \cdot \mathbf{Adv}^{\text{sound}}_{(P,V)}(\mathcal{A}_1) + \mathbf{Adv}^{\text{zk}}_{(P,V)}(\mathcal{A}_2) + n \cdot \mathbf{Adv}^{\text{hide}}_{\mathcal{CM}}(\mathcal{A}_3) + n \cdot \mathbf{Adv}^{\text{prf}}_{F}(\mathcal{A}_4) + tn/|\mathcal{Y}|$.

Outline

Practical Unique Ring Signature with *Tight* Reduction *Standard Assumptions*

Tight reduction for ring signature is HARD

Practical Unique Ring Signature with *Tight* Reduction
Standard Assumptions

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".

Practical Unique Ring Signature with *Tight* Reduction
Standard Assumptions

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".
- Loses a factor of n due to the multi-user setting.

Practical Unique Ring Signature with *Tight* Reduction

Standard Assumptions

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".
- Loses a factor of n due to the multi-user setting.

Previous constructions on linkable/traceable ring signatures:

Practical Unique Ring Signature with *Tight* Reduction
Standard Assumptions

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".
- Loses a factor of n due to the multi-user setting.

Previous constructions on linkable/traceable ring signatures:

- Loose security reduction for Liu, Wei, and Wong linkable ring signature.

Practical Unique Ring Signature with *Tight* Reduction *Standard Assumptions*

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".
- Loses a factor of n due to the multi-user setting.

Previous constructions on linkable/traceable ring signatures:

- Loose security reduction for Liu, Wei, and Wong linkable ring signature.
- Fujisaki and Suzuki traceable ring signature mentioned “online extractor"—far less efficient.

Practical Unique Ring Signature with *Tight* Reduction *Standard Assumptions*

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".
- Loses a factor of n due to the multi-user setting.

Previous constructions on linkable/traceable ring signatures:

- Loose security reduction for Liu, Wei, and Wong linkable ring signature.
- Fujisaki and Suzuki traceable ring signature mentioned “online extractor"—far less efficient.
- Other constructions use strong/exotic assumptions but less efficient.

Practical Unique Ring Signature with *Tight* Reduction
Standard Assumptions

Tight reduction for ring signature is HARD

- Cramer-Damgård-Schoemakers transformation relies on proof of knowledge—“rewinding", “forking lemma".
- Loses a factor of n due to the multi-user setting.

Previous constructions on linkable/traceable ring signatures:

- Loose security reduction for Liu, Wei, and Wong linkable ring signature.
- Fujisaki and Suzuki traceable ring signature mentioned “online extractor"—far less efficient.
- Other constructions use strong/exotic assumptions but less efficient.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Idea—Instantiating the above paradigm

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Idea—Instantiating the above paradigm

- "Commitment scheme": $y = g^x$

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Idea—Instantiating the above paradigm

- "Commitment scheme": $y = g^x$
- PRF: $F(m) = H(m)^x$

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Idea—Instantiating the above paradigm

- "Commitment scheme": $y = g^x$
- PRF: $F(m) = H(m)^x$
- Using *zero-knowledge proof of membership*, instead of *proof of knowledge*.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

The underlying zero-knowledge proof system:

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

The underlying zero-knowledge proof system:

- Combining the Chaum-Pederson (CP) for proving the equality of two discrete logarithms and Cramer-Damgård-Schoenmakers (CDS) transformation.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Chaum-Pederson:

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]
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 underlying "*or*" proof system:

- A proof system that a unique identifier τ has the same logarithm w.r.t. base $H(m||R)$ as one of the public keys $y_j := g^{x_j}$ ($j \in [n]$) w.r.t. base g.

1. For $j \in [n]$ and $j \neq i$, the prover selects $c_j, t_j \xleftarrow{\$} \mathbb{Z}_q$ 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 $r_i \xleftarrow{\$} \mathbb{Z}_q$ 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 $c \xleftarrow{\$} \mathbb{Z}_q$ 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 $j \in [n]$.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

The above "*or*" proof system:

- Sound
- Honest-verifier zero-knowledge of membership.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

The above "*or*" proof system:

- Sound (never used before!)
- Honest-verifier zero-knowledge of membership.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

The above "*or*" proof system:

- Following Fiat-Shamir transformation, the soundness-*advantage* is bounded by q_h/q, where q_h denotes the number of times the adversary makes to the random oracle.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

One more technique:

- Random self-reducibility of DDH problem.

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Security—*All* the three notions can be tightly related to DDH problems!

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Security—*All* the three notions can be tightly related to DDH problems!

- $\mathbf{Adv}^{\mathrm{uf}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathbb{G}}(\mathcal{A}_3) + (2q_h + n + 1)/q.$

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Security—*All* the three notions can be tightly related to DDH problems!

- $\mathbf{Adv}^{\mathrm{uf}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathbb{G}}(\mathcal{A}_3) + (2q_h + n + 1)/q.$
- $\mathbf{Adv}^{\mathrm{anon}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathbb{G}}(\mathcal{A}_2) + q_h/q.$

Practical Unique Ring Signature with *Tight* Reduction and *Standard Assumptions*

Security—*All* the three notions can be tightly related to DDH problems!

- $\mathbf{Adv}^{\mathrm{uf}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathbb{G}}(\mathcal{A}_3) + (2q_h + n + 1)/q.$
- $\mathbf{Adv}^{\mathrm{anon}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathbb{G}}(\mathcal{A}_2) + q_h/q.$
- $\mathbf{Adv}^{\mathrm{unique}}_{\mathcal{RS}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathbb{G}}(\mathcal{B}) + t(q_h + 1)/q + q_h/q + tn/q.$

Outline

Simplified Unique Ring Signature in CRS Model

What's Old?

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.
- Our scheme follows *exactly* our general framework.

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.
- Our scheme follows *exactly* our general framework.

What's New?

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.
- Our scheme follows *exactly* our general framework.

What's New?

- Simplifying and clarifying the overall structure.

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.
- Our scheme follows *exactly* our general framework.

What's New?

- Simplifying and clarifying the overall structure.
- Eliminating the relatively inefficient one-time signature.

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.
- Our scheme follows *exactly* our general framework.

What's New?

- Simplifying and clarifying the overall structure.
- Eliminating the relatively inefficient one-time signature.
- Employing a solo assumption (i.e., Pseudo-Random DDHI).

Simplified Unique Ring Signature in CRS Model

What's Old?

- Fujisaki scheme—*first* sublinear-size linkable ring signature without random oracles.

What's Different?

- Fujisaki's scheme is based on the ring signature due to Chandran, Groth, and Sahai.
- Our scheme follows *exactly* our general framework.

What's New?

- Simplifying and clarifying the overall structure.
- Eliminating the relatively inefficient one-time signature.
- Employing a solo assumption (i.e., Pseudo-Random DDHI).
- Requiring *no* proofs—impled by the general framework.

Outline

Future Work

- Constant-size ring signature in the standard model.

Future Work

- Constant-size ring signature in the standard model.
- Design and implementation of an E-Voting scheme *without* trusted opener.

Thank you!