| Lattices oo | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------------|-----------------|--------------------------|------------------|
| | | | |

Lattice-Based Ring Signature Scheme

Carlos Aguilar Melchor¹ Slim Bettaieb ¹ Xavier Boyen² Laurent Fousse³ Philippe Gaborit¹

¹XLIM-DMI, Université de Limoges, (France)

²Palo Alto Research Center, (États-Unis)

³Google Inc, (État-Unis)

Journées Codage et Cryptographie - 12th October 2012

| Lattices oo | Ring Signatures | Signature Scheme [Lyu09] 00 | Our Construction |
|----------------|-----------------|--------------------------------|------------------|
| Outline | | | |

- Lattices
- Ring Signatures
- Signature Scheme (V.Lyubashevsky, Asiacrypt '09)
- Our Construction

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| 00 | 000000 | 00 | 0000000 |
| | | | |

Lattices



Lattice

Let $b_1, b_2, ..., b_n \in \mathbb{R}^n$, n linearly independent vectors, the lattice generated by them is

$$\mathcal{L} := \{\sum_i x_i b_i \mid x_i \in \mathbb{Z}\}.$$

Lattice-based Cryptography

- 90s: Strong security reductions
- Belived to resist quantum computer attacks

| Lattices o● | Ring Signatures | Signature Scheme [Lyu09] oo | Our Construction |
|----------------|-----------------|--------------------------------|------------------|
| Efficient | Lattices | | |

Let $\mathcal{R} = \mathbb{Z}[x] / \langle x^n + 1 \rangle$, with *n* a power of 2.

Ideal Lattice

- Let $\mathcal{I} \subseteq \mathcal{R}$ be an ideal.
 - Polynomials in *I* can be seen as vectors.
 - \mathcal{I} corresponds to a sublattice of \mathbb{Z}^n

An ideal lattice is a sublattice of \mathbb{Z}^n that correspond to an ideal $\mathcal{I} \subseteq \mathcal{R}$.

Properties

- More efficient (SWIFFT a candidate to NIST SHA-3 competition)
- Security reduction still holds.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- ▶ Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- ▶ Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | ••••• | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- ▶ Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- ► [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | •00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | •00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |

- Introduced by Chaum and Van Heyst in 1991.
- A group manager
- There is an anonymity revocation mechanism

- Introduced by Rivest, Shamir, and Tauman in 2001.
- Allow to leak a secret anonymously
- A user sign a message on behalf of a set of members (that include himself)
- [Ad-hoc] The signer can choose any ring and sign messages without the permission or asistance of its members
- [Anonymity] The signature gives a proof that the message was signed by a member of some entity, but it does not give any information about the real signer.



Applications

- Allow to leak a secret anonymously
- Designated-verifier signatures

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|-------------|-----------------|--------------------------|------------------|
| oo | oo●ooo | oo | |
| Security Mo | odel | | |

Unforgeability property

Infeasibility of signing on behalf of a ring without knowing one of the secret keys

Anonymity of the signer

It is not possible to know which secret key was used

Strong Security Model (Unforgeability)

Unforgeability w.r.t insider corruption

- Signing query can be done with respect to any ring
- Attacker is allowed to choose any subring to corrupt (i.e, the attacker can see the secret keys of this subring).

Unforgeability Game



•
$$\mathbf{S} = \{pk_i\}_{i=1}^{\ell}$$

- access to OSign()
- access to a set of secret keys denoted C.
-) The forger outputs $(\sigma^\star,\mu^\star, {m R}^\star)$ and succeeds if
 - the forger never queried $(\cdot, \mu^{\star}, R^{\star})$ to OSign().
 - $R^* \subseteq S \setminus C$

Strong Security Model (Unforgeability)

Unforgeability w.r.t insider corruption

- Signing query can be done with respect to any ring
- Attacker is allowed to choose any subring to corrupt (i.e, the attacker can see the secret keys of this subring).

Unforgeability Game

Forger is given

•
$$S = \{pk_i\}_{i=1}^{\ell}$$

- access to OSign()
- access to a set of secret keys denoted C.
- 2 The forger outputs $(\sigma^{\star}, \mu^{\star}, R^{\star})$ and succeeds if
 - the forger never queried $(\cdot, \mu^{\star}, R^{\star})$ to OSign().
 - $R^{\star} \subseteq S \setminus C$

Strong Security Model (Anonymity)

Anonymity against chosen setting attacks

Attacker create its own users, thus he knows all the secret keys.

Anonymity Game

- Attacker sends to the challenger
 - a ring $R = \{pk_i\}_{i=1}^{\ell}$, two dististinct indices i_0, i_1
 - two secret keys sk_{i_0}, sk_{i_1} and a message μ

Challenger,

- pick random $b \in \{0, 1\}$
- send $\sigma_b \leftarrow Sign(\mu, sk_{i_b})$ to attacker
- 3 Attacker outputs a bit b' and wins the game if b' = b

Strong Security Model (Anonymity)

Anonymity against chosen setting attacks

Attacker create its own users, thus he knows all the secret keys.

Anonymity Game

- Attacker sends to the challenger
 - a ring $R = \{pk_i\}_{i=1}^{\ell}$, two dististinct indices i_0, i_1
 - two secret keys $\textit{sk}_{\textit{i}_0}, \textit{sk}_{\textit{i}_1}$ and a message μ

Challenger,

- pick random $b \in \{0, 1\}$
- send $\sigma_b \leftarrow Sign(\mu, sk_{i_b})$ to attacker

Solution Attacker outputs a bit b' and wins the game if b' = b

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | 00000 | | |
| | | | |
| | | | |

Related Work

Brakerski-Kalai (eprint 2010/086):

- Hash-and-sign / bonsai-tree approach
- Chosen subring attack unforgeability
- No insider corruption proof

Wang-Sun (ICICS '11):

- Hash-and-sign / bonsai-tree approach
- Insider corruption proof works only for log-sized rings
- Cayrel-Linder-Rückert-Silva (Latincrypt '10):
 - Threshold ring signature scheme (hard feature to obtain)
 - Uses Stern's construction for signature schemes
 - No insider corruption proof

| Lattices | |
|----------|--|
| | |

Sets and notations

• Let
$$\mathcal{R} = \mathbb{Z}_{p}[x] / \langle x^{n} + 1 \rangle$$

Let

$$\begin{aligned} C^{27} &:= \{ \hat{s} = (s_1, \dots, s_{27}) : s_i \in \mathcal{R}, \|s_i\|_{\infty} \le 1 \} \\ D^{27} &:= \{ \hat{y} = (y_1, \dots, y_{27}) : y_i \in \mathcal{R}, \|y_i\|_{\infty} \le 3 \cdot 10^6 \} \end{aligned}$$

• For any $\hat{a} = (a_1, \dots, a_{27}) \in \mathcal{R}^{27}$, we have the following hash function

$$\begin{array}{rrrr} h_{\hat{a}}: & D^{27} & \rightarrow & \mathcal{R} \\ & \hat{y} & \mapsto & \hat{y} \odot \hat{a} = \sum_{i=1}^{27} a_i \cdot y_i \end{array}$$

• Let $\hat{v}, \hat{w} \in \mathcal{R}^{27}$ and $x \in \mathcal{R}$

$$h_{\hat{a}}(x\cdot\hat{v}+\hat{w})=x\cdot h_{\hat{a}}(\hat{v})+h_{\hat{a}}(\hat{w})$$



| Lattices oo | Ring Signatures | Signature Scheme [Lyu09] ○● | Our Construction |
|----------------|-----------------|--------------------------------|------------------|
| | | | |

Key generation

Signing key: $\hat{s} \in C^{27}$ Verification key: $h_{\hat{a}}$ and $S = h_{\hat{a}}(\hat{s})$



$$\mathcal{H}: \{0,1\}^* o \{g \in \mathcal{R}: \|g\|_\infty \leq 1\}$$

Signing algorithm

$Sign(\mu)$

- Pick a random ŷ
- Compute $Y = h_{\hat{a}}(\hat{y})$
- Compute *e* = *H*(*Y*||*µ*)

•
$$\hat{z} = \mathbf{e} \cdot \hat{\mathbf{s}} + \hat{\mathbf{y}}$$

Output (2, e)

Verification algorithm

Check if

$$e \stackrel{?}{=} H(h_{\hat{a}}(\hat{z}) - e \cdot S \| \mu)$$

since

 $h_{\hat{a}}(\hat{z}) = e \cdot S + h_{\hat{a}}(\hat{y})$

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| 00 | 000000 | | 0000000 |
| | | | |

Key generation

Signing key: $\hat{s} \in C^{27}$ Verification key: $h_{\hat{a}}$ and $S = h_{\hat{a}}(\hat{s})$



$$\mathcal{H}: \{0,1\}^* o \{g \in \mathcal{R}: \|g\|_\infty \leq 1\}$$

Signing algorithm

$Sign(\mu)$

- Pick a random ŷ
- Compute $Y = h_{\hat{a}}(\hat{y})$
- Compute *e* = *H*(*Y*||*µ*)

•
$$\hat{z} = \mathbf{e} \cdot \hat{\mathbf{s}} + \hat{\mathbf{y}}$$

Output (2, e)

Verification algorithm Check if $e \stackrel{?}{=} H(h_{\hat{a}}(\hat{z}) - e \cdot S || \mu)$ since $h_{\hat{a}}(\hat{z}) = e \cdot S + h_{\hat{a}}(\hat{y})$



$$S_1 = h_1(\hat{s}_1), S_2 = h_2(\hat{s}_2), S_3 = h_3(\hat{s}_3)$$

. . У27

S27

Reminder

• Let
$$\mathcal{R} = \mathbb{Z}_p[x] / \langle x^n + 1 \rangle$$

Let

$$C^{27}:=\{\hat{\mathbf{s}}=(\mathbf{s}_1,\ldots,\mathbf{s}_{27}):\mathbf{s}_i\in\mathcal{R},\|\mathbf{s}_i\|_\infty\leq 1\}$$

$$h_{\hat{a}}(\hat{s}) = \hat{s} \odot \hat{a} = \sum_{i=1}^{27} a_i \cdot s_i$$

• Let $\hat{v}, \hat{w} \in \mathcal{R}^{27}$ and $x \in \mathcal{R}$

$$h_{\hat{a}}(\boldsymbol{x}\cdot\hat{\boldsymbol{v}}+\hat{w})=\boldsymbol{x}\cdot h_{\hat{a}}(\hat{v})+h_{\hat{a}}(\hat{w})$$

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|----------|-----------------|--------------------------|------------------|
| | | | 000000 |
| | | | |

Toy Example: a ring with 3 members (First attempt)

Ring-KeyGen

 $\begin{array}{l} \text{Secret keys: } \hat{s}_1, \hat{s}_2, \hat{s}_3 \in C^{27} \\ \text{Public keys: } h_{\hat{a}_1}, h_{\hat{a}_2}, h_{\hat{a}_3} := h_1, h_2, h_3. \end{array}$

 $S_1 = h_1(\hat{s}_1), S_2 = h_2(\hat{s}_2), S_3 = h_3(\hat{s}_3)$

Ring-Sign(μ , \hat{s}_1)

- Pick random $\hat{y}_1, \hat{y}_2, \hat{y}_3$
- Compute $Y = h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$
- Compue $e = H(Y \| \mu)$

•
$$\hat{z}_1 = \mathbf{e} \cdot \hat{s}_1 + \hat{y}_1$$

•
$$\hat{z}_2 = \hat{y}_2$$

•
$$\hat{z}_3 = \hat{y}_3$$

Send $\sigma = (\hat{z}_1, \hat{z}_2, \hat{z}_3, e)$



Ring-Sign(μ , \hat{s}_3)

- Pick random $\hat{y}_1, \hat{y}_2, \hat{y}_3$
- Compute

$$Y = h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$$

• Compue
$$e = H(Y || \mu)$$

•
$$\hat{z}_1 = \hat{y}_1$$

•
$$\hat{z}_2 = \hat{y}_2$$

•
$$\hat{z}_3 = \boldsymbol{e} \cdot \hat{\boldsymbol{s}}_3 + \hat{\boldsymbol{y}}_3$$

Send $\sigma = (\hat{z}_1, \hat{z}_2, \hat{z}_3, e)$

| Lattices oo | Ring Signatures | Si | ignature Scl | heme [| Lyu09] | | | | Our Construc o●ooooo | tion |
|----------------------------|---|------------------|--------------|-------------|------------------|-----------------|--------------------------------|-------------------|-------------------------|------|
| | Toy Example: a ring | g with 3 | memt | bers | (Fi | rst a | atter | npt) |) | |
| Ring-Key0 | Gen | | | y 1 | | a ₁ | | S ₁ | 0- | |
| Secret keys Public keys | | 3. | ŷ | _ 12 : | â | a ₂ | ŝ | • • • | S | |
| $S_1 = h_1(\hat{s})$ | $(\hat{s}_1), S_2 = h_2(\hat{s}_2), S_3 = h_3(\hat{s}_2)$ | ŝ ₃) | | Y 27 | | a ₂₇ | | \$ ₂₇ | е 📕 | |
| Ring-Sig | $n(\mu, \hat{s}_1)$ | | Ring | g-Si | gn(_/ | u, ŝ z | 3) | | | |
| Pick ratio | andom $\hat{y}_1, \hat{y}_2, \hat{y}_3$ | | ۲ | Pick | ranc | dom | ŷ ₁ ,ŷ ₂ | 2, ŷ ₃ | | |
| Comp | ute $(\hat{\alpha}) + b(\hat{\alpha}) + b(\hat{\alpha})$ | | ۲ | Com | npute | ; | h (î | | h (û) | |
| Y = II | $1(y_1) + n_2(y_2) + n_3(y_3)$ | | | r = | $n_{1}()$ | (1) + | $n_{2}(y)$ | (2) + | $n_{3}(y_{3})$ | |

• Compue $e = H(Y || \mu)$

•
$$\hat{z}_1 = \hat{y}_1$$

•
$$\hat{z}_2 = \hat{y}_2$$

•
$$\hat{z}_3 = \mathbf{e} \cdot \hat{s}_3 + \hat{y}_3$$

Send $\sigma = (\hat{z}_1, \hat{z}_2, \hat{z}_3, e)$

• $\hat{z}_1 = \mathbf{e} \cdot \hat{\mathbf{s}}_1 + \hat{\mathbf{y}}_1$

• $\hat{z}_2 = \hat{y}_2$ • $\hat{z}_3 = \hat{y}_3$

• Compue $e = H(Y||\mu)$

| oo | oooooo | 00 |)) | ne [Lyuua | | | 0000000 |
|--|--|--------|-------------------------|--|--------------------------------------|---|--------------------------------|
| | Toy Example: a ring | with 3 | membe | rs (Fi | rst a | ttempt |)) |
| Ring-Key@ Secret keys Public keys | $\begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \hat{\mathbf{s}}_{1}, \hat{\mathbf{s}}_{2}, \hat{\mathbf{s}}_{3} \in \boldsymbol{C}^{27} \\ \vdots & h_{\hat{a}_{1}}, h_{\hat{a}_{2}}, h_{\hat{a}_{3}} := h_{1}, h_{2}, h_{3}. \end{array} \end{array}$ | | $\hat{\mathcal{Y}}$: : | â | a ₁ a ₂ | \hat{s} \hat{s} \hat{s} \hat{s} | S= e |
| Ring-Sigr | (μ, \hat{s}_2) andom $\hat{y}_1, \hat{y}_2, \hat{y}_3$ | 3) | Ring-V | ∞ ′erif(μ | a_{27} | \$ ₂₇ | |
| • Compute $Y = h^2$ • Compute • $\hat{z}_1 - \hat{y}_2$ | ute $h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$ ue $e = H(Y \ \mu)$ | | e since | $\stackrel{?}{=} H(\sum_{i=1}^{3}$ | $\int_{-1}^{3} h_i(2)$ | Ż _i) − e · · | $S_2 \ \mu$) |
| • $\hat{z}_1 = \hat{y}$ • $\hat{z}_2 = \hat{e}$ • $\hat{z}_3 = \hat{y}$ Sound $z = \hat{f}$ | $\hat{s}_{2} + \hat{y}_{2}$ | | $=h_1($ | $h_1(\hat{z_1}) + \epsilon$ $\hat{y}_1) + \epsilon$ | $+ h_2(x)$ | $\hat{z_2}) + h_3 + h_2(\hat{y}_2)$ | $(\hat{z_3})$ $(\hat{z_3})$ |
| Seria σ = (| ζ ₁ , ζ ₂ , ζ ₃ , θ) | | | | | | |

| La | tti | Ce | es |
|----|-----|----|----|
| | | | |

Our Construction

Toy Example: a ring with 3 members (First attempt)

Ring-Sign(μ , \hat{s}_1)

- Pick random $\hat{y}_1, \hat{y}_2, \hat{y}_3$
- Compute $Y = h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$
- Compue $e = H(Y||\mu)$
- $\hat{z}_1 = \boldsymbol{e} \cdot \hat{s}_1 + \hat{y}_1$
- $\hat{z}_2 = \hat{y}_2$
- $\hat{z}_3 = \hat{y}_3$

Send $\sigma = (\hat{z}_1, \hat{z}_2, \hat{z}_3, e)$

To obtain anonymity

S is the same for all users !

$$S = S_1 = S_2 = S_3$$

Ring-Verif(μ, σ)

$$\mathbf{e} \stackrel{?}{=} H(\sum_{i=1}^{3} h_i(\hat{z}_i) - \mathbf{e} \cdot S_1 \| \boldsymbol{\mu})$$

since

$$h_1(\hat{z}_1) + h_2(\hat{z}_2) + h_3(\hat{z}_3)$$

= $\mathbf{e} \cdot S_1 + h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$

16/19

| La | tti | | s |
|----|-----|--|---|
| | | | |

Our Construction

Toy Example: a ring with 3 members (First attempt)

Ring-Sign(μ , \hat{s}_1)

- Pick random $\hat{y}_1, \hat{y}_2, \hat{y}_3$
- Compute $Y = h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$
- Compue $e = H(Y || \mu)$
- $\hat{z}_1 = \mathbf{e} \cdot \hat{s}_1 + \hat{y}_1$
- $\hat{z}_2 = \hat{y}_2$
- $\hat{z}_3 = \hat{y}_3$

Send $\sigma = (\hat{z}_1, \hat{z}_2, \hat{z}_3, e)$

To obtain anonymity

S is the same for all users !

$$S = S_1 = S_2 = S_3$$

Ring-Verif(μ, σ)

$$\boldsymbol{e} \stackrel{?}{=} \boldsymbol{H}(\sum_{i=1}^{3} h_{i}(\hat{\boldsymbol{z}}_{i}) - \boldsymbol{e} \cdot \boldsymbol{S}_{1} \| \boldsymbol{\mu})$$

since

$$h_1(\hat{z}_1) + h_2(\hat{z}_2) + h_3(\hat{z}_3)$$

= $\mathbf{e} \cdot S_1 + h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$

16/19

| Lattices Ring Signatures 5 00 000000 | Signature Scheme [Lyu09] Our Construction oo ooooooo |
|--|---|
| Toy Example: a rin | ng with 3 members |
| Ring-KeyGen (\mathcal{R} , S) Secret keys: $\hat{s}_1, \hat{s}_2, \hat{s}_3 \in C^{27}$ Public keys: $h_{\hat{a}_1}, h_{\hat{a}_2}, h_{\hat{a}_3} := h_1, h_2, h_3.$ $S = h_1(\hat{s}_1) = h_2(\hat{s}_2) = h_3(\hat{s}_3)$ | $\hat{y} \stackrel{\text{y}_1}{\vdots} \stackrel{\text{a}_1}{\vdots} \hat{a} \stackrel{\text{s}_1}{\vdots} \hat{s} \stackrel{\text{s}_2}{\vdots} \stackrel{\text{s}_2}{\vdots} e$ |
| Ring-Sign (μ, \hat{s}_2) | Ring-Verif (μ, σ) |
| • Compute $Y = h_1(\hat{y}_1) + h_2(\hat{y}_2) + h_3(\hat{y}_3)$ • Compue $e = H(Y \mu)$ | $\mathbf{e} \stackrel{?}{=} H(\sum_{i=1}^{3} h_i(\hat{z}_i) - \mathbf{e} \cdot \mathbf{S} \mu)$ |
| • $\hat{z}_1 = \hat{y}_1$ • $\hat{z}_2 = e \cdot \hat{s}_2 + \hat{y}_2$ • $\hat{z}_3 = \hat{y}_3$ | since $h_1(\hat{z_1}) + h_2(\hat{z_2}) + h_3(\hat{z_3})$ |
| Send $\sigma = (\hat{z}_1, \hat{z}_2, \hat{z}_3, e)$ | $= h_1(\hat{y}_1) + e \cdot S + h_2(\hat{y}_2) + h_3(\hat{y}_3)$ |

| Lattices | Ring Signatures | Signature Scheme [Lyu09] | Our Construction |
|-----------|-----------------|--------------------------|------------------|
| oo | | oo | oooooo●o |
| Contribut | tions | | |

More efficient scheme

Unforgeability in the insider corruption setting

> proof that works even if the ring is of polynomial size .

We present a modification which can be applied to other schemes to provide the unforgeability in the insider corruption setting.

Anonymity against chosen setting attacks

Lattices

Ring Signatures

Signature Scheme [Lyu09]

Our Construction

Thanks !

