Towards Tightly Secure Lattice Short Signature and Id-Based Encryption

Xavier Boyen Qinyi Li

QUT

Asiacrypt'16

2016-12-06

Queensland University of Technology
Brisbane Australia

Motivations

1. **Short** lattice signature with **tight** security reduction w/o ROs.

Techniques	Short Sig?	Tight Reduction?
Lattice Mixing [Boy'10]	✔	✘
Prefix Guessing [MP'12]	✔	✘
Confined Guessing [BHJ+'13]	✔	✘
Two-Tier Sig [BKKP'15]	✘	✔

2. Adaptively and **tightly** secure lattice IBE w/o. ROs.

Techniques	Tight Reduction?
Admissible Hash [CHKP'12]	✘
Lattice Mixing [ABB'10]	✘
Programmable Hash [ZCZ'16]	✘

Tight Security Reductions

Theorem (template)

If an adversary $\mathcal{A}$ (t, ϵ)-breaks the scheme Π in the defined security model, there exists an algorithm $\mathcal{B}$ that (t', ϵ')-breaks some computation problem P where $\epsilon' = \epsilon/\theta$ and $t' = t + o(t)$ for $\theta \geq 1$.

- θ measures tightness of reductions.
- Security parameter λ, number of adversarial queries Q
  - Tight reduction: $\theta = O(1)$;
  - Almost tight reduction: $\theta = \text{poly}(\lambda)$;
  - Lose reduction: $\theta = \text{poly}(Q)$.
- Why tight reductions?
  - In practice: a tighter reduction allows shorter security parameters and, thus, higher efficiency.
  - In theory: a tight reduction shows hardness of two computational problems is close.

Our results

Fully, tightly secure short signature/IBE schemes w/o. RO from SIS/LWE assumption and a secure pseudorandom function (PRF).

- ϵ_{PRF} be the security level of a concrete PRF.
- ϵ, ϵ' be security levels of our signature scheme and IBE scheme.
- ϵ_{LWE}, ϵ_{SIS} be the security levels of $\mathsf{LWE}_{n,q,\alpha}$ and $\mathsf{SIS}_{n,q,\beta}$.

$$\epsilon_{\mathsf{SIS}} + \epsilon_{\mathsf{PRF}} \approx \epsilon/2 \quad ; \quad \epsilon_{\mathsf{LWE}} + \epsilon_{\mathsf{PRF}} \approx \epsilon'/2$$

Digital Signatures

Algorithm:

- $(\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$
- $\mathsf{Ver}(\mathsf{vk}, m, \sigma) = \begin{cases} 1 & \text{accept} \\ 0 & \text{reject} \end{cases}$

Correctness:

- $\forall (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

  $\mathsf{Ver}\left(\mathsf{vk}, m, \mathsf{Sign}(\mathsf{sk}, m)\right) = 1$

Security Model:

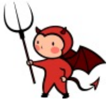
$(\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}, m_i)$

$\xrightarrow{\mathsf{vk}}$

$\xleftarrow{m_1, \ldots, m_Q}$

$\xrightarrow{\sigma_1, \ldots, \sigma_Q}$



Outputs (m^*, σ^*)

Wins if $m^* \neq m_i$

& $\mathsf{Ver}(\mathsf{vk}, m^*, \sigma^*) = 1$

Our Method

We non-trivially combine the following techniques (from different contexts):

- Katz-Wang's magic bit for tightly secure (full-domain hash) signatures. [KW'03]
- Two-sided lattice trapdoors. [GPV'08,ABB'10,Boy'10,MP'12]
- Boyen's short lattice signature (in the plain model). [Boy'10]
- GSW-FHE/Fully key-homomorphic encryption. [GSW'13,BGG+14]

Katz-Wang's Magic Bit [KW'03]

- An unpredictable bit $b_m \in \{0,1\}$ associated with every $m \in \mathcal{M}$: e.g. generated by a Pseudorandom Function (PRF)

$$b_m = \mathrm{PRF}(K, m)$$

Katz-Wang's Magic Bit [KW'03]

- An unpredictable bit $b_m \in \{0,1\}$ associated with every $m \in \mathcal{M}$: e.g. generated by a Pseudorandom Function (PRF)

$$b_m = \mathrm{PRF}(K, m)$$

- In real schemes:
  - Each m has *two* signatures: σ_b and σ_{1-b} for $b \in \{0,1\}$;
  - Signer can produce both;
  - Only *one* of them is issued.

Katz-Wang's Magic Bit [KW'03]

- An unpredictable bit $b_m \in \{0,1\}$ associated with every $m \in \mathcal{M}$: e.g. generated by a Pseudorandom Function (PRF)

$$b_m = \mathsf{PRF}(K, m)$$

- In real schemes:
  - Each m has *two* signatures: σ_b and σ_{1-b} for $b \in \{0,1\}$;
  - Signer can produce both;
  - Only *one* of them is issued.
- In security proofs:

  Query Simulator can create σ_{b_m} for m, but not σ_{1-b_m}.
  (All queries can be answered.)

  Forgery Simulator can solve problem for forgery $(m^*, \sigma_{1-b_{m^*}})$, but fails for $(m^*, \sigma_{b_{m^*}})$.
  (Adversary chooses correctly with prob. $\approx 1/2$.)

Short Integer Solution (SIS) Problem and Trapdoors

Definition

Let $q, n \geq 2$, $m = O(n \log q)$ and $\beta > 0$. Given random $A \in \mathbb{Z}_q^{n \times m}$ find a non-zero "short" vector $\sigma \in \mathbb{Z}^m$, where $\|\sigma\| \leq \beta$, such that

$$A\sigma \equiv 0 \pmod{q}$$

Short Integer Solution (SIS) Problem and Trapdoors

Definition

Let $q, n \geq 2$, $m = O(n \log q)$ and $\beta > 0$. Given random $A \in \mathbb{Z}_q^{n \times m}$ find a non-zero "short" vector $\sigma \in \mathbb{Z}^m$, where $\|\sigma\| \leq \beta$, such that

$$A\sigma \equiv 0 \pmod{q}$$

- Hard without Trapdoor: If A is chosen randomly, finding a solution $x \neq 0$ enables solving GapSVP problem with approximation factor $\approx \beta \cdot \sqrt{n}$ on any n-dimensional lattice.

Short Integer Solution (SIS) Problem and Trapdoors

Definition

Let $q, n \geq 2$, $m = O(n \log q)$ and $\beta > 0$. Given random $A \in \mathbb{Z}_q^{n \times m}$ find a non-zero "short" vector $\sigma \in \mathbb{Z}^m$, where $\|\sigma\| \leq \beta$, such that

$$A\sigma \equiv 0 \pmod{q}$$

- Hard without Trapdoor: If A is chosen randomly, finding a solution $x \neq 0$ enables solving GapSVP problem with approximation factor $\approx \beta \cdot \sqrt{n}$ on any n-dimensional lattice.
- Easy with Trapdoor: There is an algorithm TrapGen that generates a nearly random A and a trapdoor T. Using T one can find a "short", non-zero solution.

Short Integer Solution (SIS) Problem and Trapdoors

Definition

Let $q, n \geq 2$, $m = O(n \log q)$ and $\beta > 0$. Given random $A \in \mathbb{Z}_q^{n \times m}$ find a non-zero "short" vector $\sigma \in \mathbb{Z}^m$, where $\|\sigma\| \leq \beta$, such that

$$A\sigma \equiv 0 \pmod q$$

- Hard without Trapdoor: If A is chosen randomly, finding a solution $x \neq 0$ enables solving GapSVP problem with approximation factor $\approx \beta \cdot \sqrt{n}$ on any n-dimensional lattice.
- Easy with Trapdoor: There is an algorithm TrapGen that generates a nearly random A and a trapdoor T. Using T one can find a "short", non-zero solution.
- GPV-Style Signature Schemes [GPV'08]

Short Integer Solution (SIS) Problem and Trapdoors

Definition

Let $q, n \geq 2$, $m = O(n \log q)$ and $\beta > 0$. Given random $A \in \mathbb{Z}_q^{n \times m}$ find a non-zero "short" vector $\sigma \in \mathbb{Z}^m$, where $\|\sigma\| \leq \beta$, such that

$$A\sigma \equiv 0 \pmod{q}$$

- Hard without Trapdoor: If A is chosen randomly, finding a solution $x \neq 0$ enables solving GapSVP problem with approximation factor $\approx \beta \cdot \sqrt{n}$ on any n-dimensional lattice.
- Easy with Trapdoor: There is an algorithm TrapGen that generates a nearly random A and a trapdoor T. Using T one can find a "short", non-zero solution.
- GPV-Style Signature Schemes [GPV'08]
  - A trapdoor T serves as a signing key;

Short Integer Solution (SIS) Problem and Trapdoors

Definition

Let $q, n \geq 2$, $m = O(n \log q)$ and $\beta > 0$. Given random $A \in \mathbb{Z}_q^{n \times m}$ find a non-zero "short" vector $\sigma \in \mathbb{Z}^m$, where $\|\sigma\| \leq \beta$, such that

$$A\sigma \equiv 0 \pmod q$$

- Hard without Trapdoor: If A is chosen randomly, finding a solution $x \neq 0$ enables solving GapSVP problem with approximation factor $\approx \beta \cdot \sqrt{n}$ on any n-dimensional lattice.
- Easy with Trapdoor: There is an algorithm TrapGen that generates a nearly random A and a trapdoor T. Using T one can find a "short", non-zero solution.
- GPV-Style Signature Schemes [GPV'08]
    - A trapdoor T serves as a signing key;
    - A valid solution σ serves as a signature.

Two-Sided Lattice Trapdoors [ABB'10,Boy'10,MP'12]

Two-Sided Lattice Trapdoors [ABB'10,Boy'10,MP'12]

Two-Sided Trapdoor

Let $q, n \geq 2$, $m = O(n \log q)$, $A, G \in \mathbb{Z}_q^{n \times m}$-matrix, secret low-norm $R \in \mathbb{Z}^{m \times m}$, publicly known trapdoor for G, and $h \in \mathbb{Z}_q$. Set

$$F = [A | AR + hG] \bmod q$$

Two-Sided Lattice Trapdoors [ABB'10,Boy'10,MP'12]

Two-Sided Trapdoor

Let $q, n \geq 2$, $m = O(n \log q)$, $A, G \in \mathbb{Z}_q^{n \times m}$-matrix, secret low-norm $R \in \mathbb{Z}^{m \times m}$, publicly known trapdoor for G, and $h \in \mathbb{Z}_q$. Set

$$F = [A | AR + hG] \bmod q$$

- ▷ Left trapdoor for *real schemes*:
  - If A has a trapdoor, F has a trapdoor for any h.
- ▷ Right trapdoor for *proofs*:
  - $h \neq 0$: "right" trapdoor is (R, hG)
    - Generate signatures for F.
  - $h = 0$: no trapdoor
    - Can not generate signatures.
    - A signature for F results in a SIS solution for A.

Boyen's Signature [Boy'10]

- KeyGen(1^λ)
  - vk: random $\mathbb{Z}_q^{n\times m}$-matrices $A, A_0, A_1, \ldots, A_\ell$;
  - sk: A's trapdoor T.
- Sign(sk, m)
  - $m \in \{0,1\}^\ell$; m's i-th bit is m_i;
  - Uses "left" trapdoor T to find a "short" solution σ s.t.

$$F\sigma = \left[A | A_0 + \sum_{i=1}^{\ell} m_i A_i\right] \sigma = 0 \pmod q$$

- Ver(vk, σ, m)
  - Check if σ is "short" and non-zero;
  - Check if $F\sigma = 0$.

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A | AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i) G] \\ &= [A | AR_m + H(m) G] \end{aligned}$$

R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i) G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A|AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G] \\ &= [A|AR_m + H(m)G] \end{aligned}$$

  R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A|AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G] \\ &= [A|AR_m + H(m)G] \end{aligned}$$

  R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:
  $H(m) = 0$ Forgeries of m allows SIS solutions;

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A|AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G] \\ &= [A|AR_m + H(m)G] \end{aligned}$$

  R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:
  $H(m) = 0$ Forgeries of m allows SIS solutions;
  $H(m) \neq 0$ Generate signatures using "right" trapdoor.

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A|AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G] \\ &= [A|AR_m + H(m)G] \end{aligned}$$

R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:
  $H(m) = 0$ Forgeries of m allows SIS solutions;
  $H(m) \neq 0$ Generate signatures using "right" trapdoor.
- Simulator *hopes*:

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A|AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G] \\ &= [A|AR_m + H(m)G] \end{aligned}$$

R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:
  - $H(m) = 0$ Forgeries of m allows SIS solutions;
  - $H(m) \neq 0$ Generate signatures using "right" trapdoor.
- Simulator *hopes*:
  - For *all* Q queries: $H(m) \neq 0 \pmod q$, happens with prob. $(1 - 1/q)^Q$.

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \dots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A | AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i) G] \\ &= [A | AR_m + H(m) G] \end{aligned}$$

  R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i) G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:
  - $H(m) = 0$ Forgeries of m allows SIS solutions;
  - $H(m) \neq 0$ Generate signatures using "right" trapdoor.
- Simulator *hopes*:
  - For *all* Q queries: $H(m) \neq 0 \pmod q$, happens with prob. $(1 - 1/q)^Q$.
  - For forgery (σ, m): $H(m) = 0 \pmod q$, happens with prob. $1/q$.

Proof Idea of Boyen's Signature

- A is a SIS challenge. Let $h_1, \ldots, h_\ell \in \mathbb{Z}_q$ be secret. For any querying message $m \in \{0,1\}^\ell$, set

$$\begin{aligned} F &= [A|AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G] \\ &= [A|AR_m + H(m)G] \end{aligned}$$

R_m depends on m and is "short", and

$$AR_m + (1 + \Sigma_{i=1}^{\ell} m_i h_i)G \approx_s A_0 + \Sigma_{i=1}^{\ell} m_i A_i$$

- Apply the principle of two-sided trapdoor:

  $H(m) = 0$ Forgeries of m allows SIS solutions;

  $H(m) \neq 0$ Generate signatures using "right" trapdoor.

- Simulator *hopes*:
  - For *all* Q queries: $H(m) \neq 0 \pmod q$, happens with prob. $(1 - 1/q)^Q$.
  - For forgery (σ, m): $H(m) = 0 \pmod q$, happens with prob. $1/q$.
  - Gives a loose reduction: $\theta \approx \left((1 - 1/q)^Q \cdot 1/q\right)^{-1} = \mathrm{poly}(Q)$.

Magic Bit b_m Comes to Play

Magic Bit b_m Comes to Play

Our Idea

$b \in \{0,1\}$, $b_m = \mathrm{PRF}(K, m)$, "short" matrices R_m, R'_m. Replace $H(m)$ by $1 - b - b_m \in \{0,1\}$. Set (simulated) vk:

$$F_b = [A|AR_m + (1 - b - b_m)G]$$

$$F_{1-b} = [A|AR'_m + (b - b_m)G]$$

Magic Bit b_m Comes to Play

Our Idea

$b \in \{0,1\}$, $b_m = \mathrm{PRF}(K, m)$, "short" matrices R_m, R'_m. Replace $H(m)$ by $1 - b - b_m \in \{0,1\}$. Set (simulated) vk:

$$F_b = [A | AR_m + (1 - b - b_m)G]$$

$$F_{1-b} = [A | AR'_m + (b - b_m)G]$$

As required by Katz-Wang proof:

Magic Bit b_m Comes to Play

Our Idea

$b \in \{0,1\}$, $b_m = \mathrm{PRF}(K, m)$, "short" matrices R_m, R'_m. Replace $H(m)$ by $1 - b - b_m \in \{0,1\}$. Set (simulated) vk:

$$F_b = [A|AR_m + (1 - b - b_m)G]$$

$$F_{1-b} = [A|AR'_m + (b - b_m)G]$$

As required by Katz-Wang proof:

- ▷ Generating only "one" signature: σ_{b_m} from F_{b_m}:
  - Can not produce σ_{1-b_m} since F_{1-b_m} looses trapdoor;
  - Allows answering all signing queries.

Magic Bit b_m Comes to Play

Our Idea

$b \in \{0,1\}$, $b_m = \mathrm{PRF}(K, m)$, "short" matrices R_m, R'_m. Replace $H(m)$ by $1 - b - b_m \in \{0,1\}$. Set (simulated) vk:

$$F_b = [A | AR_m + (1 - b - b_m)G]$$

$$F_{1-b} = [A | AR'_m + (b - b_m)G]$$

As required by Katz-Wang proof:

- ▷ Generating only "one" signature: σ_{b_m} from F_{b_m}:
  - Can not produce σ_{1-b_m} since F_{1-b_m} looses trapdoor;
  - Allows answering all signing queries.
- ▷ "Two" valid signatures for m^*.
  - Forgery (σ^*, m^*): $\sigma^* = \begin{cases} \sigma_{b_{m^*}} & \text{Fail} \\ \sigma_{1-b_{m^*}} & \text{Solve SIS} \end{cases}$
  - $b_{m^*} = \mathrm{PRF}(K, m^*)$ is unpredictable. With prob. $\approx 1/2$, solve SIS.

Embedding PRF into F_b

- Magic bit $b_m = \mathrm{PRF}(K, m)$. For public message m and secret K, we need to somehow create

$$AR_m + \mathrm{PRF}(K, m)G$$

Embedding PRF into F_b

- Magic bit $b_m = \mathrm{PRF}(K, m)$. For public message m and secret K, we need to somehow create

$$AR_m + \mathrm{PRF}(K, m)G$$

- $\mathrm{PRF}(\cdot, \cdot)$ can be expressed as a small-depth Boolean circuit:

$$C_{\mathrm{PRF}} : \{0,1\}^{|K|} \times \{0,1\}^{|m|} \to \{0,1\}$$

Embedding PRF into F_b

- Magic bit $b_m = \mathrm{PRF}(K, m)$. For public message m and secret K, we need to somehow create

$$AR_m + \mathrm{PRF}(K, m)G$$

- $\mathrm{PRF}(\cdot, \cdot)$ can be expressed as a small-depth Boolean circuit:

$$C_{\mathrm{PRF}} : \{0,1\}^{|K|} \times \{0,1\}^{|m|} \to \{0,1\}$$

- $AR_m + \mathrm{PRF}(K, m)G$ is a ciphertext of FHE [GSW13]/ public key of fully key-homomorphic encryption [BGG+14].

Embedding PRF into F_b (cont.)

- Let $g(u, v) = w$ be a logical gate. Using evaluation algorithm of GSW-FHE/fully key-homomorphic encryption, given

$$A_u = AR_u + uG \quad ; \quad A_v = AR_v + vG$$

one can *deterministically* compute unique matrix $A_w = AR_w + wG$.

Embedding PRF into F_b (cont.)

- Let $g(u, v) = w$ be a logical gate. Using evaluation algorithm of GSW-FHE/fully key-homomorphic encryption, given

$$A_u = AR_u + uG \quad ; \quad A_v = AR_v + vG$$

one can *deterministically* compute unique matrix $A_w = AR_w + wG$.

- We "encrypt" PRF key $K = k_1 k_2, \ldots, k_t \in \{0, 1\}^t$ as

$$B_{k_i} = AR_{k_i} + k_i G$$

Embedding PRF into F_b (cont.)

- Let $g(u, v) = w$ be a logical gate. Using evaluation algorithm of GSW-FHE/fully key-homomorphic encryption, given

$$A_u = AR_u + uG \quad ; \quad A_v = AR_v + vG$$

one can *deterministically* compute unique matrix $A_w = AR_w + wG$.

- We "encrypt" PRF key $K = k_1 k_2, \ldots, k_t \in \{0, 1\}^t$ as

$$B_{k_i} = AR_{k_i} + k_i G$$

- We "encrypt" message bit m_i by $C_{m_i} = AR_{m_i} + m_i G$.

Embedding PRF into F_b (cont.)

- Let $g(u, v) = w$ be a logical gate. Using evaluation algorithm of GSW-FHE/fully key-homomorphic encryption, given

$$A_u = AR_u + uG \quad ; \quad A_v = AR_v + vG$$

  one can *deterministically* compute unique matrix $A_w = AR_w + wG$.
- We "encrypt" PRF key $K = k_1 k_2, \ldots, k_t \in \{0, 1\}^t$ as

$$B_{k_i} = AR_{k_i} + k_i G$$

- We "encrypt" message bit m_i by $C_{m_i} = AR_{m_i} + m_i G$.
- Using $B_{k_1}, \ldots, B_{k_t}$ and $C_{m_1}, \ldots, C_{m_\ell}$ and circuit C_{PRF},

$$A_{\mathrm{PRF},K,m} = AR_m + \mathrm{PRF}(K, m)G$$

  is publicly computable.

Our Signature Scheme

- KeyGen$(1^\lambda) \to (\mathsf{vk}, \mathsf{sk})$:

$$\mathsf{vk} = (C_{\mathsf{PRF}}, A, A_0, A_1, B_{k_1}, \ldots, B_{k_t}, C_0, C_1)\,;\mathsf{sk} = (T_A, K)$$

- Sign$(\mathsf{sk}, m) \to \sigma$
  - Set $b_m = \mathsf{PRF}(K, m)$;
  - Evaluating $A_{\mathsf{PRF},K,m} = \mathsf{Eval}(C_{\mathsf{PRF}}, A_{k_1}, \ldots, A_{k_t}, C_{m_1}, \ldots, C_{m_\ell})$;
  - Set $F_{b_m} = [A | A_{1-b_m} - A_{\mathsf{PRF},K,m}]$ and use T_A to output $\sigma = \sigma_{b_m}$ s.t.

$$F_{b_m} \cdot \sigma = 0 \pmod q$$

- Ver$(\mathsf{vk}, m, \sigma) \to 0/1$
  - Check if σ is small and non-zero;
  - Check if $F_0 \cdot \sigma = 0 \pmod q$ or $F_1 \cdot \sigma = 0 \pmod q$

⋆ Using T_A, one can generate signatures for F_{b_m} and F_{1-b_m}. But only "one" of them is issued.

An IBE Scheme

Our signature is "Hash-and-Sign" signature. Following ideas of [GPV08,ABB10,Boy10], we obtain an IBE scheme.

An IBE Scheme

Our signature is "Hash-and-Sign" signature. Following ideas of [GPV08,ABB10,Boy10], we obtain an IBE scheme.

- $\mathsf{KeyGen}(\mathsf{Msk}, \mathsf{id})$ There are "two" keys for one identity. We only give "one" identity key $\mathsf{sk}_{\mathsf{id}, b_{\mathsf{id}}}$ for $F_{b_{\mathsf{id}}}$, which is similar to our signature scheme.

An IBE Scheme

Our signature is "Hash-and-Sign" signature. Following ideas of [GPV08,ABB10,Boy10], we obtain an IBE scheme.

- KeyGen(Msk, id) There are "two" keys for one identity. We only give "one" identity key $\mathsf{sk}_{\mathsf{id},b_{\mathsf{id}}}$ for $F_{b_{\mathsf{id}}}$, which is similar to our signature scheme.
- Encrypt(Pub, id, Msg) We give two "dual-Regev" ciphrtexts for F_0, F_1

$$\mathsf{Ctx}_0 = s_0^\top \cdot F_0 + e_0^\top = s_0^\top [A|A_1 + A_{\mathsf{PRF},K,\mathsf{id}}] + e_0^\top$$

$$\mathsf{Ctx}_1 = s_1^\top \cdot F_1 + e_1^\top = s_1^\top [A|A_0 + A_{\mathsf{PRF},K,\mathsf{id}}] + e_1^\top$$

with adjusted noise vectors e_0, e_1.

An IBE Scheme

Our signature is "Hash-and-Sign" signature. Following ideas of [GPV08,ABB10,Boy10], we obtain an IBE scheme.

- KeyGen(Msk, id) There are "two" keys for one identity. We only give "one" identity key $\mathsf{sk}_{\mathsf{id},b_{\mathsf{id}}}$ for $F_{b_{\mathsf{id}}}$, which is similar to our signature scheme.
- Encrypt(Pub, id, Msg) We give two "dual-Regev" ciphrtexts for F_0, F_1

$$\mathsf{Ctx}_0 = s_0^\top \cdot F_0 + e_0^\top = s_0^\top [A | A_1 + A_{\mathsf{PRF},K,\mathsf{id}}] + e_0^\top$$

$$\mathsf{Ctx}_1 = s_1^\top \cdot F_1 + e_1^\top = s_1^\top [A | A_0 + A_{\mathsf{PRF},K,\mathsf{id}}] + e_1^\top$$

  with adjusted noise vectors e_0, e_1.
- Decrypt($\mathsf{sk}_{\mathsf{id}}$, Ctx) Decryptor uses $\mathsf{sk}_{\mathsf{id}}$ to try both ciphertexts.

Caveats

- ⋆ Katz-Wang uses PRFs for making signing stateless.
- ⋆ The state-of-art lattice-based PRFs, e.g. [BPR'12,BP'14], require slightly stronger LWE assumptions.
- ⋆ Want an efficient IBE scheme w/o ROs now? Pick selectively secure schemes and do "complexity leveraging" [BB'04,BB'11].
  - ⋆⋆ DO take "leveraging slack" into account setting parameters!
  - ⋆⋆ Still more efficient than native adaptive security (usually)

Conclusion

- We proposed a lattice-based signature/IBE scheme with tight security reduction in the plain model, through a non-trivial combination of the following techniques coming from different contexts:
  - Katz-Wang's tightly secure Full-Domain Hash signatures in the Random Oracle model.
  - Two-sided lattice trapdoor techniques and Boyen's lattice signature.
  - GSW-FHE/fully key-homomorphic encryption for fully homomorphic encryption and attribute-based encryption for circuits.
- Our signature scheme has both tight security reduction and short signatures.
- Our IBE scheme archives tight security and unbounded collusion in the plain model for the first time among other lattice-based IBE schemes.

Thank you!

Queensland University of Technology
Brisbane Australia