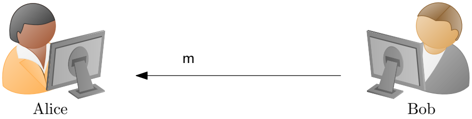
Short Identity-Based Signatures with Tight Security from Lattices

Jiaxin Pan NTNU

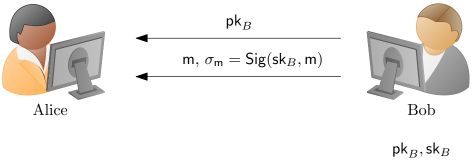
Benedikt Wagner KIT Karlsruhe Institute of Technology

Digital Signatures in Practice

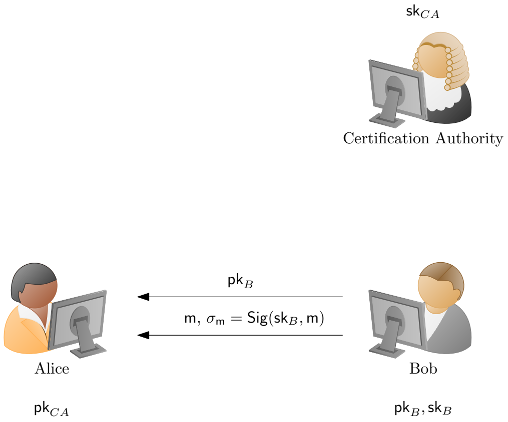
Digital Signatures in Practice



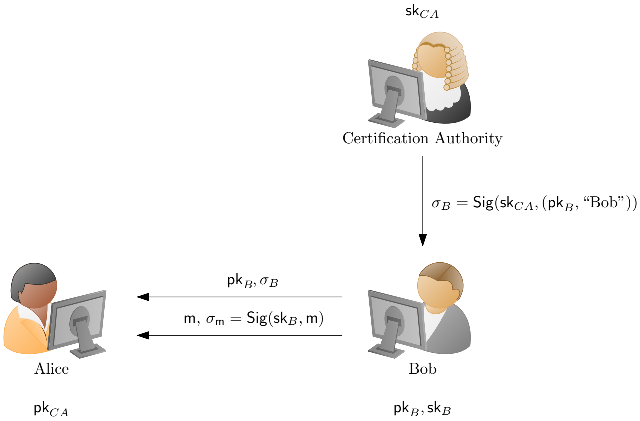
Digital Signatures in Practice



Digital Signatures in Practice



Digital Signatures in Practice



Identity-Based Signatures

$\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sig}, \mathsf{Ver})$

Identity-Based Signatures

$\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sig}, \mathsf{Ver})$

- $\mathsf{Setup}(1^\lambda) \rightarrow (\mathsf{mpk}, \mathsf{msk})$

Identity-Based Signatures

$\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sig}, \mathsf{Ver})$

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$

Identity-Based Signatures

$\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sig}, \mathsf{Ver})$

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Sig}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m}) \to \sigma$

Identity-Based Signatures

$\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sig}, \mathsf{Ver})$

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Sig}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m}) \to \sigma$
- $\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma) \to b$

Identity-Based Signatures

$\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyExt}, \mathsf{Sig}, \mathsf{Ver})$

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Sig}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m}) \to \sigma$
- $\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma) \to b$

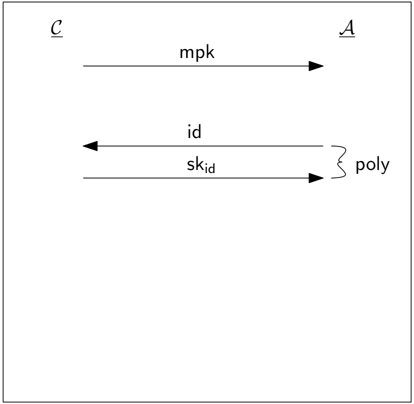
$$\underline{\mathcal{C}} \qquad \qquad \underline{\mathcal{A}}$$

$$\xrightarrow{\quad\quad\mathsf{mpk}\quad\quad}$$

Identity-Based Signatures

IBS = (Setup, KeyExt, Sig, Ver)

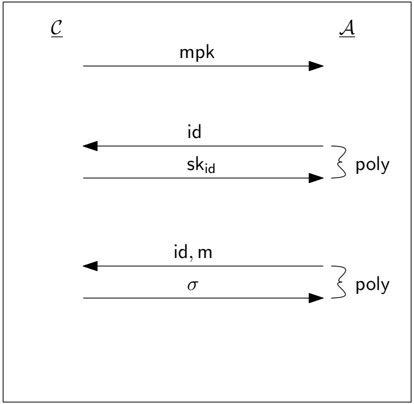
- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Sig}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m}) \to \sigma$
- $\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma) \to b$



Identity-Based Signatures

IBS = (Setup, KeyExt, Sig, Ver)

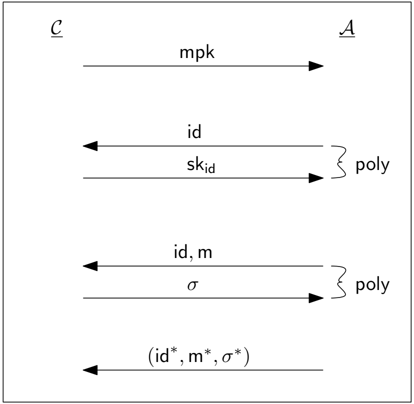
- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Sig}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m}) \to \sigma$
- $\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma) \to b$



Identity-Based Signatures

IBS = (Setup, KeyExt, Sig, Ver)

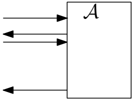
- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyExt}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Sig}(\mathsf{sk}_{\mathsf{id}}, \mathsf{m}) \to \sigma$
- $\mathsf{Ver}(\mathsf{mpk}, \mathsf{id}, \mathsf{m}, \sigma) \to b$



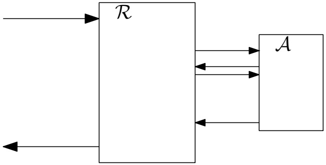
$\mathcal{A}$ wins iff id^* fresh $\wedge(\mathsf{id}^*, \mathsf{m}^*)$ fresh $\wedge \mathsf{Ver}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{m}^*, \sigma^*)$

The Typical Proof Strategy

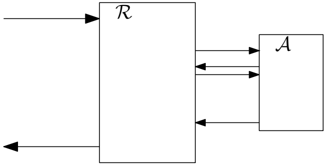
The Typical Proof Strategy



The Typical Proof Strategy



The Typical Proof Strategy

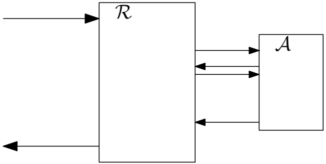


$\mathcal{A}$ breaks IBS with probability $\epsilon_{\mathcal{A}}$

$\implies$ $\mathcal{R}$ solves Π with probability $\epsilon_{\mathcal{R}}$

with $\epsilon_{\mathcal{A}} \leq L \cdot \epsilon_{\mathcal{R}}$

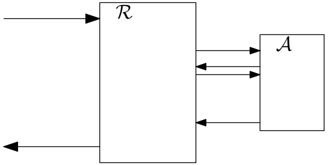
The Typical Proof Strategy



$\mathcal{A}$ breaks IBS with probability $\epsilon_{\mathcal{A}}$
$\Longrightarrow$ $\mathcal{R}$ solves Π with probability $\epsilon_{\mathcal{R}}$
with $\epsilon_{\mathcal{A}} \leq L \cdot \epsilon_{\mathcal{R}}$

- Asymptotically: Any $L = \text{poly}(n)$ sufficient.

The Typical Proof Strategy



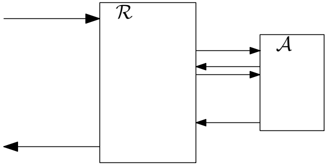
$\mathcal{A}$ breaks IBS with probability $\epsilon_{\mathcal{A}}$

$\Longrightarrow$ $\mathcal{R}$ solves Π with probability $\epsilon_{\mathcal{R}}$

with $\epsilon_{\mathcal{A}} \leq L \cdot \epsilon_{\mathcal{R}}$

- Asymptotically: Any $L = \text{poly}(n)$ sufficient.
- Concrete Instantiation: Need to pay $\log(L)$ bits of security.

The Typical Proof Strategy



$\mathcal{A}$ breaks IBS with probability $\epsilon_{\mathcal{A}}$
$\implies$ $\mathcal{R}$ solves Π with probability $\epsilon_{\mathcal{R}}$
with $\epsilon_{\mathcal{A}} \leq L \cdot \epsilon_{\mathcal{R}}$

- Asymptotically: Any $L = \text{poly}(n)$ sufficient.
- Concrete Instantiation: Need to pay $\log(L)$ bits of security.

Tightness

We say the reduction is tight, iff the loss L is a small constant.

Our Goal: IBS in the lattice setting

Our Goal: IBS in the lattice setting

Security

- adaptive security

Our Goal: IBS in the lattice setting

Security

- adaptive security
- lattice-based assumptions

Our Goal: IBS in the lattice setting

Security

- adaptive security
- lattice-based assumptions

Efficiency

- tight reduction

Our Goal: IBS in the lattice setting

Security

- adaptive security
- lattice-based assumptions

Efficiency

- tight reduction
- small signature sizes: $\tilde{O}(n)$, i.e. $\mathbb{Z}_q$ vector

Our Goal: IBS in the lattice setting

Security

- adaptive security
- lattice-based assumptions

Efficiency

- tight reduction
- small signature sizes: $\tilde{O}(n)$, i.e. $\mathbb{Z}_q$ vector

$\Longrightarrow$ **avoid certification approach**

Drawbacks of Existing Constructions

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]
  - generically non-tight

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]
  - generically non-tight
  - tight improvement [LPLL20, TCS] requires signature in presence of adaptive corruptions

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]
  - generically non-tight
  - tight improvement [LPLL20, TCS] requires signature in presence of adaptive corruptions
  - based on SIS: signature size $\tilde{O}(n^2)$

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]
  - generically non-tight
  - tight improvement [LPLL20, TCS] requires signature in presence of adaptive corruptions
  - based on SIS: signature size $\tilde{O}(n^2)$
- Construction from 2-level HIBE [GS02, AC]

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]
  - generically non-tight
  - tight improvement [LPLL20, TCS] requires signature in presence of adaptive corruptions
  - based on SIS: signature size $\tilde{O}(n^2)$
- Construction from 2-level HIBE [GS02, AC]
  - tight

Drawbacks of Existing Constructions

- Certification Approach [DKXY03, PKC], [BNN04, EC]
  - generically non-tight
  - tight improvement [LPLL20, TCS] requires signature in presence of adaptive corruptions
  - based on SIS: signature size $\tilde{O}(n^2)$
- Construction from 2-level HIBE [GS02, AC]
  - tight
  - we do not know tight 2-level HIBE from lattices

Overview

SIS

Given: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

Find: short $\mathbf{x} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}$

such that $\mathbf{A}\mathbf{x} = \mathbf{0}$

Overview

$$\mathsf{SIS} \xrightarrow{\text{ROM}} \underset{\text{}}{\overset{\text{non-adaptively secure}}{\mathsf{IBS}}}$$

<u>Given:</u> $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

<u>Find:</u> short $\mathbf{x} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}$

such that $\mathbf{Ax} = \mathbf{0}$

Overview

$$\text{SIS} \xrightarrow{\text{ROM}} \underset{\text{IBS}}{\text{non-adaptively secure}} \xrightarrow{\text{Chameleon Hash} \vee \text{ROM}} \underset{\text{IBS}}{\text{adaptively secure}}$$

Given: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

Find: short $\mathbf{x} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}$
such that $\mathbf{A}\mathbf{x} = \mathbf{0}$

Prerequisite: Lattice Trapdoors [MP12, EC]

Prerequisite: Lattice Trapdoors [MP12, EC]

- "Gadget" matrix $\mathbf{G}$
  - easy to solve SIS with respect to $\mathbf{G}$
  - fixed and publicly known

Prerequisite: Lattice Trapdoors [MP12, EC]

- "Gadget" matrix $\mathbf{G}$
  - easy to solve SIS with respect to $\mathbf{G}$
  - fixed and publicly known
- Trapdoor for matrix $\mathbf{A}$ is a short matrix $\mathbf{R}$ such that

$$\mathbf{A} = [\bar{\mathbf{A}} \mid \bar{\mathbf{A}}\mathbf{R} + \mathbf{G}].$$

Prerequisite: Lattice Trapdoors [MP12, EC]

- "Gadget" matrix $\mathbf{G}$
  - easy to solve SIS with respect to $\mathbf{G}$
  - fixed and publicly known
- Trapdoor for matrix $\mathbf{A}$ is a short matrix $\mathbf{R}$ such that

$$\mathbf{A} = [\bar{\mathbf{A}} \mid \bar{\mathbf{A}}\mathbf{R} + \mathbf{G}].$$

  - allows to solve SIS with respect to $\mathbf{A}$

Prerequisite: Lattice Trapdoors [MP12, EC]

- "Gadget" matrix $\mathbf{G}$
  - easy to solve SIS with respect to $\mathbf{G}$
  - fixed and publicly known
- Trapdoor for matrix $\mathbf{A}$ is a short matrix $\mathbf{R}$ such that

$$\mathbf{A} = [\bar{\mathbf{A}} \mid \bar{\mathbf{A}}\mathbf{R} + \mathbf{G}].$$

  - allows to solve SIS with respect to $\mathbf{A}$
  - allows to derive trapdoor for any extension $[\mathbf{A} \mid \mathbf{B}]$

Non-adaptive Security from SIS - Construction

$\mathsf{mpk} = \mathbf{A} \in \mathbb{Z}_q^{n \times m}$

Non-adaptive Security from SIS - Construction

$\mathsf{mpk} = \mathbf{A} \in \mathbb{Z}_q^{n \times m}$

$\mathsf{msk} = \mathbf{T}$: trapdoor for $\mathbf{A}$

Non-adaptive Security from SIS - Construction

$\mathsf{mpk} = \mathbf{A} \in \mathbb{Z}_q^{n \times m}$ $\longrightarrow$ $\mathbf{F}_{\mathsf{id}} = [\mathbf{A} \mid H_1(\mathsf{mpk}, \mathsf{id})]$

$\mathsf{msk} = \mathbf{T}$: trapdoor for $\mathbf{A}$ $\longrightarrow$ $\mathsf{sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}$: trapdoor for $\mathbf{F}_{\mathsf{id}}$

Non-adaptive Security from SIS - Construction

$$\begin{array}{ccc}
\mathsf{mpk} = \mathbf{A} \in \mathbb{Z}_q^{n\times m} & & \mathsf{msk} = \mathbf{T}\text{: trapdoor for } \mathbf{A} \\
\downarrow & & \downarrow \\
\mathbf{F}_{\mathsf{id}} = [\mathbf{A} \mid H_1(\mathsf{mpk}, \mathsf{id})] & & \mathsf{sk}_{\mathsf{id}} = \mathbf{T}_{\mathsf{id}}\text{: trapdoor for } \mathbf{F}_{\mathsf{id}} \\
\downarrow & & \downarrow \\
\mathbf{F}_{\mathsf{id},\mathsf{m}} = [\mathbf{A} \mid H_1(\mathsf{mpk}, \mathsf{id}) \mid H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m})] & & \sigma = \mathbf{z} \text{ short s. t. } \mathbf{F}_{\mathsf{id},\mathsf{m}}\mathbf{z} = \mathbf{0}
\end{array}$$

Non-adaptive Security from SIS - Proof

Non-adaptive Security from SIS - Proof

$\underline{\mathcal{C}}$ $\underline{\mathcal{R}}$ $\underline{\mathcal{A}}$

$$\xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}}$$

Non-adaptive Security from SIS - Proof

$\underline{\mathcal{C}}$ $\underline{\mathcal{R}}$ $\underline{\mathcal{A}}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$

Non-adaptive Security from SIS - Proof

$\underline{\mathcal{C}}$ $\qquad$ $\underline{\mathcal{R}}$ $\qquad$ $\underline{\mathcal{A}}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

Non-adaptive Security from SIS - Proof

$\underline{\mathcal{C}}$ $\xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}}$ $\underline{\mathcal{R}}$ $\xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)}$ $\underline{\mathcal{A}}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

Non-adaptive Security from SIS - Proof

$$\underline{\mathcal{C}} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \qquad \underline{\mathcal{R}} \qquad \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \underline{\mathcal{A}}$$

$$\xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L}$$

$$\xrightarrow{\mathsf{mpk} := \mathbf{A}}$$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$$\Longrightarrow \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$$

$$\Longrightarrow \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i} \text{ is a trapdoor for } \mathbf{F}_{\bar{\mathsf{id}}_i}$$

Non-adaptive Security from SIS - Proof

$\underline{\mathcal{C}}$ $\qquad$ $\underline{\mathcal{R}}$ $\qquad$ $\underline{\mathcal{A}}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$$

$$\implies \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i} \text{ is a trapdoor for } \mathbf{F}_{\bar{\mathsf{id}}_i}$$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

Non-adaptive Security from SIS - Proof

$\mathcal{C}$ $\qquad$ $\mathcal{R}$ $\qquad$ $\mathcal{A}$

$\mathcal{C} \to \mathcal{R}$: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

$\mathcal{A} \to \mathcal{R}$: $(\mathsf{id}_1, \mathsf{m}_1), \dots, (\mathsf{id}_Q, \mathsf{m}_Q)$

$\mathcal{A} \to \mathcal{R}$: $\bar{\mathsf{id}}_1, \dots, \bar{\mathsf{id}}_L$

$\mathcal{R} \to \mathcal{A}$: $\mathsf{mpk} := \mathbf{A}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$$

$$\implies \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i} \text{ is a trapdoor for } \mathbf{F}_{\bar{\mathsf{id}}_i}$$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\mathsf{id}_i,\mathsf{m}_i} = [\mathbf{A} \mid \cdots \mid \mathbf{A}\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} + \mathbf{G}]$$

$$\implies \text{use } \mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} \text{ to compute } \sigma_i$$

Non-adaptive Security from SIS - Proof

$\mathcal{C}$ $\qquad$ $\mathcal{R}$ $\qquad$ $\mathcal{A}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n\times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \dots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \dots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$$

$$\implies \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i} \text{ is a trapdoor for } \mathbf{F}_{\bar{\mathsf{id}}_i}$$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\mathsf{id}_i,\mathsf{m}_i} = [\mathbf{A} \mid \cdots \mid \mathbf{A}\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} + \mathbf{G}]$$

$$\implies \text{use } \mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} \text{ to compute } \sigma_i$$

$\mathcal{R} \xrightarrow{\sigma_1, \dots, \sigma_Q} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{sk}_1, \dots, \mathsf{sk}_L} \mathcal{A}$

Non-adaptive Security from SIS - Proof

$\mathcal{C}$ $\qquad$ $\mathcal{R}$ $\qquad$ $\mathcal{A}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \dots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \dots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$\implies \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$

$\implies \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i}$ is a trapdoor for $\mathbf{F}_{\bar{\mathsf{id}}_i}$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

$\implies \mathbf{F}_{\mathsf{id}_i,\mathsf{m}_i} = [\mathbf{A} \mid \cdots \mid \mathbf{A}\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} + \mathbf{G}]$

$\implies$ use $\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i}$ to compute σ_i

$\mathcal{R} \xrightarrow{\sigma_1, \dots, \sigma_Q} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{sk}_1, \dots, \mathsf{sk}_L} \mathcal{A}$

$\mathcal{R} \xleftarrow{(\mathsf{id}^*, \mathsf{m}^*, \mathbf{z}^*)} \mathcal{A}$

Non-adaptive Security from SIS - Proof

$\mathcal{C}$ $\qquad$ $\mathcal{R}$ $\qquad$ $\mathcal{A}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$$

$$\implies \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i} \text{ is a trapdoor for } \mathbf{F}_{\bar{\mathsf{id}}_i}$$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\mathsf{id}_i,\mathsf{m}_i} = [\mathbf{A} \mid \cdots \mid \mathbf{A}\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} + \mathbf{G}]$$

$$\implies \text{use } \mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} \text{ to compute } \sigma_i$$

$\mathcal{R} \xrightarrow{\sigma_1, \ldots, \sigma_Q} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{sk}_1, \ldots, \mathsf{sk}_L} \mathcal{A}$

$\mathcal{R} \xleftarrow{(\mathsf{id}^*, \mathsf{m}^*, \mathbf{z}^*)} \mathcal{A}$

$$\mathbf{F}_{\mathsf{id}^*,\mathsf{m}^*}\mathbf{z}^* = \mathbf{0}$$

Non-adaptive Security from SIS - Proof

$\mathcal{C}$ $\qquad\qquad$ $\mathcal{R}$ $\qquad\qquad$ $\mathcal{A}$

$$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$$

$$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$$

$$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$$

$$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$$

$$\implies \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i} \text{ is a trapdoor for } \mathbf{F}_{\bar{\mathsf{id}}_i}$$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

$$\implies \mathbf{F}_{\mathsf{id}_i,\mathsf{m}_i} = [\mathbf{A} \mid \cdots \mid \mathbf{A}\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} + \mathbf{G}]$$

$$\implies \text{use } \mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} \text{ to compute } \sigma_i$$

$$\mathcal{R} \xrightarrow{\sigma_1, \ldots, \sigma_Q} \mathcal{A}$$

$$\mathcal{R} \xrightarrow{\mathsf{sk}_1, \ldots, \mathsf{sk}_L} \mathcal{A}$$

$$\mathcal{R} \xleftarrow{(\mathsf{id}^*, \mathsf{m}^*, \mathbf{z}^*)} \mathcal{A}$$

$$\mathbf{F}_{\mathsf{id}^*,\mathsf{m}^*}\mathbf{z}^* = \mathbf{0}$$

$$\implies [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\mathsf{id}^*} \mid \mathbf{A}\mathbf{R}_{\mathsf{id}^*,\mathsf{m}^*}]\mathbf{z}^* = \mathbf{0}$$

Non-adaptive Security from SIS - Proof

$\mathcal{C}$ $\qquad$ $\mathcal{R}$ $\qquad$ $\mathcal{A}$

$\mathcal{C} \xrightarrow{\mathbf{A} \in \mathbb{Z}_q^{n \times m}} \mathcal{R}$

$\mathcal{R} \xleftarrow{(\mathsf{id}_1, \mathsf{m}_1), \ldots, (\mathsf{id}_Q, \mathsf{m}_Q)} \mathcal{A}$

$\mathcal{R} \xleftarrow{\bar{\mathsf{id}}_1, \ldots, \bar{\mathsf{id}}_L} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{mpk} := \mathbf{A}} \mathcal{A}$

$$H_1(\mathsf{mpk}, \mathsf{id}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id}} + \mathbf{G}, & \text{if } \mathsf{id} = \bar{\mathsf{id}}_i \\ \mathbf{A}\mathbf{R}_{\mathsf{id}}, & \text{otherwise} \end{cases}$$

$\Longrightarrow \mathbf{F}_{\bar{\mathsf{id}}_i} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\bar{\mathsf{id}}_i} + \mathbf{G}]$

$\Longrightarrow \mathsf{sk}_i := \mathbf{R}_{\bar{\mathsf{id}}_i}$ is a trapdoor for $\mathbf{F}_{\bar{\mathsf{id}}_i}$

$$H_2(\mathsf{mpk}, \mathsf{id}, \mathsf{m}) = \begin{cases} \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}} + \mathbf{G}, & \text{if } (\mathsf{id}, \mathsf{m}) = (\mathsf{id}_i, \mathsf{m}_i) \\ \mathbf{A}\mathbf{R}_{\mathsf{id},\mathsf{m}}, & \text{otherwise} \end{cases}$$

$\Longrightarrow \mathbf{F}_{\mathsf{id}_i,\mathsf{m}_i} = [\mathbf{A} \mid \cdots \mid \mathbf{A}\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i} + \mathbf{G}]$

$\Longrightarrow$ use $\mathbf{R}_{\mathsf{id}_i,\mathsf{m}_i}$ to compute σ_i

$\mathcal{R} \xrightarrow{\sigma_1, \ldots, \sigma_Q} \mathcal{A}$

$\mathcal{R} \xrightarrow{\mathsf{sk}_1, \ldots, \mathsf{sk}_L} \mathcal{A}$

$\mathcal{R} \xleftarrow{(\mathsf{id}^*, \mathsf{m}^*, \mathbf{z}^*)} \mathcal{A}$

$\mathbf{F}_{\mathsf{id}^*,\mathsf{m}^*}\mathbf{z}^* = \mathbf{0}$

$\Longrightarrow [\mathbf{A} \mid \mathbf{A}\mathbf{R}_{\mathsf{id}^*} \mid \mathbf{A}\mathbf{R}_{\mathsf{id}^*,\mathsf{m}^*}]\mathbf{z}^* = \mathbf{0}$

$\mathcal{C} \xleftarrow{[\mathbf{I} \mid \mathbf{R}_{\mathsf{id}^*} \mid \mathbf{R}_{\mathsf{id}^*,\mathsf{m}^*}]\mathbf{z}^*} \mathcal{R}$

Conclusion and Future Work

Conclusion and Future Work

Conclusion

- First lattice-based short IBS with tight security

Conclusion and Future Work

Conclusion

- First lattice-based short IBS with tight security
- Two step approach

Conclusion and Future Work

Conclusion

- First lattice-based short IBS with tight security
- Two step approach

Open Problems

- Analysis in the QROM

Conclusion and Future Work

Conclusion

- First lattice-based short IBS with tight security
- Two step approach

Open Problems

- Analysis in the QROM
- Non-adaptively secure IBS in the standard model
  - based on SIS
  - tight
  - small signature sizes

Conclusion and Future Work

Conclusion

- First lattice-based short IBS with tight security
- Two step approach

Open Problems

- Analysis in the QROM
- Non-adaptively secure IBS in the standard model
  - based on SIS
  - tight
  - small signature sizes

Thank you for your attention!