

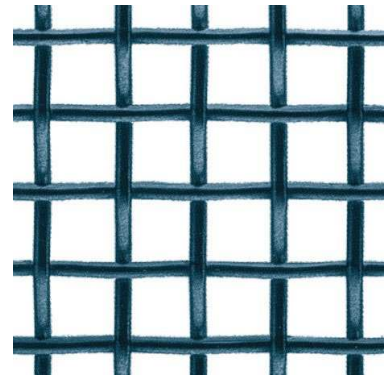
A photograph of a well-manicured pine bonsai tree. The tree has a thick, gnarled trunk that curves to the left and then back to the right. It has several clusters of green, needle-like foliage. The tree is planted in a dark, rectangular ceramic pot filled with soil. The pot sits on a simple wooden stand with four legs. The background is plain white.

Lattice-based cryptography:
Advanced Protocols

Eike Kiltz
CWI
Amsterdam

This talk

- Part I: Lattices in cryptography
(reminder)



- Part II: Applications
Bonsai trees for lattices



What is a lattice?



Why is it useful for crypto?





Lattice Problems

Worst-Case

Average-Case



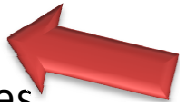
Learning With Errors (LWE)

Small Integer Solution (SIS)



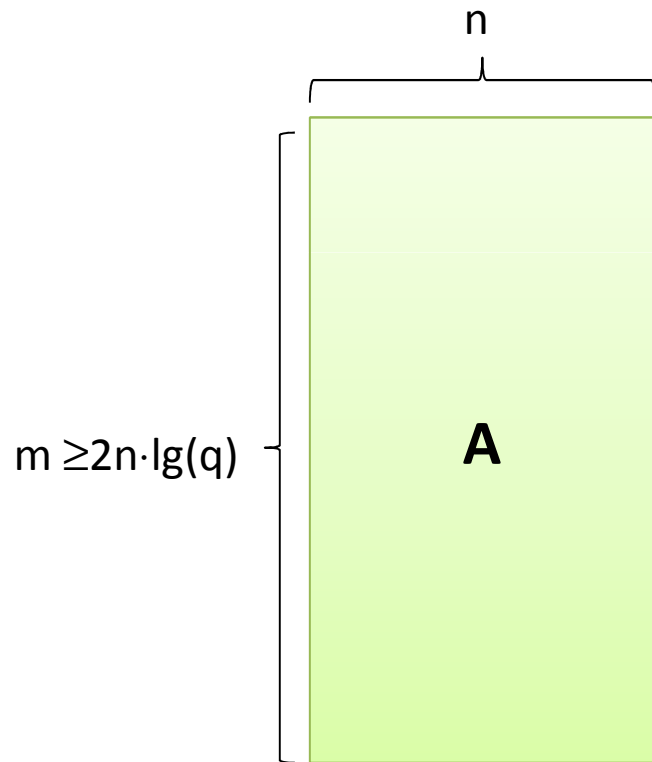
- One-Way Functions
- Collision-Resistant Hash Functions
- Digital Signatures
- Identification Schemes
- ...

- Public Key Encryption
- Oblivious Transfer
- Identity-Based Encryption
- Hierarchical Identity-Based Encryption
- Secure Multi-Party Computation



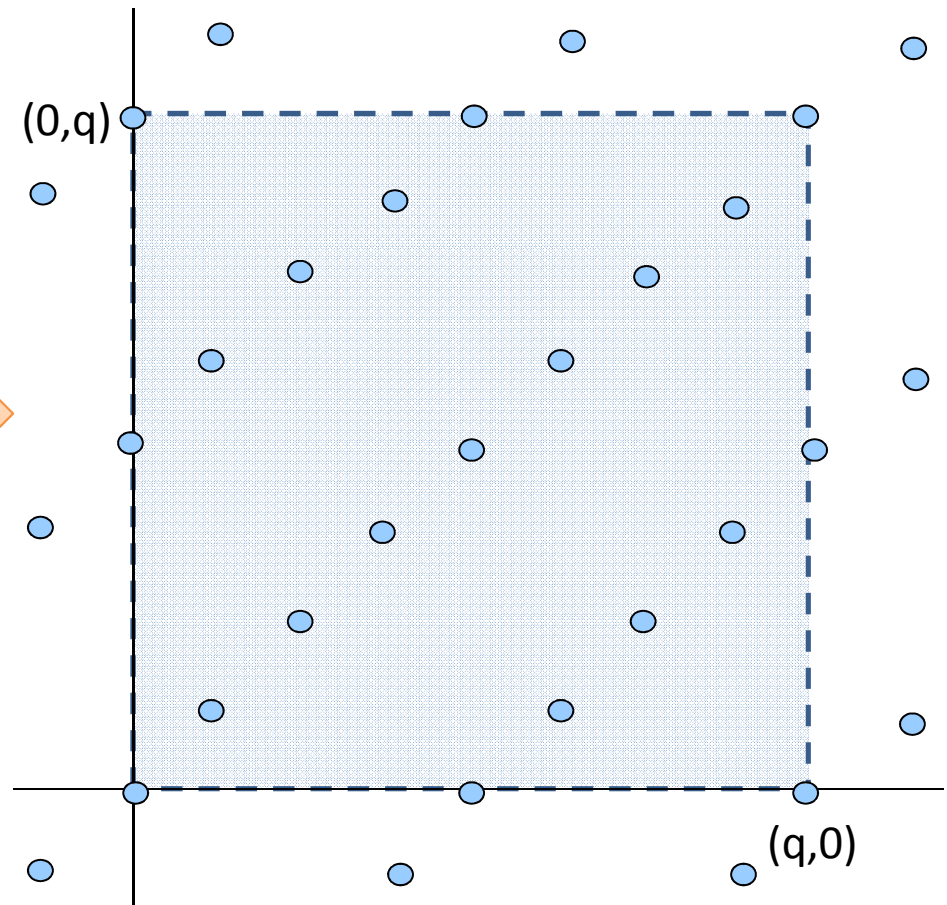
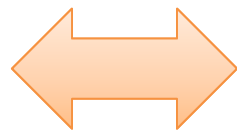
Average-case lattices

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



Full-rank “q-ary” integer lattice

$$\mathcal{L}^\perp(\mathbf{A}) := \{x \in \mathbb{Z}^m : x^t \mathbf{A} = 0 \pmod{q}\} \subseteq \mathbb{Z}^m$$



Short Integer Solutions (SIS) [Ajtai 96]

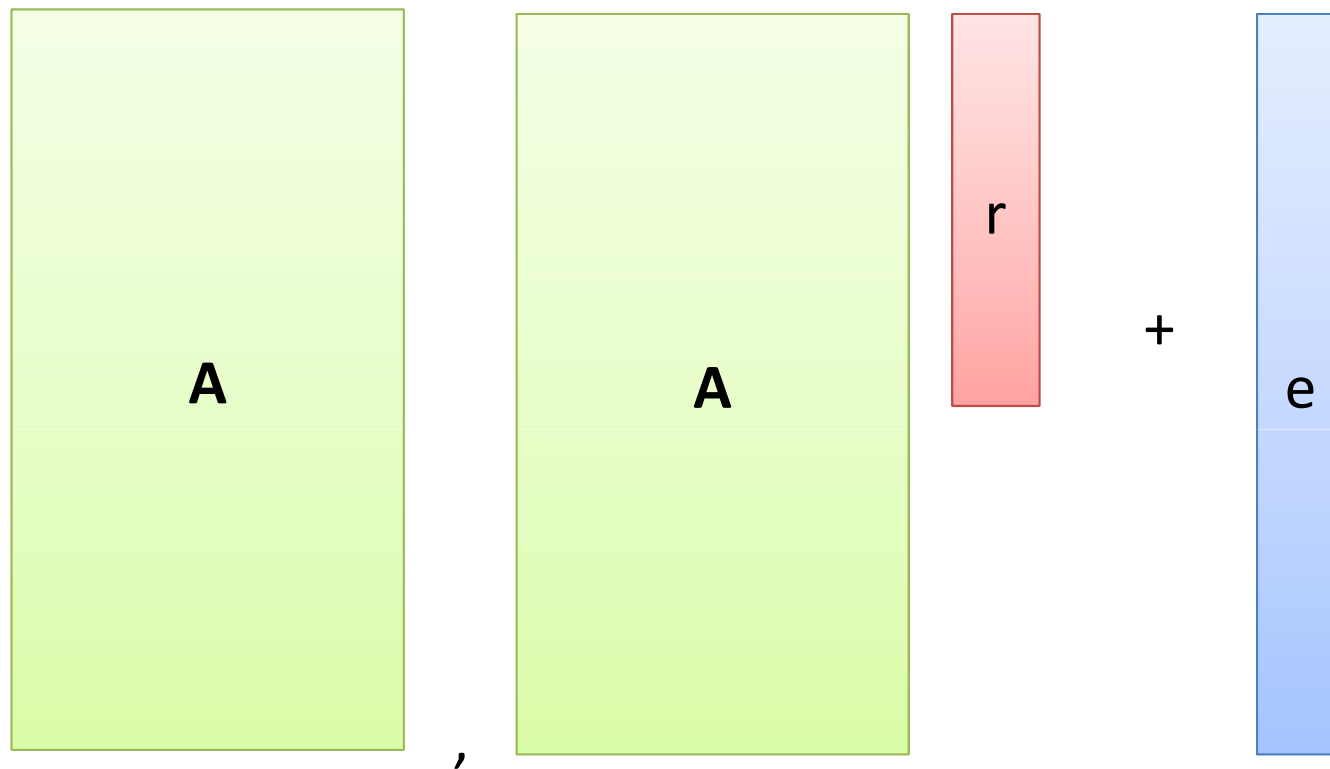
$$\mathbf{x} \mathbf{A} = \mathbf{0}$$

β -SIS problem:

Given: $A \leftarrow \mathbb{Z}_q^{n \times m}$ (uniform)

Find: (non-trivial) small $\mathbf{x} \in \mathbb{Z}^m$ ($\|\mathbf{x}\| \leq \beta$) such that $\mathbf{x}\mathbf{A} = \mathbf{0}$

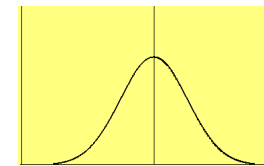
Learning With Errors (LWE) [Reg 05]



α -LWE problem (decisional):

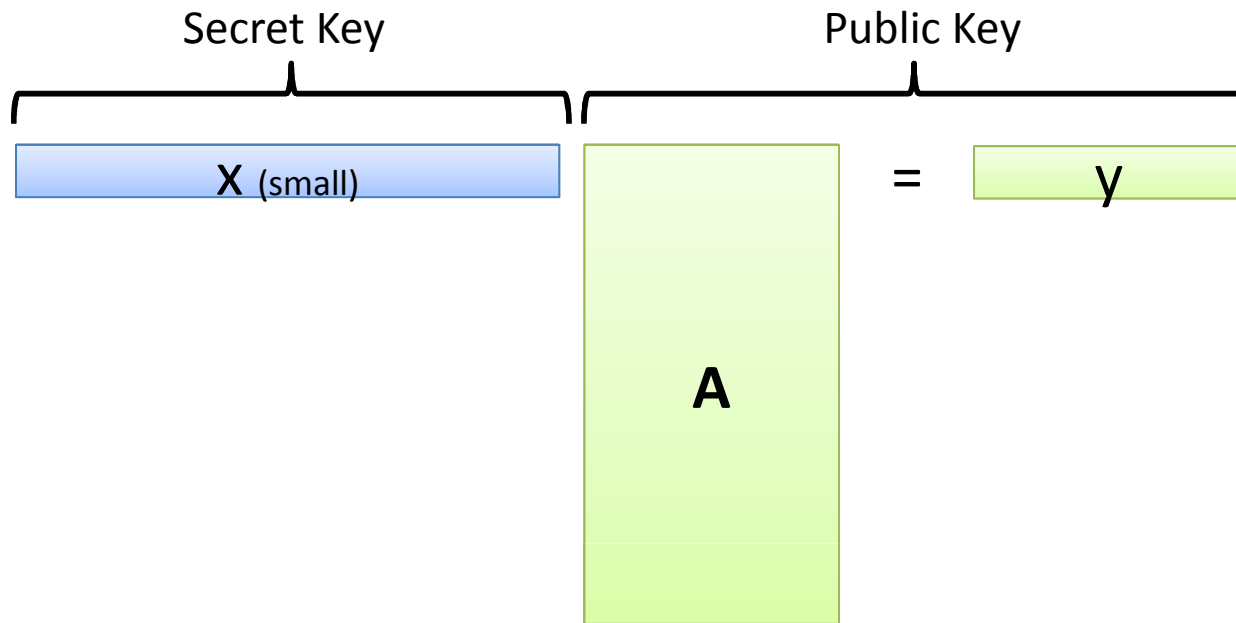
Distinguish $(A, Ar+e)$ from $(A, \text{uniform})$, where

$$A \leftarrow \mathbb{Z}_q^{n \times m}, r \leftarrow \mathbb{Z}_q^n, e \leftarrow \text{Noise}_\alpha^m$$

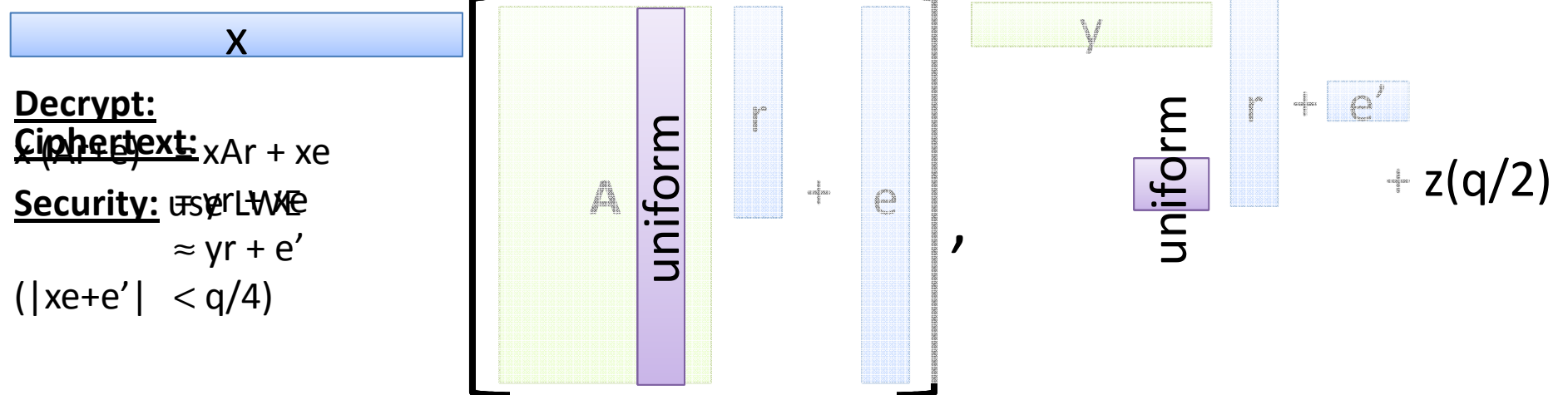


$\text{Noise}_\alpha =$ discretized Gaussian distribution of width α

Dual Public Key Encryption from LWE [Regev, GPV]




Encrypt (a bit z in $\{0,1\}$): $r \leftarrow \mathbb{Z}_q^n, e \leftarrow \text{Noise}^m, e' \leftarrow \text{Noise}.$



ID-based encryption [Shamir '84]

- Master keys: mpk, msk
- With mpk : encrypt to ID “Alice” or “Bob”,...
- With msk : extract sk_{Alice} or sk_{Bob} ,...

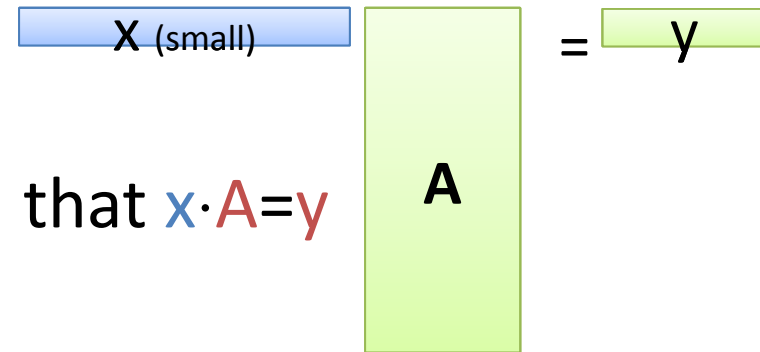
Instantiations:

- Bilinear pairings [BF 01] 
- Quadratic residuosity [Cocks 01]
- Lattices! [GPV 08]

From encryption to ID-based encryption

Public Key Encryption

- Public Key: (A, y)
- Secret Key: small x such that $x \cdot A = y$



ID-based encryption

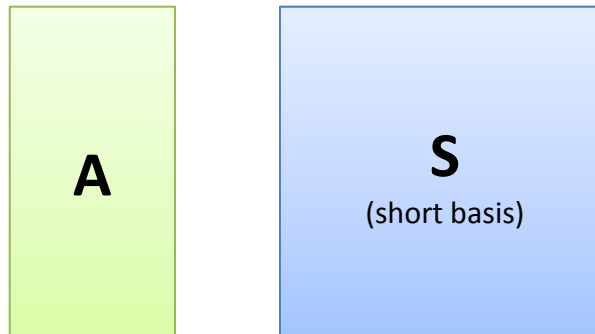
- Master Public Key: $A, H: \{0,1\}^* \rightarrow \mathbb{Z}_q^n$
- Encrypt to ID: $(A, y_{ID} = H(ID))$
- Secret Key sk_{ID} for ID: small x_{ID} such that $x_{ID} \cdot A = y_{ID}$
- Master secret key to invert function $f_A(x) := x \cdot A$?
→ short basis for $\mathcal{L}^\perp(A) = \text{trapdoor}$

Lattices with a trapdoor

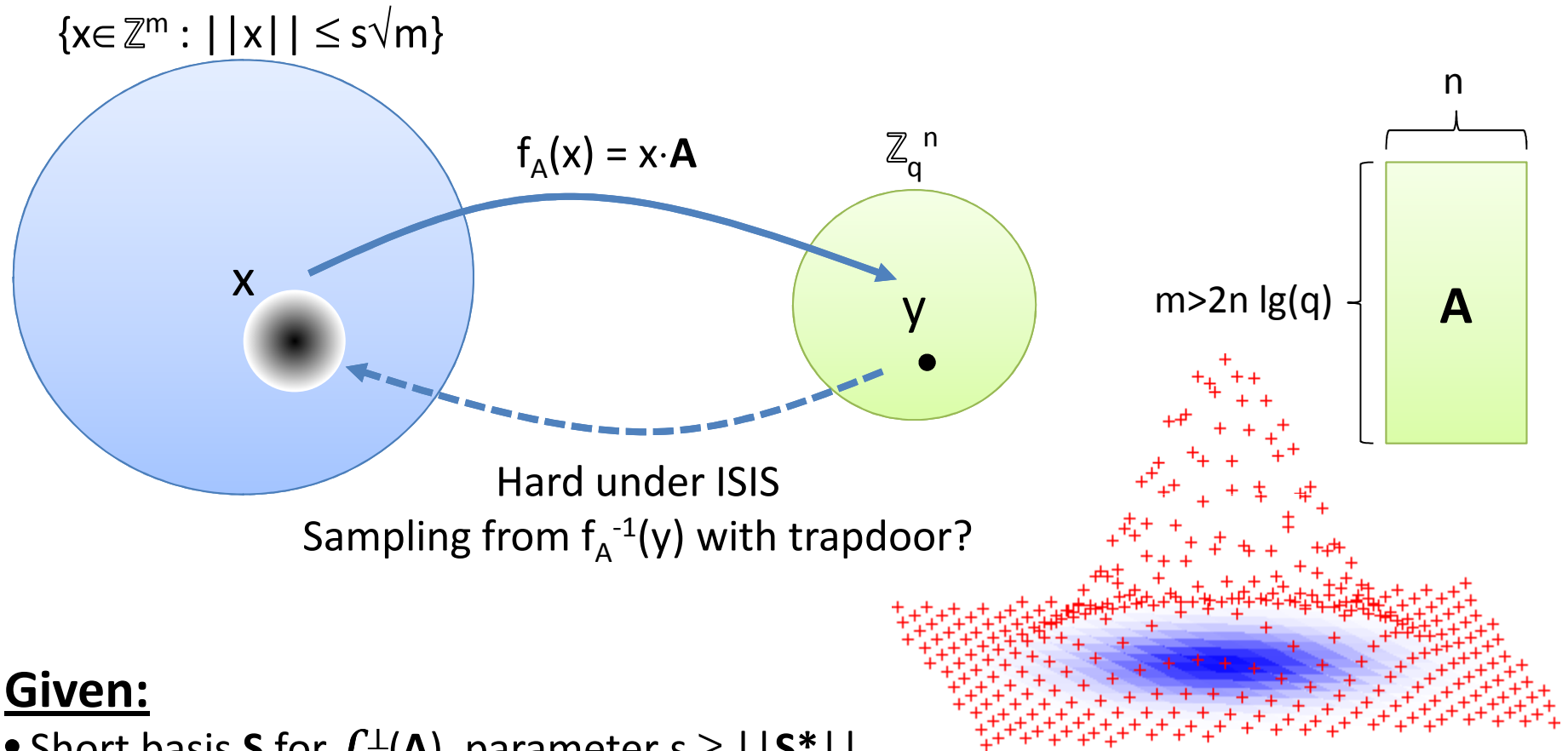
Theorem: [Ajtai 96, AP 09]

There exists a PPT algorithm that given $q, n, m \geq 2n \cdot \lg(q)$, outputs $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, $\mathbf{S} \in \mathbb{Z}^{m \times m}$ such that

- \mathbf{A} is within negl. statistical distance of uniform
- \mathbf{S} is a basis of $\mathcal{L}^\perp(\mathbf{A})$
- $\|\mathbf{S}^*\|$ small ($\leq \sqrt{m}$)



Trapdoor one-way functions/pre-image sampling [GPV08]



Given:

- Short basis \mathbf{S} for $\mathcal{L}^\perp(\mathbf{A})$, parameter $s \geq ||\mathbf{S}^*||$
- y in \mathbb{Z}_q^n

Output:

- Sample $x \leftarrow f_A^{-1}(y)$ with discrete Gaussian with parameter s (nearest plane)
 \Rightarrow Tail bounds: $||x|| \leq s\sqrt{m}$ (w.h.p.)
- Oblivious sampling: samples x independent of short basis \mathbf{S} for $\mathcal{L}^\perp(\mathbf{A})$

ID-Based Encryption from LWE in the ROM [GPV]

$$\boxed{x_{ID} \text{ (small)}} \quad \boxed{A} = \boxed{y_{ID} = H(ID)}$$

Master public key:

$$A \leftarrow \mathbb{Z}_q^{m \times n}$$

Master secret key:

Short basis S for $\mathcal{L}^\perp(A)$

Encrypt to identity ID:

Use LWE-based PKE with $pk_{ID} = (A, y_{ID} := H(ID) \in \mathbb{Z}_q^n)$

Secret Key sk_{ID} for ID:

Sample from $x_{ID} \leftarrow f_A^{-1}(y_{ID})$ with discrete Gaussian

Theorem:

LWE-based encryption scheme secure

\Rightarrow ID-based encryption scheme secure in the random oracle model.

Poof: distribution of sk_{ID} independent of short basis S .

Part II: Bonsai Trees



Bonsai Trees [CHKP '10]



Ancient art of bonsai

- Techniques for **selective control** of a tree by arborist

Cryptographic bonsai

- Tree = hierarchy of trapdoor functions
- Arborist = setup/simulator controls 2 types of growth
 1. **Undirected growth**: no privileged information
(no trapdoor=large basis)
 2. **Controlled growth**: privileged information
(trapdoor=small basis)
 3. **Extending control** down hierarchy (but not up)

www.BonsaiCareSecrets.com

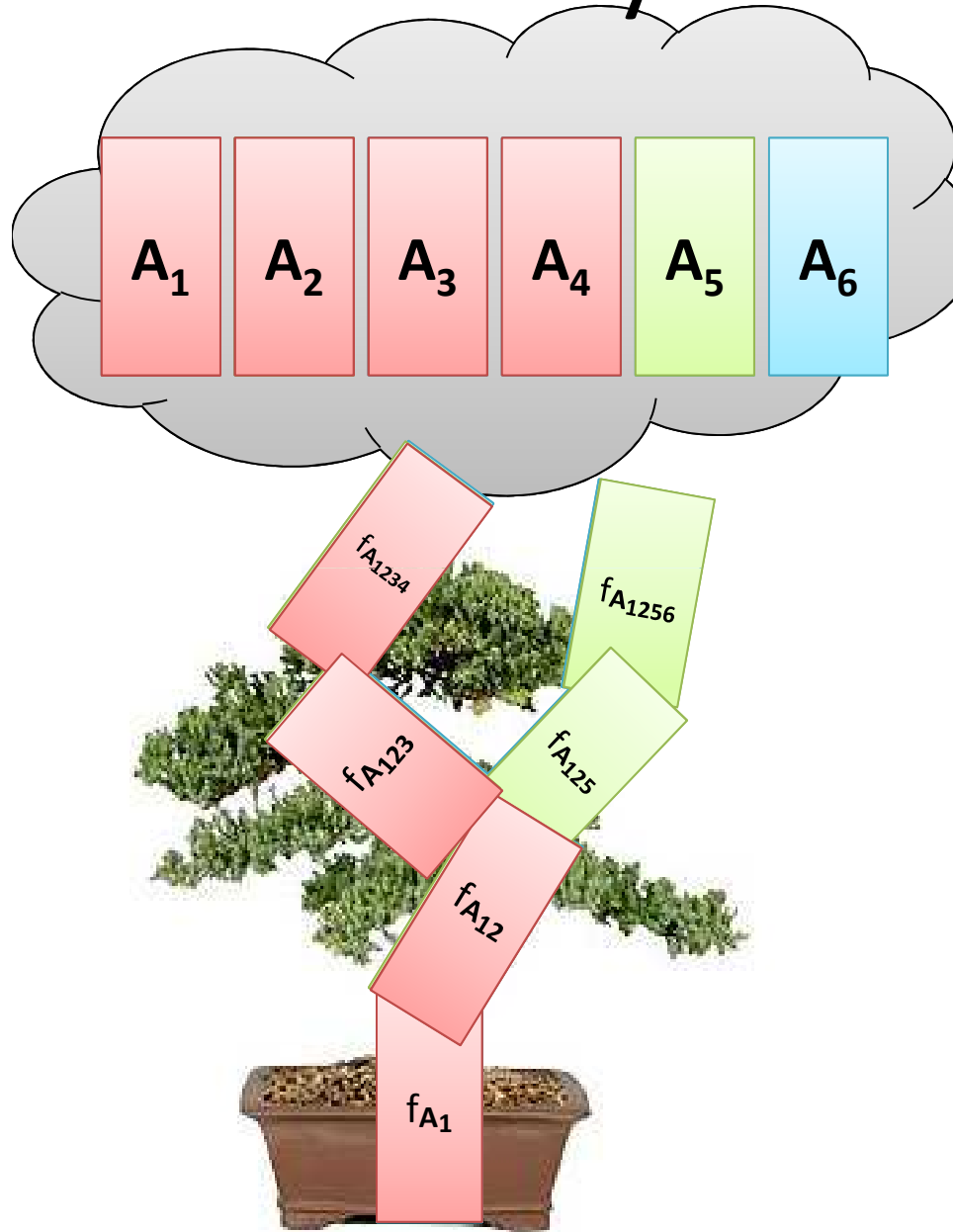
Bonsai Care Secrets



**Easy to Follow, Step by Step
Guide for Selecting, Growing
and Maintaining any Bonsai**

Bonsai Care Secrets

Hierarchy of trapdoor functions



4m-dim lattice

$$\mathcal{L}^\perp(\mathbf{A}_{1256}) := \{x \in \mathbb{Z}^{km} : x\mathbf{A}_{1256} = 0\}$$

$$\text{TDF: } f_{\mathbf{A}_{1256}}(x) = x\mathbf{A}_{1256}$$

3m-dim lattice

$$\mathcal{L}^\perp(\mathbf{A}_{1\dots k}) := \{x \in \mathbb{Z}^{km} : x\mathbf{A}_{123} = 0\}$$

$$\text{TDF: } f_{\mathbf{A}_{123}}(x) = x\mathbf{A}_{123}$$

2m-dim lattice

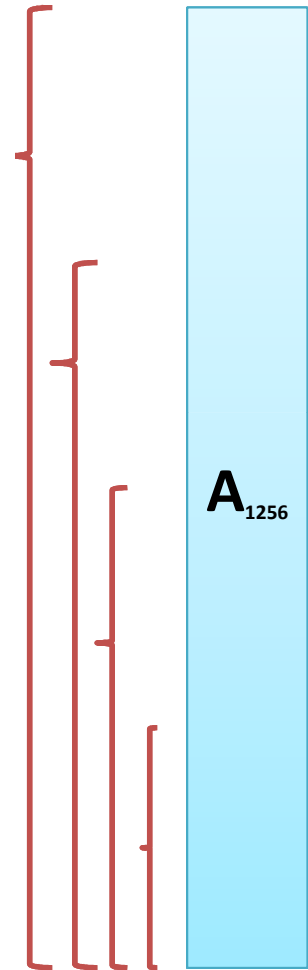
$$\mathcal{L}^\perp(\mathbf{A}_{12}) := \{x \in \mathbb{Z}^{2m} : x\mathbf{A}_{12} = 0\}$$

$$\text{TDF: } f_{\mathbf{A}_{12}}(x) = x\mathbf{A}_{12}$$

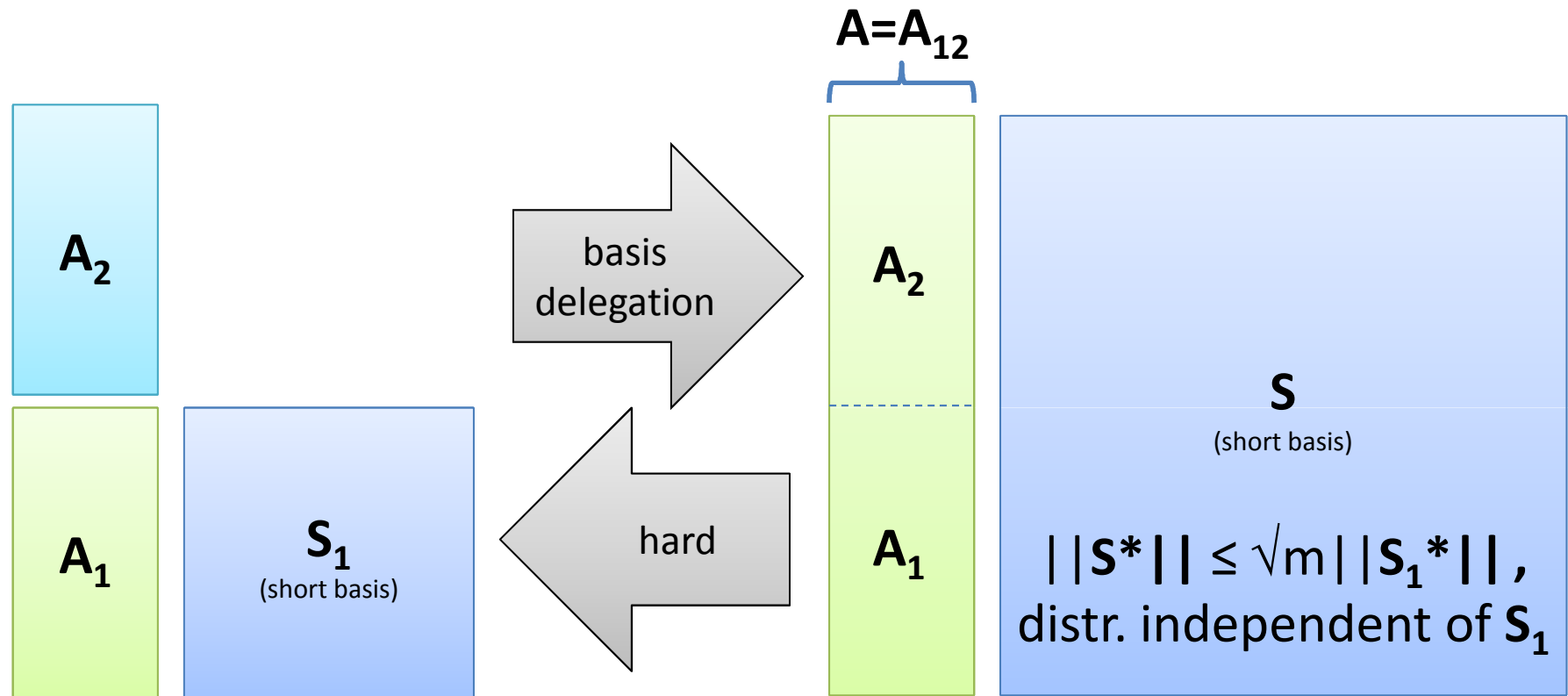
m-dim lattice

$$\mathcal{L}^\perp(\mathbf{A}_1) := \{x \in \mathbb{Z}^m : x\mathbf{A}_1 = 0\}$$

$$\text{TDF: } f_{\mathbf{A}_1}(x) = x\mathbf{A}_1$$



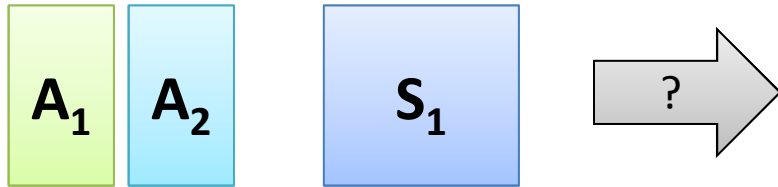
Extending control = lattice basis delegation



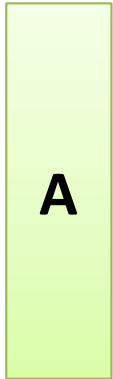
A_1, A_2 , short basis S_1 for $\mathcal{L}^\perp(A_1)$

Short basis S for (any) higher-dim. super-lattice $\mathcal{L}^\perp(A)$

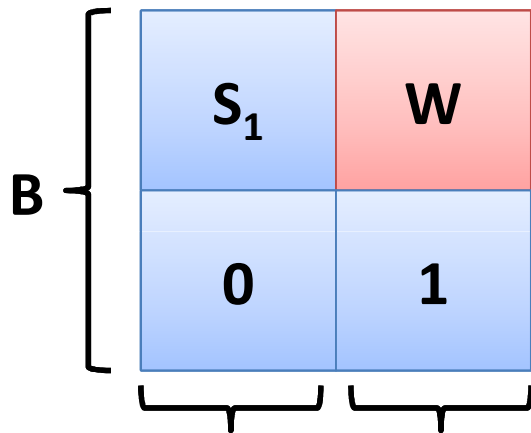
A_1, A_2 , short basis S_1 for $\mathcal{L}^\perp(A_1)$



Short basis for higher-dimensional lattice
 $\mathcal{L}^\perp(\mathbf{A}) = \{x \in \mathbb{Z}^{2m} : x_1 A_1 + x_2 A_2 = 0 \pmod{q}\}$



Step 1:

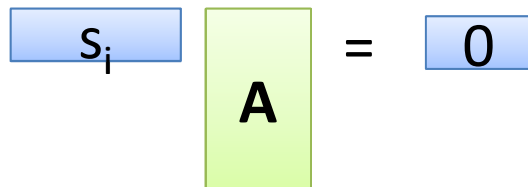


- W = arbitrary solution to $WA_1 = -A_2$
- B is a basis of $\mathcal{L}^\perp(\mathbf{A})$
- B not independent of S_1 ! ☹️
- $||B^*|| = ||S_1^*||$ ☺️

$||B_i^*|| = ||S_{1i}^*|| \quad ||B_i^*|| = ||e_i|| \leq 1$ since $\text{span}(S_1) = \text{span}(e_1, \dots, e_m) \subseteq \mathbb{R}^{2m}$

Step 2:

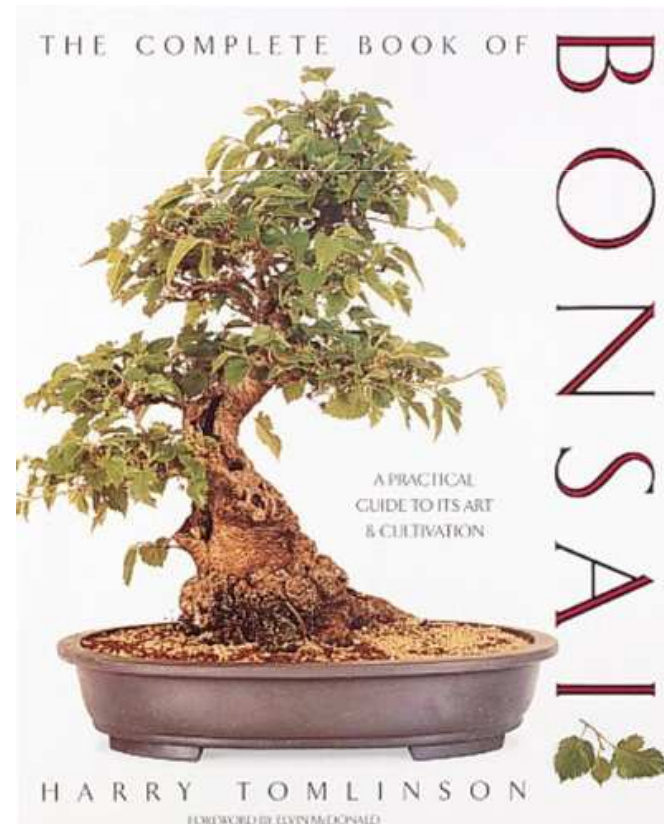
- Use B to sample many $s_i \leftarrow f_A^{-1}(0)$ with discrete Gaussian distribution



- Assemble basis S of $\mathcal{L}^\perp(\mathbf{A})$ from $\{s_1, \dots, s_{m^2}\}$
- Gaussian parameter $s = ||B^*||$
 $\Rightarrow ||S^*|| \leq \sqrt{m} ||B^*|| = \sqrt{m} ||S_1^*||$
- S independent of S_1 !

Applications of bonsai trees

- Trapdoor = short basis = ability to decrypt
- Hierarchy of trapdoors = delegation of decryption
- Applications
 - Digital signatures
 - ID-based encryption
 - (Hierarchical) ID-based encryption
 -



Application 1: Hierarchical ID-based encryption

Master keys: mpk, msk

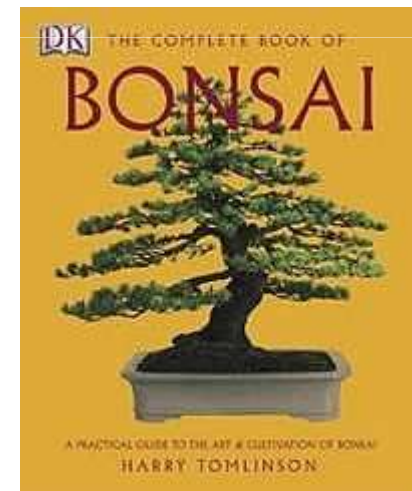
- With mpk : encrypt to hierarchical IDs “Alice@cwi.nl”,...
- With msk : extract sk_{nl} or sk_{com} , ...
- With sk_{nl} : extract $sk_{cwi.nl}$ or $sk_{ns.nl}$, ...
- With $sk_{cwi.nl}$: extract $sk_{Alice@cwi.nl}$, $sk_{Bob@cwi.nl}$, ...

Instantiations:

- Bilinear pairings [GS 01]
- Quadratic residuosity????
- Lattices! [CHKP 10]

Why?

- Implies forward-secure encryption, CCA-secure encryption,...



Hierarchical ID-based encryption from LWE [CHKP '10]

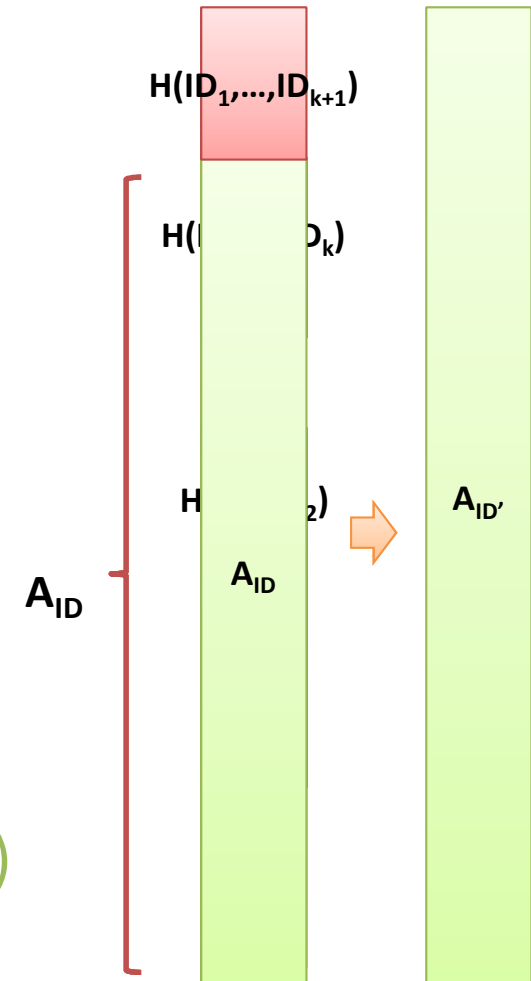
- **Public-Key:** matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$,
hash function $H: \{0,1\}^* \rightarrow \mathbb{Z}_q^{m \times n}$

- **Master Secret Key:** Short basis \mathbf{S} for $\mathcal{L}^\perp(\mathbf{A})$

- **Encrypt:** for hierarchical identity
 $ID = (ID_1, \dots, ID_k)$ use $pk_{ID} = (\mathbf{A}_{ID}, \mathbf{y})$

- **User secret key:**

- For key delegation: short basis \mathbf{S}_{ID} for $\mathcal{L}^\perp(\mathbf{A}_{ID})$
(using “extending control”)
- For decryption: sample small \mathbf{x}_{ID} with $\mathbf{x}_{ID} \cdot \mathbf{A}_{ID} = \mathbf{y}$



Application 2: digital signatures

Public Key:

Undirected: $A_{ij} \leftarrow \mathbb{Z}_q^{m \times n}$ $(i,j) \in \{1, \dots, k\} \times \{0, 1\}$

Secret key:

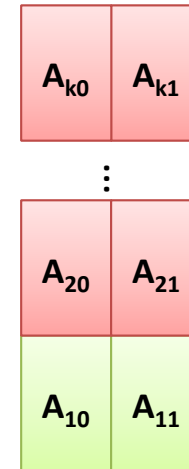
controlled: Short basis for $\mathcal{L}^\perp(\mathbf{A}_{10})$ and $\mathcal{L}^\perp(\mathbf{A}_{11})$

Sign: of message $M=(M_1, \dots, M_k) \in \{0, 1\}^k$

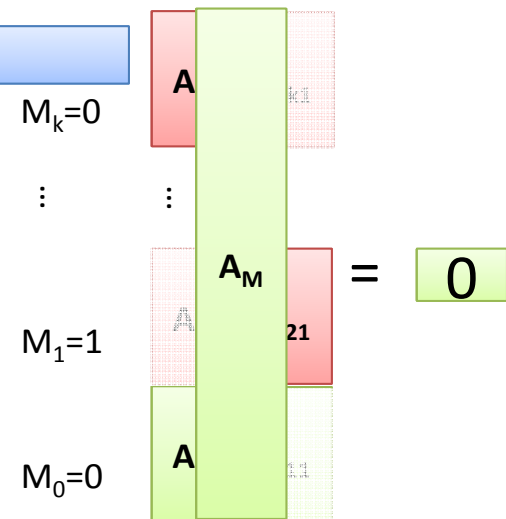
1. Assemble $\mathbf{A}_M \in \mathbb{Z}_q^{km \times n}$ from A_{ij}
2. **Extending control** to compute trapdoor for $f_{\mathbf{A}_M}$:
short basis \mathbf{S}_M for $\mathcal{L}^\perp(\mathbf{A}_M)$
3. Use \mathbf{S}_M to sample from $f_{\mathbf{A}_M}^{-1}(0)$ with discrete Gaussian
signature = small x_M : $x_M \cdot \mathbf{A}_M = 0$

Verify: sig x_M of message $M=(M_1, \dots, M_k)$

1. check if x_M is small and $x_M \cdot \mathbf{A}_M = 0$



$$\mathbf{A}_M \in \mathbb{Z}_q^{km \times n}$$



Security definition: (selective security)

1. **Adv** commits to message M he intends to forge and obtains pk
2. **Adv** obtains signatures on messages M' of his choice ($\neq M$)
3. **Adv** wins if he can forge a message on M

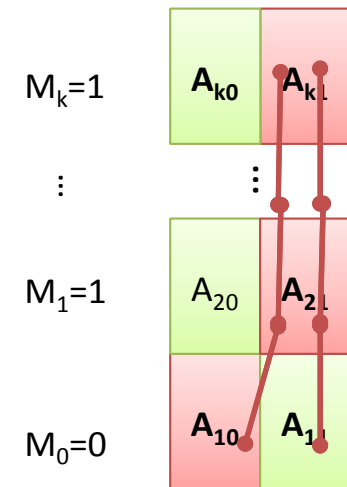
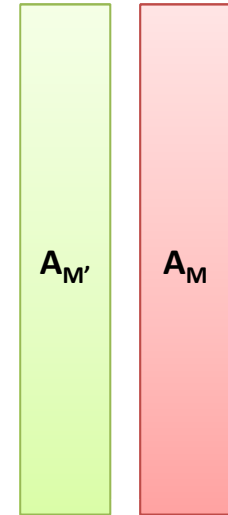
Proof of Theorem: by reduction.

Given $A=(A_1,\dots,A_k)\in \mathbb{Z}_q^{k \times n}$, find **small** x s.t. $xA = 0$ (SIS)

1. Run **Adv** to obtain M
2. Setup A_{ij} from pk such that
 - **Undirected:** $A_{iM_i} := A_i \Rightarrow A_M = A$
 - **Controlled:** $A_{i(1-M_i)} \leftarrow \mathbb{Z}_q^{m \times n}$ with short basis

3. Run **Adv** on pk answering signing queries
Extending control: signatures on $M' \neq M$ can be computed since at least one **short basis** is known for $A_{M'}$

4. A forgery from **Adv** consists of a **small** x s.t. $xA_M = 0$



Application 3: Identity-based encryption [CHKP '10]

Public Key:

Undirected: $A_{ij} \leftarrow \mathbb{Z}_q^{m \times n} ((i,j) \in \{1, \dots, k\} \times \{0, 1\})$
 $y \in \mathbb{Z}_q^n$

Secret key:

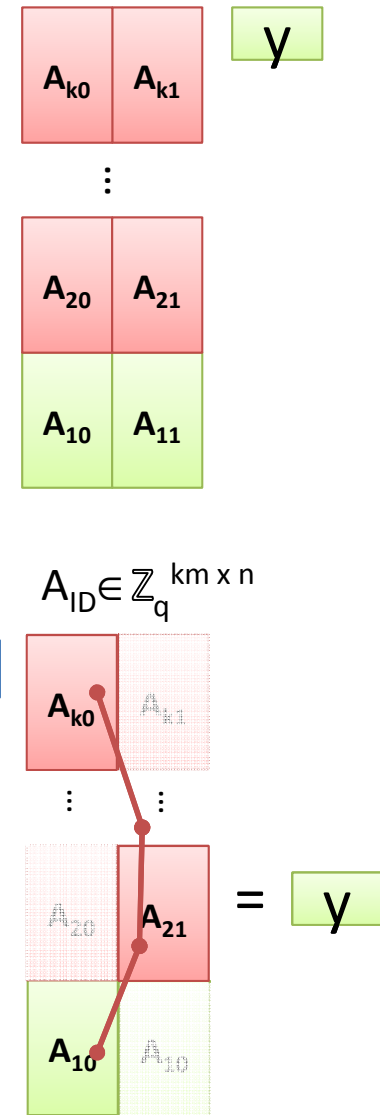
controlled: Short basis for $\mathcal{L}^\perp(\mathbf{A}_{10})$ and $\mathcal{L}^\perp(\mathbf{A}_{11})$

Encrypt: for identity $ID = (ID_1, \dots, ID_k) \in \{0, 1\}^k$

1. Assemble $\mathbf{A}_{ID} \in \mathbb{Z}_q^{km \times n}$ from A_{ij}
2. Use LWE encryption with public-key = (\mathbf{A}_{ID}, y)

User secret key: of identity $ID = (ID_1, \dots, ID_k)$

1. **Extending control:** compute short basis \mathbf{S}_{ID} for $\mathcal{L}^\perp(\mathbf{A}_{ID})$
2. Use \mathbf{S}_{ID} to sample $x_{ID} \leftarrow f^{-1}_{\mathbf{A}_{ID}}(y)$ with discrete Gaussian
3. Secret key for ID = $(\mathbf{S}_{ID}, x_{ID})$



Final slide: take-home message

1. Lattices in crypto

- Secure and versatile!
- Natural



2. Bonsai trees for lattices

- Unique: hierarchy of trapdoor functions
- Applications: Signatures, IBE, Hierarchical IBE,...
- Follow-up work: [ABB10a, B10, ABB10b, R10, ...]

