Some Recent Progress in Lattice-Based Cryptography

Chris Peikert
SRI

TCC 2009

Lattice-Based Cryptography

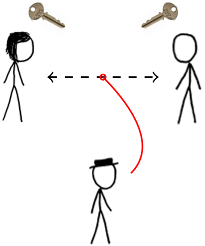
$y = g^x \bmod p$

$m^e \bmod N$

$N = p \cdot q$

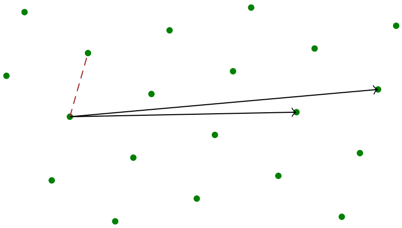
$e(g^a, g^b)$

$\Longrightarrow$

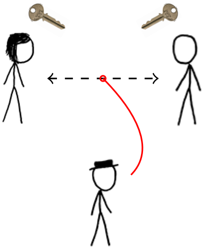


(Images courtesy xkcd.org)

Lattice-Based Cryptography

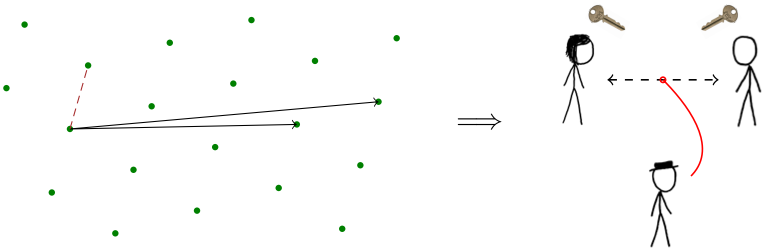


$\Longrightarrow$



(Images courtesy xkcd.org)

Lattice-Based Cryptography



Why?

- Simple & efficient: linear, parallelizable
- Resists subexp & quantum attacks (so far)
- Security from worst-case assumptions [Ajtai96, . . .]

(Images courtesy xkcd.org)

If We Had 6 Hours. . .

If We Had 6 Hours. . .

- Worst-case / average-case reductions

  [Aj96,AD97,CN97,Mi03,Re03,MR04,Re05,Pe07,GPV08,Pe09,. . .]

If We Had 6 Hours...

- Worst-case / average-case reductions

  [Aj96,AD97,CN97,Mi03,Re03,MR04,Re05,Pe07,GPV08,Pe09,...]

- Cryptanalysis & concrete parameters

  [LLL82,Sc87,BKW00,AKS01,NR06,GN08,NV08,MR08,...]

If We Had 6 Hours...

- Worst-case / average-case reductions

  [Aj96,AD97,CN97,Mi03,Re03,MR04,Re05,Pe07,GPV08,Pe09,...]

- Cryptanalysis & concrete parameters

  [LLL82,Sc87,BKW00,AKS01,NR06,GN08,NV08,MR08,...]

- Cyclic / Ideal lattices [Mi02,PR06,LM06,PR07,LM08,Ge09,...]
  - ⋆ *Efficiency* — complements general techniques
  - !! *Functionality* — uses 'extra features' of ideals

If We Had 6 Hours...

- Worst-case / average-case reductions

  [Aj96,AD97,CN97,Mi03,Re03,MR04,Re05,Pe07,GPV08,Pe09,...]

- Cryptanalysis & concrete parameters

  [LLL82,Sc87,BKW00,AKS01,NR06,GN08,NV08,MR08,...]

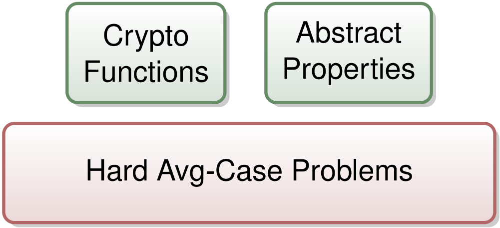
- Cyclic / Ideal lattices [Mi02,PR06,LM06,PR07,LM08,Ge09,...]
  - ⋆ *Efficiency* — complements general techniques
  - !! *Functionality* — uses 'extra features' of ideals

- Complexity of lattice problems
  - ⋆ Hardness [vEB81,Aj98,CN99,Mi00,Kh05,RR06,HR07,...]
  - ⋆ Limits on hardness [LLS90,Ba93,GG97,Ca98,AR04,GMR05,LLM06,P07,...]

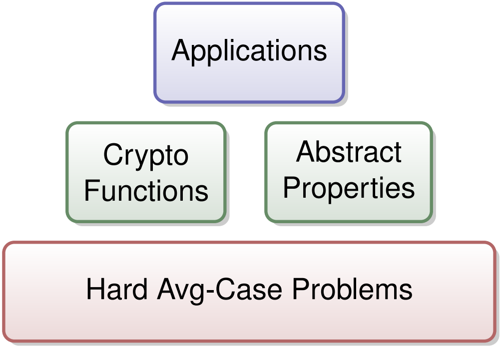
This Talk

Hard Avg-Case Problems

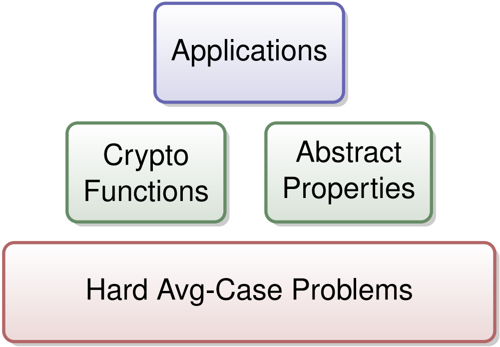
This Talk


Crypto Functions
Abstract Properties
Hard Avg-Case Problems

This Talk


Applications
Crypto Functions
Abstract Properties
Hard Avg-Case Problems

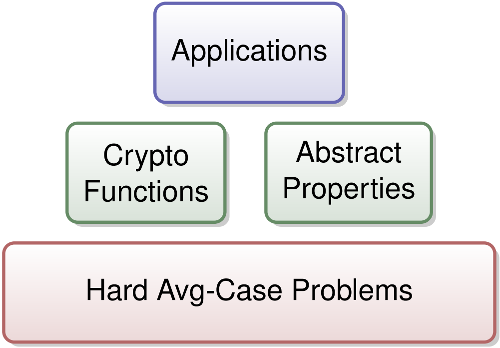
This Talk



Goals

1. ‘De-mystify’ lattice-based crypto

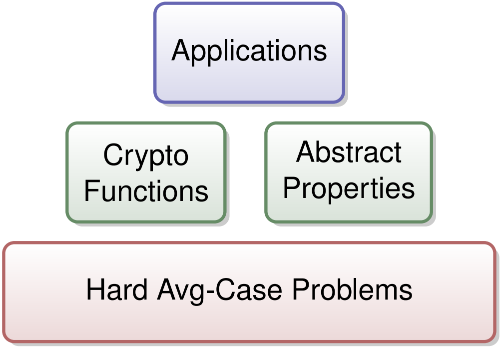
This Talk



Goals

1. 'De-mystify' lattice-based crypto
2. Advocate a geometric perspective

This Talk

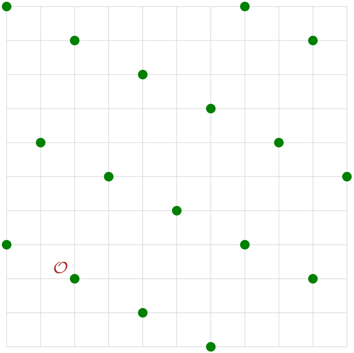


Goals

1. 'De-mystify' lattice-based crypto
2. Advocate a geometric perspective
3. Answer your questions

Lattices

- Today: full-rank subgroup $\mathcal{L}$ of $\mathbb{Z}^m$ $(\mathbf{x}, \mathbf{y} \in \mathcal{L} \Rightarrow \mathbf{x} \pm \mathbf{y} \in \mathcal{L};\ \dim \operatorname{span} = m)$

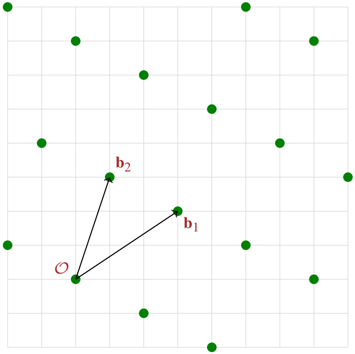


Lattices

- Today: full-rank subgroup $\mathcal{L}$ of $\mathbb{Z}^m$

- Basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$:

$$\mathcal{L} \quad = \quad \sum_{i=1}^{m} (\mathbb{Z} \cdot \mathbf{b}_i)$$

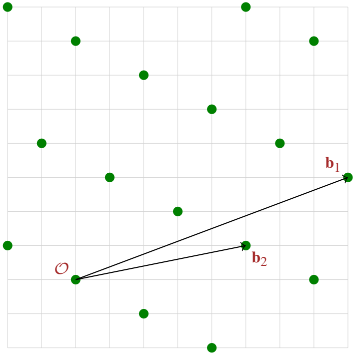


Lattices

- Today: full-rank subgroup $\mathcal{L}$ of $\mathbb{Z}^m$

- Basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_m\}$:

$$\mathcal{L} = \sum_{i=1}^{m} (\mathbb{Z} \cdot \mathbf{b}_i)$$



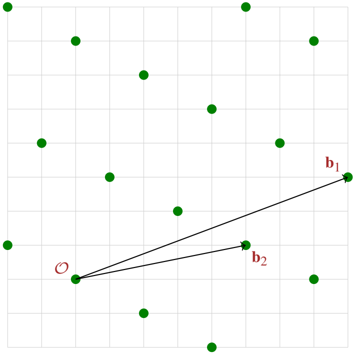
Lattices

- Today: full-rank subgroup $\mathcal{L}$ of $\mathbb{Z}^m$

- Basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$:

$$\mathcal{L} = \sum_{i=1}^{m} (\mathbb{Z} \cdot \mathbf{b}_i)$$

(Other representations too . . .)



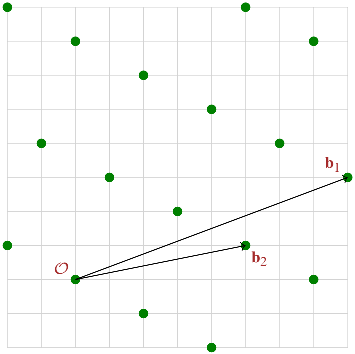
Lattices

- Today: full-rank subgroup $\mathcal{L}$ of $\mathbb{Z}^m$

- Basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$:

$$\mathcal{L} \quad = \quad \sum_{i=1}^{m} (\mathbb{Z} \cdot \mathbf{b}_i)$$

(Other representations too . . .)



Hard Computational Problems

- Find ‘relatively short’ (nonzero) vectors
- Estimate geometric quantities (minimum distance, covering radius, . . .)

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \quad \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} \quad \cdots \quad \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \quad \in \mathbb{Z}_q^n$$

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)
- Goal: find nontrivial $z_1, \ldots, z_m \in \{0, \pm 1\}$ such that:

$$z_1 \cdot \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + z_2 \cdot \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} + \cdots + z_m \cdot \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ 0 \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Hash Function [Ajtai96,GGH97]

- Set $m > n \lg q$. Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}$$

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \mathbf{z} \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Hash Function [Ajtai96,GGH97]

- Set $m > n \lg q$. Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}$$

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

A Combinatorial Problem

- Security param n, modulus q: group $\mathbb{Z}_q^n$ (e.g., $q = \text{poly}(n)$)
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \mathbf{z} \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Hash Function [Ajtai96,GGH97]

- Set $m > n \lg q$. Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}$$

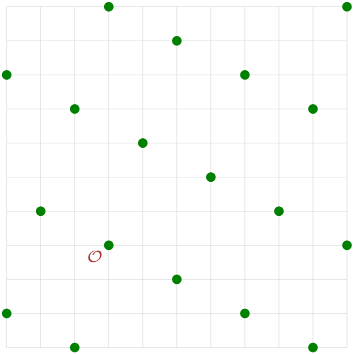
- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

...yields solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

Geometric Perspective

- 'Parity check' matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

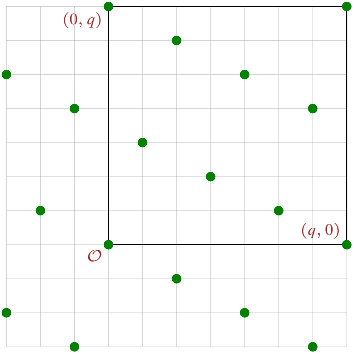
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$



Geometric Perspective

- 'Parity check' matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

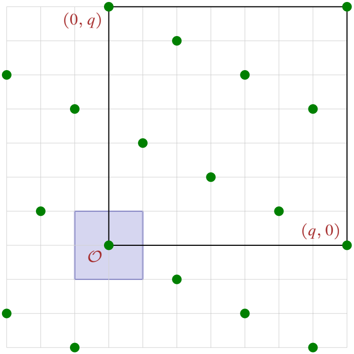
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$



Geometric Perspective

- ‘Parity check’ matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$

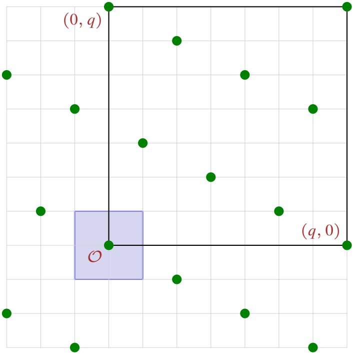
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$



Geometric Perspective

- 'Parity check' matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

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



Average / Worst-Case Connection **[Ajtai96,...]**

Finding 'short' nonzero $\mathbf{z} \in \mathcal{L}^{\perp}(\mathbf{A})$

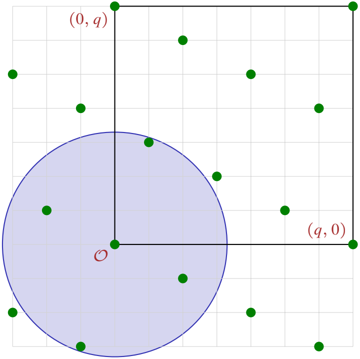
$\Downarrow$

approx lattice problems in worst case

Geometric Perspective

- ‘Parity check’ matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$

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



Average / Worst-Case Connection [Ajtai96,...]

Finding ‘short’ nonzero $\mathbf{z} \in \mathcal{L}^\perp(\mathbf{A})$

$\Downarrow$

approx lattice problems in worst case

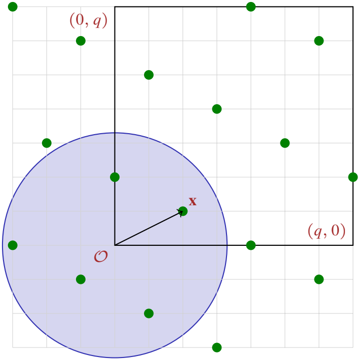
Geometric Perspective

- 'Parity check' matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

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

- Each $\mathbf{x} \in \mathbb{Z}^m$ has syndrome

$$\mathbf{u} = \mathbf{A}\mathbf{x} \in \mathbb{Z}_q^n$$



Average / Worst-Case Connection [Ajtai96,...]

Finding 'short' $\mathbf{x}$ with (uniform) syndrome $\mathbf{u}$

$$\Downarrow$$

approx lattice problems in worst case

Geometric Perspective

- 'Parity check' matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

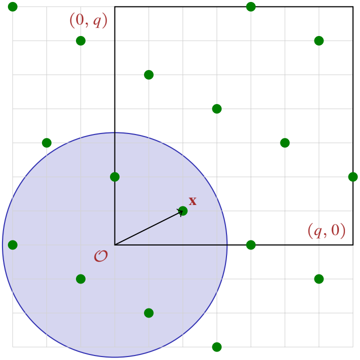
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$

- Each $\mathbf{x} \in \mathbb{Z}^m$ has syndrome

$$\mathbf{u} = \mathbf{A}\mathbf{x} \in \mathbb{Z}_q^n$$

- Enlarge domain of $f_{\mathbf{A}}$ to  ...

...still O-W & C-R!



Average / Worst-Case Connection [Ajtai96,...]

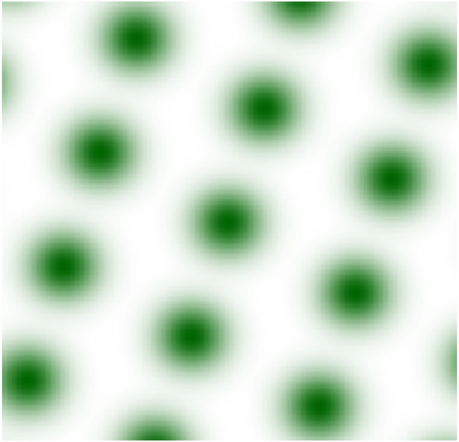
Finding 'short' $\mathbf{x}$ with (uniform) syndrome $\mathbf{u}$

$$\Downarrow$$

approx lattice problems in worst case

Gaussians and Lattices

Gaussians and Lattices



Gaussians and Lattices

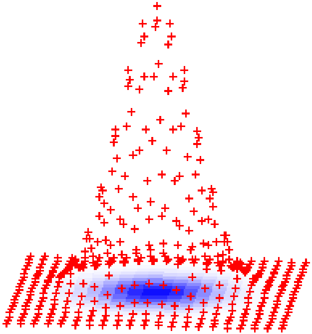
Gaussians and Lattices

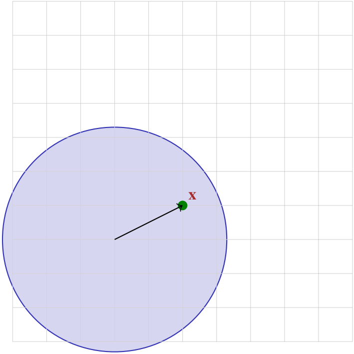
"Uniform" over $\mathbb{R}^m$ when std dev $\geq$ min basis length

(Used in worst/average-case reductions [Re03,MR04,. . .])

Discrete Gaussians

- Fix uniform $\mathbf{A}$. Choose Gaussian input $\mathbf{x} \in \mathbb{Z}^m$:

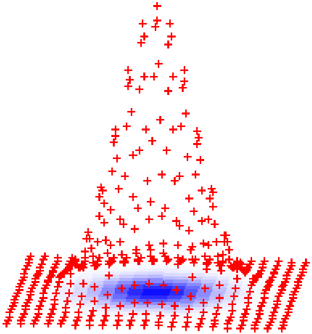


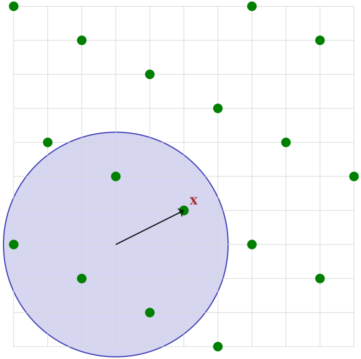


Discrete Gaussians

- Fix uniform $\mathbf{A}$. Choose Gaussian input $\mathbf{x} \in \mathbb{Z}^m$:

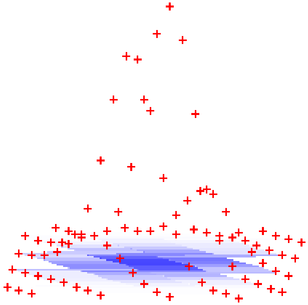
  1. Uniform coset/syndrome $\mathbf{u} = \mathbf{A}\mathbf{x} = f_{\mathbf{A}}(\mathbf{x})$

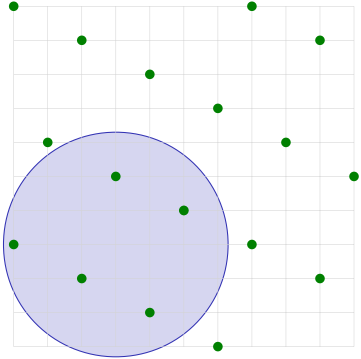




Discrete Gaussians

- Fix uniform $\mathbf{A}$. Choose Gaussian input $\mathbf{x} \in \mathbb{Z}^m$:
  1. Uniform coset/syndrome $\mathbf{u} = \mathbf{A}\mathbf{x} = f_{\mathbf{A}}(\mathbf{x})$
  2. Conditional 'discrete Gaussian' $D_{\mathbf{A},\mathbf{u}}$ on $\mathbf{x}$, given $\mathbf{u}$

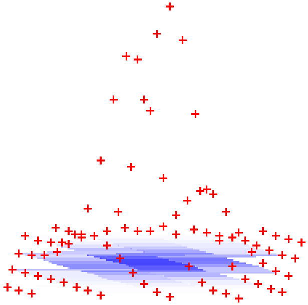


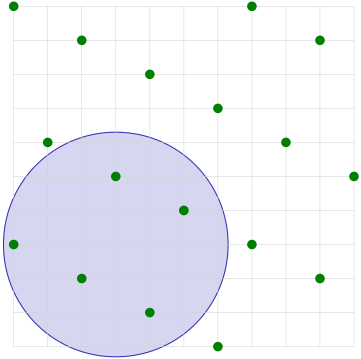


Discrete Gaussians

- Fix uniform $\mathbf{A}$. Choose Gaussian input $\mathbf{x} \in \mathbb{Z}^m$:
  1. Uniform coset/syndrome $\mathbf{u} = \mathbf{A}\mathbf{x} = f_{\mathbf{A}}(\mathbf{x})$
  2. Conditional 'discrete Gaussian' $D_{\mathbf{A},\mathbf{u}}$ on $\mathbf{x}$, given $\mathbf{u}$

  (Analyzed in [Ba93,Re03,AR04,MR04,Re05,PR06,LM06,Pe07,...])





A ‘Master’ Trapdoor

Suitable ‘trapdoor’

$\Downarrow$

Invert $f_{\mathbf{A}}$ in a very strong sense

A ‘Master’ Trapdoor

Short basis $\mathbf{B}$ of $\mathcal{L}^{\perp}(\mathbf{A})$

$$\Downarrow$$

Invert $f_{\mathbf{A}}$ in a very strong sense

A ‘Master’ Trapdoor

Short basis $\mathbf{B}$ of $\mathcal{L}^{\perp}(\mathbf{A})$

$\Downarrow$

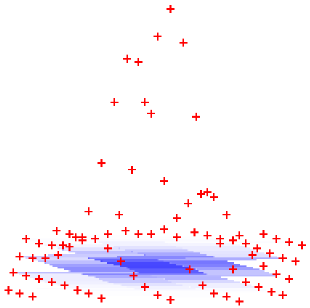
Invert $f_{\mathbf{A}}$ in a very strong sense

Theorem **[GPV08]**

Given *any* short $\mathbf{B}$ and $\mathbf{u}$,

can efficiently sample $\mathbf{x} \leftarrow f_{\mathbf{A}}^{-1}(\mathbf{u})$

according to $D_{\mathbf{A},\mathbf{u}}$



A 'Master' Trapdoor

Short basis $\mathbf{B}$ of $\mathcal{L}^{\perp}(\mathbf{A})$

$\Downarrow$

Invert $f_{\mathbf{A}}$ in a very strong sense

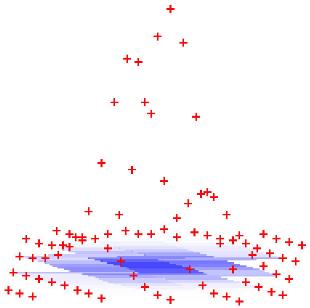
Theorem **[GPV08]**

Given *any* short $\mathbf{B}$ and $\mathbf{u}$,

can efficiently sample $\mathbf{x} \leftarrow f_{\mathbf{A}}^{-1}(\mathbf{u})$

according to $D_{\mathbf{A},\mathbf{u}}$

- Dist $D_{\mathbf{A},\mathbf{u}}$ leaks nothing about $\mathbf{B}$!



A ‘Master’ Trapdoor

Short basis $\mathbf{B}$ of $\mathcal{L}^{\perp}(\mathbf{A})$

$\Downarrow$

Invert $f_{\mathbf{A}}$ in a very strong sense

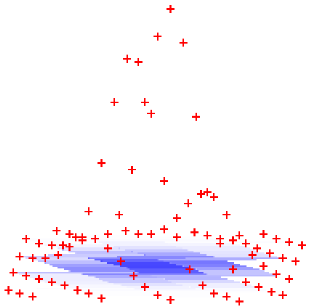
Theorem **[GPV08]**

Given *any* short $\mathbf{B}$ and $\mathbf{u}$,

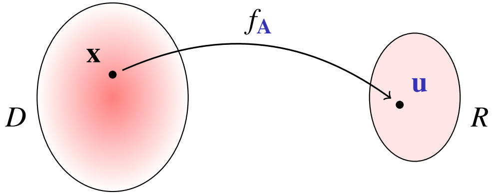
can efficiently sample $\mathbf{x} \leftarrow f_{\mathbf{A}}^{-1}(\mathbf{u})$

according to $D_{\mathbf{A},\mathbf{u}}$

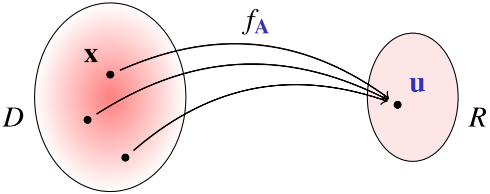
- Dist $D_{\mathbf{A},\mathbf{u}}$ leaks nothing about $\mathbf{B}$!
- Generate $\mathbf{A}$ with $\mathbf{B}$ [Aj99,AP09]



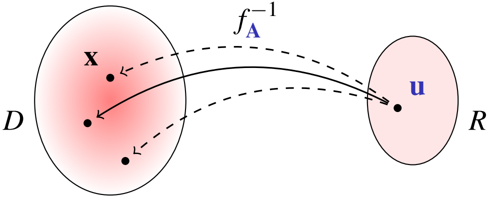
Abstractly: Preimage Sampleable Function



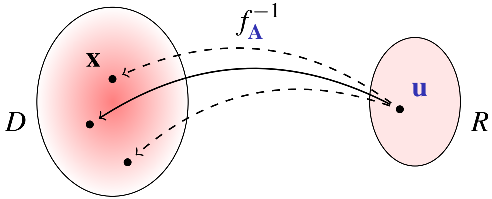
Abstractly: Preimage Sampleable Function



Abstractly: Preimage Sampleable Function

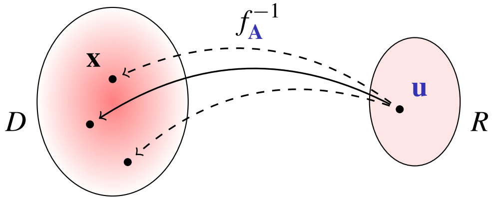


Abstractly: Preimage Sampleable Function



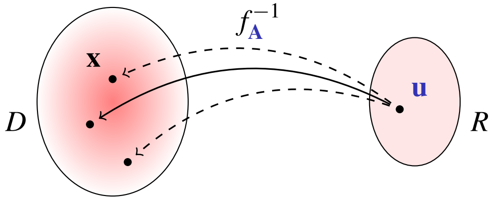
- Generalizes TDPs, claw-free pairs, Rabin, . . .

Abstractly: Preimage Sampleable Function

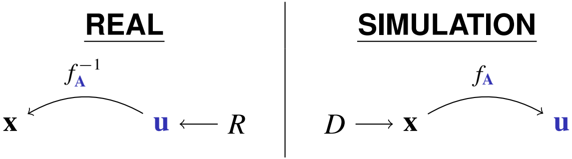


- Generalizes TDPs, claw-free pairs, Rabin, ...
- Can generate $(\mathbf{x}, \mathbf{u})$ in two equivalent ways:

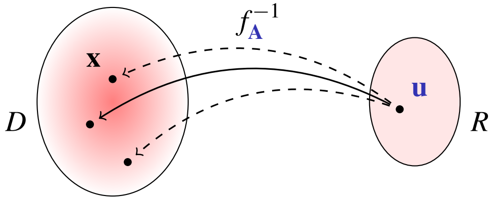
Abstractly: Preimage Sampleable Function



- Generalizes TDPs, claw-free pairs, Rabin, ...
- Can generate $(\mathbf{x}, \mathbf{u})$ in two equivalent ways:



Abstractly: Preimage Sampleable Function



- Generalizes TDPs, claw-free pairs, Rabin, ...
- Can generate $(\mathbf{x}, \mathbf{u})$ in two equivalent ways:

REAL	**SIMULATION**
$\mathbf{x} \xleftarrow{f_{\mathbf{A}}^{-1}} \mathbf{u} \longleftarrow R$	$D \longrightarrow \mathbf{x} \xrightarrow{f_{\mathbf{A}}} \mathbf{u}$

- Apps: 'hash-and-sign' sigs [GPV08], NISZK [PV08], ...

Onward, to Cryptomania . . .

Learning with Errors

- Goal: distinguish 'noisy inner products' from uniform.

$$
\begin{array}{ccc}
\mathbf{a}_1 & , & b_1 = \langle \mathbf{a}_1 , \mathbf{s} \rangle + e_1 \\
\mathbf{a}_2 & , & b_2 = \langle \mathbf{a}_2 , \mathbf{s} \rangle + e_2 \\
 & \vdots &
\end{array}
$$

Learning with Errors

- Goal: distinguish 'noisy inner products' from uniform.

$$\begin{array}{ccc} \mathbf{a}_1 & , & b_1 \\ \mathbf{a}_2 & , & b_2 \\ & \vdots & \end{array}$$

Learning with Errors

- Goal: distinguish 'noisy inner products' from uniform.

$$m \left\{ \begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix} \right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t \mathbf{s} + \mathbf{e}$$

Learning with Errors

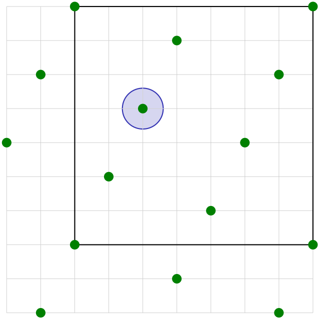
- Goal: distinguish 'noisy inner products' from uniform.

$$m\left\{\begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix}\right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

- Generator matrix $\mathbf{A}^t$:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \; : \; \exists \mathbf{s}. \; \mathbf{z} \equiv \mathbf{A}^t\mathbf{s} \bmod q\}$$

'Bounded-distance' (unique) decoding



Learning with Errors

- Goal: distinguish 'noisy inner products' from uniform.

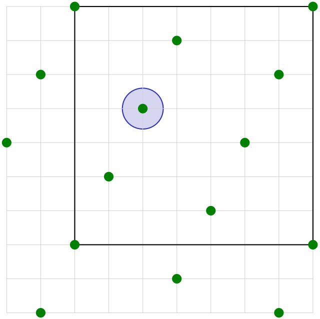
$$m\left\{\left(\begin{array}{c}\vdots\\ \mathbf{A}^t\\ \vdots\end{array}\right)\right., \quad \left(\begin{array}{c}\vdots\\ \mathbf{b}\\ \vdots\end{array}\right) = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

- Generator matrix $\mathbf{A}^t$:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \exists \mathbf{s}.\ \mathbf{z} \equiv \mathbf{A}^t\mathbf{s} \bmod q\}$$

  'Bounded-distance' (unique) decoding

- Worst-case hardness [Re05,Pe09]



Learning with Errors

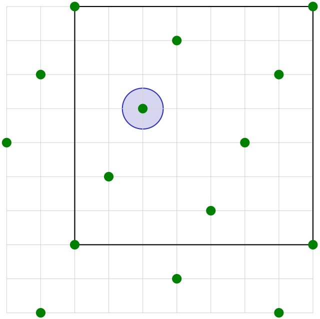
- Goal: distinguish 'noisy inner products' from uniform.

$$m\left\{\begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix}\right. , \quad \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

- Generator matrix $\mathbf{A}^t$:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \exists \mathbf{s}.\ \mathbf{z} \equiv \mathbf{A}^t\mathbf{s} \bmod q\}$$

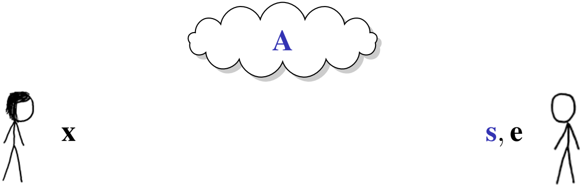
'Bounded-distance' (unique) decoding



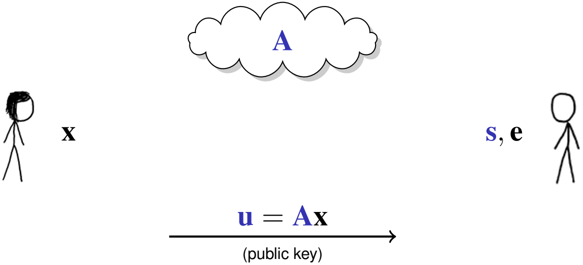
- Worst-case hardness [Re05,Pe09]
- Basis of much crypto

[Re05,PW08,GPV08,PVW08,CDMW08,AGV09,CPS09,. . .]

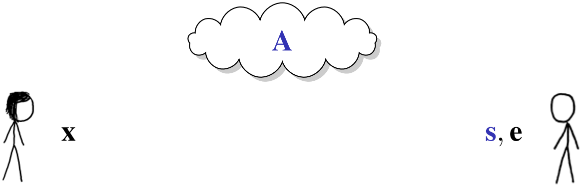
Key Agreement & Encryption



Key Agreement & Encryption



Key Agreement & Encryption



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

$\longrightarrow$

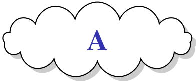
(public key)

$$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

$\longleftarrow$

(ciphertext ‘preamble’)

Key Agreement & Encryption



$\mathbf{x}$

$\mathbf{s}, \mathbf{e}$

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

→ (public key)

$$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

← (ciphertext ‘preamble’)

$$\boxed{b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'}$$

(key / ‘pad’)

Key Agreement & Encryption

$\mathbf{A}$

 $\mathbf{x}$

$\mathbf{s}, \mathbf{e}$ 

$$\mathbf{u} = \mathbf{A}\mathbf{x} \longrightarrow$$

(public key)

$$\longleftarrow \mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$$

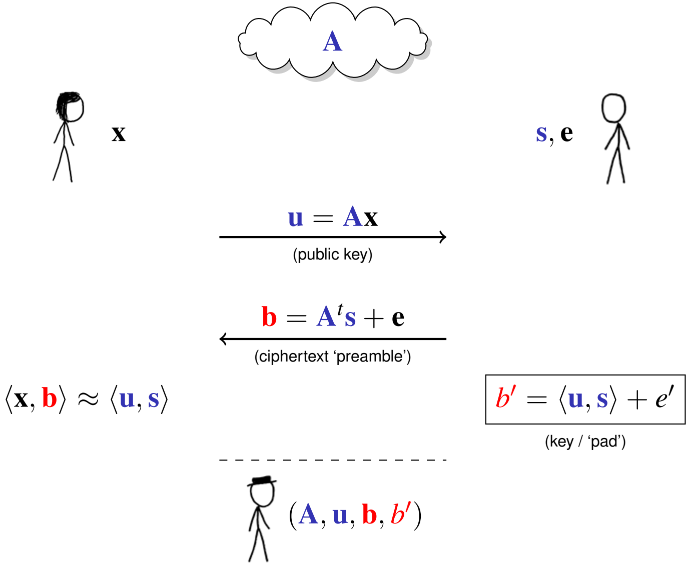
(ciphertext ‘preamble’)

$$\langle \mathbf{x}, \mathbf{b} \rangle \approx \langle \mathbf{u}, \mathbf{s} \rangle$$

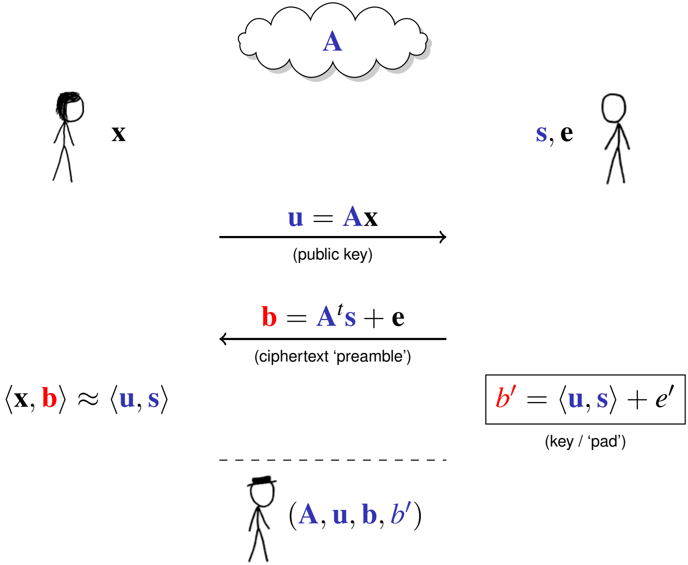
$$\boxed{b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'}$$

(key / ‘pad’)

Key Agreement & Encryption

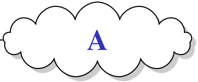


Key Agreement & Encryption



ID-Based Encryption [GPV08]

$\mathbf{x} \leftarrow f_{\mathbf{A}}^{-1}(\mathbf{u})$



$\mathbf{s}, \mathbf{e}$

$\mathbf{u} = H(\text{“alice”})$

(public key)

$\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$

(ciphertext randomness)

$\langle \mathbf{x}, \mathbf{b} \rangle \approx \langle \mathbf{u}, \mathbf{s} \rangle$

$b' = \langle \mathbf{u}, \mathbf{s} \rangle + e'$

(key / ‘pad’)

Some Open Areas

1. Hash-and-sign sigs / IBE without random oracle ?

   RSA / pairing-style 'accumulator' ?

Some Open Areas

1. Hash-and-sign sigs / IBE without random oracle ?

   RSA / pairing-style ‘accumulator’ ?

2. More expressive encryption / IBE schemes ?

Some Open Areas

1. Hash-and-sign sigs / IBE without random oracle ?

   RSA / pairing-style ‘accumulator’ ?

2. More expressive encryption / IBE schemes ?

3. Connections to number-theoretic problems ?

Further Reading

- Survey "*Cryptographic functions from worst-case complexity assumptions*" [Micciancio07]
- Survey "*Lattice-based cryptography*" [MicciancioRegev09]

Further Reading

- Survey "*Cryptographic functions from worst-case complexity assumptions*" [Micciancio07]
- Survey "*Lattice-based cryptography*" [MicciancioRegev09]

Thanks!