Presentation

Article presentation, for the ENS Lattice Based Crypto Workgroup
http://www.di.ens.fr/~pnguyen/LBC.html

Léo Ducas, 30 September 2009

How to Use Short Basis : Trapdoors for Hard Lattices and new Cryptographic Constructions

http://www.cc.gatech.edu/~cpeikert/pubs/trap_lattice.pdf

Craig Gentry Chris Peikert Vinod Vaikuntanathan

Previous Trapdoors Using Lattice

$$A \in \mathbb{Z}_q^{n \times m} \quad (m > n)$$

$$\mathbb{Z}_q^m \cap S_d \xrightarrow{\quad f_A(e) = Ae \quad} \mathbb{Z}_q^n$$

Short error vector e — Syndrome u

Hard to invert ? Yes : finding a short solution e to $Ae = u$

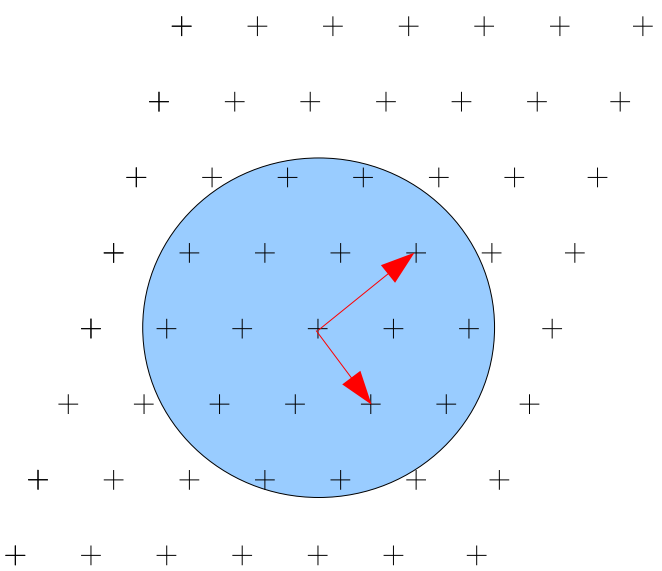
(ISIS for a random u, SIS for u=0 and e<>0)

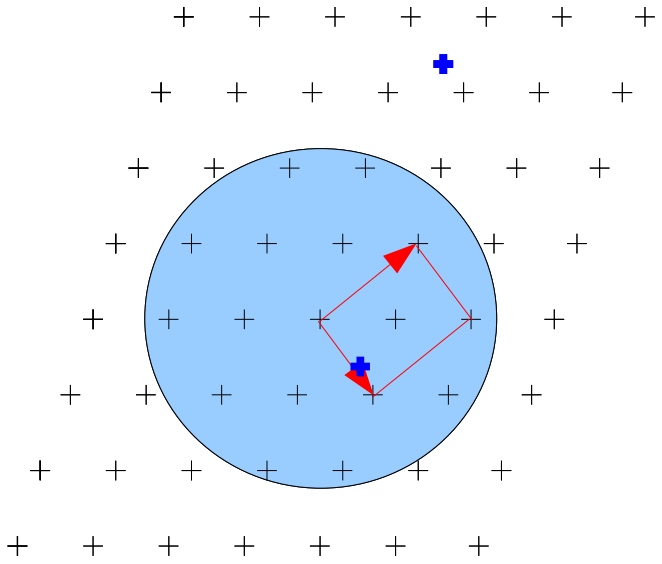
Trapdoor ? Yes : A short basis for the lattice

$$\Lambda = \{ e \in \mathbb{Z}^m / Ae = 0 \, mod \, q \}$$

Previous Trapdoors Using Lattice

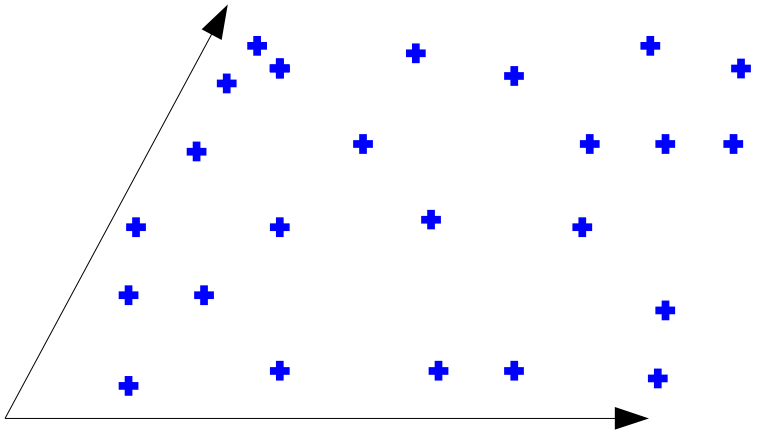
Trapdoor : Reducing the point modulo a short basis





But ...

Previous Trapdoors Using Lattice : information leakage

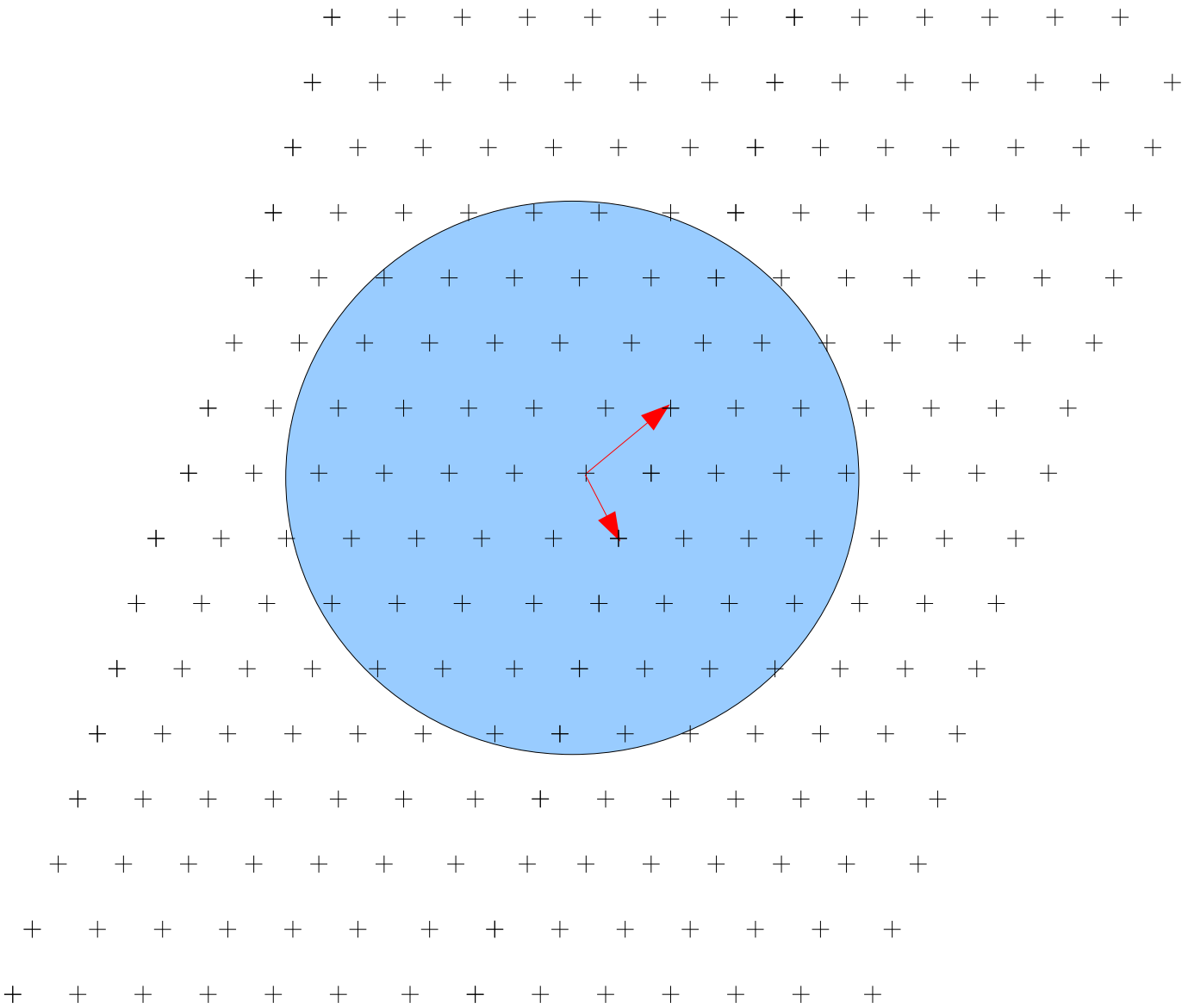


Inverting enough random points reveal the trapdoor basis

Randomization ?

Avoiding information leakage ?

If the domain is big enough, we may sample random preimage without revealing the basis



Avoiding information leakage ! [Sec 3,4]

Theorem 4.1. *There is a probabilistic polynomial-time algorithm that, given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* $\Lambda = \mathcal{L}(\mathbf{B})$*, a parameter* $s \geq \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$*, and a center* $\mathbf{c} \in \mathbb{R}^n$*, outputs a sample from a distribution that is statistically close to* $D_{\Lambda,s,\mathbf{c}}$.

$D_{\Lambda,s,c}$: Discrete Gaussian distribution on the lattice Λ
With deviation s and center c

Randomized version of the nearest plane algorithm

1. Let $\mathbf{v}_n \leftarrow \mathbf{0}$ and $\mathbf{c}_n \leftarrow \mathbf{c}$. For $i \leftarrow n, \ldots, 1$, do:
   (a) Let $c'_i = \langle \mathbf{c}_i, \tilde{\mathbf{b}}_i \rangle / \langle \tilde{\mathbf{b}}_i, \tilde{\mathbf{b}}_i \rangle \in \mathbb{R}$ and $s'_i = s / \|\tilde{\mathbf{b}}_i\| > 0$.
   (b) Choose $z_i \sim D_{\mathbb{Z},s'_i,c'_i}$ (this is the only step that differs from the nearest-plane algorithm).
   (c) Let $\mathbf{c}_{i-1} \leftarrow \mathbf{c}_i - z_i \mathbf{b}_i$ and let $\mathbf{v}_{i-1} \leftarrow \mathbf{v}_i + z_i \mathbf{b}_i$.
2. Output $\mathbf{v}_0$.

Preimage Sampleable Functions [Sec 5]

Previous algorithm can be used to construct a new cryptographic primitive :

A collection of one-way Preimage Sampleable Functions (PSFs)

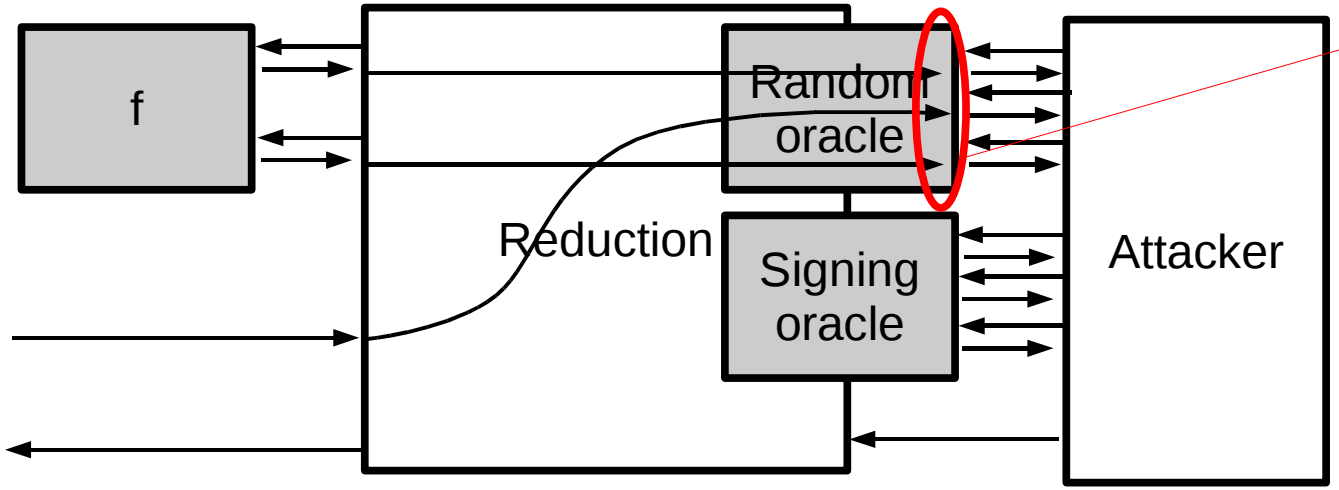
- Generation of a function with a trapdoor
- Uniform output for a given input distribution
- Preimage sampleable with trapdoor (following conditional distribution)
- One-wayness without trapdoor

That are also collision resistant without the trapdoor

(and have many preimage, high min-entropy)

Tightly secure FDH signature scheme [Sec 6]

Reduction to One-wayness



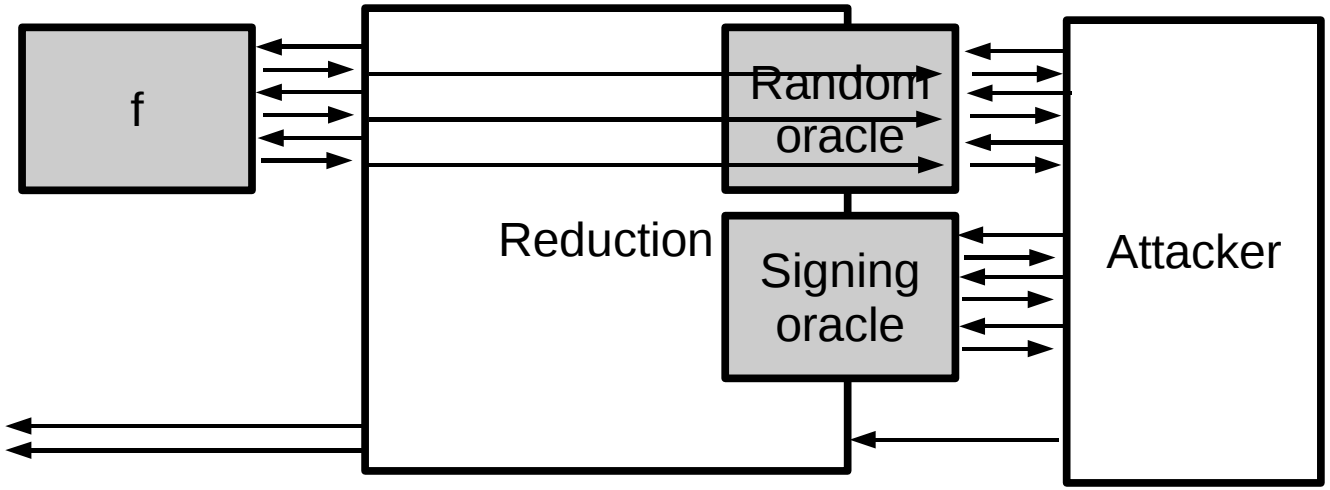
Need to guess on which digest the Attacker will choose

↓

Q_{hash} loss with generic trapdoor permutation (provable)

Q_{sign} loss with RSA (provable)

Reduction to Collision Resistance (with high min-entropy)



Tight Reduction

Another Trapdoor using LWE [Sec 7,8]

The Learning With Error problem also yield to trapdoor functions

$$A \in \mathbb{Z}_q^{n \times m} \quad (m > n)$$

	Alice	Bob
Secret	$e \leftarrow D_{\mathbb{Z}^m, r}$	$s \leftarrow \mathbb{Z}^n, x \leftarrow D_{\mathbb{Z}^m, \alpha}$
Public	$u \leftarrow Ae \in \mathbb{Z}_q^n$ $(u = f_A(e) \in \mathbb{Z}_q)$	$p \leftarrow A^T s + x \in \mathbb{Z}_q^m$ $(p = f'_A(s, x) \in \mathbb{Z}_q^m)$
Common secret	$k_A = e^T \cdot p$	$k_B = u^T \cdot s$

$$k_A - k_B = e^T \cdot p - u^T \cdot s = e^T \cdot (A^T s + x) - (Ae)^T s$$
$$= e^T A^T s + e^T \cdot x - (Ae)^T \cdot s = e^T \cdot x$$

$|k_A - k_B| \leqslant C\, r\, \alpha\, m$ With overwhelming probability

Two dual cryptosystems (1) [Sec 8]

Public key cryptosystem for a single-bit message b (let B = b [q/2])

	Alice	Bob
Key Generation		$sk = s \leftarrow \mathbb{Z}^n, x \leftarrow D$ $pk = p \leftarrow A^T s + x$
Encryption	$e \leftarrow D_{\mathbb{Z}^m, r}$ $u \leftarrow Ae \in Z^n$ $k_A = e^T \cdot p$ $c = (u, C = B - k_A)$	
Decryption		$k_B = u^T \cdot s$ $B' = B + k_B$

Variant of the cryptosystem from [Reg05]

Two dual cryptosystems (2) [Sec 7]

Public key cryptosystem for a single-bit message b (let B = b [q/2])

	Alice	Bob
Key Generation	$sk = e \leftarrow D_{\mathbb{Z}^m, r}$ $pk = u \leftarrow Ae \in \mathbb{Z}_q^n$	
Encryption		$s \leftarrow \mathbb{Z}_q^n, x \leftarrow D_{\mathbb{Z}^m, \alpha}$ $p \leftarrow A^T s + x \in \mathbb{Z}_q^m$ $k_B = u^T \cdot s$ $c = (p, C = k_B + B)$
Decryption	$k_A = e^T \cdot p$ $B' = c_2 - k_A$	

IBE Construction [Sec 7,8]

	Alice	Bob
Secret	$e \leftarrow D_{\mathbb{Z}^m, r}$	$s \leftarrow \mathbb{Z}^n, x \leftarrow D_{\mathbb{Z}^m, \alpha}$
Public	$u \leftarrow Ae \in \mathbb{Z}_q^n$ $(u = f_A(e))$	$p \leftarrow A^T s + x \in \mathbb{Z}_q^m$ $(p = f'_A(s, x))$

A short basis for the lattice Λ gives a trapdoor for those two functions

The common matrix A generation must be trusted.

f_A

Surjective, not injective

↓

Identity based Encryption System
(secure in the Random Oracle Model)

f'_A

Injective, not surjective
(image exponentially sparse)