Identity Based Encryption from lattices

Pauline Bert

October 3, 2017

Outline

Preliminaries

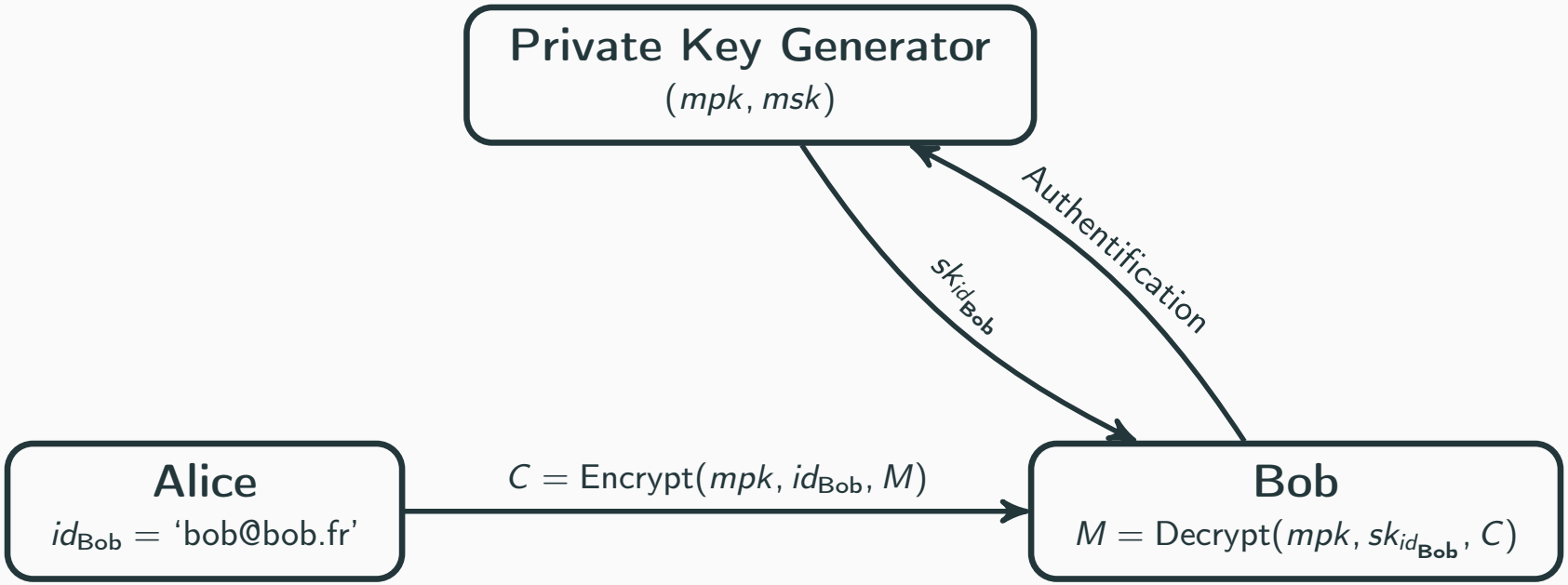
The first IBE from lattices

Our IBE from lattices

Ring-LWE construction

Implementation

Identity Based Encryption

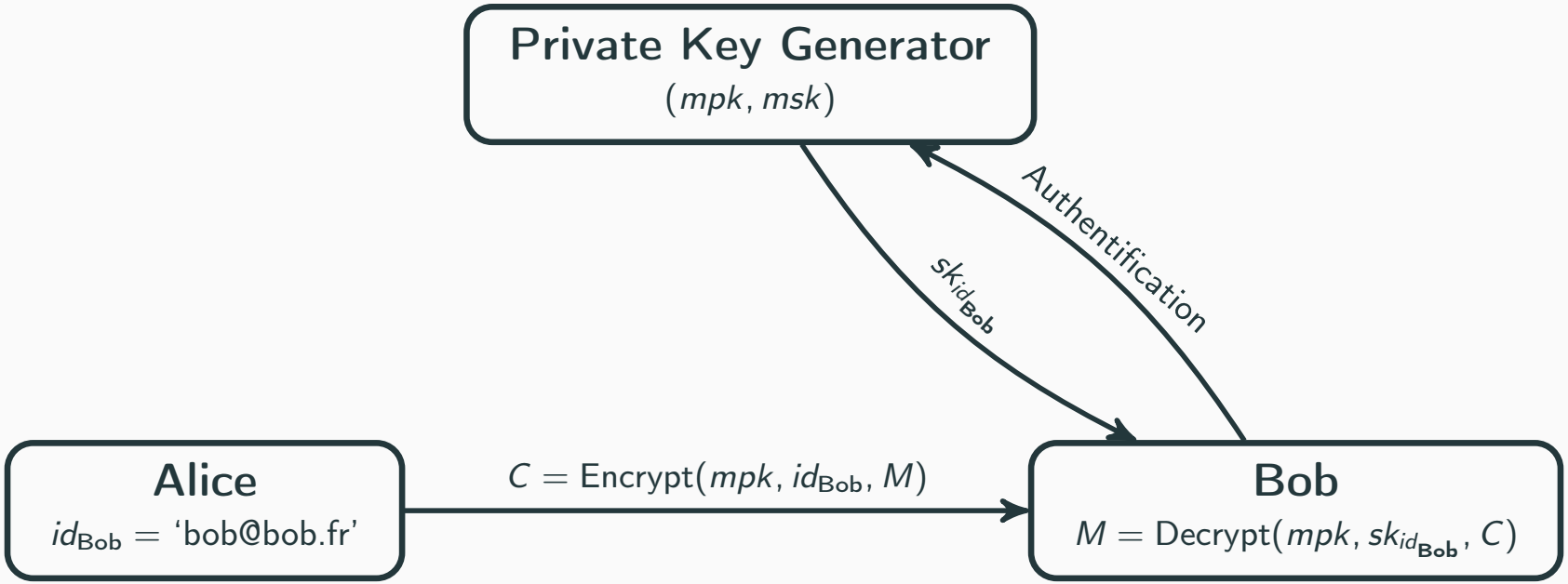


1984 Concept introduced by Shamir,

2001 First realizations based on bilinear maps (by Boneh and Franklin) and on quadratic residue assumptions (by Cocks),

2008 First lattice based IBE, by Gentry, Peikert, and Vaikuntanathan.

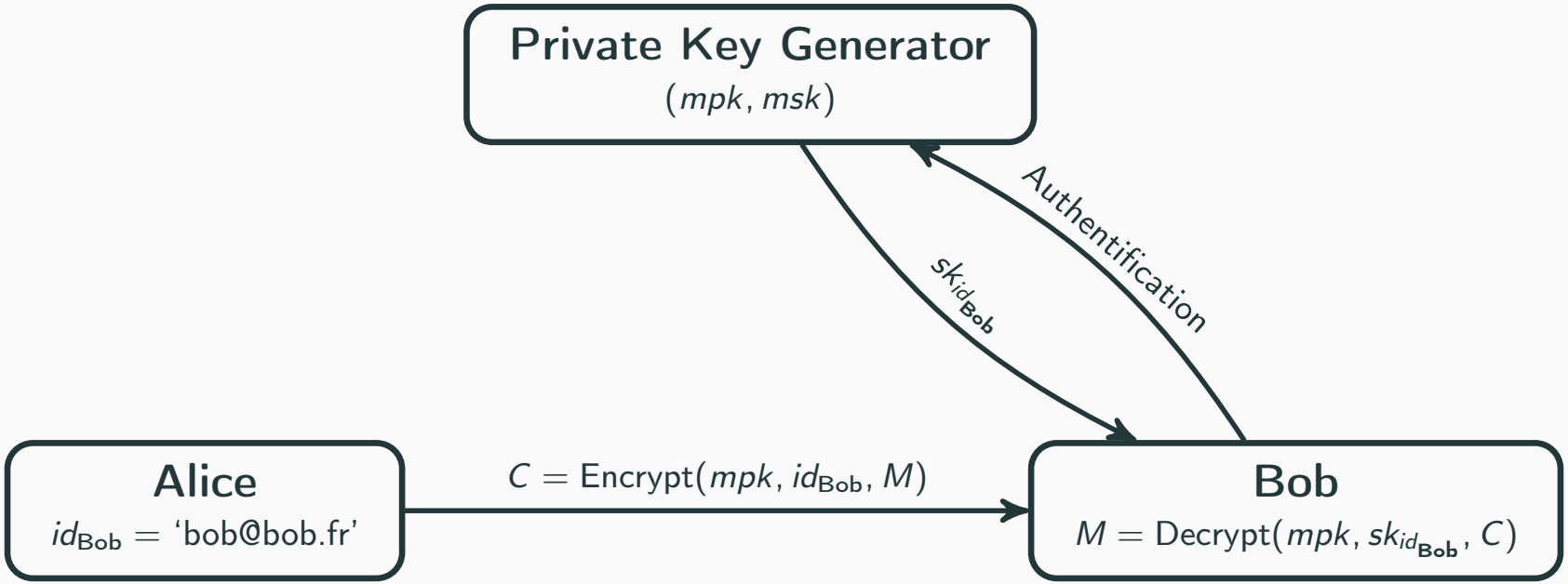
Identity Based Encryption



Advantages:

- we no longer need certificates, PKI, cross-certification, revocation lists $\mathrm{etc.}$,
- we can add information together with the identity, for $\mathrm{e.g.}$, identity | 2017 or identity | 25.04.2017.

Identity Based Encryption

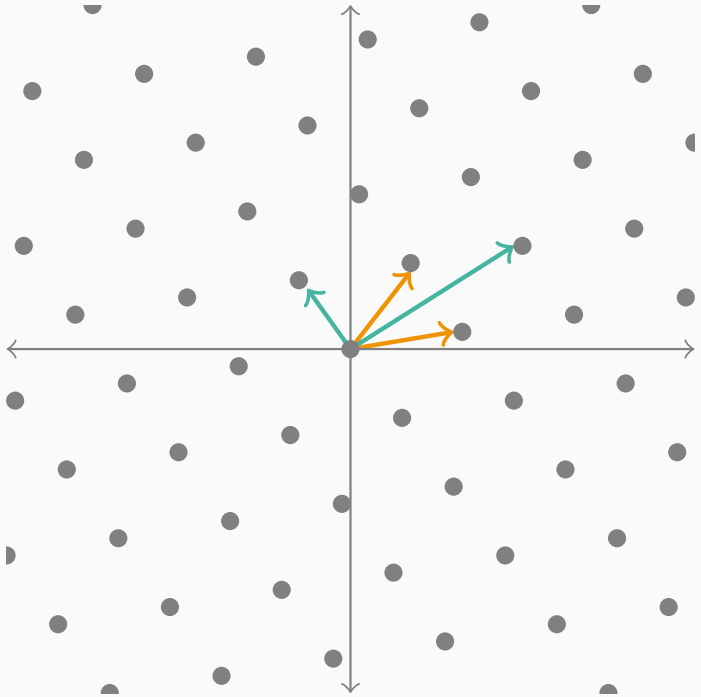


Contributions:

- We propose a new IBE scheme,
- We implement it to see if this kind of construction can be practical.

Preliminaries

Lattices

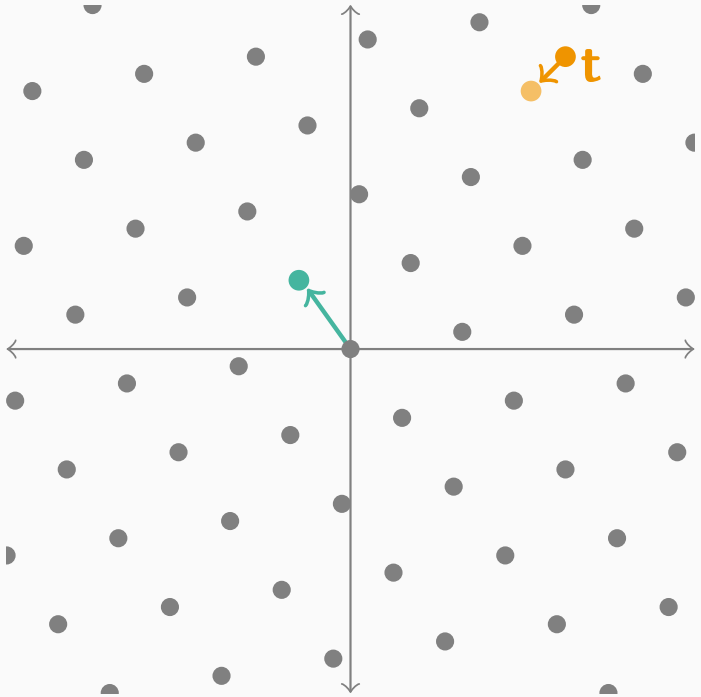


Basis

A lattice $\Lambda \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of some linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_k\}$,

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{k} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

Lattices



SVP

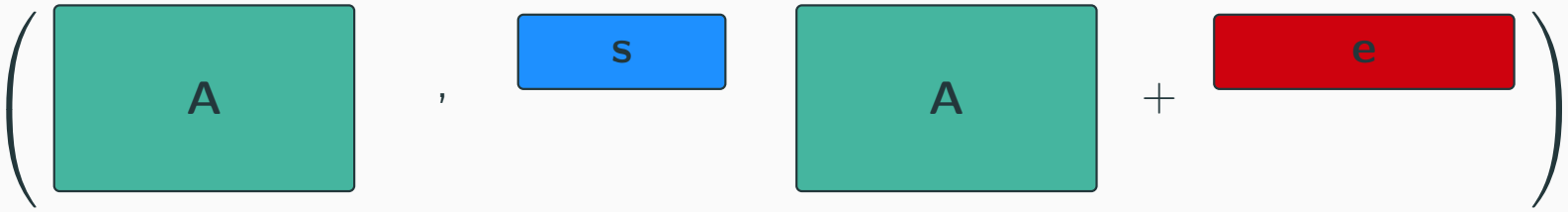
Given a basis $\mathbf{B}$ of a lattice Λ, find one of the shortest non zero vector of Λ.

CVP

Given a basis $\mathbf{B}$ of a lattice Λ, and a vector $\mathbf{t} \in \mathbb{R}^n$ find the closest lattice vector of the target vector $\mathbf{t}$.

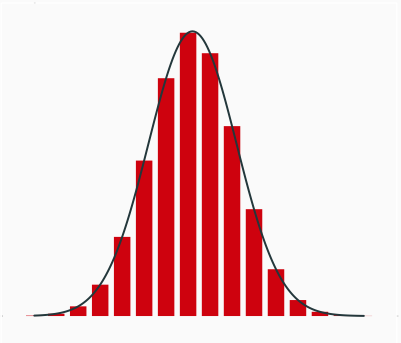
Learning With Errors problem

Given

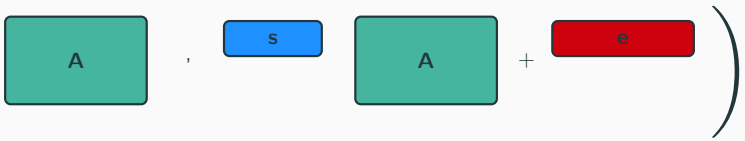


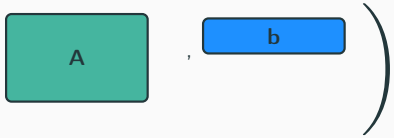
where:

- $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$,
- $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$,
- $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.



The search problem is to find $\mathbf{s}$.

The decision problem is to distinguish 

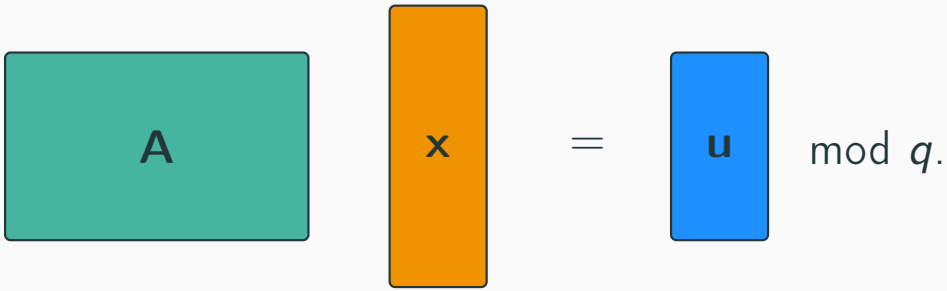
from 

with $\mathbf{b} \hookleftarrow U(\mathbb{Z}_q^m)$.

$\rightarrow$ This two variants are equivalent.

Short Integer Solution problem

Given an uniformly random matrix $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$, the Inhomogeneous Short Integer Solution problem is to find a non trivial short vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\|\mathbf{x}\| \leq \beta$ and:



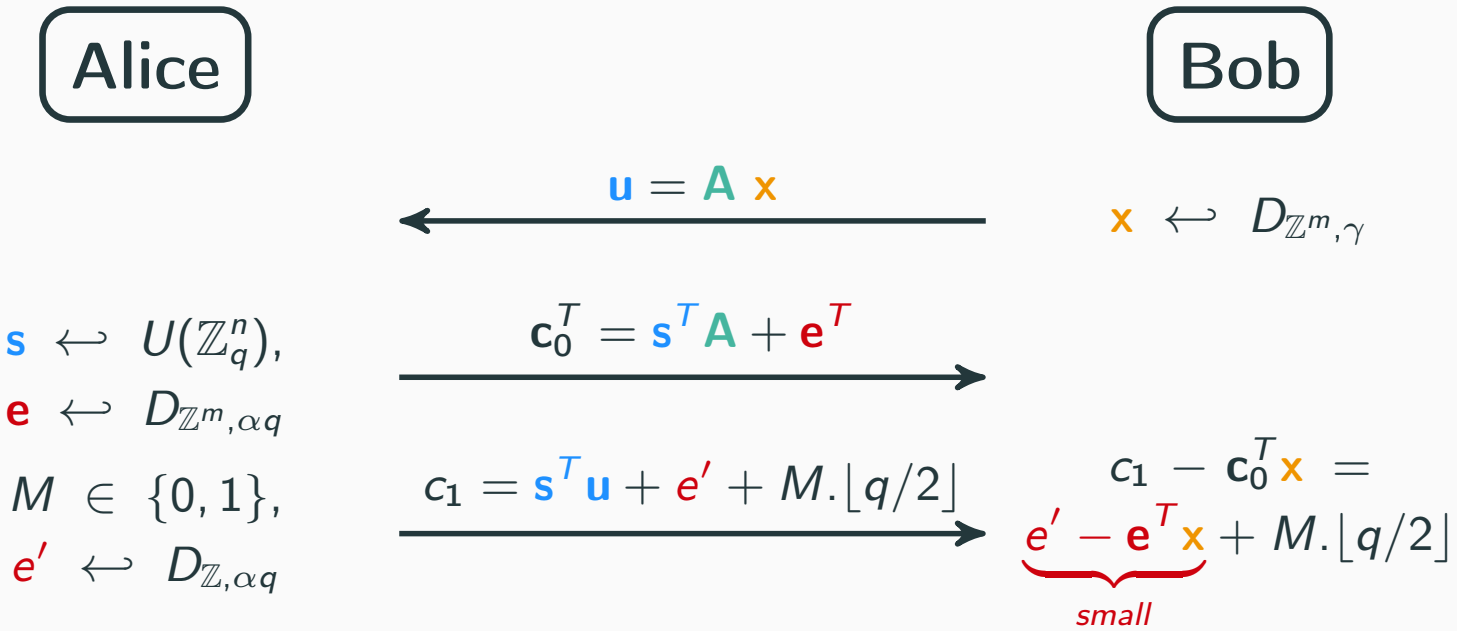
The Short Integer Solution problem is to find a non trivial short vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\|\mathbf{x}\| \leq \beta$ and $\mathbf{Ax} = \mathbf{0} \mod q$.

$\longrightarrow$ LWE/SIS are hard: Regev/Ajtai gave reductions from worst-case problems on lattices (eg. approximate decisional SVP problem) to the average-case LWE/SIS problems.

The first IBE from lattices

Public Key Encryption of Dual-Regev[1]

In this scheme, users share a public matrix $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$.



[1] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan (2008). "How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions". In: *STOC 2008*. http://eprint.iacr.org/2007/432.pdf.

Full trapdoor for LWE and SIS

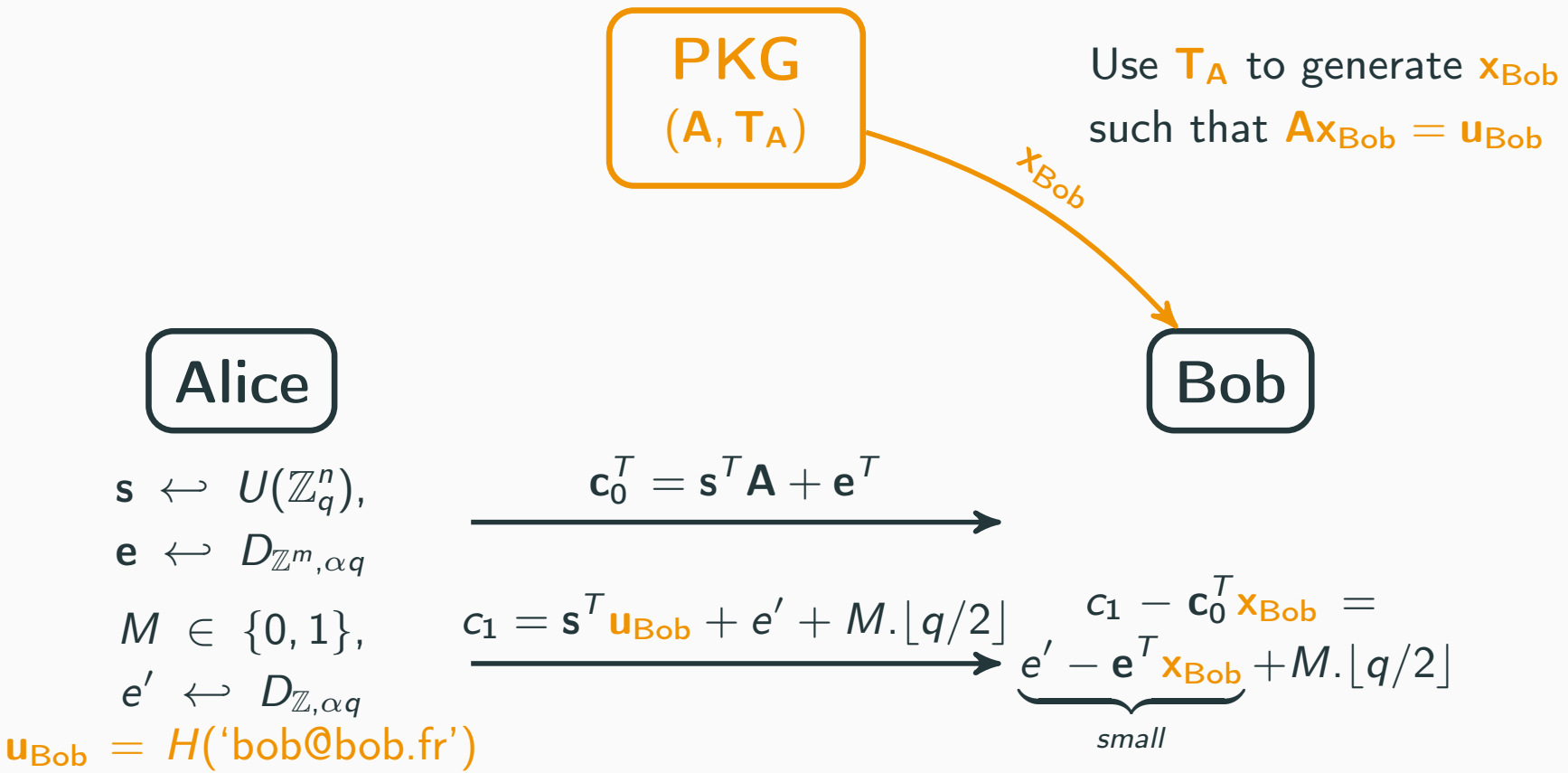
A full trapdoor for the LWE and SIS problems is a short basis $\mathbf{T_A}$ of the lattice

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \text{ such that } \mathbf{Ax} = \mathbf{0} \mod q\}.$$

- Given $\mathbf{A}$, it's hard to find such basis,
- we can generate $\mathbf{A}$ together with $\mathbf{T_A}$,
- we can use $\mathbf{T_A}$ to solve the SIS problem, i.e. find a non trivial $\mathbf{x} \in \mathbb{Z}^m$ s.t. $\mathbf{Ax} = \mathbf{0} \mod q$, (resp. $\mathbf{Ax} = \mathbf{u} \mod q$).

The first IBE from lattices

Let $H : \{0,1\}^* \to \mathbb{Z}_q^n$ a hash function.



Our IBE from lattices

Trapdoor construction[2]

Let $k = \lceil \log_2 q \rceil$, the matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is now generated with a trapdoor matrix $\mathbf{R}$ as:

$$\mathbf{A} = (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R}) .$$

- $\mathbf{G} \in \mathbb{Z}_q^{n \times nk}$ a public 'gadget matrix' associated to an highly structured basis,
- $\mathbf{A}' \hookleftarrow U\left(\mathbb{Z}_q^{n \times (m-nk)}\right)$ a uniform matrix,
- $\mathbf{H} \in \mathbb{Z}_q^{n \times n}$ an invertible tag,
- $\mathbf{R} \hookleftarrow D_{\mathbb{Z}^{(m-nk) \times nk}, \beta}$ the trapdoor matrix associated to $\mathbf{H}$,

$\longrightarrow$ Smaller trapdoor, faster algorithms.

---

[2] Daniele Micciancio and Chris Peikert (2012). "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller". In: *EUROCRYPT 2012*. https://eprint.iacr.org/2011/501.pdf.

Our IBE scheme (1)

We can remark that, if $\mathbf{A} = (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R})$ has trapdoor $\mathbf{R}$ with tag $\mathbf{H}$, then

$$\mathbf{A} - (\mathbf{0} \,|\, \mathbf{H}'\mathbf{G}) = (\mathbf{A}' \,|\, (\mathbf{H} - \mathbf{H}')\mathbf{G} - \mathbf{A}'\mathbf{R})$$

has also trapdoor $\mathbf{R}$ but with tag $(\mathbf{H} - \mathbf{H}')$,

$\longrightarrow$ $(\mathbf{H} - \mathbf{H}')$ needs to be invertible $\longrightarrow$ FRD map[3].

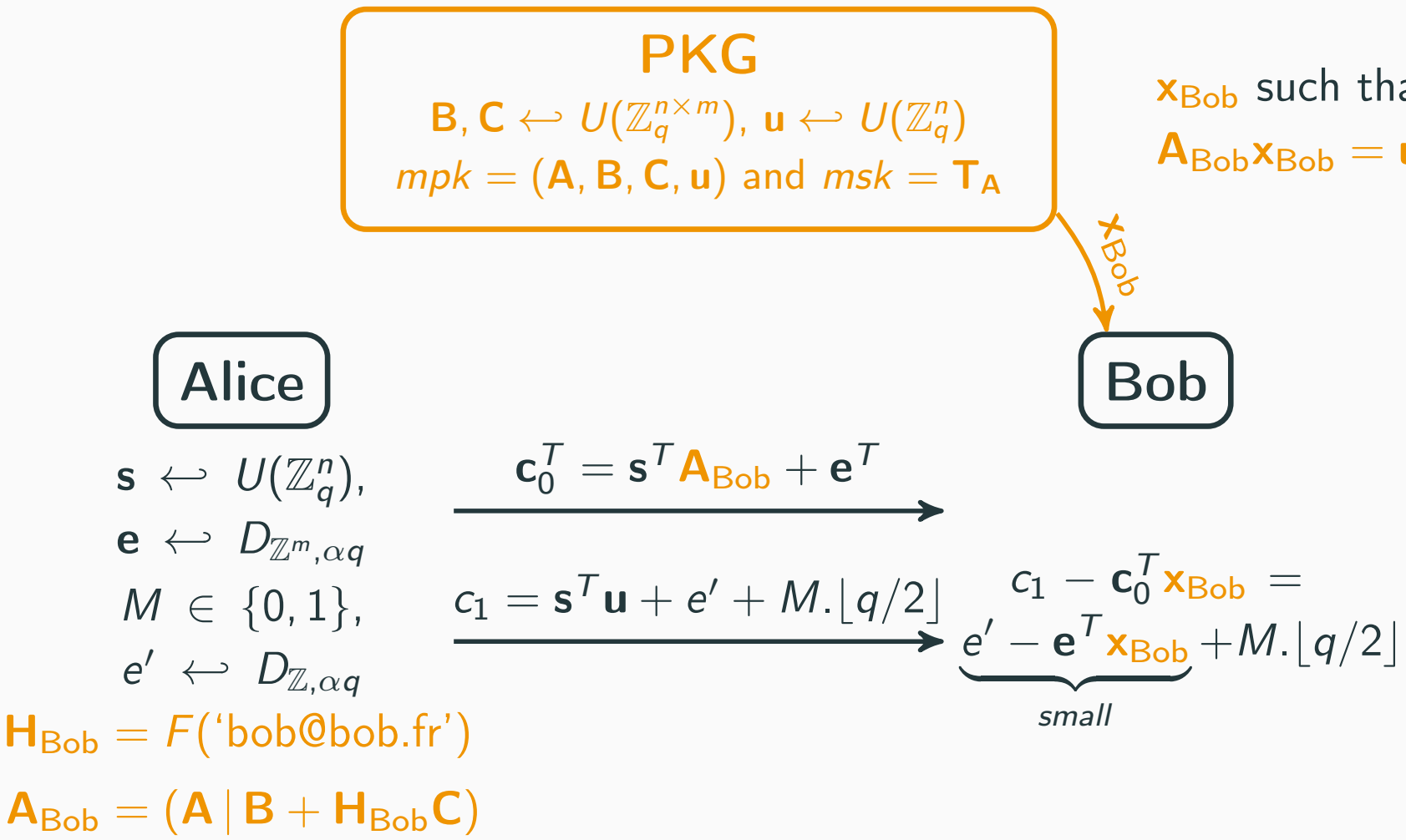
FRD map

A function $F : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ is an encoding with *Full-Rank Differences* if:

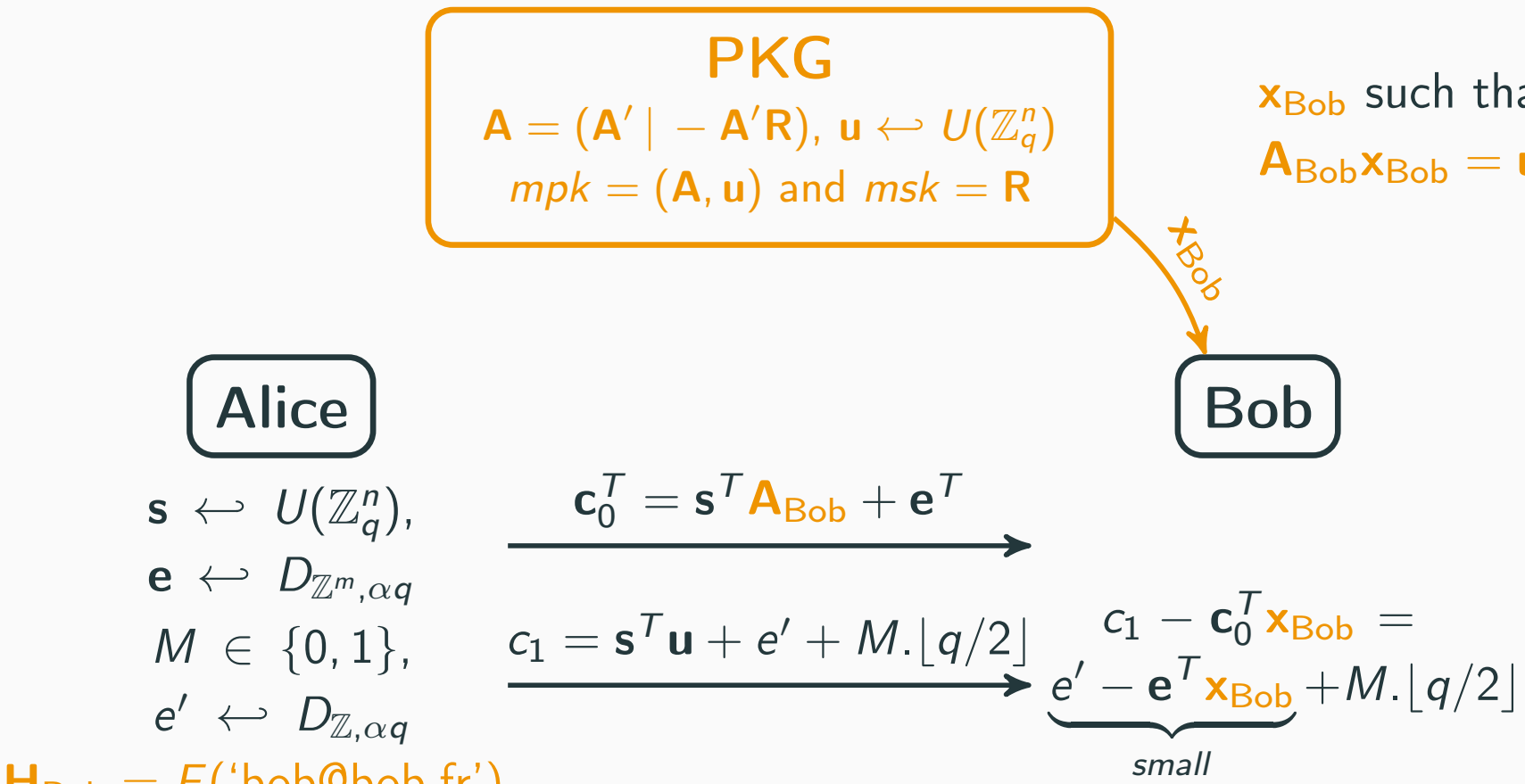
- for all $u \in \mathbb{Z}_q^n$ the matrix $F(u)$ is invertible,
- for all distinct u, $v \in \mathbb{Z}_q^n$ the matrix $F(u) - F(v)$ is full rank.

[3] Shweta Agrawal, Dan Boneh, and Xavier Boyen (2010). "Efficient Lattice (H) IBE in the Standard Model". In: *EUROCRYPT 2010*. http://www.iacr.org/archive/eurocrypt2010/66320276/66320276.pdf.

IBE scheme of ABB



Our IBE scheme (2)



$\mathbf{H}_{\text{Bob}} = F(\text{'bob@bob.fr'})$

$\mathbf{A}_{\text{Bob}} = \mathbf{A} + (\mathbf{0} \mid \mathbf{H}_{\text{Bob}}\mathbf{G})$

$= (\mathbf{A}' \mid \mathbf{H}_{\text{Bob}}\mathbf{G} - \mathbf{A}'\mathbf{R})$

Private key extraction (1)

Given $\mathbf{A} = (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R})$, $\mathbf{H}$, $\mathbf{R}$ and a target vector $\mathbf{u} \in \mathbb{Z}_q^n$,

$\rightarrow$ we want to get a short vector $\mathbf{x}$ such that $\mathbf{Ax} = \mathbf{u} \mod q$.

First idea:

1. Compute $\mathbf{v} = \mathbf{H}^{-1}\mathbf{u}$,
2. Sample a short vector $\mathbf{y}$ such that $\mathbf{Gy} = \mathbf{v} \mod q$,
3. Then $\mathbf{x} = \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \mathbf{y}$ works.

Private key extraction (1)

Given $\mathbf{A} = (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R})$, $\mathbf{H}$, $\mathbf{R}$ and a target vector $\mathbf{u} \in \mathbb{Z}_q^n$,

$\rightarrow$ we want to get a short vector $\mathbf{x}$ such that $\mathbf{Ax} = \mathbf{u} \mod q$.

First idea:

1. Compute $\mathbf{v} = \mathbf{H}^{-1}\mathbf{u}$,
2. Sample a short vector $\mathbf{y}$ such that $\mathbf{Gy} = \mathbf{v} \mod q$,
3. Then $\mathbf{x} = \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \mathbf{y}$ works.
   Proof:

$$\begin{aligned} \mathbf{Ax} &= (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R}) \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \mathbf{y} \\ &= \mathbf{A}'\mathbf{Ry} + (\mathbf{HG} - \mathbf{A}'\mathbf{R})\,\mathbf{y} \\ &= \mathbf{H} \underbrace{\mathbf{Gy}}_{\mathbf{H}^{-1}\mathbf{u}} = \mathbf{u} \end{aligned}$$

Private key extraction (1)

Given $\mathbf{A} = (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R})$, $\mathbf{H}$, $\mathbf{R}$ and a target vector $\mathbf{u} \in \mathbb{Z}_q^n$,

$\rightarrow$ we want to get a short vector $\mathbf{x}$ such that $\mathbf{Ax} = \mathbf{u} \mod q$.

First idea:

1. Compute $\mathbf{v} = \mathbf{H}^{-1}\mathbf{u}$,
2. Sample a short vector $\mathbf{y}$ such that $\mathbf{Gy} = \mathbf{v} \mod q$,
3. Then $\mathbf{x} = \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \mathbf{y}$ works.
   Proof:

$$\begin{aligned} \mathbf{Ax} &= (\mathbf{A}' \,|\, \mathbf{HG} - \mathbf{A}'\mathbf{R}) \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \mathbf{y} \\ &= \mathbf{A}'\mathbf{Ry} + (\mathbf{HG} - \mathbf{A}'\mathbf{R})\,\mathbf{y} \\ &= \mathbf{H} \underbrace{\mathbf{Gy}}_{\mathbf{H}^{-1}\mathbf{u}} = \mathbf{u} \end{aligned}$$

$\longrightarrow$ $\mathbf{x}$ leaks the trapdoor matrix $\mathbf{R}$, has covariance $\mathbf{COV}_\mathbf{x} = r^2 \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{R}^T & \mathbf{I} \end{pmatrix}$.

Private key extraction (2)

Solution: add perturbation vector $\mathbf{p}$ to correct the distribution[4]:

1. Sample $\mathbf{p} \hookleftarrow D_{\mathbb{Z}^m, \mathbf{COV_p}}$,
   $\rightarrow$ need to compute the square root of the matrix
   $\mathbf{COV_p} = \gamma^2 \mathbf{I} - r^2 \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{R}^T & \mathbf{I} \end{pmatrix}$.
2. Compute $\mathbf{v} = \mathbf{H}^{-1}(\mathbf{u} - \mathbf{Ap})$,
3. Sample a short $\mathbf{y}$ such that $\mathbf{Gy} = \mathbf{v} \mod q$,
4. Then $\mathbf{x} = \mathbf{p} + \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \mathbf{y}$ has covariance
   $\mathbf{COV_x} = \mathbf{COV_p} + r^2 \begin{pmatrix} \mathbf{R} \\ \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{R}^T & \mathbf{I} \end{pmatrix} = \gamma^2 \mathbf{I}$ and satisfies $\mathbf{Ax} = \mathbf{u}$.

---

[4] Chris Peikert (2010). "An Efficient and Parallel Gaussian Sampler for Lattices". In: *Advances in Cryptology–CRYPTO 2010*. https://eprint.iacr.org/2010/088.pdf.

Ring-LWE construction

From random lattice to ideal lattice (1)

Consider the rings $R = \mathbb{Z}[x]/(x^n + 1)$ or $R_q = R/qR$, with n a power of 2.

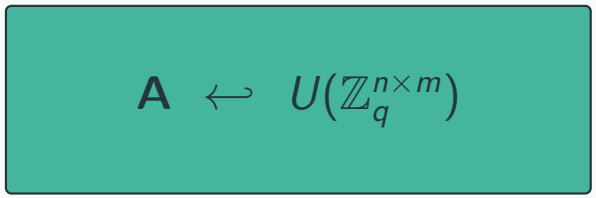
If we have s, $a \in R_q$, $s = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$,

$$s \cdot a = \begin{pmatrix} s_0 & s_1 & \cdots & s_{n-1} \end{pmatrix} \underbrace{\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ & & \ddots & \\ -a_1 & -a_2 & \cdots & a_0 \end{pmatrix}}_{=\mathrm{rot}(a)}$$

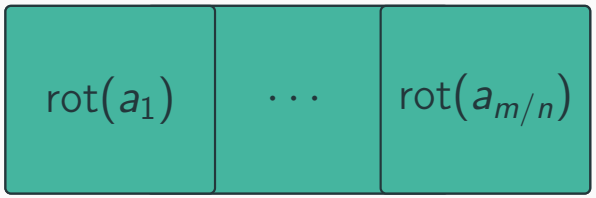
$\longrightarrow$ Smaller storage, faster operations.

From random lattice to ideal lattice (2)

Random lattice: integer elements in $\mathbb{Z}$ or $\mathbb{Z}_q$.



Ideal lattice: polynomial elements in R or R_q, with n a power of 2.



LWE:
Given $\left(\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T\right)$ find $\mathbf{s} \in \mathbb{Z}_q^n$.

SIS:
Given $\mathbf{A}$, find a short vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{u}$.

Ring-LWE:
Given $\left(s \cdot a_1 + e_1, \cdots, s \cdot a_{m/n} + e_{m/n}\right)$ find $s \in R_q$.

Ring-SIS:
Given $a_1, \cdots, a_{m/n}$, find $x_1, \cdots, x_{m/n}$ such that $\sum_{i=1}^{m/n} a_i \cdot x_i = u$.

Implementation

Librairies used

- NFLlib[5] / GMP [6] for the operations over the ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ with n a power of two, q a product of primes of size 14, 30 or 62 bits.
- FLINT [7] / MPFR [8] for the operations over $\mathbb{Q}[x]/(x^n + 1)$.

---

[5] Carlos Aguilar-Melchor et al. (2016). "NFLlib: NTT-based Fast Lattice Library". In: *RSA Conference Cryptographers' Track*. https://hal.archives-ouvertes.fr/hal-01242273/file/main.pdf.

[6] https://gmplib.org/

[7] http://www.flintlib.org/

[8] http://www.mpfr.org/

Proposed parameters / Timings (ms)

n	m	$\lceil \log_2 q \rceil$	λ [9]	KeyGen	Extract	Enc	Dec
256	60	30	52	1525	215	0,59	0,06
512	60	30	100	4690	690	1,3	0,12
1024	60	30	192	14960	1360	2,4	0,2

where

- n is the degree of the polyomials,
- m is the number of polynomials in the master public key,
- k is the size of the modulus q.

[9] `https://bitbucket.org/malb/lwe-estimator`

Comparison with other implementations (ms)

Scheme	Assumption	λ	Extract	Enc	Dec
Our	Ring-LWE	100	690	1,3	0,12
Our	Ring-LWE	192	1360	2,4	0,2
GPV[10]	NTRU/Ring-LWE	80	8,6	0,91	0,62
GPV	NTRU/Ring-LWE	192	32,7	1,87	1,27
BF[11]	DL	128	0,55	7,51	5,05
BF	DL	192	3,44	40,3	34,2

[10] Leo Ducas, Vadim Lyubashevsky, and Thomas Prest (2014). "Efficient identity-based encryption over NTRU lattices". In: *ASIACRYPT 2014*. https://eprint.iacr.org/2014/794.pdf.

[11] Aurore Guillevic (2013). "Arithmetic of pairings on algebraic curves for cryptography". https://tel.archives-ouvertes.fr/tel-00921940/file/Guillevic2013thesis.pdf. PhD thesis.

Comparison with other implementations (ms)

Scheme	Assumption	λ	Extract	Enc	Dec
Our	Ring-LWE	100	690	1,3	0,12
Our	Ring-LWE	192	1360	2,4	0,2
GPV	NTRU/Ring-LWE	80	8,6	0,91	0,62
GPV	NTRU/Ring-LWE	192	32,7	1,87	1,27
BF	DL	128	0,55	7,51	5,05
BF	DL	192	3,44	40,3	34,2

- We proposed a IBE scheme based on the Ring-LWE assumption, and we implement it.

$\longrightarrow$ Future work: omptimize our code, and improve the construction.