Anonymity-oriented Signatures based on Lattices

YACC 2014

Fabien Laguillaumie

fabien.laguillaumie@ens-lyon.fr
http://perso.ens-lyon.fr/fabien.laguillaumie

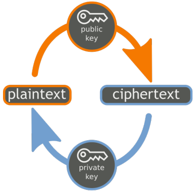
Roadmap

- Introduction
- Lattice-based cryptography and *Learning with Errors*
- Motivation for anonymity-oriented signatures
- Lattice-based group signatures
- Conclusion

Introduction

- Cryptography = design of secure protocols
  confidentiality - authenticity - integrity

- Public Key Cryptography:



  - Concept: Diffie & Hellman '76
  - The secret is secret $\rightsquigarrow$ a public key is available

$$sk \longleftrightarrow pk$$

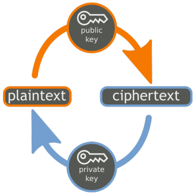
  - First realizations:
    - RSA '78 — factorization
    - Merkle-Hellman '78 — knapsack
    - McEliece'78 — decoding of error correction codes
    - Elgamal '84 — discrete logarithm over $(\mathbb{F}_q)^\star$
    - Koblitz / Miller '85 — discrete logarithm over elliptic curves

Introduction

- Cryptography = design of secure protocols

  confidentiality - authenticity - integrity

- Public Key Cryptography:

  - Concept: Diffie & Hellman '76
  - The secret is secret $\rightsquigarrow$ a public key is available

$$sk \longleftrightarrow pk$$

  - First realizations:
    - RSA '78 — factorization
    - Merkle-Hellman '78 — knapsack
    - McEliece'78 — decoding of error correction codes
    - Elgamal '84 — discrete logarithm over $(\mathbb{F}_q)^\star$
    - Koblitz / Miller '85 — discrete logarithm over elliptic curves

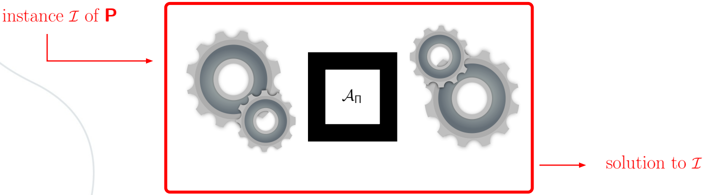
Not enough any more !

Introduction

What does secure mean ? depends on the application

- $\rightsquigarrow$ *security model* for a cryptographic primitive
- $\rightsquigarrow$ *proof* of its (in)security

  to prove = to reduce a "hard" problem **P** to an attack against the scheme **Π**



Introduction

Public-Key Cryptography:

Protocols

- e-cash
- e-voting
- anonymous access in the cloud

Cryptographic Primitives

- encryption
- signatures

Algorithmics

- hardness of arithmetic problems
- efficient operations

BE STRONG - BE QUICK - BE FUNCTIONAL

Lattice-based Cryptography and LWE

What is a good algorithmic problem for a cryptographer ?

Few problems are actually used in cryptography.

What is a good algorithmic problem for a cryptographer ?

Few problems are actually used in cryptography.

- Its instances must be hard to solve.
  Breaking the cryptographic primitive must be hard.

What is a good algorithmic problem for a cryptographer ?

Few problems are actually used in cryptography.

- Its instances must be hard to solve.
  Breaking the cryptographic primitive must be hard.
- They must be easy to generate.
  The cryptographic primitive must be efficient.

What is a good algorithmic problem for a cryptographer ?

Few problems are actually used in cryptography.

- Its instances must be hard to solve.
  Breaking the cryptographic primitive must be hard.
- They must be easy to generate.
  The cryptographic primitive must be efficient.
- They must be described shortly.
  Space and communication must be low.

What is a good algorithmic problem for a cryptographer ?

Few problems are actually used in cryptography.

- Its instances must be hard to solve.
  Breaking the cryptographic primitive must be hard.
- They must be easy to generate.
  The cryptographic primitive must be efficient.
- They must be described shortly.
  Space and communication must be low.
- The problem must be rich, flexible and expressive.
  Some applications need advanced cryptographic primitives.

Good Algorithmic Problems

1. Instances hard to solve.
2. Instances easy to generate.
3. Instances short.
4. Rich, flexible, expressive.

The three first criteria are quantifiable:

Good Algorithmic Problems

1. Instances hard to solve.
2. Instances easy to generate.
3. Instances short.
4. Rich, flexible, expressive.

The three first criteria are quantifiable:

- Security parameter λ : the best known algorithm to break the scheme must have a cost of at least 2^{λ}.
- Underlying arithmetic algorithms have a cost of $\lambda^{\mathcal{O}(1)}$.
- Instances should be represented using $\lambda^{\mathcal{O}(1)}$ bits.

Good Algorithmic Problems

1. Instances hard to solve.
2. Instances easy to generate.
3. Instances short.
4. Rich, flexible, expressive.

The three first criteria are quantifiable:

- Security parameter λ : the best known algorithm to break the scheme must have a cost of at least 2^{λ}.
- Underlying arithmetic algorithms have a cost of $\lambda^{\mathcal{O}(1)}$.
- Instances should be represented using $\lambda^{\mathcal{O}(1)}$ bits.
- The last criteria is less quantifiable...

Popular Algorithmic Problems for Cryptography

- Factorisation and e-th root modulo a composite number (RSA) :

  Poor balance efficiency / security
  Not very riche, nor flexible, nor expressif.

Popular Algorithmic Problems for Cryptography

- Factorisation and e-th root modulo a composite number (RSA) :

  Poor balance efficiency / security
  Not very riche, nor flexible, nor expressif.

- Discrete Log and Diffie-Hellman in $(\mathbb{Z}/p\mathbb{Z})^*$:

  Same.

Popular Algorithmic Problems for Cryptography

- Factorisation and e-th root modulo a composite number (RSA) :

  Poor balance efficiency / security
  Not very riche, nor flexible, nor expressif.

- Discrete Log and Diffie-Hellman in $(\mathbb{Z}/p\mathbb{Z})^*$:

  Same.

- Discrete Log and Diffie-Hellman in the group of points of an algebraic curve :

  Good balance efficiency / security (excellent in space).
  Not very riche, nor flexible, nor expressif.

Popular Algorithmic Problems for Cryptography

- Factorisation and e-th root modulo a composite number (RSA) :

  Poor balance efficiency / security
  Not very riche, nor flexible, nor expressif.

- Discrete Log and Diffie-Hellman in $(\mathbb{Z}/p\mathbb{Z})^*$:

  Same.

- Discrete Log and Diffie-Hellman in the group of points of an algebraic curve :

  Good balance efficiency / security (excellent in space).
  Not very riche, nor flexible, nor expressif.

- Discrete Log and Diffie-Hellman in the group of points of a curve equipped with a pairing :

  Poor balance efficiency / security

  Richer, more flexible and expressif (e.g.. : IBE, ABE).

The *Learning With Errors* problem – **LWE**

Informally: Resolution of an overdetermined $m \times n$ linear system which is random, noisy, and modulo a short integer q.

Find $(s_1, s_2, s_3, s_4, s_5)$ such that :

$$\begin{aligned}
s_1 + 22s_2 + 17s_3 + 2s_4 + s_5 &\approx 16 \mod 23 \\
3s_1 + 2s_2 + 11s_3 + 7s_4 + 8s_5 &\approx 17 \mod 23 \\
15s_1 + 13s_2 + 10s_3 + s_4 + 22s_5 &\approx 3 \mod 23 \\
17s_1 + 11s_2 + s_3 + 10s_4 + 3s_5 &\approx 8 \mod 23 \\
2s_1 + s_2 + 13s_3 + 6s_4 + 2s_5 &\approx 9 \mod 23 \\
4s_1 + 4s_2 + s_3 + 5s_4 + s_5 &\approx 18 \mod 23 \\
11s_1 + 12s_2 + 5s_3 + s_4 + 9s_5 &\approx 7 \mod 23
\end{aligned}$$

We can have an arbitrary number of equations.

Other interpretation : decoding of a random linear code for the Euclidean distance.

The *Learning With Errors* problem – **LWE**

Informally: Resolution of an overdetermined $m \times n$ linear system which is random, noisy, and modulo a short integer q.

- The best known attacks are exponential in $n \log q$.

  $\Rightarrow \lambda$ is linear in $n \log q$.

- Cost of the generation of the instance is in $mn \log q$.

  It is often λ^2.

- Binary size of the instance : $mn \log q$.

The *Learning With Errors* problem – **LWE**

Informally: Resolution of an overdetermined $m \times n$ linear system which is random, noisy, and modulo a short integer q.

- The best known attacks are exponential in $n \log q$.

  $$\Rightarrow \lambda \text{ is linear in } n \log q.$$

- Cost of the generation of the instance is in $mn \log q$.

  It is often λ^2.

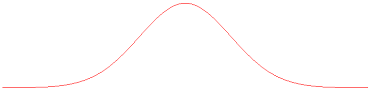
- Binary size of the instance : $mn \log q$.

- Very rich, flexible and expressive : encryption, identity-based encryption, attribute-based encryption, homomorphic encryption, functional encryption, etc.

Gaussian Distributions

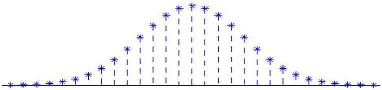
Gaussian distribution of parameter s :

$$D_s(x) \sim \frac{1}{s} \exp\left(-\pi \frac{x^2}{s^2}\right)$$
$$\forall x \in \mathbb{R}$$



Discrete Gaussian Distribution of support $\mathbb{Z}$ and of parameter s :

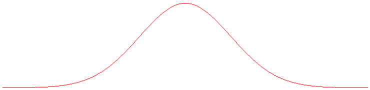
$$D_s(x) \sim \frac{1}{s} \exp\left(-\pi \frac{x^2}{s^2}\right)$$
$$\forall x \in \mathbb{Z}$$



Gaussian Distributions

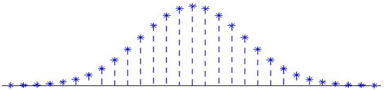
Gaussian distribution of parameter s :

$$\left| \begin{array}{l} D_s(x) \sim \frac{1}{s} \exp\left(-\pi \frac{x^2}{s^2}\right) \\ \forall x \in \mathbb{R} \end{array} \right.$$



Discrete Gaussian Distribution of support $\mathbb{Z}$ and of parameter s :

$$\left| \begin{array}{l} D_s(x) \sim \frac{1}{s} \exp\left(-\pi \frac{x^2}{s^2}\right) \\ \forall x \in \mathbb{Z} \end{array} \right.$$



- We know how to sample efficiently.
- Most of the values are in $[-c \cdot s, +c \cdot s]$ for a constant c, if s is not too small.

The LWE problem [Regev05]

Let $n \geq 1, q \geq 2$ and $\alpha \in]0, 1[$.
For all $\mathbf{s} \in \mathbb{Z}_q^n$, let us define the distribution $D_{n,q,\alpha}(\mathbf{s})$ by :

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)\,, \text{ avec } \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \text{ et } e \hookleftarrow D_{\mathbb{Z},\alpha q}.$$

Computational LWE

For all $\mathbf{s}$:

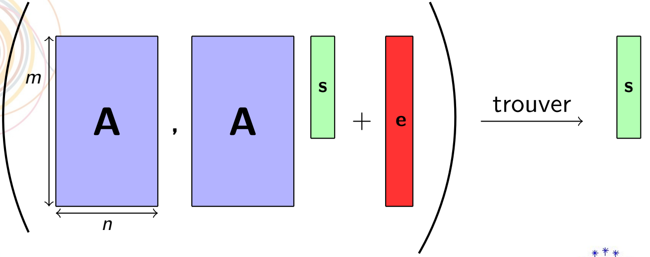
from an arbitrary number of samples of $D_{n,q,\alpha}(\mathbf{s})$, recover $\mathbf{s}$.

Decisional LWE

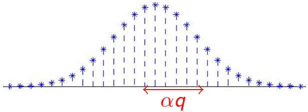
With non-negligeable probability on $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$:

distinguish the two distributions $D_{n,q,\alpha}(\mathbf{s})$ and $U(\mathbb{Z}_q^{n+1})$.

LWE: matricial view



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



Discrete Gaussian error

Decisional variant :
determine if $(\mathbf{A}, \mathbf{b})$ is of the form above, or uniform.

LWE: hardness

Brute Force

First variant:

- try all the possible $\mathbf{s} \in \mathbb{Z}_q^n$
- is $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ small ?

$\Rightarrow$ Cost $\approx q^n$.

LWE: hardness

Brute Force

First variant:

- try all the possible $\mathbf{s} \in \mathbb{Z}_q^n$
- is $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ small ?

$\Rightarrow$ Cost $\approx q^n$.

Second variant:

- guess the n first errors.
- compute the corresponding $\mathbf{s}$.
- is $\mathbf{b} - \mathbf{A} \cdot \mathbf{s}$ small?

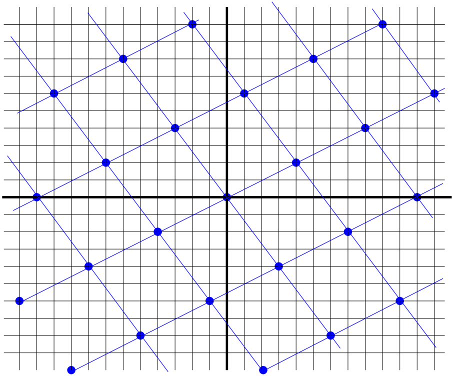
$\Rightarrow$ Cost $\approx (\alpha q \sqrt{n})^n$.

LWE and lattices

A lattice:

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

If the $\mathbf{b}_i$ are linearly independant, they are called a basis.

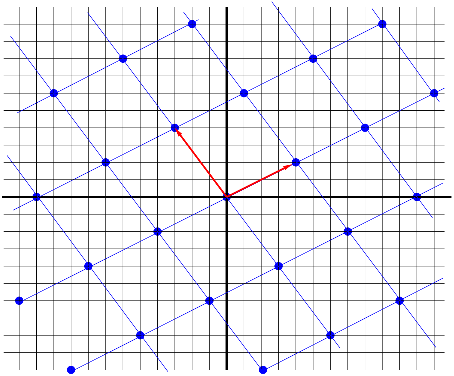


Lattices

A lattice:

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

If the $\mathbf{b}_i$ are linearly independant, they are called a basis.

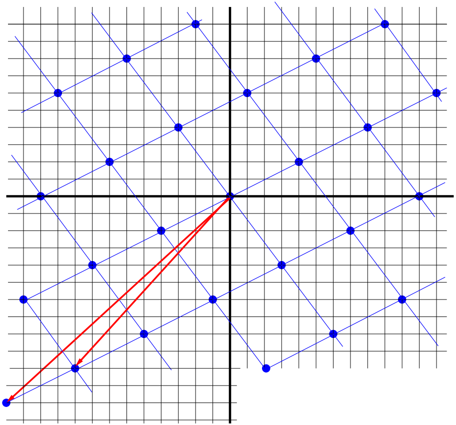


Lattices

A lattice:

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

If the $\mathbf{b}_i$ are linearly independant, they are called a basis.



There are infinitely many basis.

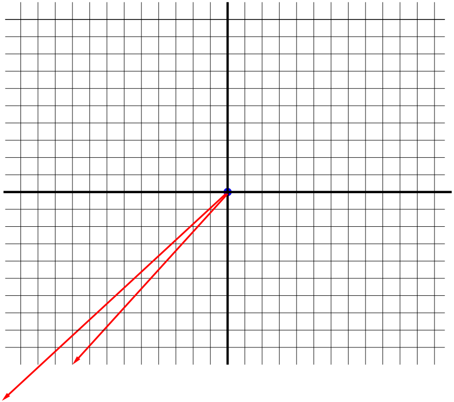
$$\begin{pmatrix} 4 & -3 \\ 2 & 4 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} -4 & -3 \\ -1 & -1 \end{pmatrix}}_{\det=1} = \begin{pmatrix} -13 & -9 \\ -12 & -10 \end{pmatrix}$$

Lattices

Provide hard problems:

Shortest Vector Problem (SVP$_\gamma$)

Minimum :
$\lambda(L) = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.



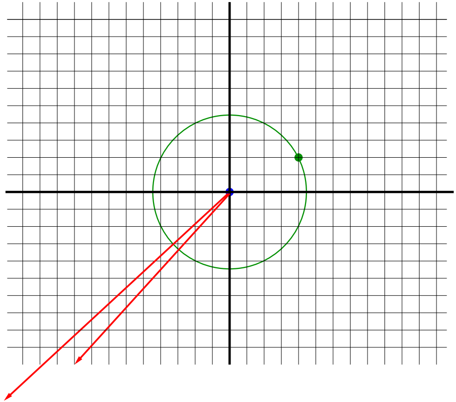
Lattices

Provide hard problems:

Shortest Vector Problem (SVP$_\gamma$)

Minimum :
$\lambda(L) = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.

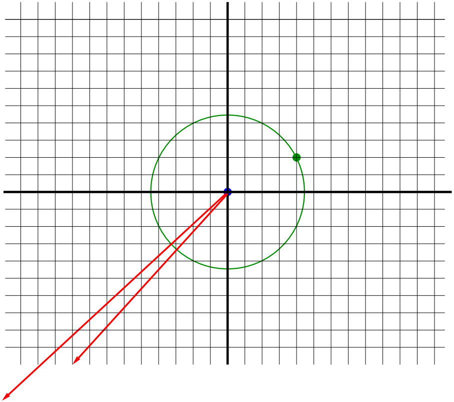
SVP$_\gamma$: Given a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.



Lattices

Provide hard problems:

Shortest Vector Problem (SVP$_\gamma$)



Minimum :
$\lambda(L) = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.

SVP$_\gamma$: Given a basis of L, find $\mathbf{b} \in L$
s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

Best known algorithm : BKZ

Time $2^t \cdot (n + \log \|B\|)^{\mathcal{O}(1)}$

$\Downarrow$

Approximation factor $\gamma \approx t^{\mathcal{O}(n/t)}$

Algorithm due to [SchnorrEuchner91], analysed by [HanrotPujolStehlé11].

Hardness of SVP

- SVP$_\gamma$: Given a basis of L, find $\mathbf{b} \in L$ s.t.

$$0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$$

Hardness of SVP

- SVP_γ : Given a basis of L, find $\mathbf{b} \in L$ s.t.

$$0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$$

- GapSVP_γ: Given a basis of L and t, answer

$$\textbf{YES} \text{ if } \lambda(L) \leq t \quad \text{and} \quad \textbf{NO} \text{ if } \lambda(L) > \gamma \cdot t$$

Hardness of SVP

- SVP_γ : Given a basis of L, find $\mathbf{b} \in L$ s.t.

$$0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$$

- GapSVP_γ: Given a basis of L and t, answer

$$\textbf{YES} \text{ if } \lambda(L) \leq t \quad \text{and} \quad \textbf{NO} \text{ if } \lambda(L) > \gamma \cdot t$$

Hardness of GapSVP_γ

- **NP-hard** if $\gamma \leq \mathcal{O}(1)$ (probabilistic reductions) [Ajtai98,HavivRegev12]
- **in NP$\cap$coNP** if $\gamma \geq \sqrt{n}$ [GoldreichGoldwasser97,AharonovRegev05]
- **in P** si $\gamma \geq \exp\left(n \cdot \frac{\log\log n}{\log n}\right)$

LWE : difficulty

- Decisional LWE $\Longleftrightarrow$ Computational LWE
- Solving LWE using BKZ :

LWE : difficulty

- Decisional LWE $\iff$ Computational LWE
- Solving LWE using BKZ :

  From $\mathbf{A}$ and $\mathbf{b}$, we wish to determine if $\mathbf{b}$ is an LWE sample or a uniform vector.

  Let $L = L(\boxed{\mathbf{A}}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \boxed{\mathbf{A}} = \mathbf{0}^T \bmod q\}$

  - L is a lattice.
  - Its dimension is m: $q \cdot \mathbb{Z}^m \subset L$
  - Pigeonhole principle: $\lambda_1(L) \leq \sqrt{m} q^{n/m}$
  - If $\mathbf{x} \in L \setminus \mathbf{0}$ is short, then $\langle \mathbf{x}, \mathbf{b} \rangle$:
    - is small if $\mathbf{b}$ is an LWE sample because it is $\langle \mathbf{x}, \mathbf{e} \rangle$,
    - is uniforme modulo q otherwise.

  $\Rightarrow$ For the attack to work, we need

$$\|\mathbf{x}\| \alpha q \leq q \iff \|\mathbf{x}\| \leq 1/\alpha.$$

LWE : difficulty

- Decisional LWE $\iff$ Computational LWE

- Solving LWE using BKZ :
  - $\lambda_1(L) \leq \sqrt{m} q^{n/m}$.
  - We want to find $\mathbf{x} \in L$ s.t. $0 < \|\mathbf{x}\| \leq 1/\alpha$.

  In time 2^t, BKZ computes $\mathbf{x} \in L$ s.t.: $\|\mathbf{x}\| \leq t^{\mathcal{O}(m/t)} \sqrt{m} q^{n/m}$.

  The optimal m is $\approx \sqrt{tn \frac{\log q}{\log t}}$ and we get $\|\mathbf{x}\| \leq 2^{\mathcal{O}(\sqrt{\frac{n}{t} \log q \log t})}$.

BKZ's cost to break LWE

$$\text{Time: } \left(\frac{n \log q}{\log^2 \alpha}\right)^{\mathcal{O}(\frac{n \log q}{\log^2 \alpha})}.$$

LWE : difficulty

- Decisional LWE $\iff$ Computational LWE
- Solving LWE using BKZ : $\left(\frac{n \log q}{\log^2 \alpha}\right)^{\mathcal{O}\left(\frac{n \log q}{\log^2 \alpha}\right)}$
- Suppose that $\alpha q \geq 2\sqrt{n}$ and that q is prime and polynomial in n. Then there exists a quantum polynomial reduction from GapSVP_γ in dimension n to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n/\alpha$.
  [Regev05]
- There exists a classical polynomial reduction from GapSVP_γ in dimension $\approx \sqrt{n}$ to $\mathrm{LWE}_{n,q,\alpha}$, with $\gamma \approx n^2/\alpha$.
  [BrakerskiLangloisPeikertRegevStehlé13]

Regev's encryption [Regev05]

- **Parameters** : $n, m, q \in \mathbb{Z}$, $\alpha \in]0,1[$.

- **Keys** : $\mathrm{sk} = \mathbf{s}$ and $\mathrm{pk} = (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  where $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.

- **Encryption** $(M \in \{0,1\})$ **:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rceil \cdot M.$$

Regev's encryption [Regev05]

- **Parameters** : $n, m, q \in \mathbb{Z}$, $\alpha \in \,]0, 1[$.
- **Keys** : sk $=$ $\mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathrm{e} \bmod q$ where $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathrm{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.
- **Encryption** $(M \in \{0, 1\})$ **:** Let $\mathbf{r} \hookleftarrow U(\{0, 1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rceil \cdot M.$$

- **Decryption** $(\mathbf{u}, v)$: Compute $v - \mathbf{u}^T \mathbf{s} \bmod q$, because:

$$\underbrace{\mathbf{r}^T \left[\mathbf{A}\,\mathbf{s} + \mathrm{e} \right] + \lfloor q/2 \rceil \cdot M}_{v} - \underbrace{\mathbf{r}^T \mathbf{A}\,\mathbf{s}}_{\mathbf{u}^T \mathbf{s}} = \text{small} + \lfloor q/2 \rceil \cdot M$$

If close to 0, output 0, else, output 1.

Correctness (probabilistic)

- sk = $\mathbf{s}$ and pk = ($\mathbf{A}$, $\mathbf{b}$), with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$.
- **Encryption** $(M \in \{0,1\})$ **:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rceil \cdot M.$$

- **Decryption** $(\mathbf{u}, v)$: Compute $v - \mathbf{u}^T \mathbf{s} \bmod q$.

Correctness (probabilistic)

- sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$.
- **Encryption** $(M \in \{0,1\})$ **:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rceil \cdot M.$$

- **Decryption** $(\mathbf{u}, v)$: Compute $v - \mathbf{u}^T\mathbf{s} \bmod q$.

Why does it work?

- We have $v - \mathbf{u}^T\mathbf{s} = \mathbf{r}^T\mathbf{e} + \lfloor q/2 \rceil \cdot M \bmod q$
- But $|\mathbf{r}^T\mathbf{e}| \leq \|\mathbf{r}\|\|\mathbf{e}\| \leq m\alpha q$, with probability ≈ 1.

Correctness (probabilistic)

- sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$.
- **Encryption** $(M \in \{0,1\})$ **:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}^T \mathbf{A}, \quad v = \mathbf{r}^T \mathbf{b} + \lfloor q/2 \rceil \cdot M.$$

- **Decryption** $(\mathbf{u}, v)$: Compute $v - \mathbf{u}^T\mathbf{s} \bmod q$.

Why does it work?

- We have $v - \mathbf{u}^T\mathbf{s} = \mathbf{r}^T\mathbf{e} + \lfloor q/2 \rceil \cdot M \bmod q$
- But $|\mathbf{r}^T\mathbf{e}| \leq \|\mathbf{r}\|\|\mathbf{e}\| \leq m\alpha q$, with probability ≈ 1.
- If $M = 0$, then $v - \mathbf{u}^T\mathbf{s} \bmod q$ is at most of the order of $m\alpha q$.

  We set α so that it is $\ll q$.
- If $M = 1$, then $v - \mathbf{u}^T\mathbf{s} \bmod q$ is close to $\lfloor q/2 \rceil$.

A trapdoor for LWE

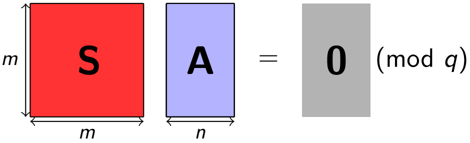
Let's recall :

$$L(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0}^T \bmod q\}$$

- It is a lattice of dimension m,
- A short basis allows to generate short vectors in $L(\mathbf{A})$,
- An arbitrary basis does not give any information (solution to LWE).

GenBasis : sample $\mathbf{A}$ and $\mathbf{S}$, a short basis of $L(\mathbf{A})$, simultaneously.

- $\mathbf{S} \in \mathbb{Z}^{m \times m}$ short
- We have $\mathbf{S}\,\mathbf{A} = 0 \bmod q$.
- $\mathbf{S}$ allows to invert LWE
- Can add constraints: ex. $\mathbf{B}^T \cdot \mathbf{A} = \mathbf{0}$ (with trapdoor)



Another problem

The security of our group signature also relies on :

- Short Integer Solution (SIS)

$$\boxed{\text{Given } \mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n}), \text{ find } \mathbf{x} \in \mathbb{Z}^m \setminus \{\mathbf{0}\} \text{ small s.t. } \mathbf{x}^T \cdot \mathbf{A} = 0 \pmod q}$$

L., Langlois and Stehlé. *Chiffrement avancé à partir du problème Learning With Errors*. Chapitre de l'ouvrage "Informatique Mathématique, une photographie en 2014", Presses Universitaires de Perpignan (2014)

Lattice-based Cryptography Toolbox

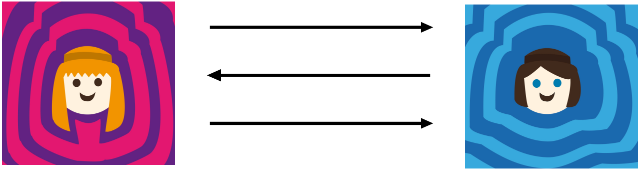
- Last tool :

  Given public $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{y} \in \mathbb{Z}_q^n$,

  there exist a (3-round) interactive protocol to prove that one knows $\mathbf{x}$ small such that

$$\mathbf{x}^T \mathbf{A} = \mathbf{y}^T$$

  without revealing any information of $\mathbf{x}$.



zero-knowledge proof of knowledge

Anonymity-Oriented Signatures

Cryptographic motivations

Need for authenticity *and* anonymity

- Anonymous credentials: anonymous use of certified attributes
  - Ex.: student card - name, picture, date, grade,...

    $\rightsquigarrow$ non-anonymous
  - Idemix (Identity-Mixer) of IBM
    Anonymous credential system developed at IBM Research [...] that enables strong authentication and privacy at the same time.

    selective revelation of attributes
- Traffic management (Vehicle Safety Communications project of the U.S. Dept. of Transportation)

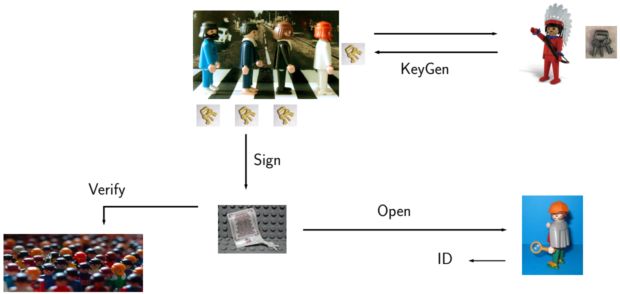
  vehicle-based collision countermeasures

Intensive use of group signatures

Group Signatures

> Group signatures allow member of a group to anonymously and accountably sign on behalf of this group

- [ChaumVanHeyst91]
- Involve :
  - Group manager $(mpk, msk) + gsk_i$ — KeyGen
  - Opening authority (osk) — Open
  - Group members (gsk_i) — Sign
  - Verify



signature $\surd$ but who signed ??

Group Signatures

Security requirements [BellareMicciancioWarinschi03] :

- Anonymity

  a given signature does not leak the identity of its originator

- Traceability

  no collusion of malicious users can produce a valid signature that cannot be traced to one of them

Issues :

- security model

  ex. anonymity

- efficiency

  compact signatures, short keys, fast operations

- additional properties

  revocation, dynamicity

Group Signatures

Generic construction [BellareMicciancioWarinschi03] :

Ingredients :

- Signature & Encryption schemes
- non-interactive zero knowledge proof system
  [FeigeLapidotShamir99] + [Sahai99] :
  if trapdoor permutations exist, then any NP-relation has a such a proof

Scheme:

- Group manager produces a certificate $Cert_i = \mathsf{Sign}_{sk_s}(i||pk_i)$
- Member i :
  1. $\sigma = \mathsf{Sign}_{\mathsf{sk}_i}(m)$
  2. $c = Encrypt_{\mathsf{pk}_o}(i||pk_i||Cert_i||\sigma)$
  3. $\Pi = \mathsf{Proof}(\sigma \text{ valid} \wedge Cert_i \text{ valid})$
  4. Output $\Sigma = (c, \Pi)$
- Verification: check the validity of proof
- Opening authority decrypts C if Π valid

Group Signatures

Security of this construction :

- It is fully-anonymous if the encryption scheme and the proof are "secure"
- It is traceable if the signature scheme and the proof are "secure"

Remarks:

- Inefficient in general
- Many constructions nevertheless follow this paradigm
- Breakthrough : [Groth06,GrothSahai2006]
  Pairing-based simulation-sound NIZK Proofs *without random oracles*

Lattice-based Group Signatures

Group Signatures with Lattices

- First lattice-based construction : [GordonKatzVaikuntanathan2010]
- Main drawbacks : size of the signatures - $O(N)$ N group members
- Ideas :
  - Keys of the authority :
    $$\begin{cases} \text{public parameters} = \{\mathbf{A}_i, \mathbf{B}_i\}_i \text{ s.t. } \mathbf{A}_i \cdot \mathbf{B}_i^T = 0 \pmod q \\ \text{tracing key} = \mathbf{S}_i \qquad \text{short basis} \\ sk_i = \mathbf{T}_i \text{ (members)} \qquad \text{short basis} \end{cases}$$
  - A signature:
    - compute short $\mathbf{e}_i$ s.t. $\mathbf{A}_i\mathbf{e}_i = H(m) \pmod q$ $(\mathbf{T}_i)$
    - $\forall j \neq i$ compute $\mathbf{e}_j$ s.t. $\mathbf{A}_j\mathbf{e}_j = H(m) \pmod q$ "pseudo-signature"
    - Encrypt each $\mathbf{e}_i$ variant of [Regev2009]
    - a proof Π disjunction of [MicciancioVadhan03]

Secure under LWE (anonymity) and GapSVP (traceability).

Group Signatures with Lattices

A new compact construction based on lattices [L.LangloisLibertStehlé2013]

Ingredients:

- [Boyen2010]'s signature (standard model)
- [GentryPeikertVaikuntanathan2008] encryption scheme

- $N = 2^\ell$ group members
- public matrices $\mathbf{A}_i$'s and $\mathbf{B}_i$'s (almost as before)
- each user is given a *short* basis $\mathbf{T}_{\mathrm{id}}$ of a public lattice associated to its identity

$$\mathbf{A}_{\mathrm{id}} = \left(\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}[i]\mathbf{A}_i} \right)$$

Group Signatures with Lattices

A new compact construction based on lattices [L.LangloisLibertStehlé2013]

To sign (1/3) :

- Produce $(\mathbf{x}_1 || \mathbf{x}_2)^T$ short s.t. :
$$\mathbf{x}_1{}^T \mathbf{A} + \mathbf{x}_2{}^T \cdot (\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}[i] \cdot \mathbf{A}_i) = 0 \pmod q$$

- Encrypt $\mathbf{x}_2$ as $\mathbf{c}_0 = \mathbf{B}_0 \cdot \mathbf{s}_0 + \mathbf{x}_2$ $\qquad (\mathbf{s}_0 \hookleftarrow U(\mathbb{Z}_q^n))$

  $+$ generate a proof π_0: $\mathbf{c}_0$ is close to a point in the $\mathbb{Z}_q$-span of $\mathbf{B}_0$ [Lyubashevsky2012]

- For all $i = 1, \ldots, \ell$ encrypt $\mathrm{id}_i \cdot \mathbf{x}_2$ as
$$\mathbf{c}_i = \mathbf{B}_i \cdot \mathbf{s} + p \cdot \mathbf{e}_i + \mathrm{id}_i \cdot \mathbf{x}_2$$

  so that $\begin{cases} \mathbf{c}_i \text{ and } \mathbf{c}_0 \text{ encrypt the same } \mathbf{x}_2 & (\mathrm{id}_i = 1) \\ \text{or } \mathbf{c}_i \text{ encrypts } \mathbf{0} & (\mathrm{id}_i = 0) \end{cases}$

Group Signatures with Lattices

A new compact construction based on lattices [L.LangloisLibertStehlé2013]

To sign (2/3) :

- Generate a proof $\pi_{\mathrm{OR},i}$ of these relations (disjunctions)

  [Lyubashevsky2012] for LWE + OR

- Generate a proof π_K of knowledge of the $\mathbf{e}_i$'s and $\mathrm{id}_i \cdot \mathbf{x}_2$'s with their corresponding relation

  [Lyubashevsky2012] for SIS + OR

= encode a valid Boyen's signature

Group Signatures with Lattices

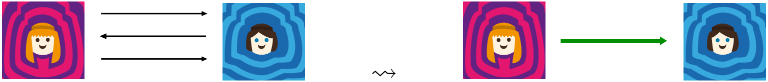
A new compact construction based on lattices [L.LangloisLibertStehlé2013]

To sign (3/3) :

What about the message ?

- interactive ZKPoK $\rightsquigarrow$ non-interactive ZKPoK *via* Fiat-Shamir

  incorporating the message in π_K



- Final signature:

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \leq i \leq \ell}, \pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \leq i \leq \ell}, \pi_K \right)$$

Group Signatures with Lattices

A new compact construction based on lattices [L.LangloisLibertStehlé2013]

To Verify :

- Check the proofs

To Open :

- Decrypt $\mathbf{c}_0$ ($\rightsquigarrow \mathbf{x_2}$) and check whether $p^{-1}\mathbf{c}_i$ or $p^{-1}(\mathbf{c}_i - \mathbf{x}_2)$ is close to the $\mathbb{Z}_q$-span of $\mathbf{B}_i$.

Group Signatures with Lattices

A new compact construction based on lattices [L.LangloisLibertStehlé2013]

To Verify :

- Check the proofs

To Open :

- Decrypt $\mathbf{c}_0$ ($\rightsquigarrow \mathbf{x_2}$) and check whether $p^{-1}\mathbf{c}_i$ or $p^{-1}(\mathbf{c}_i - \mathbf{x}_2)$ is close to the $\mathbb{Z}_q$-span of $\mathbf{B}_i$.

- Size of the signatures : $\tilde{\mathcal{O}}(\lambda \cdot \log(N))$
- Size of the key of member i: $\tilde{\mathcal{O}}(\lambda^2)$
- Weak anonymity under LWE
- Traceability under SIS
- We provide a variant with full anonymity

Conclusion

- Anonymity-oriented signatures are useful, ex.: group signature
- Lattices are convenient to design such schemes
- Lattice-based group signatures
  - reduce the size ?
  - efficient revocation
- Lattice-based cryptography
  - competition with pairings on curves
  - functional cryptography
  - implementation
  - multi-linear maps *vs* pairings