Finding Waldo in Euclidean Lattices: An introduction to Search-To-Decision reduction and applications to cryptography

Maxime Bombar

GT Oisillons

March 5, 2021

Caution. This Tlak is not a Tlak about lattices !

What will we talk about ?

- LWE based crypto.
- ~~Lattices~~, ~~Codes~~, Both !
- Hopefully, some Algebraic Number Theory

Outline

LWE: A search problem

- **Parameters**: Some space $E \times S$ endowed with a bilinear map $\langle \cdot, \cdot \rangle$ to a group $\mathbb{G}$ of cardinality q, an error distribution χ over $\mathbb{G}$.
- **Data**: I choose some $\boldsymbol{s} \in S$ and I give you many noisy "noisy products"

$$
\begin{array}{ccc}
\boldsymbol{a}_1 \leftarrow E & , & b_1 = \langle \boldsymbol{a}_1, \boldsymbol{s} \rangle + e_1 \in \mathbb{G}, \quad e_1 \leftarrow \chi \\
\boldsymbol{a}_2 \leftarrow E & , & b_2 = \langle \boldsymbol{a}_2, \boldsymbol{s} \rangle + e_2 \in \mathbb{G}, \quad e_2 \leftarrow \chi \\
 & \vdots &
\end{array}
$$

- **Question:** Can you find $\boldsymbol{s}$?

Random decoding

E and S are two $\mathbb{F}_q$ linear spaces of dimension k. I give you n noisy products :

$$\underbrace{\left(\begin{array}{c|c|c} \vdots & \vdots & \\ \boldsymbol{a}_1 & \boldsymbol{a}_2 & \cdots \\ \vdots & \vdots & \end{array}\right)}_{\boldsymbol{A}} \quad , \quad \boldsymbol{b} = \boldsymbol{s}\boldsymbol{A} + \boldsymbol{e} \in \mathbb{F}_q^n, \quad \boldsymbol{e} \leftarrow \chi^n$$

Finding $\boldsymbol{s}$ is decoding in a random code of rate $\frac{k}{n} \ll 1$!

Regev' LWE ('05)

- **Parameters**: An integer n, a modulus $q = poly(n)$, χ some Gaussian distribution.
- **Secret** $\boldsymbol{s} \in (\mathbb{Z}/q\mathbb{Z})^n$.

$$\begin{array}{lcl} \boldsymbol{a}_1 \leftarrow \mathbb{Z}^n & , & b_1 = \langle \boldsymbol{a}_1, \boldsymbol{s} \rangle + e_1 \mod q\mathbb{Z} \\ \boldsymbol{a}_2 \leftarrow \mathbb{Z}^n & , & b_2 = \langle \boldsymbol{a}_2, \boldsymbol{s} \rangle + e_2 \mod q\mathbb{Z} \\ & \vdots & \end{array}$$

LWE: A decision problem

- **Parameters:** An integer n, a modulus $q = poly(n)$, χ some Gaussian distribution.
- **Secret:** $\boldsymbol{s} \in (\mathbb{Z}/q\mathbb{Z})^n$.
- **Question:** Can you distinguish between (a_i, b_i) pairs comming from LWE with secret $\boldsymbol{s}$; and uniform (a_i, b_i) ?

Some properties

- Can I check a candidate solution $\boldsymbol{s}'$?
- Given an LWE sample with secret $\boldsymbol{s}$, can I build an LWE sample with secret $\boldsymbol{s} + \boldsymbol{t}$ for some $\boldsymbol{t}$ of my choice ?

Some properties

- Can I check a candidate solution $\boldsymbol{s}'$?

$$\boldsymbol{b} - \langle \boldsymbol{a}, \boldsymbol{s}' \rangle = \begin{cases} \text{small error} & \text{if } \boldsymbol{s}' = \boldsymbol{s} \\ \text{well-spread} & \textit{otherwise} \end{cases}$$

- Given an LWE sample with secret $\boldsymbol{s}$, can I build an LWE sample with secret $\boldsymbol{s} + \boldsymbol{t}$ for some $\boldsymbol{t}$ of my choice ?

Some properties

- Can I check a candidate solution $\boldsymbol{s}'$?

$$\boldsymbol{b} - \langle \boldsymbol{a}, \boldsymbol{s}' \rangle = \begin{cases} \text{small error} & \text{if } \boldsymbol{s}' = \boldsymbol{s} \\ \text{well-spread} & \textit{otherwise} \end{cases}$$

- Given an LWE sample with secret $\boldsymbol{s}$, can I build an LWE sample with secret $\boldsymbol{s} + \boldsymbol{t}$ for some $\boldsymbol{t}$ of my choice ?

Some properties

- Can I check a candidate solution $\boldsymbol{s}'$?

$$\boldsymbol{b} - \langle \boldsymbol{a}, \boldsymbol{s}' \rangle = \begin{cases} \text{small error} & \text{if } \boldsymbol{s}' = \boldsymbol{s} \\ \text{well-spread} & \textit{otherwise} \end{cases}$$

- Given an LWE sample with secret $\boldsymbol{s}$, can I build an LWE sample with secret $\boldsymbol{s} + \boldsymbol{t}$ for some $\boldsymbol{t}$ of my choice ? Given $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$ output

$$\begin{aligned} \boldsymbol{a}, b' &= b + \langle \boldsymbol{a}, \boldsymbol{t} \rangle \\ &= \langle \boldsymbol{a}, \boldsymbol{s} + \boldsymbol{t} \rangle + e \end{aligned}$$

Some properties

- Can I check a candidate solution $\boldsymbol{s}'$?

$$\boldsymbol{b} - \langle \boldsymbol{a}, \boldsymbol{s}' \rangle = \begin{cases} \text{small error} & \text{if } \boldsymbol{s}' = \boldsymbol{s} \\ \text{well-spread} & \textit{otherwise} \end{cases}$$

- Given an LWE sample with secret $\boldsymbol{s}$, can I build an LWE sample with secret $\boldsymbol{s} + \boldsymbol{t}$ for some $\boldsymbol{t}$ of my choice ? Given $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$ output

$$\begin{aligned} \boldsymbol{a}, b' &= b + \langle \boldsymbol{a}, \boldsymbol{t} \rangle \\ &= \langle \boldsymbol{a}, \boldsymbol{s} + \boldsymbol{t} \rangle + e \end{aligned}$$

Random $\boldsymbol{t} \Rightarrow$ just need non negligeable success on average !

Success on ***uniform*** secret $\boldsymbol{s} \Rightarrow$ Success on ***any*** $\boldsymbol{s}$ with proba ≈ 1.

Search VS Decision

Can I distinguish between random picture of people and a picture with Waldo in it ? Is it easier than *spotting* Waldo ?

Search to Decision Reduction

Suppose $\mathcal{A}$ distinguishes between pairs $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$ and $(\boldsymbol{a}, b)$. Can I recover $\boldsymbol{s}$?

Search to Decision Reduction

Suppose $\mathcal{A}$ distinguishes between pairs $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$ and $(\boldsymbol{a}, b)$. Can I recover $\boldsymbol{s}$?

Remark: It suffices to test whether $\boldsymbol{s}_1 = 0$ because we can shift $\boldsymbol{s}_1$ by $0, 1, \ldots, q-1$ (Recall $q = poly(n)$). Same for other coordinates.

Search to Decision Reduction

Suppose $\mathcal{A}$ distinguishes between pairs $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$ and $(\boldsymbol{a}, b)$. Can I recover $\boldsymbol{s}$?

Remark: It suffices to test whether $\boldsymbol{s}_1 = 0$ because we can shift $\boldsymbol{s}_1$ by $0, 1, \ldots, q-1$ (Recall $q = poly(n)$). Same for other coordinates.

For each $(\boldsymbol{a}, b)$, choose $r \in \mathbb{Z}/q\mathbb{Z}$, set $\boldsymbol{a}' := \boldsymbol{a} - (r, 0, \ldots, 0)$ and call $\mathcal{A}$ on $(\boldsymbol{a}', b)$.

Search to Decision Reduction

Suppose $\mathcal{A}$ distinguishes between pairs $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$ and $(\boldsymbol{a}, b)$. Can I recover $\boldsymbol{s}$?

Remark: It suffices to test whether $\boldsymbol{s}_1 = 0$ because we can shift $\boldsymbol{s}_1$ by $0, 1, \ldots, q-1$ (Recall $q = poly(n)$). Same for other coordinates.

For each $(\boldsymbol{a}, b)$, choose $r \in \mathbb{Z}/q\mathbb{Z}$, set $\boldsymbol{a}' := \boldsymbol{a} - (r, 0, \ldots, 0)$ and call $\mathcal{A}$ on $(\boldsymbol{a}', b)$.

$b = \langle \boldsymbol{a}', \boldsymbol{s} \rangle + \boldsymbol{s}_1 \cdot r + e.$

- If $\boldsymbol{s}_1 = 0$, then $(\boldsymbol{a}', b)$ is an LWE pair and $\mathcal{A}$ accepts.
- If $\boldsymbol{s}_1 \neq 0$, and q is prime, then b is uniform and $\mathcal{A}$ rejects.
- One can relax condition q prime, and consider failure of $\mathcal{A}$ (Many papers).

LWE with short secrets

B. Applebaum, D. Cash, C. Peikert, A. Sahai 2009

LWE is no easier when the secret $\mathbf{s}$ is drawn from the error distribution χ^n.

(Normal form of LWE)

LWE with short secrets

B. Applebaum, D. Cash, C. Peikert, A. Sahai 2009

LWE is no easier when the secret $\boldsymbol{s}$ is drawn from the error distribution χ^n.

(Normal form of LWE)

- Intuition: Finding $\boldsymbol{e} \Leftrightarrow$ Finding $\boldsymbol{s}$: $\boldsymbol{b} - \boldsymbol{e} = \boldsymbol{s}\boldsymbol{A}$ and solve for $\boldsymbol{s}$.

LWE with short secrets

B. Applebaum, D. Cash, C. Peikert, A. Sahai 2009

LWE is no easier when the secret $\boldsymbol{s}$ is drawn from the error distribution χ^n.

(Normal form of LWE)

- Intuition: Finding $\boldsymbol{e} \Leftrightarrow$ Finding $\boldsymbol{s}$: $\boldsymbol{b} - \boldsymbol{e} = \boldsymbol{s}\boldsymbol{A}$ and solve for $\boldsymbol{s}$.

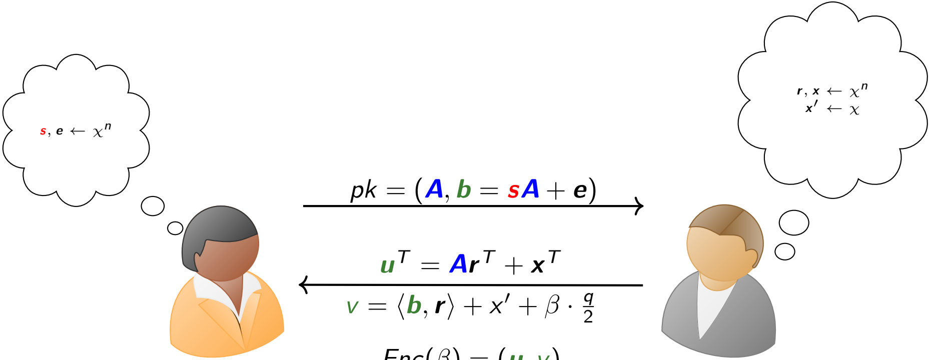
Transformation from secret $\boldsymbol{s}$ to secret $\hat{\boldsymbol{e}} \leftarrow \chi^n$:

(1) Draw samples until we get $(\hat{\boldsymbol{A}}, \hat{\boldsymbol{b}} = \boldsymbol{s}\hat{\boldsymbol{A}} + \hat{\boldsymbol{e}})$ for some invertible $\hat{\boldsymbol{A}}$.

(2) For each additional sample $(\boldsymbol{a}, b = \langle \boldsymbol{s}, \boldsymbol{a} \rangle + e)$:
   - Set $\boldsymbol{a}'^T := -\boldsymbol{a}\hat{A}^{-1}$
   - $b' := b + \langle \hat{\boldsymbol{b}}, \boldsymbol{a}' \rangle = \langle \hat{\boldsymbol{e}}, \boldsymbol{a}' \rangle + e$

LWE based encryption scheme

Encrypt one bit $\beta \in \{0, 1\}$.

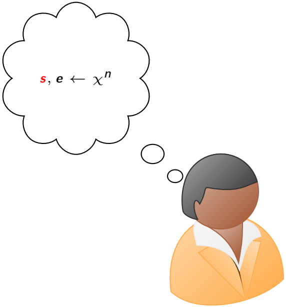


$$Enc(\beta) = (\boldsymbol{u}, v)$$

Decryption ?

LWE based encryption scheme

Encrypt one bit $\beta \in \{0,1\}$.



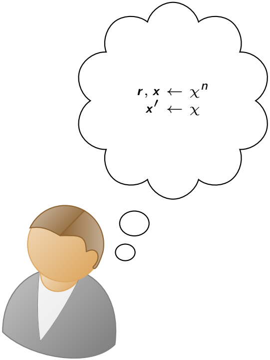
$$pk = (\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{s}\boldsymbol{A} + \boldsymbol{e}) \longrightarrow$$

$$\boldsymbol{u}^T = \boldsymbol{A}\boldsymbol{r}^T + \boldsymbol{x}^T$$

$$\longleftarrow$$

$$v = \langle \boldsymbol{b}, \boldsymbol{r} \rangle + x' + \beta \cdot \frac{q}{2}$$

$$Enc(\beta) = (\boldsymbol{u}, v)$$

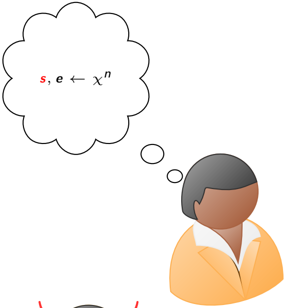


Decryption ?

$$v - \langle \boldsymbol{s}, \boldsymbol{u} \rangle \approx \beta \cdot \frac{q}{2} \qquad (\boldsymbol{s} \text{ is “short”})$$

LWE based encryption scheme

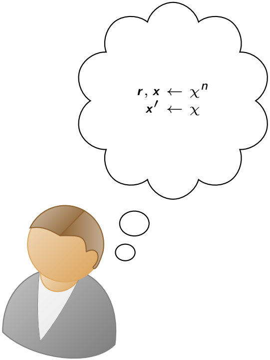
Encrypt one bit $\beta \in \{0, 1\}$.

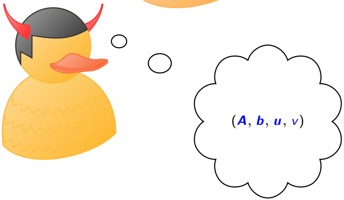


$$pk = (\mathbf{A}, \mathbf{b} = \mathbf{sA} + \mathbf{e}) \longrightarrow$$

$$\longleftarrow \mathbf{u}^T = \mathbf{A}\mathbf{r}^T + \mathbf{x}^T$$

$$v = \langle \mathbf{b}, \mathbf{r} \rangle + x' + \beta \cdot \frac{q}{2}$$





$\mathbf{b}, \mathbf{u} \approx$ uniform (LWE in normal form)
$\Rightarrow v \approx$ uniform (same argument).

LWE: A hard problem

Search-LWE $\leq$ Decision-LWE $\leq$ Crypto

Search-To-Decision reduction

LWE: A hard problem

Hard problem on *any* lattice (worst-case) $\leq$ Search-LWE $\leq$ Decision-LWE $\leq$ Crypto

- Quantum reduction of Regev (2005).
- Classical reduction of Peikert (2009), worse parameters.

Outline

What is a Lattice ?

~~It's like a code, but where you transpose everything~~

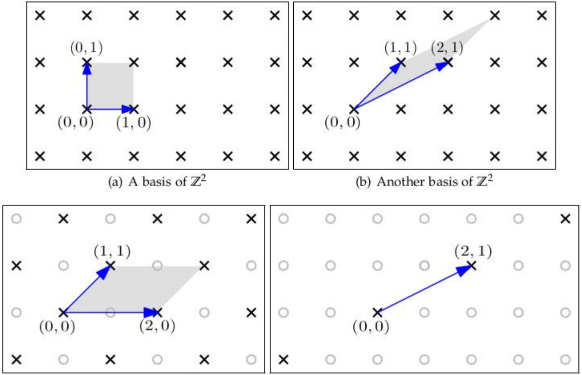
- Discrete subgroup of $\mathbb{R}^n$
- Full-rank
- Equivalently: $\mathbb{Z}$-span of any basis of $\mathbb{R}^n$.
- Usually, endowed with the Euclidean norm.

Examples:

- $\mathbb{Z}^n$
- $c\mathcal{L}$ for any $c \in \mathbb{R}$ and lattice $\mathcal{L}$
- $\mathcal{L}^* := \{w \mid \langle w, \mathcal{L} \rangle \subset \mathbb{Z}\}$ the dual lattice of $\mathcal{L}$.

What is a Lattice ?

- Discrete subgroup of $\mathbb{R}^n$
- Full-rank
- Equivalently: $\mathbb{Z}$-span of any basis of $\mathbb{R}^n$.
- Usually, endowed with the Euclidean norm.



(a) A basis of $\mathbb{Z}^2$

(b) Another basis of $\mathbb{Z}^2$

(c) Not a basis of $\mathbb{Z}^2$

(d) Not a full-rank lattice

Hard Lattice Problems

- $\lambda_1(\mathcal{L}) :=$ minimum distance of the Lattice.
- $\lambda_i(\mathcal{L})$ is the smallest r such that $\mathcal{L}$ has i linearly independent vectors of norm at most r.

Shortest Vector Problem (SVP)

Given a basis B of some lattice $\mathcal{L}$, find a shortest non-zero vector: $v \in \mathcal{L}$ such that $\|v\| = \lambda_1(\mathcal{L})$.

Closest Vector Problem (CVP)

Given a basis B of some lattice $\mathcal{L}$ and $\boldsymbol{x} \in \mathbb{R}^n$ find the closest lattice vector to $\boldsymbol{x}$ (when exists).

Hard Lattice Problems

- $\lambda_1(\mathcal{L}) :=$ minimum distance of the Lattice.
- $\lambda_i(\mathcal{L})$ is the smallest r such that $\mathcal{L}$ has i linearly independent vectors of norm at most r.

Approximate Shortest Vector Problem (γ-SVP)

Given a basis B of some n-dimensional lattice $\mathcal{L}$, and an approximation factor $\gamma = \gamma(n)$, find a shortest non-zero vector: $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1(\mathcal{L})$.

Approximate Shortest Independent Vector Problem (γ-SIVP)

Given a basis B of some n-dimensional lattice $\mathcal{L}$, and an approximation factor $\gamma = \gamma(n)$, output a set $S = \{s_i\}$ of n linearly independent vectors such that $\|s_i\| \leq \gamma\lambda_n(\mathcal{L})$.

Easy with a "good" basis (almost orthogonal short vectors), but intractable with random "bad" basis and subexponential approximation factor.

Babai, LLL ...

Gaussian Sampling

Discrete Gaussian Sampling (DGS) (Regev 05)

Given a coset $\boldsymbol{c} + \mathcal{L}$, output a sample from the discrete Gaussian $\mathcal{D}_{\boldsymbol{c}+\mathcal{L}}$ (Gaussian restricted to coset).

Smoothing Parameter (Miccianccio and Regev 04)

Limit parameter of a Gaussian beyond which it looks like "uniform". Only depends on the lattice structure.

Regev 05

DGS beyond the smoothing parameter is a quantum hard problem over Lattices.

Outline

Making LWE efficient ?

- Encrypting *one* bit requires n-dimensional inner product.
- Can amortize the a_i over many secrets $\boldsymbol{s}$, but still $\geq \tilde{O}(n^2)$ to encrypt and decrypt an n-bit message, and big key sizes.

$$\begin{pmatrix} \cdots & \boldsymbol{a}_i & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ \boldsymbol{s}_i \\ \vdots \end{pmatrix} + e = b \in (\mathbb{Z}/q\mathbb{Z}).$$

$$pk = \begin{pmatrix} & \vdots & \\ & \boldsymbol{A} & \\ & \vdots & \end{pmatrix}, \begin{pmatrix} \vdots \\ \boldsymbol{b} \\ \vdots \end{pmatrix}$$

What would we dream for ?

Can we do better ? Encrypt n bits with one *cheap* product operation ?

$$\begin{pmatrix} \cdots & \boldsymbol{a}_i & \cdots \end{pmatrix} \star \begin{pmatrix} \vdots \\ \boldsymbol{s} \\ \vdots \end{pmatrix} + \begin{pmatrix} \cdots & \boldsymbol{e}_i & \cdots \end{pmatrix} = \boldsymbol{b} \in (\mathbb{Z}/q\mathbb{Z})^n.$$

Caution

- We need $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ to be pseudorandom.
- With small error, coordinate-wise multiplication is insecure.

Answer

- $\star =$ multiplication in some polynomial ring $(\mathbb{Z}/q\mathbb{Z})[X]/(P)$.
- More generally, multiplication in some ring of integers O_K of a finite extension field $K/\mathbb{Q}$.

Ring-LWE: A hard problem ?

Hard problem on *any* **ideal** lattice (worst-case) $\leq$ Search-R-LWE $\leq$ Decision-R-LWE $\leq$ Crypto

- LWE is quantumly as hard as worst-case problems on **ideal** lattices (arise from fractional ideals of O_K under the canonical Minkowski embedding).
- No known classical reduction.
- Cool maths involved
- (Classical) Search-to-Decision reduction if K is Galois over $\mathbb{Q}$. No idea how to do that without the Galois hypothesis.
- More recently: Direct reduction from Lattices to Decision for any ring and modulus (Quantum).

Conclusion and perspectives

- **Perspectives:** A search-to-decision reduction for decoding random algebraically structured codes ?
- **Idea:** Quasi-cyclic codes share many properties with Module-Lattices, which are involved in generalizations of Ring-LWE.

The End.

Thanks for your attention !