DIVERGENCE DE RÉNYI EN CRYPTOGRAPHIE REPOSANT SUR LES RÉSEAUX EUCLIDIENS

Adeline Roux-Langlois

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, Caen, FRANCE

GREYC
Electronics and Computer Science Laboratory

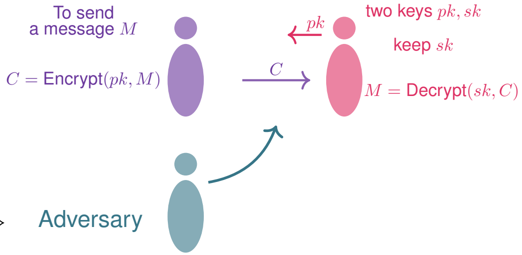
Normandie Université

Cryptography

Let's start with a simple example: you want to send a message to someone.

Two possibilities:

- Either you share a secret key (AES...),
- Either you don't
  $\Rightarrow$ public key cryptography (RSA...).



Solve a difficult algorithmic problem $\Leftrightarrow$

Example: factorisation

- Solving those problems needs an exponential complexity on a classical computer.
- Shor's algorithm (1995): **polynomial time on a quantum computer**.

Post quantum cryptography

$\rightarrow$ Need for alternatives

- Post-quantum secure, efficient,
- New functionalities, different types of constructions.

$\rightarrow$ Lattice-based cryptography: security relies on hard problems on lattices.

NIST competition
signature and encryption
69 submissions

2017-2024

Lattice-based
3 over 4 standards

Code-based

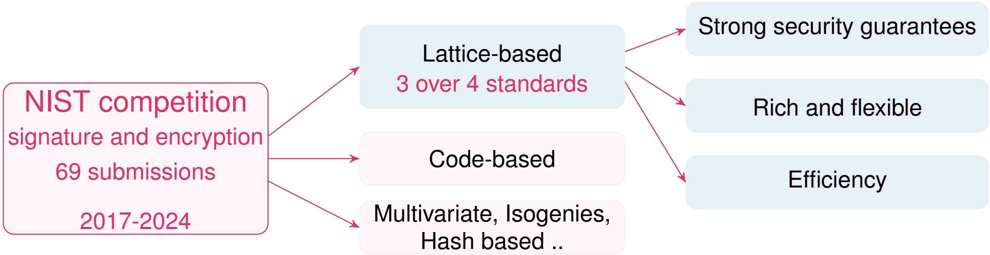
Multivariate, Isogenies,
Hash based ..

Post quantum cryptography

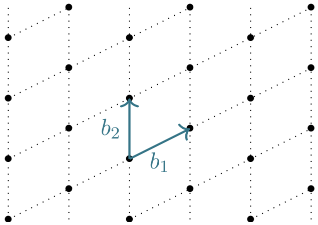
→ Need for alternatives

- Post-quantum secure, efficient,
- New functionalities, different types of constructions.

→ Lattice-based cryptography: security relies on hard problems on lattices.

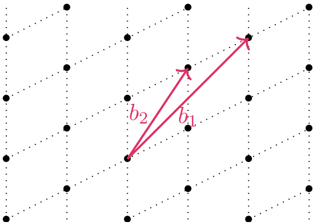


Shortest Vector Problem



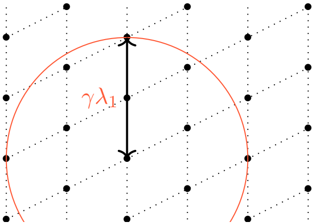
- **Lattice**
  $\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$,
  $(\mathbf{b}_i)_{1 \leq i \leq n}$ basis of $\mathcal{L}(\mathbf{B})$.

Shortest Vector Problem



- **Lattice**
  $\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$,
  $(\mathbf{b}_i)_{1 \leq i \leq n}$ basis of $\mathcal{L}(\mathbf{B})$.

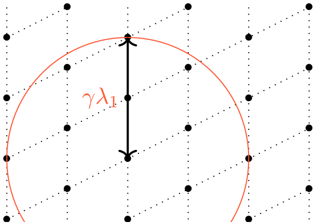
Shortest Vector Problem



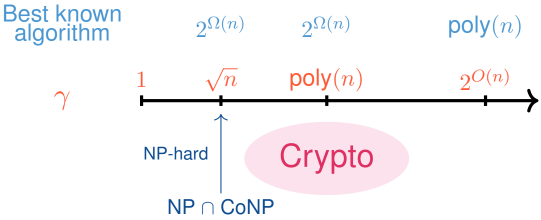
- **Lattice**
  $\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$,
  $(\mathbf{b}_i)_{1 \le i \le n}$ basis of $\mathcal{L}(\mathbf{B})$.
- λ_1 norm of the shortest vector,
- **Approx SVP$_{\gamma}$:** Given $\mathcal{L}(\mathbf{B})$, find a non zero $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\| \le \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$.

Shortest Vector Problem

GREYC
Electronics and Computer Science Laboratory



- **Lattice**
  $\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$,
  $(\mathbf{b}_i)_{1 \leq i \leq n}$ basis of $\mathcal{L}(\mathbf{B})$.
- λ_1 norm of the shortest vector,
- **Approx SVP$_\gamma$:** Given $\mathcal{L}(\mathbf{B})$, find a non zero $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\| \leq \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$.



At the heart of lattice-based cryptography
the Learning With Errors problem

- Introduced by Regev in 2005

Problem: solve a linear system with noise.

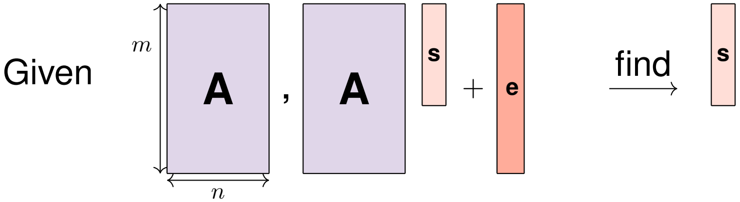
Find $(s_1, s_2, s_3, s_4, s_5)$ such that:

$$
\begin{aligned}
s_1 + 22s_2 + 17s_3 + 2s_4 + s_5 &\approx 16 \mod 23\\
3s_1 + 2s_2 + 11s_3 + 7s_4 + 8s_5 &\approx 17 \mod 23\\
15s_1 + 13s_2 + 10s_3 + 3s_4 + 5s_5 &\approx 3 \mod 23\\
17s_1 + 11s_2 + 20s_3 + 9s_4 + 3s_5 &\approx 8 \mod 23\\
2s_1 + 14s_2 + 13s_3 + 6s_4 + 7s_5 &\approx 9 \mod 23\\
4s_1 + 21s_2 + 9s_3 + 5s_4 + s_5 &\approx 18 \mod 23\\
11s_1 + 12s_2 + 5s_3 + s_4 + 9s_5 &\approx 7 \mod 23
\end{aligned}
$$

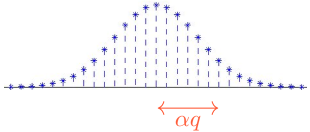
$\rightsquigarrow$ With an arbitrary number of equations.

The Learning With Errors problem

LWE$_q^n$



- **A** $\leftarrow U(\mathbb{Z}_q^{m \times n})$,
- **s** $\leftarrow U(\mathbb{Z}_q^{n})$,
- e small compared to q.

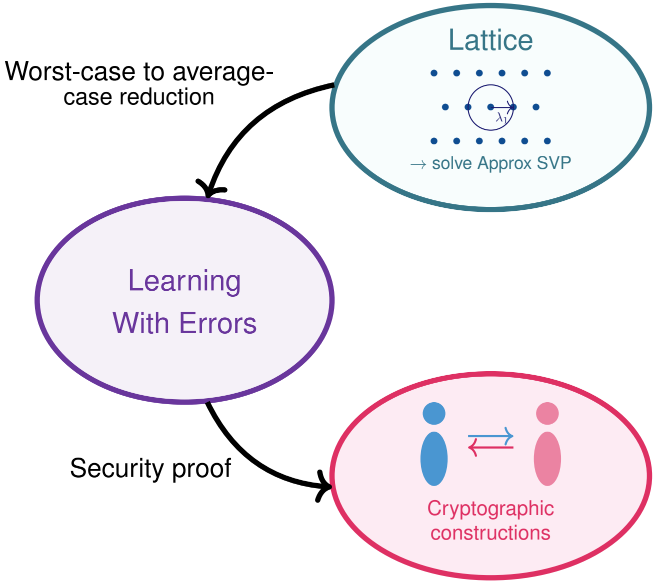


Discrete Gaussian error $D_{\mathbb{Z},\alpha q}$

Search version: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$, find **s**.

Decision version: Distinguish from $(\mathbf{A}, \mathbf{b})$ with **b** uniform.

Using LWE to build provable constructions - theory



Cryptography and security proof

Use of reductions in security proof:

- To study the hardness of a problem (for example LWE),
- To show the security of a cryptographic scheme.

When involving distributions, **the standard approach** is to use the statistical distance (SD) as measure of closeness:

$$\Delta(D_1, D_2) = \frac{1}{2} \sum_{x \in \mathsf{Supp}(D_1)} |D_1(x) - D_2(x)|\,,$$

and to apply the **probability preservation property** of SD:

- For any event E, $\Pr_{D_2}[E] \geq \Pr_{D_1}[E] - \Delta(D_1, D_2)$,

Example on LWE

Consider two LWE problems:

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

- Event S = success of an attack against LWE, $\Pr_D[S]$ is its probability under D.

Example on LWE

Consider two LWE problems:

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

- Event S = success of an attack against LWE, $\Pr_D[S]$ is its probability under D.
- If LWE_D is an hard problem, then $\varepsilon = \Pr_D[S]$ is negligible.

Example on LWE

Consider two LWE problems:

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

- Event S = success of an attack against LWE, $\Pr_D[S]$ is its probability under D.
- If LWE_D is an hard problem, then $\varepsilon = \Pr_D[S]$ is negligible.

- Reduction from LWE_{D_2} to LWE_{D_1}, we want:
  (LWE_{D_2} is hard $\Rightarrow$ LWE_{D_1} is hard) which means ε_2 negligible $\Rightarrow$ ε_1 negligible.

Example on LWE

Consider two LWE problems:

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

- Event S = success of an attack against LWE, $\Pr_D[S]$ is its probability under D.
- If LWE_D is an hard problem, then $\varepsilon = \Pr_D[S]$ is negligible.

- Reduction from LWE_{D_2} to LWE_{D_1}, we want:
  (LWE_{D_2} is hard $\Rightarrow$ LWE_{D_1} is hard) which means ε_2 negligible $\Rightarrow$ ε_1 negligible.
- By the probability preservation property of SD, we have $\varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2)$.

Example on LWE

Consider two LWE problems:

- LWE_{D_1}: Given (**A** , **b** $=$ **A** **s** $+$ e) with e $\leftarrow D_1$, find **s** .
- LWE_{D_2}: Given (**A** , **b** $=$ **A** **s** $+$ e) with e $\leftarrow D_2$, find **s** .

- Event S = success of an attack against LWE, $\Pr_D[S]$ is its probability under D.
- If LWE_D is an hard problem, then $\varepsilon = \Pr_D[S]$ is negligible.

- Reduction from LWE_{D_2} to LWE_{D_1}, we want:
  (LWE_{D_2} is hard $\Rightarrow$ LWE_{D_1} is hard) which means ε_2 negligible $\Rightarrow$ ε_1 negligible.
- By the probability preservation property of SD, we have $\varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2)$.
- $\Delta(D_1, D_2)$ negligible then gives a reduction.

Using the Rényi divergence

In some cases, the probability preservation property may not be tight.

Let D_1, D_2 be two discrete probability distributions.

Statistical distance
$$\Delta(D_1, D_2) = \frac{1}{2} \sum_{x \in \mathrm{Supp}(D_1)} |D_1(x) - D_2(x)|,$$

Rényi divergence
$$R_2(D_1, D_2) = \sum_{x \in \mathrm{Supp}(D_1)} \frac{D_1(x)^2}{D_2(x)}.$$

Both fulfill the probability preservation property for an event E:

$$\begin{array}{rcll} D_1(E) - \Delta(D_1, D_2) & \leq & D_2(E) & \text{(additive)} \\ D_1(E)^2 / R_2(D_1, D_2) & \leq & D_2(E) & \text{(multiplicative)} \end{array}$$

Using the Rényi divergence in reductions

Attack S (with D_1) with success $\varepsilon_1 \Rightarrow$ S (with D_2) with success ε_2, we want $\varepsilon_2 \Rightarrow \varepsilon_1$ negligible:

$$
\begin{array}{lcll}
\varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2) & \Rightarrow & \Delta(D_1, D_2) & \text{negligible} \\
\varepsilon_2 \geq \varepsilon_1^2 \;/\; R_2(D_1, D_2) & \Rightarrow & R_2(D_1, D_2) & \text{constant}
\end{array}
$$

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

Using the Rényi divergence in reductions

Attack S (with D_1) with success $\varepsilon_1 \Rightarrow$ S (with D_2) with success ε_2,
we want $\varepsilon_2 \Rightarrow \varepsilon_1$ negligible:

$$\begin{array}{lcll} \varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2) & \Rightarrow & \Delta(D_1, D_2) & \text{negligible} \\ \varepsilon_2 \geq \varepsilon_1^2 \,/\, R_2(D_1, D_2) & \Rightarrow & R_2(D_1, D_2) & \text{constant} \end{array}$$

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

Using the Rényi divergence in reductions

Attack S (with D_1) with success $\varepsilon_1 \Rightarrow$ S (with D_2) with success ε_2,
we want $\varepsilon_2 \Rightarrow \varepsilon_1$ negligible:

$$\begin{array}{lcll} \varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2) & \Rightarrow & \Delta(D_1, D_2) & \text{negligible} \\ \varepsilon_2 \geq \varepsilon_1^2 \,/\, R_2(D_1, D_2) & \Rightarrow & R_2(D_1, D_2) & \text{constant} \end{array}$$

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

- Reduction from LWE_{D_2} to LWE_{D_1}, we want ε_2 negligible $\Rightarrow \varepsilon_1$ negligible.

Using the Rényi divergence in reductions

Attack S (with D_1) with success $\varepsilon_1 \Rightarrow$ S (with D_2) with success ε_2,
we want $\varepsilon_2 \Rightarrow \varepsilon_1$ negligible:

$$\begin{array}{lcll} \varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2) & \Rightarrow & \Delta(D_1, D_2) & \text{negligible} \\ \varepsilon_2 \geq \varepsilon_1^2 \;/\; R_2(D_1, D_2) & \Rightarrow & R_2(D_1, D_2) & \text{constant} \end{array}$$

- LWE_{D_1}: Given ($\mathbf{A}$, $\mathbf{b}$ $=$ $\mathbf{A}$ $\mathbf{s}$ $+$ e) with e $\leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given ($\mathbf{A}$, $\mathbf{b}$ $=$ $\mathbf{A}$ $\mathbf{s}$ $+$ e) with e $\leftarrow D_2$, find $\mathbf{s}$.

- Reduction from LWE_{D_2} to LWE_{D_1}, we want ε_2 negligible $\Rightarrow \varepsilon_1$ negligible.
- By the probability preservation property of RD, we have $\varepsilon_2 \geq \varepsilon_1^2 \;/\; R_2(D_1, D_2)$.

Using the Rényi divergence in reductions

Attack S (with D_1) with success $\varepsilon_1 \Rightarrow$ S (with D_2) with success ε_2,
we want $\varepsilon_2 \Rightarrow \varepsilon_1$ negligible:

$$
\begin{array}{lcll}
\varepsilon_2 \geq \varepsilon_1 - \Delta(D_1, D_2) & \Rightarrow & \Delta(D_1, D_2) & \text{negligible} \\
\varepsilon_2 \geq \varepsilon_1^2 \; / \; R_2(D_1, D_2) & \Rightarrow & R_2(D_1, D_2) & \text{constant}
\end{array}
$$

- LWE_{D_1}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_1$, find $\mathbf{s}$.
- LWE_{D_2}: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{e} \leftarrow D_2$, find $\mathbf{s}$.

- Reduction from LWE_{D_2} to LWE_{D_1}, we want ε_2 negligible $\Rightarrow \varepsilon_1$ negligible.
- By the probability preservation property of RD, we have $\varepsilon_2 \geq \varepsilon_1^2 \; / \; R_2(D_1, D_2)$.
- $R_2(D_1, D_2)$ constant then gives a reduction.

Example on a Gaussian distribution [1]

Example: two Gaussians D_β and $D_{\beta,s}$,

$$RD(D_\beta, D_{\beta,s}) = \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right)$$

$$SD(D_\beta, D_{\beta,s}) = \frac{\sqrt{2\pi}\|s\|}{\beta}$$

Let $\|\mathbf{s}\| \leq \alpha$:

$$\begin{aligned} SD(D_\beta, D_{\beta,s}) &= \frac{\sqrt{2\pi}\|s\|}{\beta} && \Rightarrow \alpha/\beta \leq \text{negligible} \\ RD(D_\beta, D_{\beta,s}) &= \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} && \Rightarrow \alpha/\beta \leq \textbf{constant} \end{aligned}$$

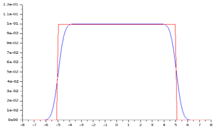
(Taylor expansion at 0)

[1] Thanks to Katharina Boudgoust for the slide.

Hardness of LWE with small uniform noise

$$\boxed{\text{Decision LWE noise } D_\alpha} \xrightarrow{\psi = D_\alpha + U_\beta} \boxed{\text{Search LWE noise } \psi} \longrightarrow \boxed{\text{Search LWE noise } U_\beta} \longrightarrow \boxed{\text{Decision LWE noise } U_\beta}$$

- Quite direct by adding samples, then decision-to-search reduction.
- Using that the Rényi divergence $R_2(U_\beta || \psi)$ can be bounded by $1 + 1.05 \cdot \frac{\alpha}{\beta}$.



- Using **Micciancio Mol 11** sample preserving search-to-decision reduction (needs prime q).

More general result

Using the Rényi divergence, we have a reduction:

$$\begin{tikzcd}
\boxed{\text{Search LWE noise } D_\alpha} \arrow[d] \\
\boxed{\text{Search LWE noise } \psi}
\end{tikzcd}$$

- Either $R_2(\psi || D_\alpha)$ is small,
- Either $R_2(\psi || \psi + D_\alpha)$ is small.

- Works nicely if the two distributions are close enough,
- Only needs to compute R_2,
- Distributions may be too far from each other (example: binary).

More generally

Often a **security gap** between:

- Cryptographic security **assumptions/problems**: use ideal probability distributions,
- Cryptographic **schemes/implementations**: use imperfect probability distributions.

The problem is to choose the 'imperfect' distribution parameters to account the security gap $\rightarrow$ can have a significant impact!

The Rényi Divergence often gives a better approach to analyse this security gap and allow relaxed 'imperfect' parameters $\rightarrow$ efficiency gain!

Limitation: It only works on search problems, where we often need decisional problems in cryptography.