

USING RÉNYI DIVERGENCE IN LATTICE-BASED CRYPTOGRAPHY

Adeline Roux-Langlois

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

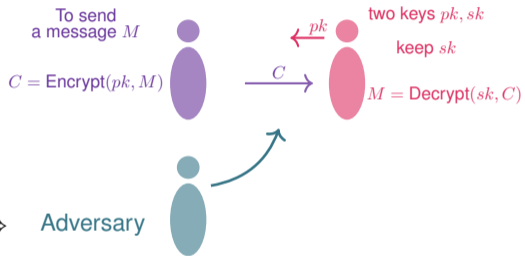


Let's start with a simple example: you want to send a message to someone.

Two possibilities:

- ▶ Either you share a secret key (AES...),
- ▶ Either you don't
⇒ public key cryptography (RSA...).

Solve a difficult algorithmic problem ⇔ Adversary
Example: factorisation

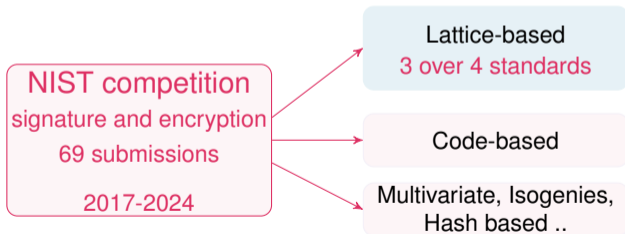


- ▶ Solving those problems needs an exponential complexity on a classical computer.
- ▶ Shor's algorithm (1995): **polynomial time on a quantum computer.**

→ Need for alternatives

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

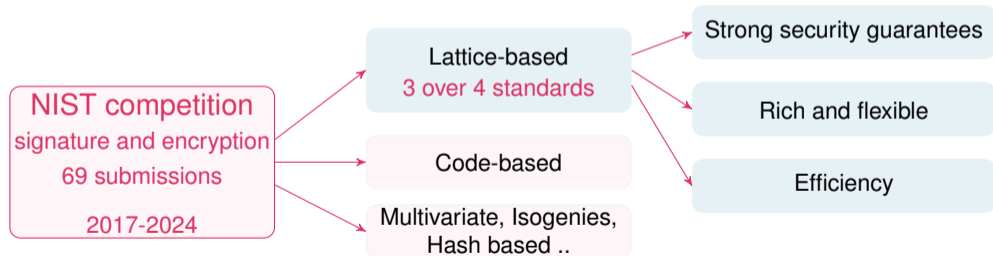
→ Lattice-based cryptography: security relies on hard problems on lattices.



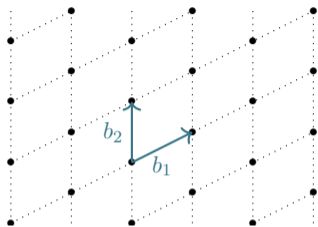
→ Need for alternatives

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

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



Shortest Vector Problem

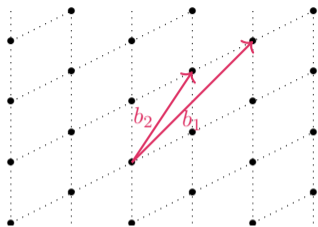


► Lattice

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^n a_i \mathbf{b}_i, a_i \in \mathbb{Z} \right\},$$

$(\mathbf{b}_i)_{1 \leq i \leq n}$ basis of $\mathcal{L}(\mathbf{B})$.

Shortest Vector Problem

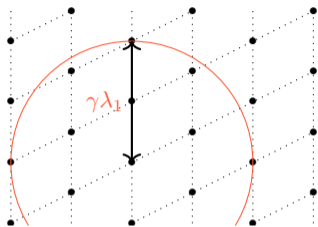


► Lattice

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^n a_i \mathbf{b}_i, a_i \in \mathbb{Z} \right\},$$

$(\mathbf{b}_i)_{1 \leq i \leq n}$ basis of $\mathcal{L}(\mathbf{B})$.

Shortest Vector Problem



► Lattice

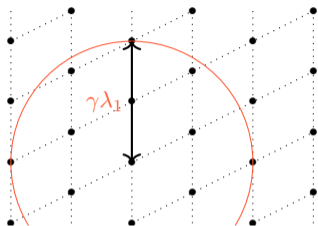
$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^n a_i \mathbf{b}_i, a_i \in \mathbb{Z} \right\},$$

$(\mathbf{b}_i)_{1 \leq i \leq n}$ 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 $\|\mathbf{x}\| \leq \gamma \lambda_1(\mathcal{L}(\mathbf{B}))$.

Shortest Vector Problem



► Lattice

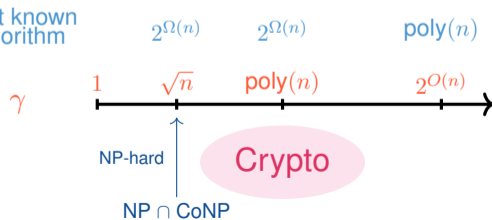
$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^n a_i \mathbf{b}_i, a_i \in \mathbb{Z} \right\},$$

$(\mathbf{b}_i)_{1 \leq i \leq n}$ 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 $\|\mathbf{x}\| \leq \gamma \lambda_1(\mathcal{L}(\mathbf{B}))$.

Best known algorithm



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

- ▶ Introduced by Regev in 2005

Problem: solve a linear system with noise.

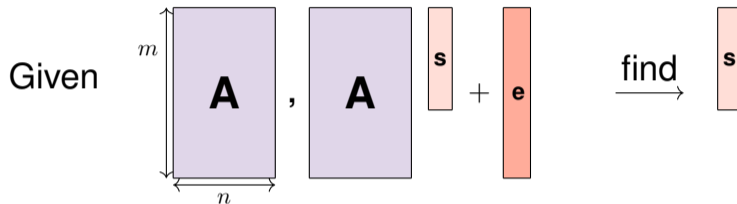
Find $(s_1, s_2, s_3, s_4, s_5)$ such that:

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

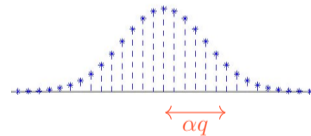
↪ With an arbitrary number of equations.

The Learning With Errors problem

LWE_q^n



- ▶ $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$,
- ▶ $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
- ▶ 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 \mathbf{s} .

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

Decisional LWE

Decision LWE can also be seen as a game:

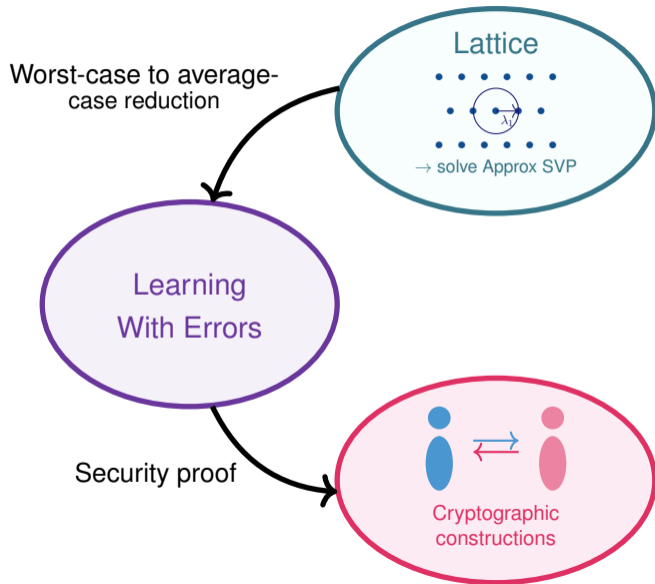
$$\begin{array}{c} \mathcal{C} \qquad \qquad \qquad \mathcal{B} \\ \hline \mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n}) \\ \text{RAND } (b = 0): \mathbf{b} \leftarrow U(\mathbb{Z}_q^m) \\ \text{LWE } (b = 1): \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \quad \xrightarrow{(\mathbf{A}, \mathbf{b})} \\ \hline \text{output } b' \end{array}$$

$$\text{Adv}(\mathcal{B}) = \left| \Pr[\mathcal{B} \xrightarrow{\text{RAND}} 1] - \Pr[\mathcal{B} \xrightarrow{\text{LWE}} 1] \right|$$

The Decision problem is difficult to solve if for all Probabilistic Polynomial Time (PPT) algorithm \mathcal{B} , there exists a negligible function $\text{negl}(n)$ such that:

$$\text{Adv}(\mathcal{B}) \leq \text{negl}(n).$$

Using LWE to build provable constructions - theory



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:

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

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 a 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 a hard problem, then $\varepsilon = \Pr_D[S]$ is negligible.
- ▶ Reduction from LWE_{D_2} to LWE_{D_1} , we want:
 $(\text{LWE}_{D_2} \text{ is hard} \Rightarrow \text{LWE}_{D_1} \text{ is hard})$ which means $\varepsilon_2 \text{ negligible} \Rightarrow \varepsilon_1 \text{ negligible}$.

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 a hard problem, then $\varepsilon = \Pr_D[S]$ is negligible.
- ▶ Reduction from LWE_{D_2} to LWE_{D_1} , we want:
 $(\text{LWE}_{D_2} \text{ is hard} \Rightarrow \text{LWE}_{D_1} \text{ is hard})$ which means $\varepsilon_2 \text{ negligible} \Rightarrow \varepsilon_1 \text{ negligible}$.
- ▶ 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 $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ 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 a 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

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

Rényi divergence

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

Both fulfill the **probability preservation property** for an event E :

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

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:

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

- ▶ 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:

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

- ▶ 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:

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

- ▶ 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:

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

- ▶ 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 $\varepsilon_2 \geq \varepsilon_1^2 / R_2(D_1, D_2)$.

Using the Rényi divergence in reductions

Attack S (with D_1) with success $\epsilon_1 \Rightarrow$ S (with D_2) with success ϵ_2 ,
we want $\epsilon_2 \Rightarrow \epsilon_1$ negligible:

$$\begin{aligned}\epsilon_2 &\geq \epsilon_1 - \Delta(D_1, D_2) &\Rightarrow & \Delta(D_1, D_2) \text{ negligible} \\ \epsilon_2 &\geq \epsilon_1^2 / R_2(D_1, D_2) &\Rightarrow & R_2(D_1, D_2) \text{ constant}\end{aligned}$$

- ▶ 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 $\Rightarrow \epsilon_1$ negligible.
- ▶ By the probability preservation property of RD, we have $\epsilon_2 \geq \epsilon_1^2 / R_2(D_1, D_2)$.
- ▶ $R_2(D_1, D_2)$ constant then gives a reduction.

Example on a Gaussian distribution ¹



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

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

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

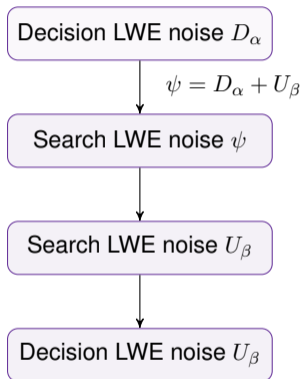
Let $\|s\| \leq \alpha$:

$$SD(D_\beta, D_{\beta,s}) = \frac{\sqrt{2\pi}\|s\|}{\beta} \Rightarrow \alpha/\beta \leq \text{negligible}$$

$$RD(D_\beta, D_{\beta,s}) = \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} \Rightarrow \alpha/\beta \leq \text{constant}$$

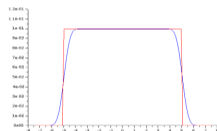
(Taylor expansion at 0)

¹Thanks to Katharina Boudgoust for the slide.



► Quite direct by adding samples, then decision-to-search reduction.

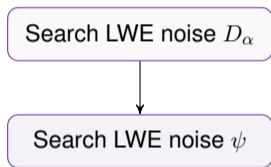
► Using that the Rényi divergence $R_2(U_\beta || \psi)$ can be bounded by $1 + 1.05 \cdot \frac{\alpha}{\beta}$.



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

More general result

Using the Rényi divergence, we have a reduction:



- ▶ 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 → can have a significant impact!

The Rényi Divergence often gives a better approach to analyse this security gap and allow relaxed ‘imperfect’ parameters → efficiency gain!

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