ProvSec2015@Kanazawa

Tighter Security for Efficient Lattice Cryptography via the Rényi Divergence of Optimized Orders

Katsuyuki Takashima
Mitsubishi Electric

Atsushi Takayasu
The University of Tokyo

2015, November 26

Background

Lattice Cryptography

- Lattice cryptography has novel properties.
  - Resist quantum attacks
  - Worst-case/Average-case reduction
  - Faster computation and parallelizable

Lattice Cryptography

- Lattice cryptography has novel properties.
  - Resist quantum attacks
  - Worst-case/Average-case reduction
  - Faster computation and parallelizable
- In the security reduction, there are *statistical* steps; to measure the closeness of two probability distributions.

  e.g., zero centered and non-zero centered discrete Gaussian distributions.

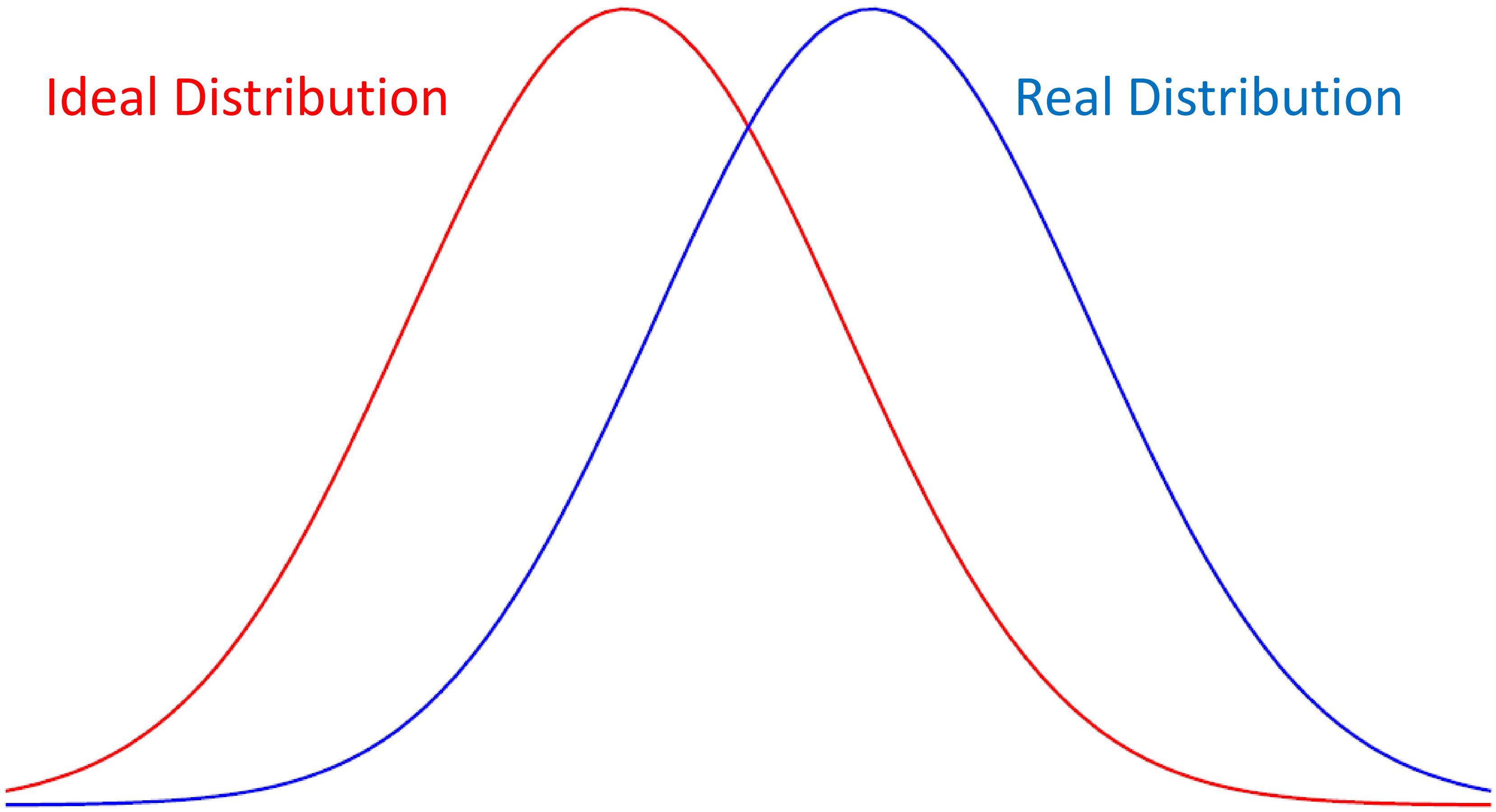
Lattice Cryptography

- Lattice cryptography has novel properties.
  - Resist quantum attacks
  - Worst-case/Average-case reduction
  - Faster computation and parallelizable
- In the security reduction, there are *statistical* steps; to measure the closeness of two probability distributions.

  e.g., zero centered and non-zero centered discrete Gaussian distributions.

The security reduction follows through when the distributions are *statistically close*.

Statistical Analysis



Statistical Analysis

Ideal Distribution

Real Distribution

Ideal distributions and real distributions are *statistically close*

Simulated cryptographic scheme and real scheme are *statistically indistinguishable*.

Statistical Analysis

The larger parameters (e.g. Gaussian deviations),

- two distributions become statistically close e.g. the real schemes become *secure*,
- the scheme becomes *less efficient*.

✓ We want to analyze the appropriate trade-off.

The analyses owe to *statistical measures*.

Which measure should be used?

Statistical Distance vs Rényi Divergence

Statistical Measure

Statistical Distance (SD)

- SD is widely used in security reduction.
- SD should be much smaller than the advantage for the reduction.
  inefficient parameters
- Small SD offers tight reduction.

Rényi Divergence (RD)

- RD is recently used in security reduction for lattice crypto. [LPR13,LSS14,LPSS14,BLL+15].
- RD can be independent of the advantage.
  smaller parameters
- Even if RD is small, reductions always lose the tightness.

Statistical Measure

Statistical Distance (SD)

- SD is widely used in security reduction.
- SD
  the
  ine
- Small SD offers tight reduction.

Rényi Divergence (RD)

- RD is recently used in security reduction for lattice crypto. [LPR13,LSS14,LPSS14,BLL+15].
- Even if RD is small, reductions always lose the tightness.

Can we prove the security with *both* small parameters and tight reduction?

Our Solution

- In the previous RD based analyses, *the order* is fixed to $\alpha = 2$.
- In this work, we use the *optimized order*.
  The optimization offers *tighter reduction* even if we use the RD.

Our Solution

- In the previous RD based analyses, ***the order*** is fixed to $\alpha = 2$.
- In this work, we use the ***optimized order***.
  The optimization offers *tighter reduction* even if we use the RD.

Our approach offers

- tighter reduction than the previous RD based analyses,
- with smaller parameters than the SD based analyses.

Precomputed Table Size for BLISS Signature

statistical measure	table bit-size	reduction loss ε/ε'
SD [DDLL13]	6003	≤ 2
KLD [PDG14]	4872	≤ 2
RD, $\alpha = +\infty$ [BLL+15]	2291	≤ 2
RD, $\alpha = 2$ [BLL+15]	1160	$\approx 2^{128}$
RD, optimized order Ours	1276	≤ 2

Our Approach

Overview of the Security Reduction

- Problem *P*: given $X = \{x_i : x_i \leftarrow \Phi\}_{i=1,\ldots,k}$ and compute $f(X)$
- Problem *P'*: given $X' = \{x'_i : x'_i \leftarrow \Phi'\}_{i=1,\ldots,k}$ and compute $f(X')$

✓ When two probability distributions Φ and Φ' are *statistically close*, the adversary for the problem *P* is also the adversary for the problem *P'*.

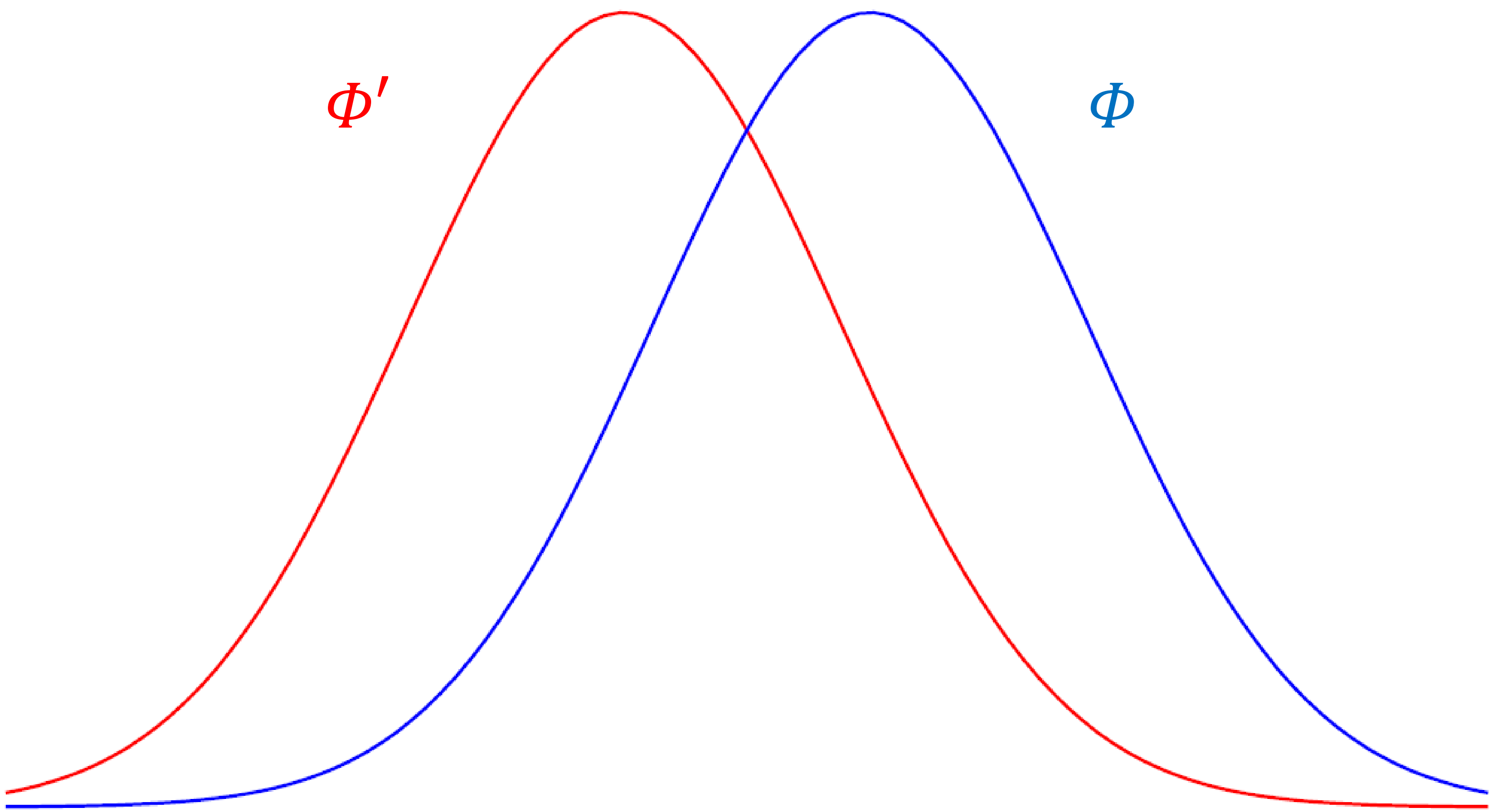
SD Based Analysis

- ε: the advantage for the adversary to solve *P*
- ε': the advantage for the adversary to solve *P'*

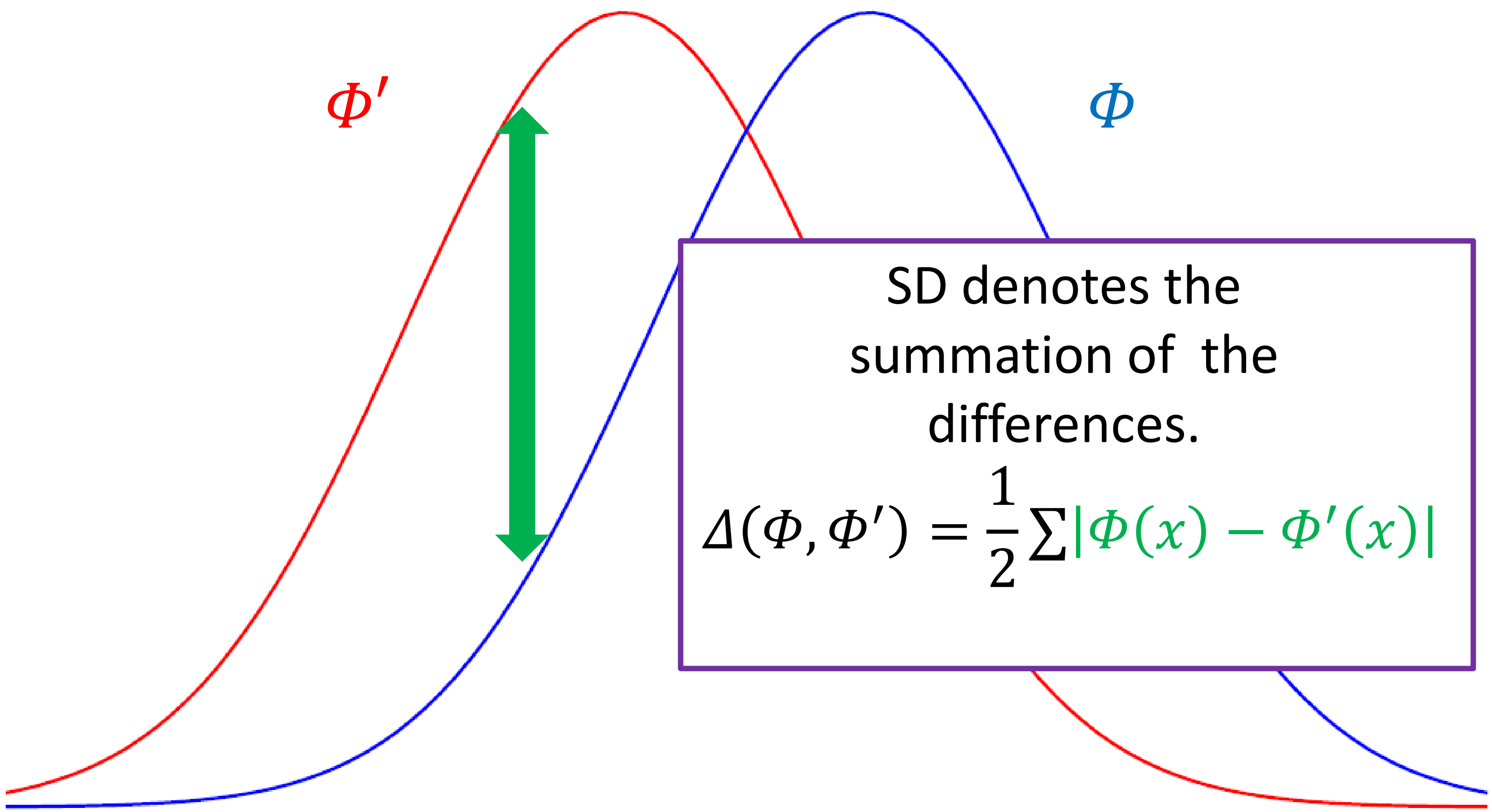
The SD between Φ and Φ':

$$\Delta(\Phi, \Phi') = \frac{1}{2} \sum |\Phi(x) - \Phi'(x)|$$

SD Based Analysis



SD Based Analysis



SD denotes the summation of the differences.

$$\Delta(\Phi, \Phi') = \frac{1}{2}\sum|\Phi(x) - \Phi'(x)|$$

SD Based Analysis

- ε: the advantage for the adversary to solve *P*
- ε': the advantage for the adversary to solve *P'*

The SD between Φ and Φ':

$$\Delta(\Phi, \Phi') = \frac{1}{2}\sum|\Phi(x) - \Phi'(x)|$$

$$\Rightarrow \quad \varepsilon \leq \varepsilon' + k\Delta(\Phi, \Phi')$$

SD should be <u>*much smaller than* ε/k</u>

The *strong requirement* leads to inefficient parameters.

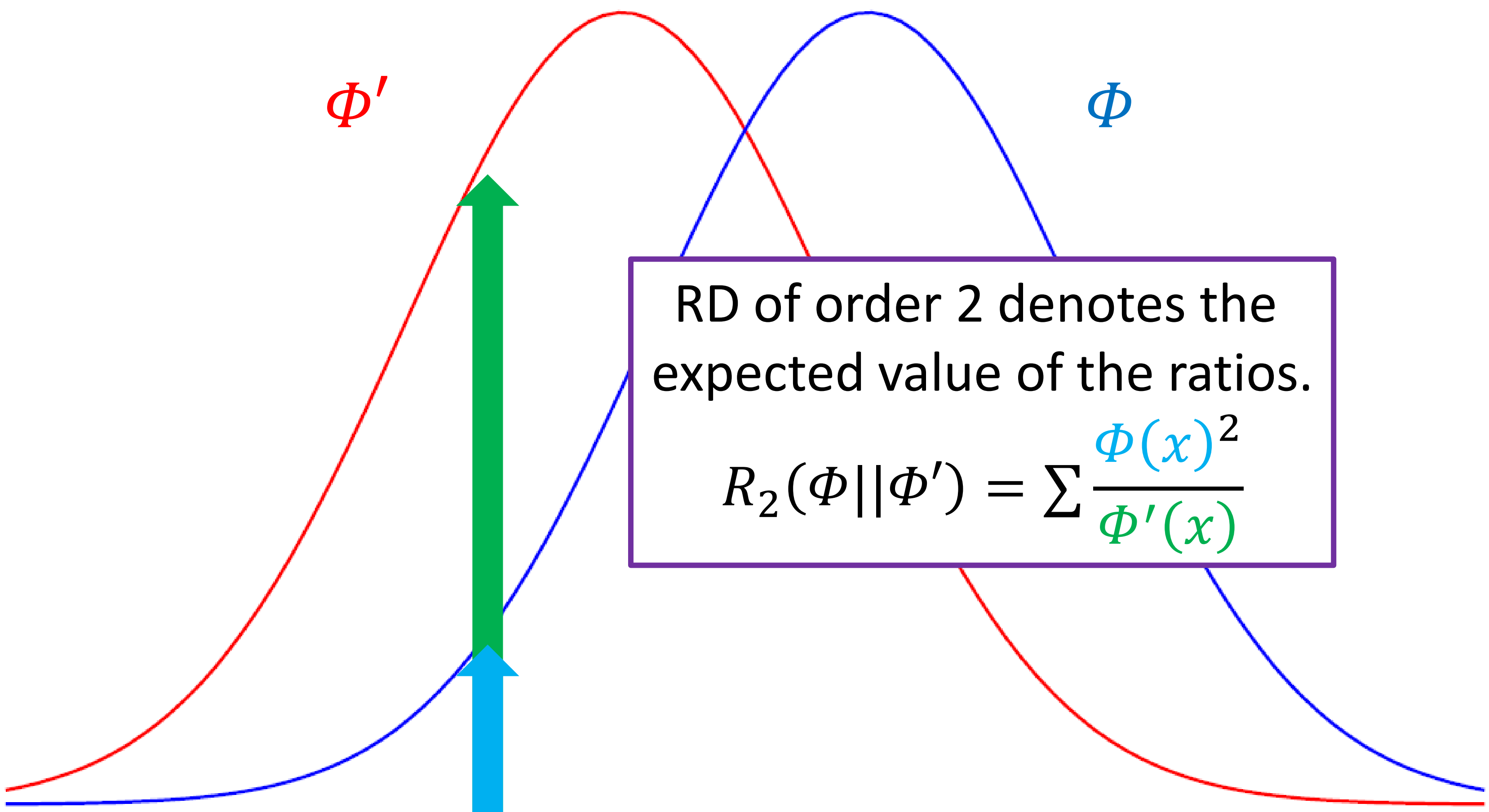
Previous RD Based Analysis

- ε: the advantage for the adversary to solve *P*
- ε': the advantage for the adversary to solve *P'*

The RD (of order 2) between Φ and Φ':

$$R_2(\Phi||\Phi') = \sum \frac{\Phi(x)^2}{\Phi'(x)}$$

Previous RD Based Analysis



RD of order 2 denotes the expected value of the ratios.

$$R_2(\Phi||\Phi') = \sum \frac{\Phi(x)^2}{\Phi'(x)}$$

Previous RD Based Analysis

- ε: the advantage for the adversary to solve *P*
- ε': the advantage for the adversary to solve *P'*

The RD (of order 2) between Φ and Φ':

$$R_2(\Phi||\Phi') = \sum \frac{\Phi(x)^2}{\Phi'(x)}$$

$$\Rightarrow \quad \varepsilon \leq \left(\varepsilon' \cdot R_2(\Phi||\Phi')^k\right)^{\frac{1}{2}}$$

Previous RD Based Analysis

$$\varepsilon \leq \left(\varepsilon' \cdot R_2(\Phi||\Phi')^k\right)^{\frac{1}{2}}$$

- RD are allowed to be larger bounds (small constant).

⇒ Significant parameter savings!

Previous RD Based Analysis

$$\varepsilon \leq \left(\varepsilon' \cdot R_2(\Phi||\Phi')^k\right)^{\frac{1}{2}}$$

- RD are allowed to be larger bounds (small constant).

⇒ Significant parameter savings!

- Even if RD is extremely small (almost 1), the RHS is always larger than $\varepsilon'^{1/2}$.

⇒ The reduction always loses the tightness.

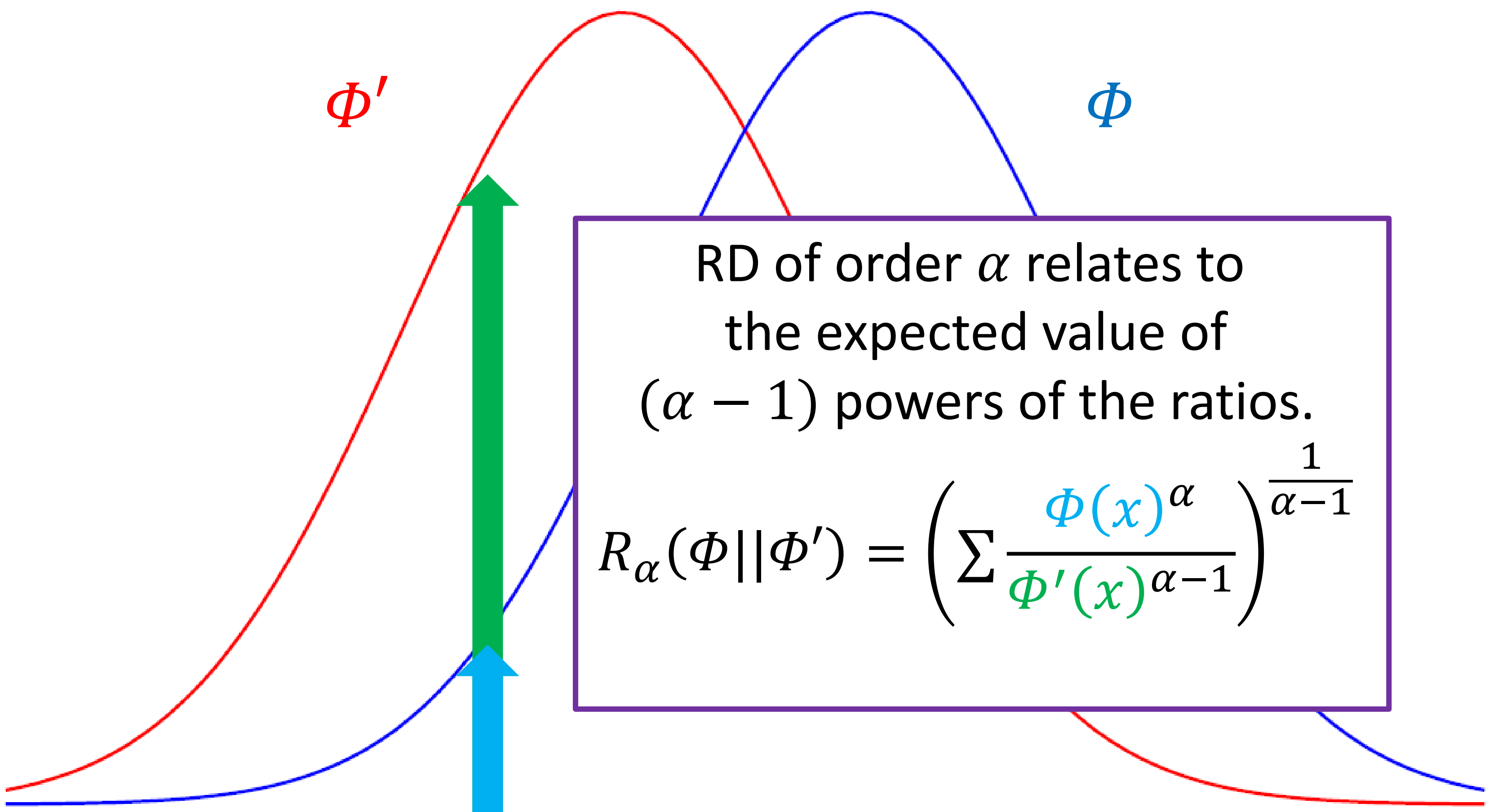
Our RD Based Analysis

- ε: the advantage for the adversary to solve *P*
- ε': the advantage for the adversary to solve *P'*

The RD between Φ and Φ':

$$R_\alpha(\Phi||\Phi') = \left(\sum \frac{\Phi(x)^\alpha}{\Phi'(x)^{\alpha-1}}\right)^{\frac{1}{\alpha-1}}$$

Our RD Based Analysis



RD of order α relates to the expected value of $(\alpha - 1)$ powers of the ratios.

$$R_\alpha(\Phi||\Phi') = \left(\sum \frac{\Phi(x)^\alpha}{\Phi'(x)^{\alpha-1}}\right)^{\frac{1}{\alpha-1}}$$

Our RD Based Analysis

- ε: the advantage for the adversary to solve *P*
- ε': the advantage for the adversary to solve *P'*

The RD between Φ and Φ':

$$R_\alpha(\Phi||\Phi') = \left(\sum \frac{\Phi(x)^\alpha}{\Phi'(x)^{\alpha-1}}\right)^{\frac{1}{\alpha-1}}$$

$$\Rightarrow \quad \varepsilon \leq \left(\varepsilon' \cdot R_\alpha(\Phi||\Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$

Our RD Based Analysis

$$\varepsilon \le \left(\varepsilon' \cdot R_\alpha(\Phi || \Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$

When the *larger* α is used, the exponent of ε' becomes close to 1.

Tighter reduction!

Our RD Based Analysis

$$\varepsilon \le \left(\varepsilon' \cdot R_\alpha(\Phi||\Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$

When the *larger α* is used, the exponent of ε' becomes close to 1.

Tighter reduction!

✓ Since RD becomes exponential of α, α cannot be infinitely large.

Our RD Based Analysis

$$\varepsilon \le \left(\varepsilon' \cdot R_\alpha(\Phi||\Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$

When the *larger* α is used, the exponent of ε' becomes close to 1.

We *adaptively optimize* the order α for the reduction to become as tight as possible.

✓ Since RD becomes exponential of α, α cannot be infinitely large.

Adaptive Optimization of the Order

Assume $R_\alpha(\Phi||\Phi') \leq \exp(\alpha \cdot \gamma)$,

$$\varepsilon \leq \left(\varepsilon' \cdot R_\alpha(\Phi||\Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$
$$\leq \exp\left(\frac{\alpha-1}{\alpha} \cdot \ln(\varepsilon') + (\alpha-1) \cdot k\gamma\right).$$

Adaptive Optimization of the Order

Assume $R_\alpha(\Phi||\Phi') \le \exp(\alpha \cdot \gamma)$,

$$\varepsilon \le \left(\varepsilon' \cdot R_\alpha(\Phi||\Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$

$$\le \exp\left(\frac{\alpha - 1}{\alpha} \cdot \ln(\varepsilon') + (\alpha - 1) \cdot k\gamma\right).$$

The RHS is lower bounded as

$$= \exp\left(\ln(\varepsilon') - k\gamma + \left(\frac{-\ln(\varepsilon')}{\alpha} + \alpha \cdot k\gamma\right)\right)$$

Adaptive Optimization of the Order

Assume $R_\alpha(\Phi||\Phi') \leq \exp(\alpha \cdot \gamma)$,

$$\varepsilon \leq \left(\varepsilon' \cdot R_\alpha(\Phi||\Phi')^k\right)^{\frac{\alpha-1}{\alpha}}$$
$$\leq \exp\left(\frac{\alpha - 1}{\alpha} \cdot \ln(\varepsilon') + (\alpha - 1) \cdot k\gamma\right).$$

The RHS is lower bounded as

$$= \exp\left(\ln(\varepsilon') - k\gamma + \left(\frac{-\ln(\varepsilon')}{\alpha} + \alpha \cdot k\gamma\right)\right)$$
$$\geq \exp\left(\ln(\varepsilon') - k\gamma + 2\sqrt{-\ln(\varepsilon') \cdot k\gamma}\right)$$

by the inequality of arithmetic mean and geometric mean.

Adaptive Optimization of the Order

The equality holds iff

$$\frac{-\ln(\varepsilon')}{\alpha} = \alpha \cdot k\gamma \quad \Rightarrow \quad \alpha = \sqrt{\frac{-\ln(\varepsilon')}{k\gamma}}.$$

Adaptive Optimization of the Order

The equality holds iff

$$\frac{-\ln(\varepsilon')}{\alpha} = \alpha \cdot k\gamma \quad \Rightarrow \quad \alpha = \sqrt{\frac{-\ln(\varepsilon')}{k\gamma}}.$$

We use the order and the inequality becomes

$$\varepsilon \leq \exp\left(\ln(\varepsilon') - k\gamma + 2\sqrt{-\ln(\varepsilon') \cdot k\gamma}\right)$$
$$= \exp\left(-\left(\sqrt{-\ln(\varepsilon')} - \sqrt{k\gamma}\right)^2\right).$$

When RD is small ($\gamma \approx 0$), the RHS of the inequality becomes $\approx \varepsilon'$.

Summary of Our Results

- Our approach offers security reduction where
  - $\approx \varepsilon' \leftarrow \approx \varepsilon'^{1/2}$ for computing problems and
  - $\approx \varepsilon'^{1/2} \leftarrow \approx \varepsilon'^{1/3}$ for distinguishing problems.
- Applications of our approaches are
  - Sampling discrete Gaussian over the integers with smaller precomputed tables for BLISS signatures.
  - Tighter LWE to *k*-LWE reduction.
  - Tighter SIS to *k*-SIS reduction.

Sampling Discrete Gaussian over the Integers

Bimodal Lattice Signature Scheme

BLISS signatures [DDLL13]

- are secure under the worst case ideal lattice problem (SIS).
- are comparably efficient as RSA and ECDSA
- requires to sample several hundreds of independent samples from one-dimensional *discrete Gaussian distributions over the integers* for a signing.

Sampling Discrete Gaussian over the Integers [DDLL13]

Discrete Gaussian distributions $D_{\mathbb{Z},s}$ can be sampled by using *Bernoulli random variables* with probabilities

$c_i = \exp\left(-\frac{\pi 2^i}{s^2}\right)$ for $i = 0, \ldots, l-1$.

Sampling Discrete Gaussian over the Integers [DDLL13]

Discrete Gaussian distributions $D_{\mathbb{Z},s}$ can be sampled by using *Bernoulli random variables* with probabilities

$c_i = \exp\left(-\frac{\pi 2^i}{s^2}\right)$ for $i = 0, \ldots, l-1$.

Storing the truncated probabilities $\widetilde{c_i}$ with bit precisions p, Bernoulli random variables can be sampled efficiently.

Sampling Discrete Gaussian over the Integers [DDLL13]

Discrete Gaussian distributions $D_{\mathbb{Z},s}$ can be sampled by using *Bernoulli random variables* with probabilities $c_i = \exp\left(-\frac{\pi 2^i}{s^2}\right)$ for $i = 0, \ldots, l-1$.

Storing the truncated probabilities $\widetilde{c_i}$ with bit precisions p, Bernoulli random variables can be sampled efficiently.

> Larger p with security
> vs
> Smaller p with efficiency

✓ An appropriate trade-off should be analyzed.

Statistical Analyses

The trade-off can be analyzed by estimating the statistical closeness between the *real distributions* (with probabilities $\widetilde{c_i}$) and the *ideal distributions* (with probabilities c_i).

Statistical Analyses

The trade-off can be analyzed by estimating the statistical closeness between the *real distributions* (with probabilities $\widetilde{c_i}$) and the *ideal distributions* (with probabilities c_i).

Several statistical measures have been used

- SD [DDLL13]
- Kullback-Leibler divergence [PDG14]
- RD of order $\alpha = 2$ and $+\infty$ [BLL+15]

✓ We use the RD of *optimized orders*.

Comparison

statistical measure	table bit-size	reduction loss ε/ε'
SD [DDLL13]	6003	≤ 2
KLD [PDG14]	4872	≤ 2
RD, $\alpha = +\infty$ [BLL+15]	2291	≤ 2
RD, $\alpha = 2$ [BLL+15]	1160	$\approx 2^{128}$
RD, optimized order Ours	1276	≤ 2

Our Results

- In the security reduction of lattice cryptography, the closeness of two probability distributions should be measured. To bound the closeness via the *Rényi divergence*, we adaptively optimize the order.
- Applications of our approach are
  – Sampling discrete Gaussian over the integers with smaller precomputed tables
  – Tighter LWE to *k*-LWE reduction
  – Tighter SIS to *k*-SIS reduction