Leftover Hash Lemmas for Cyclotomic Rings

joint work with Katharina Boudgoust

Sasha Lapiha, Silence Laboratories @ Eurocrypt 2026
*work done while I was a PhD student at Royal Holloway, University of London

Origins of Leftover Hash Lemma (LHL)

randomness extraction [HILL99]

For $x \leftarrow \chi \in \{0,1\}^m$ with high entropy

Hash is $H_{\text{seed}}(x) \sim \mathcal{U}(\{0,1\}^n)$ for some $n \leq m$

The hash function is public, but chosen at random using seed

Lattice case

The hash is a matrix multiplication

$$(\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q) \sim (\mathbf{A}, \mathcal{U}(\mathscr{R}_q^n))$$

where

$$\mathbf{A} \leftarrow \mathcal{U}(\mathscr{R}_q^{n \times m}), \quad \mathbf{x} \leftarrow \chi$$

and χ is usually a short distribution over $\mathscr{R}^m$ or $\mathscr{R}_q^m$

Field case - $\mathbb{Z}_q$

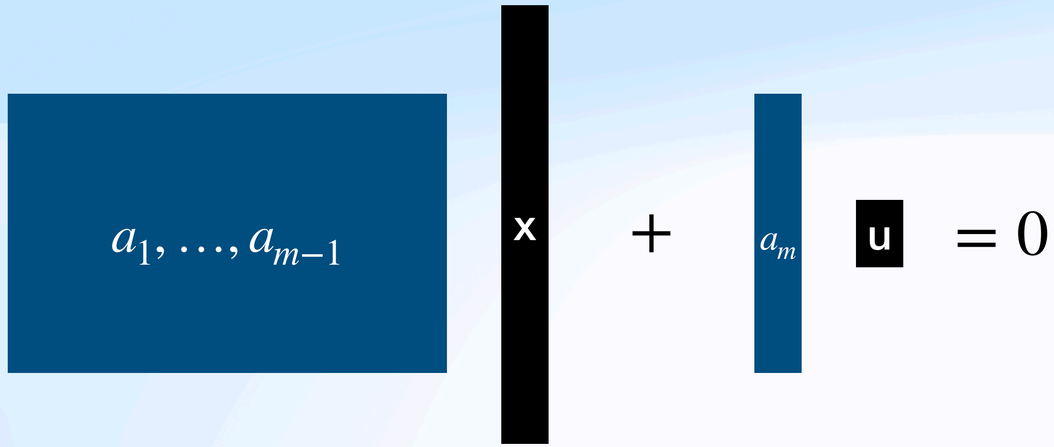
Common strategy - $\mathbf{A}$ defines a universal hash function.

For $\mathbf{x}' \neq \mathbf{x}$: $\Pr_A(\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{x}') = \Pr_A(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/q^n$

Field case - $\mathbb{Z}_q$

Common strategy - $\mathbf{A}$ defines a universal hash function.

For $\mathbf{x}' \neq \mathbf{x}$: $\Pr_A(\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{x}') = \Pr_A(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/q^n$



Field case - $\mathbb{Z}_q$

Common strategy - $\mathbf{A}$ defines a universal hash function.

For $\mathbf{x}' \neq \mathbf{x}$: $\Pr(\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{x}') = \Pr(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/q^n$

Then $\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q), (\mathbf{A}, \mathcal{U}(\mathcal{R}_q^n))) \leq \frac{1}{2}\sqrt{q^n \cdot \mathsf{Coll}(\chi)}$

where $\mathsf{Coll}(\chi) = \Pr(\mathbf{x} = \mathbf{x}' \mid \mathbf{x}, \mathbf{x}' \leftarrow \chi)$

Field case - $\mathbb{Z}_q$

Common strategy - $\mathbf{A}$ defines a universal hash function.

For $\mathbf{x}' \neq \mathbf{x} : \Pr(\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{x}') = \Pr(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/q^n$

Then $\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q), (\mathbf{A}, \mathcal{U}(\mathcal{R}_q^n))) \leq \frac{1}{2}\sqrt{q^n \cdot \mathsf{Coll}(\chi)}$

where $\mathsf{Coll}(\chi) = \Pr(\mathbf{x} = \mathbf{x}' \mid \mathbf{x}, \mathbf{x}' \leftarrow \chi)$

note $\mathsf{Coll}(\chi) \leq 2^{-H_\infty(\chi)}$

Notations

Cyclotomic rings $\mathscr{R} \sim \mathbb{Z}[X]/\Phi(X)$ with $\deg(\Phi(X)) = d$

Quotient ring for $q \geq 1 : \mathscr{R}_q = \mathscr{R} \bmod q \sim \prod \mathbb{Z}_q[X]/\Phi_i(X)$ s.t.

$\prod \Phi_i(X) = \Phi(X) \bmod q$. Denote $\deg(\Phi_i(X)) = \delta, f = d/\delta$

Ring case $\mathscr{R}_q \sim \Pi(\mathbb{Z}_q[X]/\Phi_i(X))$

- For most parameterisations $\mathscr{R}_q$ is not a field (e.g. never for power-of-2 cyclotomics)
- $\mathbf{x} - \mathbf{x}'$ may have non-unit coordinates

Ring case $\mathscr{R}_q \sim \Pi(\mathbb{Z}_q[X]/\Phi_i(X))$

- For most parameterisations $\mathscr{R}_q$ is not a field (e.g. never for power-of-2 cyclotomics)
- $\mathbf{x} - \mathbf{x}'$ may have non-unit coordinates
- Hence, a $\mathbf{A}$ is not a universal hash function

Ring case $\mathscr{R}_q \sim \Pi(\mathbb{Z}_q[X]/\Phi_i(X))$

- For most parameterisations $\mathscr{R}_q$ is not a field (e.g. never for power-of-2 cyclotomics)
- $\mathbf{x} - \mathbf{x}'$ may have non-unit coordinates
- Hence, a $\mathbf{A}$ is not a universal hash function

Instead:

- take into account ring structure
- properties of $\mathbf{x}$ modulo ideals of $\mathscr{R}_q$

Our Contributions

- Modular proof structure (Counting and Smoothing)
- Systematise and generalise existing literature
- Compute concrete entropy properties

Our Contributions

- Modular proof structure (Counting and Smoothing)
- Systematise and generalise existing literature
- Compute concrete entropy properties
- Statistical distance and Rényi divergence
- Coefficient and canonical embeddings

Our Contributions

- Modular proof structure (Counting and Smoothing)
- Systematise and generalise existing literature
- Compute concrete entropy properties
- Statistical distance and Rényi divergence
- Coefficient and canonical embeddings
- LHL with leakage $(\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q, f(\mathbf{x})) \sim (\mathbf{A}, \mathcal{U}(\mathcal{R}_q^n), f(\mathbf{x}))$:

$$f_0(\mathbf{x}) = (\mathbf{E}, \mathbf{E} \cdot \mathbf{x}), f_1(\mathbf{x}) = (\mathbf{E}, \mathbf{E} \cdot \mathbf{x} + \mathbf{y})$$

Counting Approach

Counting approach

Summarising [Mic07], [MM11], [KY16], [LW20], etc.

$$\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q), (\mathbf{A}, \mathcal{U}(\mathscr{R}_q^n))) \leq \frac{1}{2}\sqrt{\Sigma_{\mathscr{I} \in \mathbf{I}} N(\mathscr{I}) \cdot \mathsf{Coll}(\chi \bmod \mathscr{I}) - 1}$$

where $\mathsf{Coll}(\chi \bmod \mathscr{I}) = \Pr(\mathbf{x} = \mathbf{x}' \bmod \mathscr{I} \mid \mathbf{x}, \mathbf{x}' \leftarrow \chi)$

and $\mathbf{I}$ - set of ideals in $\mathscr{R}_q$

Counting approach

- Because if $\langle x_0 - x'_0, \ldots, x_{d-1} - x'_{d-1} \rangle = \mathcal{I}_{\mathbf{x},\mathbf{x}'} = \mathcal{I}$ then
- $\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') \sim \mathcal{U}(\mathcal{I}^n)$ and $\Pr(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/|\mathcal{I}|^n$

Counting approach

- Because if $\langle x_0 - x'_0, \ldots, x_{d-1} - x'_{d-1} \rangle = \mathscr{I}_{\mathbf{x},\mathbf{x}'} = \mathscr{I}$ then
- $\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') \sim \mathscr{U}(\mathscr{I}^n)$ and $\Pr(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/|\mathscr{I}|^n$

$$Pr(\mathscr{I}_{\mathbf{x},\mathbf{x}'} = \mathscr{I}) \leq \mathsf{Coll}(\chi \bmod \mathscr{I})$$

Counting approach

- Because if $\langle x_0 - x'_0, \ldots, x_{d-1} - x'_{d-1} \rangle = \mathcal{I}_{\mathbf{x},\mathbf{x}'} = \mathcal{I}$ then
- $\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') \sim \mathcal{U}(\mathcal{I}^n)$ and $\Pr(\mathbf{A} \cdot (\mathbf{x} - \mathbf{x}') = 0) = 1/|\mathcal{I}|^n$

$$Pr(\mathcal{I}_{\mathbf{x},\mathbf{x}'} = \mathcal{I}) \leq \mathrm{Coll}(\chi \bmod \mathcal{I})$$

Note: for the counting approach $\mathbf{A}$ has to be uniformly random

With leakage

[JLWG25]

$$\widetilde{\mathsf{Coll}}(\chi \mid f(\chi)) = \mathbb{E}_{\mathbf{y} \leftarrow f(\chi)} \Pr_{\mathbf{x},\mathbf{x}'}(\mathbf{x} = \mathbf{x}' \mid f(\mathbf{x}) = f(\mathbf{x}') = \mathbf{y})$$

$$\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q, f(\mathbf{x})), (\mathbf{A}, \mathcal{U}(\mathscr{R}_q^n), f(\mathbf{x}))) \leq \frac{1}{2}\sqrt{\Sigma_{\mathscr{I} \in \mathbf{I}} N(\mathscr{I}) \cdot \widetilde{\mathsf{Coll}}(\chi \bmod \mathscr{I} \mid f(\chi)) - 1}$$

Corollaries

$$\mathsf{SD} \leq \frac{1}{2}\sqrt{\Sigma_{\mathscr{J}\in\mathbf{I}} N(\mathscr{J})^n \cdot \mathsf{Coll}(\chi \bmod \mathscr{J}) - 1}$$

Corollaries

$$\mathsf{SD} \leq \frac{1}{2}\sqrt{\Sigma_{\mathscr{I}\in\mathbf{I}} N(\mathscr{I})^n \cdot \mathsf{Coll}(\chi \bmod \mathscr{I}) - 1}$$

$$\mathbf{x} \leftarrow \mathscr{U}(\{-\eta, \ldots, \eta\}^{md})$$

$$\mathsf{SD} \leq \frac{1}{2}\sqrt{\left(\left(\frac{q^n}{(2\eta+1)^m}\right)^{\delta} + 1\right)^{f} - 1}$$

$$\mathbf{x} \leftarrow \mathscr{D}_{\mathscr{R}^m,\sigma}$$

$$\mathsf{SD} \leq \frac{1}{\sqrt{2}}\sqrt{\left(\left(\frac{q^n}{\sigma^m}\right)^{\delta} + 1\right)^{f} - 1}$$

Corollaries

$$\mathsf{SD} \leq \frac{1}{2}\sqrt{\Sigma_{\mathscr{I}\in\mathbf{I}} N(\mathscr{I})^n \cdot \mathsf{Coll}(\chi \bmod \mathscr{I}) - 1}$$

$$\mathsf{SD} \leq \frac{1}{2}\sqrt{|\mathscr{R}_q|^n \cdot \mathsf{Coll}(\chi)}$$

$$\mathsf{SD} \leq \frac{1}{2}\sqrt{\left(\left(\frac{q^n}{(2\eta+1)^m}\right)^{\delta} + 1\right)^{f} - 1}$$

$$\mathsf{SD} \leq \frac{1}{\sqrt{2}}\sqrt{\left(\left(\frac{q^n}{\sigma^m}\right)^{\delta} + 1\right)^{f} - 1}$$

short distributions in low-splitting rings

Corollaries

$$\mathsf{SD} \le \frac{1}{2}\sqrt{\Sigma_{\mathscr{I}\in\mathbf{I}} N(\mathscr{I})^n \cdot \mathsf{Coll}(\chi \bmod \mathscr{I}) - 1}$$

$$\mathsf{SD} \le \frac{1}{2}\sqrt{|\mathscr{R}_q|^n \cdot \mathsf{Coll}(\chi)}$$

$$\mathsf{SD} \le \frac{1}{2}\sqrt{|\mathscr{R}_q|^n \cdot B^m \cdot (1 + 2fq^{-\delta n})}$$

$$\mathsf{SD} \le \frac{1}{2}\sqrt{\left(\left(\frac{q^n}{(2\eta+1)^m}\right)^{\delta} + 1\right)^{f} - 1}$$

$$\mathsf{SD} \le \frac{1}{\sqrt{2}}\sqrt{\left(\left(\frac{q^n}{\sigma^m}\right)^{\delta} + 1\right)^{f} - 1}$$

short distributions in low-splitting rings

well-spreadness, $B \ge 1/q^{\delta}$

Distributions we cover

- Bounded uniform
- Discrete Gaussian
- Centred Binomial
- Biased ternary
- Ternary with bounded Hamming weight

Distributions we cover

- Bounded uniform
- Discrete Gaussian
- Centred Binomial
- Biased ternary
- Ternary with bounded Hamming weight

} via well-spreadness

Distributions we cover

- Bounded uniform
- Discrete Gaussian
- Centred Binomial
- Biased ternary
- Ternary with bounded Hamming weight

} via well-spreadness

Open question: tailored leakage analysis

Smoothing Approach

Smoothing approach

[SS11],[LPR13],[RSW18], etc.

If $\sigma > \eta_\varepsilon(\Lambda_q^\perp(\mathbf{A}))$ and $\mathsf{im}(\mathbf{A}) = \mathscr{R}_q^n$ with probability $\geq 1 - \delta$ for random $\mathbf{A}$

Then $\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathscr{D}_{\mathscr{R}^m,\sigma} \bmod q), (\mathbf{A}, \mathscr{U}(\mathscr{R}_q^n))) \leq \dfrac{\varepsilon}{1-\varepsilon} + \delta$

Smoothing approach

If $\sigma > \eta_\varepsilon(\Lambda_q^\perp(\mathbf{A}))$ and $\mathsf{im}(\mathbf{A}) = \mathscr{R}_q^n$ with probability $\geq 1 - \delta$ for random $\mathbf{A}$

Then $\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathscr{D}_{\mathscr{R}^m,\sigma} \bmod q), (\mathbf{A}, \mathscr{U}(\mathscr{R}_q^n))) \leq \dfrac{\varepsilon}{1-\varepsilon} + \delta$

Note: can consider distributions $\mathbf{A} \leftarrow \mathscr{U}(\mathscr{R}_q^\times)^{n \times m}$, $\mathbf{A} = [\mathbf{I} \mid \mathscr{U}(\mathscr{R}_q^{n \times (m-n)})]$

Approximate leakage via Hint-MLWE

$$\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q, \mathbf{E} \cdot \mathbf{x} + \mathbf{y}), (\mathbf{A}, \mathcal{U}(\mathcal{R}_q^n), \mathbf{E} \cdot \mathbf{x} + \mathbf{y})) \leq ?$$

Approximate leakage via Hint-MLWE

[KLSS23]

$$D_1 = \left\{ (\mathbf{x}, \mathbf{z}) \,|\, \mathbf{x} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \sigma_\mathbf{x}}, \mathbf{y} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \sigma_\mathbf{y}}, \mathbf{z} = \mathbf{E} \cdot \mathbf{x} + \mathbf{y} \right\}$$

$$D_2 = \left\{ (\hat{\mathbf{x}}, \mathbf{z}) \mid \mathbf{x} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \sigma_\mathbf{x}}, \mathbf{y} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \sigma_\mathbf{y}}, \mathbf{z} = \mathbf{E} \cdot \mathbf{x} + \mathbf{y} \right\}$$

and $\hat{\mathbf{x}} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \sqrt{\mathbf{\Sigma}}, \mathbf{c}}$, $\quad \mathbf{\Sigma} = \left(\frac{1}{\sigma_\mathbf{x}^2} \mathbf{I} + \frac{1}{\sigma_\mathbf{y}^2} \cdot \mathbf{E}^T \mathbf{E} \right)^{-1}, \quad \mathbf{c} = \mathbf{\Sigma} \cdot \frac{1}{\sigma_\mathbf{y}^2} \mathbf{E}^T \mathbf{z}$

Exact leakage via lattice analysis

[SSEKYZ24]

$$\mathrm{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q, \mathbf{E} \cdot \mathbf{x}), (\mathbf{A}, \mathscr{U}(\mathscr{R}_q^n), \mathbf{E} \cdot \mathbf{x})) \leq ?$$

Exact leakage via lattice analysis

$\mathrm{SD}((\mathbf{A}, \mathbf{A} \cdot \mathbf{x} \bmod q, \mathbf{E} \cdot \mathbf{x}), (\mathbf{A}, \mathcal{U}(\mathcal{R}_q^n), \mathbf{E} \cdot \mathbf{x})) \leq ?$

Analyse $\eta_\varepsilon(\Lambda_q^\perp(\mathbf{A}) \cap \Lambda^\perp(\mathbf{E}))$ and probability of $\mathbf{A} \cdot \Lambda^\perp(\mathbf{E}) = \mathcal{R}_q^n$

We give a result for $s_{\max}(\mathbf{E}) < B, \quad \mathbf{E} = [\mathbf{I} \mid \bar{\mathbf{E}}]$

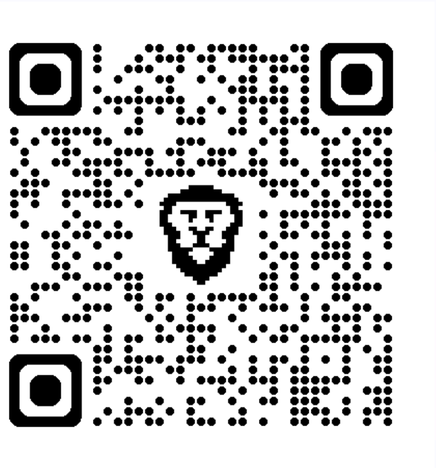
Open questions

- Link between counting and smoothing
- Tailored leakage for non-Gaussian distributions
- Extending matrix and vector distributions
- Improving the study of distributions modulo ideals

Summary

“Leftover Hash Lemma(s) Over Cyclotomic Rings” | ia.cr/2025/1080

- General theorems for Counting and Smoothing
- Corollaries for different algebraic settings
- Concrete instantiations for selection of distributions
- Two leakage families (for Gaussian vectors)



Summary

“Leftover Hash Lemma(s) Over Cyclotomic Rings” | ia.cr/2025/1080

- General theorems for Counting and Smoothing
- Corollaries for different algebraic settings
- Concrete instantiations for selection of distributions
- Two leakage families (for Gaussian vectors)

Thank you!

Sasha Lapiha, Silence Laboratories @ Eurocrypt 2026

References

[HILL99] - Johan Hastad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. SIAM Journal on Computing 1999.

[LW20] - Feng-Hao Liu and Zhedong Wang. Rounding in the rings. CRYPTO 2020.

[JLWG25] - Haoxiang Jin, Feng-Hao Liu, Zhedong Wang, and Dawu Gu. Discrete gaussians modulo sub-lattices: New leftover hash lemmas for discrete gaussians, PKC 2025.

[AABKT24] - Marius A. Aardal, Diego F. Aranha, Katharina Boudgoust, Sebastian Kolby, and Akira Takahashi. Aggregating Falcon signatures with LaBRADOR, CRYPTO 2024.

References

[SS11] - Damien Stehle and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices, EUROCRYPT 2011.

[KLSS23] - Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE. Duhyeong Kim, Dongwon Lee, Jinyeong Seo, and Yongsoo Song, CRYPTO 2023.

[SSEKYZ24] - Ron Steinfeld, Amin Sakzad, Muhammed F. Esgin, Veronika Kuchta, Mert Yassi, and Raymond K. Zhao. LUNA: Quasi-optimally succinct designated-verifier zero-knowledge arguments from lattices, CCS 2024

Well-spreadness

[AABKT24]

CRT decomposition $\mathscr{R}_q = \mathscr{R} \bmod q \sim \prod \mathbf{Z}_q[X]/\Phi_i(X)$

Let $B > 0$ and distribution χ over $\mathscr{R}_q$ such that

$$\max_{i \in [1,f], y \in \mathscr{R}_q} (x \bmod \Phi_i(X) = y \mid x \leftarrow \chi) \leq B$$

Well-spreadness

CRT decomposition $\mathscr{R}_q = \mathscr{R} \bmod q \sim \prod \mathbf{Z}_q[X]/\Phi_i(X)$

Let $B > 0$ and distribution χ over $\mathscr{R}_q$ such that

$$\max_{i \in [1,f], y \in \mathscr{R}_q} (x \bmod \Phi_i(X) = y \mid x \leftarrow \chi) \leq B$$

Then $\mathsf{Coll}(\chi^m \bmod \mathscr{I}) \leq \mathsf{Coll}(\chi^m \bmod \Phi_i(X)) \leq B^m$