QUANTUM OBLIVIOUS LWE SAMPLING AND INSECURITY OF STANDARD MODEL LATTICE-BASED SNARKS

NOVEL LATTICE ASSUMPTIONS '26

Thomas Debris-Alazard, Pouria Fallahpour and Damien Stehlé

July 17, 2026

Inria, École Polytechnique

Funded by the European Union

European Research Council
Established by the European Commission

THE LEARNING WITH ERRORS PROBLEM

A mod-q linear system "with errors" to solve

LWE(m, n, q, σ): Learning With Errors

- **Input**: $(\mathbf{A}, \mathbf{As} + \mathbf{e})$ where,

$$\mathbf{A} \xleftarrow{unif} (\mathbb{Z}/q\mathbb{Z})^{m \times n}, \quad \mathbf{s} \xleftarrow{unif} (\mathbb{Z}/q\mathbb{Z})^{n} \quad \text{and} \quad \mathbf{e} \longleftarrow \mathcal{D} \quad \text{s.t. } |e_i| \approx \sigma$$

- **Output**: $\mathbf{s}$

$\longrightarrow$ Distribution $\mathcal{D}$ ensures small coefficients for $\mathbf{e}$

Parameters m, n, q, σ are chosen to ensure unicity of the solution $\mathbf{s}$

$(\mathbf{s}, \mathbf{e}) \mapsto \mathbf{As} + \mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$ is sparse in its range

LWE AND VARIATIONS FOR CRYPTOGRAPHY

Variants of the LWE*-hardness have been introduced*

to design some advanced cryptographic primitives

LWE AND VARIATIONS FOR CRYPTOGRAPHY

Variants of the LWE*-hardness have been introduced*

to design some advanced cryptographic primitives

Assumption: Efficient Oblivious LWE-Sampling is Impossible

Every algorithm generating LWE samples $\left(\mathbf{A}, \mathbf{b} \stackrel{\text{def}}{=} \mathbf{A}\mathbf{s} + \mathbf{e}\right)$

knows the underlying secret $\mathbf{s}$

- Assumption used [GMNO18, NYI+20, ISW21, SSEK22, CKKK23, GNSV23] to ensure security of lattice SNARKs $\left(\text{Succinct Non-interactive Arguments of Knowledge}\right)$

BUT WHY?

- It seems hard: sample $\mathbf{b} \leftarrow (\mathbb{Z}/q\mathbb{Z})^{m \times n}$ won't give $\mathbf{As} + \mathbf{e}$ with $\mathbf{e}$ short $\Big($sparse in its range$\Big)$

- Useful for security reductions

  (i) suppose access to a decryption oracle

  (ii) any adversary asking decryption of a well formed encryption $\mathbf{As} + \mathbf{e}$ won't learn more that it already knows $\Big($to form the encryption it necessarily knows $\mathbf{s}\Big)$

OUR RESULT

An Oblivious Sampler for LWE:

A quantum algorithm generating LWE samples $\left(\mathbf{A}, \mathbf{b} \stackrel{\text{def}}{=} \mathbf{As} + \mathbf{e}\right)$ without knowing $\mathbf{s}$

$\longrightarrow$ The only way to extract $\mathbf{s}$ from the sampler is to solve the LWE-problem $(\mathbf{A}, \mathbf{As} + \mathbf{e})$

- Our quantum oblivious sampler takes advantage of:
  - complex phases in quantum computation
  - an optimal unambiguous quantum measurement
- First application: it invalidates security proofs of some lattice-based SNARK but does not break them

ROADMAP

1. Basics on Quantum Computing
2. A Fundamental Quantum State to Build
3. How to Build this Quantum State
4. Quantum Oblivious LWE Sampler

BASICS ON QUANTUM COMPUTING

CLASSICAL BITS VERSUS QUANTUM BITS

Classical bits	Quantum bits
$(\mathbb{Z}/q\mathbb{Z})^n$	$\left(\mathcal{H}, \|\cdot\|_2\right)$ Hilbert space
$(b_1, \ldots, b_n) \in (\mathbb{Z}/q\mathbb{Z})^n$	$\sum_{(b_1,\ldots,b_n)\in(\mathbb{Z}/q\mathbb{Z})^n} \lambda_{(b_1,\ldots,b_n)} \|b_1, \ldots, b_n\rangle \in \mathcal{H}$ where $\sum_{(b_1,\ldots,b_n)} \|\lambda_{(b_1,\ldots,b_n)}\|^2 = 1$ and the $\|b_1, \ldots, b_n\rangle \in \mathcal{H}$ being orthonormal

For us the result of a computation will always be integers **mod** q *...*

Could we extract integers **mod** q from quantum states?

MEASUREMENT: FROM A QUANTUM STATE TO CLASSICAL INFORMATION

Measurement in the computational basis:

$$\sum_{(b_1,\ldots,b_n)} \lambda_{(b_1,\ldots,b_n)} |b_1,\ldots,b_n\rangle \xrightarrow{measure} (b_1,\ldots,b_n) \text{ with probability } \left|\lambda_{(b_1,\ldots,b_n)}\right|^2$$

- If you know classically how to sample $\mathbf{x}$ according to $|f|^2$, then you can build

$$\sum_{\mathbf{x}} f(\mathbf{x}) \, |\mathbf{x}\rangle$$

- If you know classically to compute $\mathbf{x} \mapsto g(\mathbf{x})$, then you can perform the operation

$$\sum_{\mathbf{x},\mathbf{y}} \lambda_{\mathbf{x},\mathbf{y}} \, |\mathbf{x}\rangle \, |\mathbf{y}\rangle \longrightarrow \sum_{\mathbf{x},\mathbf{y}} \lambda_{\mathbf{x},\mathbf{y}} \, |\mathbf{x}\rangle \, |\mathbf{y} + g(\mathbf{x})\rangle$$

A FUNDAMENTAL TOOL: QUANTUM FOURIER TRANSFORM

One of the most useful tool in quantum computing: **QFT**

Classical and Quantum Fourier transforms over $(\mathbb{Z}/q\mathbb{Z})^n$

Classical Fourier Transform	Quantum Fourier Transform: QFT
$f = (f(\mathsf{x}))_{\mathsf{x}\in(\mathbb{Z}/q\mathbb{Z})^n}$	$\lvert\psi_f\rangle = \sum_{\mathsf{x}\in(\mathbb{Z}/q\mathbb{Z})^n} f(\mathsf{x})\,\lvert\mathsf{x}\rangle$ $(\lVert f\rVert_2 = 1)$
$\widehat{f}(\mathsf{x}) = \frac{1}{\sqrt{q^n}} \sum_{\mathsf{y}\in(\mathbb{Z}/q\mathbb{Z})^n} f(\mathsf{y}) e^{2i\pi\langle \mathsf{x},\mathsf{y}\rangle/q}$	$\mathbf{QFT}\,\lvert\psi\rangle \stackrel{\text{def}}{=} \lvert\widehat{\psi_f}\rangle = \sum_{\mathsf{x}\in(\mathbb{Z}/q\mathbb{Z})^n} \widehat{f}(\mathsf{x})\,\lvert\mathsf{x}\rangle$

$\longrightarrow$ In particular: $\forall \mathsf{x} \in (\mathbb{Z}/q\mathbb{Z})^n$, $\mathbf{QFT}\,\lvert\mathsf{x}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathsf{y}\in\mathbb{F}_q^n} e^{2i\pi\langle \mathsf{x},\mathsf{y}\rangle/q}\,\lvert\mathsf{y}\rangle$

$\lvert\mathsf{x}\rangle \mapsto \mathbf{QFT}\,\lvert\mathsf{x}\rangle$ is quantum efficiently computable

A FUNDAMENTAL QUANTUM STATE

OBLIVIOUS SAMPLING: THE KEY IDEA

Key Idea:

To achieve oblivious LWE sampling,

$$(i)\ \text{build}\quad \sum_{\mathsf{s},\mathsf{e}} \left(\prod_i \sqrt{\mathsf{Gauss}(\sigma)(e_i)} \right) |\mathsf{As}+\mathsf{e}\rangle \quad \text{and} \quad (ii)\ \text{measure}$$

$$\left(\mathrm{Gauss}(\sigma)(x) \stackrel{\text{def}}{=} \frac{\mathrm{e}^{-\pi x^2/\sigma^2}}{\sigma} \right)$$

A FUNDAMENTAL QUANTUM STATE TO BUILD

$$\textit{Is it hard to build } \sum_{\mathsf{s},\mathsf{e}} \left(\prod_i \sqrt{\mathsf{Gauss}(\sigma)(e_i)} \right) |\mathsf{As} + \mathsf{e}\rangle ?$$

A FUNDAMENTAL QUANTUM STATE TO BUILD

$$\textit{Is it hard to build } \sum_{\mathsf{s},\mathsf{e}} \left(\prod_i \sqrt{\mathsf{Gauss}(\sigma)(e_i)} \right) |\mathsf{As}+\mathsf{e}\rangle ?$$

Yes!

$\longrightarrow$ Building $\sum_{\mathsf{s},\mathsf{e}} \left(\prod_i \sqrt{\mathsf{Gauss}(\sigma)(e_i)} \right) |\mathsf{As}+\mathsf{e}\rangle$ implies the ability to compute

a short vector in a lattice which is a hard problem...

Quantum Regev Reduction in a Nutshell:

(*i*) $\sum_{\mathsf{s},\mathsf{e}} \left(\prod_i \sqrt{\mathsf{Gauss}(\sigma)(e_i)} \right) |\mathsf{As}+\mathsf{e}\rangle \xrightarrow{\text{QFT}} \sum_{\mathsf{x}:\, \mathsf{x}^\top \mathsf{A}=0} \left(\prod_i \sqrt{\mathsf{Gauss}(4/\sigma)(x_i)} \right) |\mathsf{x}\rangle$

(*ii*) Then measuring gives a short $\mathbf{x}_0$ in the lattice $\{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^\top \mathbf{A} = \mathbf{0} \bmod q\}$

NOT A DEAD-END

Fundamental Remark: Adding Phases

Considering $\sum_{\mathbf{s},\mathbf{e}} \lambda_{\mathbf{s},\mathbf{e}} \left(\prod_i \sqrt{\text{Gauss}(\sigma)(e_i)} \right) |\mathbf{As}+\mathbf{e}\rangle$ where $\lambda_{\mathbf{s},\mathbf{e}} \in \mathbb{C}$ and $|\lambda_{\mathbf{s},\mathbf{e}}| = 1$

- Measuring with phases still gives a quantum oblivious LWE sampler
- Measuring after applying QFT does not necessarily give a short lattice vector

$$\text{QFT}\left(\sum_{\mathbf{s},\mathbf{e}} \lambda_{\mathbf{s},\mathbf{e}} \left(\prod_i \sqrt{\text{Gauss}(\sigma)(e_i)} \right) |\mathbf{As}+\mathbf{e}\rangle \right) \neq \sum_{\mathbf{x}:\mathbf{x}^\top \mathbf{A}=\mathbf{0}} \prod_i \sqrt{\text{Gauss}(4/\sigma)(x_i)}\, |\mathbf{x}\rangle$$

How to build the fundamental quantum state

Naive Approach to Build $\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{As}+\mathbf{e}\rangle$**:**

- Build,

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}\rangle\,|\mathbf{e}\rangle \quad \left(f \text{ is efficiently computable} \right)$$

- Multiplication by $\mathbf{A}$ and add to the second register,

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}\rangle\,|\mathbf{As}+\mathbf{e}\rangle$$

- Disentangle by applying an LWE-solver, *i.e.*, $\mathcal{A}\,(\mathbf{As}+\mathbf{e}) \mapsto \mathbf{s}$,

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}-\mathcal{A}\,(\mathbf{As}+\mathbf{e})\rangle\,|\mathbf{As}+\mathbf{e}\rangle = \sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |0\rangle\,|\mathbf{As}+\mathbf{e}\rangle$$

$\longrightarrow$ Not efficient: it relies on an LWE-solver

VIA AN LWE-SOLVER

Naive Approach to Build $\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$**:**

- Build,

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}\rangle\,|\mathbf{e}\rangle \quad \left(f \text{ is efficiently computable}\right)$$

- Multiplication by $\mathbf{A}$ and add to the second register,

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}\rangle\,|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

- Disentangle by applying an LWE-solver, *i.e.*, $\mathcal{A}(\mathbf{A}\mathbf{s}+\mathbf{e}) \mapsto \mathbf{s}$,

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}-\mathcal{A}(\mathbf{A}\mathbf{s}+\mathbf{e})\rangle\,|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle = \sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |0\rangle\,|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$$

$\longrightarrow$ Not efficient: it relies on an LWE-solver

- $$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i \sqrt{\mathrm{Gauss}(\sigma)(e_i)} \right) |\mathbf{A}\mathbf{s}+\mathbf{e}\rangle \xrightarrow{\text{QFT}} \sum_{\mathbf{x}:\ \mathbf{x}^\top\mathbf{A}=0} \left(\prod_i \sqrt{\mathrm{Gauss}(4/\sigma)(x_i)} \right) |\mathbf{x}\rangle$$

PREVIOUS WORK: [CLZ22]

[CLZ22][1] proposed a new approach to build

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{A}\mathbf{s} + \mathbf{e}\rangle$$

$\longrightarrow$ Unambiguous measurement to disentangle $\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}\rangle\, |\mathbf{A}\mathbf{s} + \mathbf{e}\rangle$

[1] Yilei Chen, Qipeng Liu, and Mark Zhandry. *Quantum algorithms for variants of average-case lattice problems via filtering*. In EUROCRYPT, 2022.

A Game From Quantum Information Theory:

- **Input**: a random quantum state $|\psi_i\rangle$ from a set of known state $\left\{ |\psi_1\rangle, \ldots, |\psi_N\rangle \right\}$
- **Output**: i, *i.e.*, which state has been chosen

- If the $|\psi\rangle_i$'s are orthogonal: we can perfectly distinguish them: it corresponds to to a classical source $\Big($distinguishing sequences of bits$\Big)$
- If the $|\psi\rangle_i$'s are not orthogonal: we cannot perfectly distinguish them. However we can unambiguously distinguish them

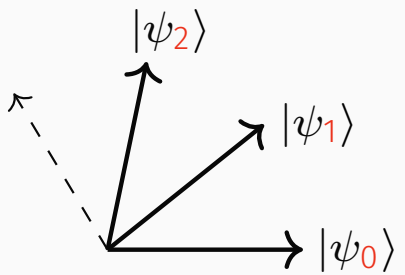
$$|\psi_i\rangle \xrightarrow{measure} \begin{cases} i: \text{ success} \\ \perp: \text{ failure} \end{cases}$$

Previous work: [CLZ22] and unambiguous measurement

Given $\mathbf{A} = (\mathbf{a}_1| \cdots |\mathbf{a}_m)^\top$ and denoting $\mathbf{x} \cdot \mathbf{y} \stackrel{\text{def}}{=} \sum_i x_i y_i \in \mathbb{Z}/q\mathbb{Z}$

$$\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i f(e_i) \right) |\mathbf{s}\rangle |\mathbf{A}\mathbf{s} + \mathbf{e}\rangle = \sum_{\mathbf{s}} |\mathbf{s}\rangle \bigotimes_i \Big(\underbrace{\sum_{e_i} f(e_i) |\mathbf{a}_i \cdot \mathbf{s} + e_i\rangle}_{\stackrel{\text{def}}{=} |\psi_{\mathbf{a}_i \cdot \mathbf{s}}\rangle} \Big)$$

$$\forall j \in \mathbb{Z}/q\mathbb{Z}, \quad |\psi_j\rangle \stackrel{\text{def}}{=} \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f(e) |j + e\rangle$$



Key-Idea: Quantum Unambiguous Measure

$$|\psi_{\mathbf{a}_i \cdot \mathbf{s}}\rangle \xrightarrow[\text{measure}]{\text{unambiguous}} \begin{cases} \mathbf{a}_i \cdot \mathbf{s} & \text{with probability } p \\ \perp & \text{with probability } 1 - p \end{cases}$$

Using a quantum unambiguous measure reduces to solve a linear system with erasure

QUANTUM OBLIVIOUS LWE SAMPLER

AN OPTIMAL QUANTUM UNAMBIGUOUS MEASUREMENT

$$\sum_{\mathbf{s}} |\mathbf{s}\rangle \left(\sum_{e_1} f(e_1) \, |\mathbf{a}_1 \cdot \mathbf{s} + e_1\rangle \right) \otimes \cdots \otimes \left(\sum_{e_m} f(e_m) \, |\mathbf{a}_m \cdot \mathbf{s} + e_m\rangle \right)$$

$$\downarrow \qquad\qquad\qquad\qquad\qquad\qquad \downarrow$$

$$\perp \qquad\qquad\qquad\qquad\qquad\qquad \mathbf{a}_m \cdot \mathbf{s}$$

We succeed to recover $\mathbf{a}_i \cdot \mathbf{s}$ with probability p

We are successful on $\approx pm$ coordinates: it is necessary that $pm \geq n$ to recover $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$

- In [CLZ22]: $p^{\mathrm{CLZ}} = \frac{\min_x |\widehat{f}(x)|^2}{q}$
- Optimal unambiguous measurement [CB98][2]: $p^{\mathrm{CB}} = q \cdot \min_x |\widehat{f}(x)|^2$

[2] Anthony Chefles and Stephen M. Barnett. *Optimum unambiguous discrimination between linearly independent symmetric states.* Phys. Lett. A, 1998.

ADD PHASES

Our quantum algorithm uses m registers with $m = \frac{n}{p^{\mathrm{CB}}} = \frac{n}{q \cdot \min_x |\widehat{f}(x)|^2}$

Issue:

$$\text{If } f = \sqrt{\mathrm{Gauss}(q, \sigma)}, \quad \text{then} \quad \widehat{f} = \mathrm{Gauss}(2/\sigma)$$

$$m = \frac{n}{q \cdot \min_x |\widehat{f}(x)|^2} = \mathrm{e}^{\Omega(n)}$$

Key-Idea: Use Phases

$$f(x) = \begin{cases} \sqrt{\mathrm{Gauss}(\sigma)(x)} & \text{if } x > 0 \\ (-1) \cdot \sqrt{\mathrm{Gauss}(\sigma)(x)} & \text{otherwise} \end{cases}$$

Then,

$$m = \frac{n}{q \cdot \min_x |\widehat{f}(x)|^2} \leq \frac{n}{\mathrm{Gauss}(\sigma)(0)} \approx n \cdot \sigma$$

$\Big($with measurement from [CLZ22]: $m = q^2 \cdot n \cdot \sigma = \mathrm{e}^{\Omega(n)}$ when $q = \mathrm{e}^{\Omega(n)}\Big)$

SUMMARY

Theorem:

Parameters m, n, q, σ are functions of λ and they satisfy,

$$q \text{ prime}, \quad m, \log q \leq \text{poly}(\lambda), \quad m \geq n\sigma \cdot \omega(\log \lambda) \quad \text{and} \quad 2 \leq \sigma \leq \frac{q}{\sqrt{8m \ln q}} .$$

Then, there exists a $\text{poly}(\lambda)$-time quantum oblivious $\text{LWE}(m, n, q, \sigma)$ instance sampler, under the assumption that $\text{LWE}(m, n, q, \sigma)$ is hard.

$\longrightarrow$ To reach other parametrizations (σ larger, q not prime, etc. . .)

we use reductions (modulus switching, noise flooding) conserving obliviousness

ANOTHER QUANTUM OBLIVIOUS SAMPLER

The following sampler has been proposed by an anonymous reviewer at *QIP* '25

1. Generate
$$\sum_{\mathbf{x}} \left(\prod_i \sqrt{\mathrm{Gauss}(4/\sigma)(x_i)} \right) |\mathbf{x}\rangle \left| \mathbf{x}^\top \mathbf{A} \right\rangle$$
2. Measure the second register: we observe $\mathbf{x}_0^\top \mathbf{A}$ and the quantum state collapses to:
$$\sum_{\mathbf{x}:\ \mathbf{x}^\top \mathbf{A} = \mathbf{0}} \left(\prod_i \sqrt{\mathrm{Gauss}(4/\sigma)(x_i)} \right) |\mathbf{x} + \mathbf{x}_0\rangle \left| \mathbf{x}_0^\top \mathbf{A} \right\rangle$$
3. Applying the **QFT** leads to $\big($same computation as Regev's reduction + translation becomes phase after Fourier$\big)$:
$$\sum_{\mathbf{s},\mathbf{e}} \omega_q^{\mathbf{x}_0 \cdot (\mathbf{A}\mathbf{s}+\mathbf{e})} \left(\prod_i \sqrt{\mathrm{Gauss}(\sigma)(e_i)} \right) |\mathbf{A}\mathbf{s} + \mathbf{e}\rangle \left| \mathbf{x}_0^\top \mathbf{A} \right\rangle$$

CONCLUSION

Our result: a quantum algorithm which **obliviously** samples $\Big($given $\mathbf{A}\Big)$,

$$\mathbf{As} + \mathbf{e} \quad \text{with} \quad \mathbf{s} \xleftarrow{unif} (\mathbb{Z}/q\mathbb{Z})^n \quad \text{and} \quad \mathbf{e} \leftarrow \text{Gauss}(\sigma)^{\otimes m}$$

What we did not discuss:

- Definition of classical and quantum oblivious sampling
- How to efficiently run the unambiguous measurement from [CB98]
- Why does it invalidate the security proofs of some SNARKs

Future Work:

Is this oblivious LWE-sampler can be used to design advanced quantum protocols?


Anthony Chefles and Stephen M. Barnett.

Optimum unambiguous discrimination between linearly independent symmetric states.

Phys. Lett. A, 1998.


Heewon Chung, Dongwoo Kim, Jeong Han Kim, and Jiseung Kim.

Amortized efficient zk-SNARK from linear-only RLWE encodings.

J. Comm. Netw., 2023.


Yilei Chen, Qipeng Liu, and Mark Zhandry.

Quantum algorithms for variants of average-case lattice problems via filtering.

In *EUROCRYPT*, 2022.


Rosario Gennaro, Michele Minelli, Anca Nitulescu, and Michele Orrù.

Lattice-based ZK-SNARKs from square span programs.

In *CCS*, 2018.


Chaya Ganesh, Anca Nitulescu, and Eduardo Soria-Vazquez.

Rinocchio: SNARKs for ring arithmetic.

J. Cryptol., 2023.


Yuval Ishai, Hang Su, and David J. Wu.

Shorter and faster post-quantum designated-verifier zkSNARKs from lattices.

In *CCS*, 2021.

Ken Naganuma, Masayuki Yoshino, Atsuo Inoue, Yukinori Matsuoka, Mineaki Okazaki, and Noboru Kunihiro.

Post-quantum zk-SNARK for arithmetic circuits using QAPs.

In *AsiaJCIS*, 2020.

Ron Steinfeld, Amin Sakzad, Muhammed F. Esgin, and Veronika Kuchta.

Private re-randomization for module LWE and applications to quasi-optimal ZK-SNARKs, 2022.

Available at `https://eprint.iacr.org/2022/1690`.