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

STOC '24

Thomas Debris-Alazard, Pouria Fallahpour and Damien Stehlé

June 25, 2024

Inria, École Polytechnique

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

LWE(m, n, q, σ): Learning With Errors

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

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

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

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

LWE *is conjectured as being hard on average*

even in the quantum computational model

LWE Source of Hardness:

- enjoys self-reducibility (as hard as its worst-case variant)
- no easier than computing short vector in a lattice (Regev quantum reduction)

LWE hardness ensures the security of some:

- Encryption schemes,
- Fully Homomorphic Encryption schemes

$\longrightarrow$ LWE *is a very versatile problem to design cryptographic primitives*

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 some lattice SNARK (Succinct Non-interactive Arguments of Knowledge)

OUR RESULT

An Oblivious Sampler for LWE:

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

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

- 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. A Fundamental Quantum State to Build
2. Quantum Unambiguous Measurement
3. Quantum Oblivious LWE Sampler

A FUNDAMENTAL QUANTUM STATE

$$\mathbf{e} \leftarrow \mathrm{Gauss}(\sigma)^{\otimes m}\text{: the } e_i \text{ are i.i.d and } \mathbb{P}(e_i = x) = \mathrm{Gauss}(\sigma)(x) = \frac{e^{-\pi x^2/\sigma^2}}{\sigma}$$

$$\left(\text{ up to normalization mod } q\right)$$

LWE(m, n, q, σ): Learning With Errors

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

$$\mathbf{A} \xleftarrow{unif} (\mathbb{Z}/q\mathbb{Z})^{m \times n}, \quad \mathbf{s} \xleftarrow{unif} (\mathbb{Z}/q\mathbb{Z})^{n} \quad \text{and} \quad \mathbf{e} \longleftarrow \mathrm{Gauss}(\sigma)^{\otimes m}$$

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

Key Idea:

To achieve oblivious LWE sampling,

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

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

Quantum Regev Reduction in a Nutshell:

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

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

$\longrightarrow$ Building $\sum_{\mathbf{s},\mathbf{e}} \left(\prod_i \sqrt{\mathrm{Gauss}(\sigma)(e_i)} \right) |\mathbf{As}+\mathbf{e}\rangle$ implies the ability to compute a short vector in a lattice **which is a hard problem. . .**

Fundamental Remark: Adding Phases

Considering $\sum_{\mathbf{s},\mathbf{e}} \lambda_{\mathbf{s},\mathbf{e}} \left(\prod_i \sqrt{\mathrm{Gauss}(\sigma)(e_i)} \right) |\mathbf{A}\mathbf{s} + \mathbf{e}\rangle$ 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

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

QUANTUM UNAMBIGUOUS MEASUREMENT

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.*, $\mathcal{A}\left(\mathbf{A}\mathbf{s}+\mathbf{e}\right) \mapsto \mathbf{s}$,

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

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

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

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

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

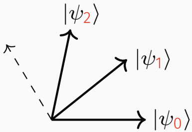
(1) Yilei Chen, Qipeng Liu, and Mark Zhandry. *Quantum algorithms for variants of average-case lattice problems via filtering*. In EUROCRYPT, 2022.

PREVIOUS WORK: [CLZ22] AND UNAMBIGUOUS MEASUREMENT

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

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

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



Key-Idea: Quantum Unambiguous Measure

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

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

QUANTUM OBLIVIOUS LWE SAMPLER

AN OPTIMAL QUANTUM UNAMBIGUOUS MEASUREMENT

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

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

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

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,

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

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

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

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

CONCLUSION

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

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

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`.