An Update on Lattice Cryptanalysis Vol. 1

The Dual Attack on LWE

Martin R. Albrecht

RWPQC

King's College London & SandboxAQ

Kyber

WIKIPEDIA
The Free Encyclopedia

Kyber

2 languages

Article Talk Tools

From Wikipedia, the free encyclopedia

For the fictional crystals, see Lightsaber. For the computing I/O scheduler, see I/O scheduling. For other uses, see Khyber (disambiguation).

Kyber is a key encapsulation mechanism (KEM) designed to be resistant to cryptanalytic attacks with future powerful quantum computers. It is used to establish a shared secret between two communicating parties without an (IND-CCA2) attacker in the transmission system being able to decrypt it. This asymmetric cryptosystem uses a variant of the learning with errors lattice problem as its basic trapdoor function. It won the NIST competition for the first post-quantum cryptography (PQ) standard.[1] NIST calls its draft standard **Module-Lattice-Based Key-Encapsulation Mechanism** (**ML-KEM**).[2]

Properties [edit]

The system is based on the module learning with errors (M-LWE) problem, in conjunction with cyclotomic rings.[3] Recently, there has also been a tight formal mathematical security reduction of the ring-LWE problem to MLWE.[4][5] Compared to competing PQ methods, it has typical advantages of lattice-based methods, e.g. in regard to runtime as well as the size of the ciphertexts and the key material.[6]

The reason you cannot find information about lightsaber crystals any longer ...

Learning with Errors

Given $(\mathbf{A}, \mathbf{c}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$, find $\mathbf{s} \in \mathbb{Z}^n$ when

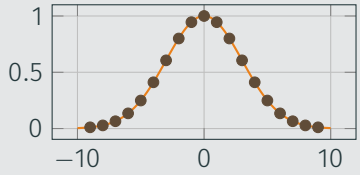
$$\begin{pmatrix} \\ \mathbf{c} \\ \\ \end{pmatrix} \equiv \begin{pmatrix} \leftarrow & n & \rightarrow \\ & \mathbf{A} & \end{pmatrix} \cdot \begin{pmatrix} \\ \mathbf{s} \\ \\ \end{pmatrix} + \begin{pmatrix} \\ \mathbf{e} \\ \\ \end{pmatrix} \bmod q$$

for $\mathbf{e} \in \mathbb{Z}^m$ with small entries.

Example

$n = 1024, m = 2048, q = 7681, |e_i| \approx 2$

“Small Entries”



No loss in security if secret $\mathbf{s}$ and error $\mathbf{e}$ have same distribution [ACPS09]

We can reformulate $\mathbf{c} - \mathbf{A} \cdot \mathbf{s} \equiv \mathbf{e} \bmod q$ over the Integers as:

$$\begin{pmatrix} q\mathbf{I} & -\mathbf{A} \\ 0 & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} * \\ \mathbf{s} \end{pmatrix} + \begin{pmatrix} \mathbf{c} \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{e} \\ \mathbf{s} \end{pmatrix}$$

Alternatively:

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I} & -\mathbf{A} & \mathbf{c} \\ 0 & \mathbf{I} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{B} \cdot \begin{pmatrix} * \\ \mathbf{s} \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{e} \\ \mathbf{s} \\ 1 \end{pmatrix}$$

A Unique Shortest Vector

There exists an integer-linear combination of the columns of $\mathbf{B}$ that produces a vector with "unusually" small entries

uSVP

Find a unique shortest vector amongst the integer combinations of the columns of:

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I} & -\mathbf{A} & \mathbf{c} \\ 0 & \mathbf{I} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $\mathbf{B} \in \mathbb{Z}^{d \times d}$.

Dual Attack

- Consider $\mathbf{c} \equiv \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \bmod q$ with both $\mathbf{s}$ and $\mathbf{e}$ short or $\mathbf{c}$ uniform.
- Let $\mathbf{u}$ be short such that $\mathbf{v}^T := \mathbf{u}^T \cdot \mathbf{A} \bmod q$ is short.
- Compare:
  - $\mathbf{u}^T \cdot \mathbf{c} \equiv \mathbf{u}^T \cdot \mathbf{A} \cdot \mathbf{s} + \mathbf{u}^T \cdot \mathbf{e} \equiv \mathbf{v}^T \cdot \mathbf{s} + \mathbf{u}^T \cdot \mathbf{e} \Rightarrow$ short-ish
  - $\mathbf{u}^T \cdot \mathbf{c} \Rightarrow$ uniform
- The shorter $(\mathbf{u}, \mathbf{v})$ the fewer $\mathbf{u}^T \cdot \mathbf{c}$ we need
- Note

$$\begin{pmatrix} q\mathbf{I} & \mathbf{A}^T \\ 0 & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} * \\ \mathbf{u} \end{pmatrix} = \begin{pmatrix} \mathbf{v} \\ \mathbf{u} \end{pmatrix}$$

Approx-SVP

Find vectors $(\mathbf{u}_i, \mathbf{v}_i)$ of norm $\|(\mathbf{u}_i, \mathbf{v}_i)\| \leq \beta$ amongst the integer combinations of the columns of $\mathbf{B} \in \mathbb{Z}^{d \times d}$:

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I} & \mathbf{A}^T \\ 0 & \mathbf{I} \end{pmatrix}$$

Can extend this to recover $\mathbf{s}$: guess a component and run the distinguisher

Why we're here I

NIST's ask:

AES 128	2^{170} / MAXDEPTH quantum gates or 2^{143} classical gates[1]

Current estimates:

```
from estimator import *
_ = LWE.estimate(schemes.Kyber512)
```

```
bkw                 :: rop: ≈2^178.8, m: ≈2^166.8, mem: ≈2^167.8, b: 14, t1: 0, t2: 16, ...
usvp                :: rop: ≈2^143.8, red: ≈2^143.8, δ: 1.003941, β: 406, d: 998, tag: usvp
bdd                 :: rop: ≈2^140.3, red: ≈2^139.7, svp: ≈2^138.8, β: 391, η: 421, d: 1013, tag: bdd
dual                :: rop: ≈2^149.9, mem: ≈2^97.1, m: 512, β: 424, d: 1024, ↻: 1, tag: dual
dual_hybrid         :: rop: ≈2^139.2, red: ≈2^139.0, guess: ≈2^136.2, β: 385, p: 6, ζ: 15, ...
```

139.2 < 143

[1] *"In particular, NIST will define a separate category for each of the following security requirements (listed in order of increasing strength): 1) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)"* NIST. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals. Jan. 2017

Why we're here II

Ethical considerations. *Although Picante demonstrates significant progress towards attacking real-world LWE problems with sparse binary secrets, it cannot yet break problems with real-world-size parameters. In particular, the LWE schemes standardized by NIST use smaller modulus q and non-sparse secret distributions. Hence, we do not believe our paper raises any ethical concerns. Nonetheless, we shared a copy of the current paper with the NIST Cryptography group, to inform them of our approach.*

- Cathy Yuanchen Li, Jana Sotáková, Emily Wenger, Mohamed Malhou, Evrard Garcelon, François Charton, and Kristin E. Lauter. SalsaPicante: A Machine Learning Attack on LWE with Binary Secrets. In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023*. Ed. by Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda. ACM, 2023, pp. 2606–2620

Programme

This Talk:

- Higher-level discussion of the “dual attack” which seems to come out on top in security estimates
- Discussion of ML attacks on LWE

John’s Talk:

- Opening the box of the underlying algorithm for finding short vectors (sieving) and its costs

Dual-Sieve Attacks

An Abridged History of ...

- [AR05] use short vectors to distinguish
- [ADPS16] a lattice sieve **yields many short vectors**
- [Alb17] guess **multiple coordinates** of the secret and **reuse reduced bases**
- [GJ21] speed up evaluating distinguisher with a Fast Fourier Transform (FFT)
- [MAT22] improve dual attack with modulus switching technique

... Dual-Sieve Attacks, Reconsidered

- Léo Ducas and Ludo Pulles. **Does the Dual-Sieve Attack on Learning with Errors even Work?** Cryptology ePrint Archive, Report 2023/302. `https://eprint.iacr.org/2023/302`. 2023
- Amaury Pouly and Yixin Shen. **Provable Dual Attacks on Learning with Errors.** Cryptology ePrint Archive, Paper 2023/1508. `https://eprint.iacr.org/2023/1508`. 2023. URL: `https://eprint.iacr.org/2023/1508`
- Léo Ducas and Ludo N. Pulles. **Accurate Score Prediction for Dual-Sieve Attacks.** Cryptology ePrint Archive, Paper 2023/1850. `https://eprint.iacr.org/2023/1850`. 2023. URL: `https://eprint.iacr.org/2023/1850`

Dual-Sieve Attacks

- Consider $\mathbf{c} \equiv \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \bmod q$ with both $\mathbf{s}$ and $\mathbf{e}$ short or $\mathbf{c}$ uniform.
- Write $\mathbf{s} = (\mathbf{s}_\ell, \mathbf{s}_g)$ and $\mathbf{A} = [\mathbf{A}_\ell \mid \mathbf{A}_g]$
- Let $\mathbf{u}_i$ be short such that $\mathbf{v}_i^T := \mathbf{u}_i^T \cdot \mathbf{A}_\ell \bmod q$ is short.
- Pressing the "sieve" button once gives us exponentially many such vectors.
- We have $\mathbf{u}_i^T \cdot \mathbf{c} \equiv \mathbf{u}_i^T \cdot (\mathbf{A}_\ell \cdot \mathbf{s}_\ell + \mathbf{A}_g \cdot \mathbf{s}_g) + \mathbf{u}_i^T \cdot \mathbf{e} \equiv \mathbf{v}_i^T \cdot \mathbf{s}_\ell + \mathbf{u}_i^T \cdot \mathbf{A}_g \cdot \mathbf{s}_g + \mathbf{u}_i^T \cdot \mathbf{e}$
- Let $\tilde{\mathbf{s}}_g$ be a guess for $\mathbf{s}_g$ and consider

$$\mathbf{v}^T \cdot \mathbf{s}_\ell + \mathbf{u}_i^T \cdot \mathbf{A}_g \cdot \mathbf{s}_g - \mathbf{u}_i^T \cdot \mathbf{A}_g \cdot \tilde{\mathbf{s}}_g + \mathbf{u}_i^T \cdot \mathbf{e} \equiv \mathbf{v}_i^T \cdot \mathbf{s}_\ell + \mathbf{u}_i^T \cdot \mathbf{A}_g \cdot (\mathbf{s}_g - \tilde{\mathbf{s}}_g) + \mathbf{u}_i^T \cdot \mathbf{e}$$

- Correct guess: **small-ish** value; incorrect guess **uniform-ish** value.
- Score guesses by sums of these values for different $(\mathbf{v}_i, \mathbf{u}_i)$

“Small-ish” and “Uniform-ish” Unpacked

Success depends on the geometry of

$$\Lambda \subset \Lambda_q^{\perp}(\mathbf{A}_\ell) = \{\mathbf{u} \in \mathbb{Z}^m \mid \mathbf{u}^T \cdot \mathbf{A}_\ell \equiv \mathbf{0} \bmod q\},$$

lattice spanned by outputs of the sieve.

- We are asking our correct guess to “win” against all wrong guesses for $\tilde{\mathbf{s}}_g$
- “Winning” means being closer to Λ
- [DP23a] shows that this goes wrong when modelling the outcome of the wrong guesses as uniformly random
- Given enough targets there will be random targets that are closer to Λ than the correct $\Rightarrow$ “contradictory regime”

Follow-up work

Accurate Score Prediction for Dual-Sieve Attacks

Léo Ducas[1,2] and Ludo N. Pulles[1]

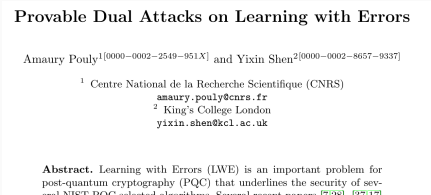
[1] CWI, Cryptology Group, Amsterdam, the Netherlands
[2] Mathematical Institute, Leiden University, Leiden, the Netherlands

Abstract. The Dual-Sieve Attack on Learning with Errors (LWE), or more generally Bounded Distance Decoding (BDD), has seen many improvements in the recent years, and ultimately led to claims that it outperforms the primal attack against certain lattice-based schemes in the PQC standardization process organised by NIST. However, the work of Ducas–Pulles (Crypto ’23) revealed that the so-called “Independence Heuristic”, which all recent dual attacks used, leads to wrong predictions in a contradictory regime, which is relevant for the security of cryptoschemes. More specifically, the stated distributions of scores for the actual solution and for incorrect candidates were both incorrect.
In this work, we propose to use the weaker heuristic that the output vectors of a lattice sieve are uniformly distributed in a ball. Under this heuristic, we give an analysis of the score distribution in the case of an error of fixed length. Integrating over this length, we extend this analysis to any radially distributed error, in particular the gaussian as a fix for the score distribution of the actual solution. This approach also provides a prediction for the score of incorrect candidates, using a ball as an approximation of the Voronoi cell of a lattice.
We compare the predicted score distributions to extensive experiments, and observe them to be qualitatively and quantitatively quite accurate. This constitutes a first step towards fixing the analysis of the dual-sieve attack: we can now accurately estimate false-positives and false-negatives. Now that the analysis is fixed, one may consider how to fix the attack itself, namely exploring the opportunities to mitigate a large number of false-positives.

Keywords: Lattices · Cryptanalysis · Heuristics · Learning with Errors · Dual Attack · Bessel Functions

Alternative Approach

- Starts over and proves a variant of the dual attack **without any statistical assumption**
- Does not model/prove "modulus switching" which greatly reduces guessing cost.
- Provable variant works in a regime that complements the contradictory regime of [DP23a]
- **Caveat:** premises of provable variant and of contradictory regime differ
- Work also gives a guestimate of what this attack with modulus-switching added could cost (spoiler: similar to costs of [MAT22].)



Provable Dual Attacks on Learning with Errors

Amaury Pouly[1][0000−0002−2549−951X] and Yixin Shen[2][0000−0002−8657−9337]

[1] Centre National de la Recherche Scientifique (CNRS)
amaury.pouly@cnrs.fr
[2] King's College London
yixin.shen@kcl.ac.uk

Abstract. Learning with Errors (LWE) is an important problem for post-quantum cryptography (PQC) that underlines the security of several NIST PQC selected algorithms. Several recent papers [7,28], [37,17] have claimed improvements on the complexity of so-called dual attacks on LWE. These improvements make dual attacks comparable to or even better than primal attacks in certain parameter regimes. Unfortunately, those improvements rely on a number of untested and hard-to-test statistical assumptions. Furthermore, a recent paper [23] claims that the whole premise of those improvements might be incorrect.
The goal of this paper is to improve the situation by proving the correctness of a dual attack without relying on any statistical assumption. Although our attack is greatly simplified compared to the recent ones, it shares many important technical elements with those attacks and can serve as a basis for the analysis of more advanced attacks. We provide some rough estimates on the complexity of our simplified attack on Kyber using a Monte Carlo Markov Chain discrete Gaussian sampler.
Our main contribution is to clearly identify a set of parameters under which our attack (and presumably other recent dual attacks) can work. Furthermore, our analysis completely departs from the existing statistics-based analysis and is instead rooted in geometry. We also compare the regime in which our algorithm works to the "contradictory regime" of [23]. We observe that those two regimes are essentially complementary.
Finally, we give a quantum version of our algorithm to speed up the computation. The algorithm is inspired by [10] but is completely formal and does not rely on any heuristics.

Summary

- Heuristics used in dual-attack analysis are being cleaned up, community is gaining clarity on its expected performance
- But this only treats statistical/geometric questions, but not computational costs
  - See John's talk

- It seems **morally wrong** that the dual attack would beat the primal attack. If the universe is **just**, the somewhat direct approach **should** beat running lattice reduction on the transpose and computing inner products.

ML Attacks

- Emily Wenger, Mingjie Chen, François Charton, and Kristin E. Lauter. **SALSA: Attacking Lattice Cryptography with Transformers.** In: *Annual Conference on Neural Information Processing Systems 2022, NeurIPS 2022*. Ed. by Sanmi Koyejo, S. Mohamed, A. Agarwal, Danielle Belgrave, K. Cho, and A. Oh. 2022
- Cathy Yuanchen Li, Jana Sotáková, Emily Wenger, Mohamed Malhou, Evrard Garcelon, François Charton, and Kristin E. Lauter. **SalsaPicante: A Machine Learning Attack on LWE with Binary Secrets.** In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023*. Ed. by Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda. ACM, 2023, pp. 2606–2620
- Cathy Yuanchen Li, Jana Sotáková, Emily Wenger, Zeyuan Allen-Zhu, François Charton, and Kristin E. Lauter. **SALSA VERDE: a machine learning attack on Learning with Errors with sparse small secrets.** 2023. URL: `https://eprint.iacr.org/2023/968`
- Samuel Stevens, Emily Wenger, Cathy Yuanchen Li, Niklas Nolte, Eshika Saxena, François Charton, and Kristin E. Lauter. **SALSA FRESCA: Angular Embeddings and Pre-Training for ML Attacks on Learning With Errors.** 2024. URL: `https://eprint.iacr.org/2024/150`

Ethics and Broader Impact. *The primary value of this work is in alerting the cryptographic and ML communities to the risk of ML-based attacks on PQC. Even if current attacks do not succeed, we believe that* ***providing early warning of potential threats is critical****. However, we emphasize that SALSA represents a proof of concept that cannot be used against real-world implementations (i.e. the PQC schemes which NIST standardized on July 5, 2022). Additional scaling work would be necessary before these techniques would be relevant to attacking real-world cryptosystems.“ – [WCCL22]*

Claims II

Ethical considerations. *Although Picante demonstrates significant progress towards attacking real-world LWE problems with sparse binary secrets, it cannot yet break problems with real-world-size parameters. In particular, the LWE schemes standardized by NIST use smaller modulus q and non-sparse secret distributions. Hence, we do not believe our paper raises any ethical concerns. Nonetheless, we shared a copy of the current paper with the NIST Cryptography group, to inform them of our approach. – [LSWMGCL23]*

Limitations and broader impact. *Despite significantly advancing the state-of-the-art in ML-based LWE attacks, VERDE* ***cannot yet break*** *standardized LWE-based PQC schemes, limiting its real-world impact. Because of this, our paper raises no immediate security concerns. Nevertheless, we have shared a copy of our paper with the NIST PQC group to make them aware of this attack. – [LSWACL23]*

8. Impact Statement *The main ethical concern related to this work is the possibility of our attack compromising currently-deployed PQC system. However,* ***at present, our proposed attack does not threaten current standardized systems****. If our attack scales to higher h and lower q settings, then its impact is significant, as it would necessitate changing PQC encryption standards. For reproducibility of these results, our code will be open sourced after publication and is available to reviewers upon request. – [SWLNSCL24]*

Attack Description

The preprocessing step strives to reduce the norm of the rows of $\mathbf{A}$ by applying a carefully selected integer linear operator $\mathbf{R}$. Because $\mathbf{R}$ is linear with integer entries, the transformed pairs $(\mathbf{RA}, \mathbf{Rb}) \mod \mathbf{q}$ are also LWE pairs with the same secret, albeit larger error. In practice, $\mathbf{R}$ is found by performing lattice reduction on the $(m+n) \times (m+n)$ matrix $\mathbf{\Lambda} = \begin{bmatrix} 0 & q \cdot \mathbf{I}_n \\ \omega \cdot \mathbf{I}_m & \mathbf{A} \end{bmatrix}$, and finding linear operators $\begin{bmatrix} \mathbf{C} & \mathbf{R} \end{bmatrix}$ such that the norms of $\begin{bmatrix} \mathbf{C} & \mathbf{R} \end{bmatrix} \mathbf{\Lambda} = \begin{bmatrix} \omega \cdot \mathbf{R} & \mathbf{RA} + q \cdot \mathbf{C} \end{bmatrix}$ are small. This achieves a reduction of the norms of the entries of $\mathbf{RA} \mod q$, but also increases the error in the calculation of $\mathbf{Rb} = \mathbf{RA} \cdot \mathbf{s} + \mathbf{Re}$, making secret recovery more difficult. Although ML models can learn from noisy data, too much noise will make the distribution of $\mathbf{Rb}$ uniform on $[0, q)$ and inhibit learning. The parameter ω controls the trade-off between norm reduction and error increase. Reduction strength is measured by $\rho = \frac{\sigma(\mathbf{RA})}{\sigma(\mathbf{A})}$, where σ denotes the mean of the standard deviations of the rows of $\mathbf{RA}$ and $\mathbf{A}$.

Li et al. (2023a) use BKZ (Schnorr, 1987) for lattice reduction. Li et al. (2023b) improves the reduction time by $45\times$ via a modified definition of the Λ matrix and by interleaving `BKZ2.0` (Chen & Nguyen, 2011) and `polish` (Charton et al., 2024) (see Appendix C).

This preprocessing step produces many $(\mathbf{RA}, \mathbf{Rb})$ pairs that can be used to train models. Individual rows of $\mathbf{RA}$ and associated elements of $\mathbf{Rb}$, denoted as reduced LWE samples $(\mathbf{Ra}, \mathbf{R}b)$ with some abuse of notation, are used for model training. Both the subsampling of m samples from the original t LWE samples and the reduction step are

Recent versions of the attack (VERDE/FRESCA) are essentially variants of the dual attack.

- $\mathbf{u}^T \cdot \mathbf{c} \equiv \mathbf{u}^T \cdot \mathbf{A} \cdot \mathbf{s} + \mathbf{u}^T \cdot \mathbf{e} \equiv \mathbf{v}^T \cdot \mathbf{s} + \mathbf{u}^T \cdot \mathbf{e} \Rightarrow$ short-ish
- $\mathbf{u}^T \cdot \mathbf{c} \Rightarrow$ uniform

Distinguishers

Modelling $\mathbf{v}^T \cdot \mathbf{s} + \mathbf{u}^T \cdot \mathbf{e}$ as a discrete Gaussian mod q we can compute the statistical distance between these two distributions and thus the number of samples we need to distinguish with constant advantage.

Comparison with State of the Art: SALSA VERDE I

Table 15. Comparison of VERDE's and uSVP attack performance on LWE problems with $n = 256$, binary secrets, varying q and h. *VERDE's total attack time is the sum of preprocessing and training time (with recovery included). Preprocessing time assumes full parallelization, and training time is the number of epochs to recovery multiplied by epoch time (1.5 hours/epoch). N/A means no successful secret recovery.*

LWE parameters		VERDE attack time			uSVP attack time (hrs)
$\log_2 q$	h	*Preprocessing (hrs)*	*Training*	*Total (hrs)*	
12	8	1.5	2 epochs	4.5	N/A
14	12	2.5	2-5 epochs	5.5-10	N/A
16	14	8.0	2 epochs	11	N/A
18	18	7.0	3 epochs	11.5	558
18	20	7.0	1-8 epochs	8.5-19	259
20	22	7.5	5 epochs	15	135-459
20	23	7.5	3-4 epochs	12-15	167-330
20	24	7.5	4 epochs	13.5	567
20	25	7.5	5 epochs	15	76 - 401

To summarize the comparison, VERDE outperforms existing classical attacks in two senses: 1) VERDE fully recovers sparse binary and ternary secrets for n and q where existing classical attacks do not succeed in several weeks or months using *fplll* BKZ 2.0 [19] with the required block size;

https://crypto.iacr.org/2023/rump/crypto2023rump-paper13.pdf

Comparison with State of the Art: SALSA VERDE II

Table 15. Comparison of VERDE's and uSVP attack performance on LWE problems with $n = 256$, binary secrets, varying q and h. *VERDE's total attack time is the sum of preprocessing and training time (with recovery included). Preprocessing time assumes full parallelization, and training time is the number of epochs to recovery multiplied by epoch time (1.5 hours/epoch). N/A means no successful secret recovery.*

LWE parameters		VERDE attack time			State of the Art Attack (hrs, 1core)
$\log_2 q$	h	*Preprocessing (hrs)*	*Training*	*Total* (hrs × CPU)	
12	8	1.5	2 epochs	4.5 × ???	0.2 (MITM ... in Py)
14	12	2.5	2-5 epochs	5.5-10 × 270	Implementation in Progress
16	14	8.0	2 epochs	11 × ???	(Hybrid MITM-Lattice) Models and predictions exists, but no open source implem.
18	18	7.0	3 epochs	11.5 × 990	
18	20	7.0	1-8 epochs	8.5-19 × ???	
20	22	7.5	5 epochs	15 × ???	
20	23	7.5	3-4 epochs	12-15 × ???	
20	24	7.5	4 epochs	13.5 × ???	
20	25	7.5	5 epochs	15 × ???	12 -- 24 (rescaled uSVP)

To summarize the comparison, VERDE is several orders of magnitude behind the state of the art, even on these custom made instances.

https://crypto.iacr.org/2023/rump/crypto2023rump-paper13.pdf

Comparison with Something: SALSA FESCA I

SALSA FRESCA: Angular Embeddings and Pre-Training for ML Attacks on LWE

Table 1. **Best results from our attack** for LWE problems in dimensions n (higher is harder), modulus q (lower is harder) and Hamming weights h (higher is harder). Our work recovers secrets for $n = 1024$ for the first time in ML-based LWE attacks and reduces total attack time for $n = 512, \log_2 q = 41$ to only 50 hours (assuming full CPU parallelization).

n	$\log_2 q$	highest h	LWE (A, b) matrices needed	preprocessing time (hrs/CPU/matrix)	training time (hrs)	total time (hrs)
512	41	44	1955	13.1	36.9	50.0
768	35	9	1302	12.4	14.8	27.2
1024	50	13	977	26.0	47.4	73.4

```
from estimator import *
params = LWE.Parameters(n=1024, q=2^50, Xs=ND.SparseTernary(n=1024, p=7, m=7), Xe=ND.DiscreteGaussian(3))
LWE.primal_hybrid(params)
```

```
rop: ≈2^48.4, red: ≈2^48.1, svp: ≈2^46.2, β: 41, η: 2, ζ: 478, |S|: ≈2^42.6, d: 1213, prob: 0.189, ↻: 22, …
```

$$\approx 52 \text{ hrs vs } 977 \cdot 26 + 47.4 \approx 25402 \text{ hrs}$$

Comparison with Something: SALSA FESCA II

The “lattice estimator”[2] picks $\beta = 40$ as a lower bound, it is not designed to handle such easy instances.

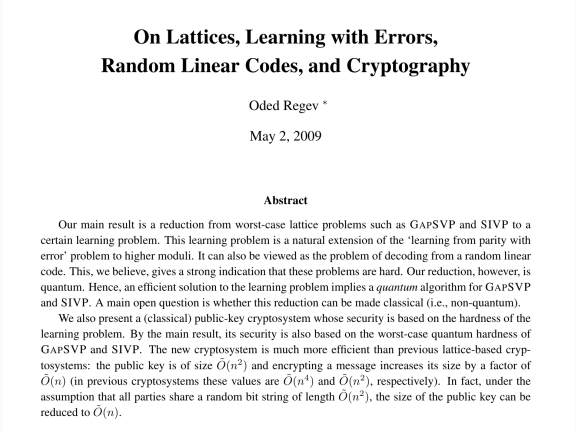
```
with local_minimum(40, max(2 * params.n, 41), precision=5) as it:
    for beta in it:
        cost = self.cost_gsa(
            beta=beta, params=params, m=m, red_cost_model=red_cost_model, **kwds
        )
        it.update(cost)
    for beta in it.neighborhood:
        cost = self.cost_gsa(
            beta=beta, params=params, m=m, red_cost_model=red_cost_model, **kwds
        )
        it.update(cost)
    cost = it.y
```

https://github.com/malb/lattice-estimator/blob/main/estimator/lwe_primal.py#L209-L220

[2] https://github.com/malb/lattice-estimator

High-Level

There is no particular reason to believe that ML can threaten LWE.



On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Oded Regev *

May 2, 2009

Abstract

Our main result is a reduction from worst-case lattice problems such as GAPSVP and SIVP to a certain learning problem. This learning problem is a natural extension of the 'learning from parity with error' problem to higher moduli. It can also be viewed as the problem of decoding from a random linear code. This, we believe, gives a strong indication that these problems are hard. Our reduction, however, is quantum. Hence, an efficient solution to the learning problem implies a *quantum* algorithm for GAPSVP and SIVP. A main open question is whether this reduction can be made classical (i.e., non-quantum).

We also present a (classical) public-key cryptosystem whose security is based on the hardness of the learning problem. By the main result, its security is also based on the worst-case quantum hardness of GAPSVP and SIVP. The new cryptosystem is much more efficient than previous lattice-based cryptosystems: the public key is of size $\tilde{O}(n^2)$ and encrypting a message increases its size by a factor of $\tilde{O}(n)$ (in previous cryptosystems these values are $\tilde{O}(n^4)$ and $\tilde{O}(n^2)$, respectively). In fact, under the assumption that all parties share a random bit string of length $\tilde{O}(n^2)$, the size of the public key can be reduced to $\tilde{O}(n)$.

- **LWE** is (designed to be) a hard learning problem.
- **ML** classifiers exploit statistical patterns in the data.[a]

Open Problem

Not easy to establish the state of the art for LWE instances within range of experiments. More advanced algorithms lack efficient, versatile and public implementations.

[a] This is a reason why they work somewhat well on e.g. side-channel traces.

Thank You

KCL Academic staff, postdocs and PhD students (all areas of cryptography)

SandboxAQ Postdoc/PhD/FTEs/Consultants: PQC PhD residencies, PQC Postdocs, Cryptography SWE

References I

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In: *CRYPTO 2009*. Ed. by Shai Halevi. Vol. 5677. LNCS. Springer, Heidelberg, Aug. 2009, pp. 595–618. DOI: 10.1007/978-3-642-03356-8_35.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343.

[Alb17] Martin R. Albrecht. On Dual Lattice Attacks Against Small-Secret LWE and Parameter Choices in HElib and SEAL. In: *EUROCRYPT 2017, Part II*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10211. LNCS. Springer, Heidelberg, 2017, pp. 103–129. DOI: 10.1007/978-3-319-56614-6_4.

[AR05] Dorit Aharonov and Oded Regev. Lattice problems in NP ∩ coNP. In: *Journal of the ACM* 52.5 (Sept. 2005), pp. 749–765. ISSN: 0004-5411 (print), 1557-735X (electronic). DOI: http://doi.acm.org/10.1145/1089023.1089025.

[DP23a] Léo Ducas and Ludo Pulles. Does the Dual-Sieve Attack on Learning with Errors even Work? Cryptology ePrint Archive, Report 2023/302. https://eprint.iacr.org/2023/302. 2023.

[DP23b] Léo Ducas and Ludo N. Pulles. Accurate Score Prediction for Dual-Sieve Attacks. Cryptology ePrint Archive, Paper 2023/1850. https://eprint.iacr.org/2023/1850. 2023. URL: https://eprint.iacr.org/2023/1850.

References II

[GJ21] Qian Guo and Thomas Johansson. Faster Dual Lattice Attacks for Solving LWE with Applications to CRYSTALS. In: *ASIACRYPT 2021, Part IV*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13093. LNCS. Springer, Heidelberg, Dec. 2021, pp. 33–62. DOI: 10.1007/978-3-030-92068-5_2.

[LSWACL23] Cathy Yuanchen Li, Jana Sotáková, Emily Wenger, Zeyuan Allen-Zhu, François Charton, and Kristin E. Lauter. SALSA VERDE: a machine learning attack on Learning with Errors with sparse small secrets. 2023. URL: https://eprint.iacr.org/2023/968.

[LSWMGCL23] Cathy Yuanchen Li, Jana Sotáková, Emily Wenger, Mohamed Malhou, Evrard Garcelon, François Charton, and Kristin E. Lauter. SalsaPicante: A Machine Learning Attack on LWE with Binary Secrets. In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023*. Ed. by Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda. ACM, 2023, pp. 2606–2620.

[MAT22] MATZOV. Report on the Security of LWE: Improved Dual Lattice Attack. Available at https://doi.org/10.5281/zenodo.6412487. Apr. 2022. DOI: 10.5281/zenodo.6412487. URL: https://doi.org/10.5281/zenodo.6412487.

[NIS17] NIST. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals. Jan. 2017.

References III

[PS23] Amaury Pouly and Yixin Shen. Provable Dual Attacks on Learning with Errors. Cryptology ePrint Archive, Paper 2023/1508. https://eprint.iacr.org/2023/1508. 2023. URL: https://eprint.iacr.org/2023/1508.

[SWLNSCL24] Samuel Stevens, Emily Wenger, Cathy Yuanchen Li, Niklas Nolte, Eshika Saxena, François Charton, and Kristin E. Lauter. SALSA FRESCA: Angular Embeddings and Pre-Training for ML Attacks on Learning With Errors. 2024. URL: https://eprint.iacr.org/2024/150.

[WCCL22] Emily Wenger, Mingjie Chen, François Charton, and Kristin E. Lauter. SALSA: Attacking Lattice Cryptography with Transformers. In: *Annual Conference on Neural Information Processing Systems 2022, NeurIPS 2022*. Ed. by Sanmi Koyejo, S. Mohamed, A. Agarwal, Danielle Belgrave, K. Cho, and A. Oh. 2022.