PRivacy preserving pOst-quantuM systEms from
advanced crypTograpHic mEchanisms Using latticeS

Tools for Parameter Selection

Eamonn Postlethwaite, CWI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780701.

Parameters and their estimation

This presentation concerns the tools for estimating lattice parameters that have been {created, expanded, maintained} under the PROMETHEUS project.

Specifically:

- the lattice-estimator [APS15] (`github:malb/lattice-estimator`),
- the leaky-LWE-estimator [DDGR20] (`github:lducas/leaky-LWE-Estimator`),
- NTRUFatigue-estimator [DvW21] (`github:WvanWoerden/NTRUFatigue`).

The high level *why*

Selecting parameters for lattice based cryptography that are both *secure* and *efficient* seems more challenging that for much of classical cryptography.

The high level *why*

Selecting parameters for lattice based cryptography that are both *secure* and *efficient* seems more challenging that for much of classical cryptography.

Understanding the balance between security and efficiency is also important for lattice based cryptography, given its overheads compared to classical cryptography.

The high level *why*

Selecting parameters for lattice based cryptography that are both *secure* and *efficient* seems more challenging that for much of classical cryptography.

Understanding the balance between security and efficiency is also important for lattice based cryptography, given its overheads compared to classical cryptography.

The complexity of the parameter and attack spaces, as well as the increased importance of understanding efficiency trade offs, can make parameter selection daunting.

The high level *why*

Selecting parameters for lattice based cryptography that are both *secure* and *efficient* seems more challenging that for much of classical cryptography.

Understanding the balance between security and efficiency is also important for lattice based cryptography, given its overheads compared to classical cryptography.

The complexity of the parameter and attack spaces, as well as the increased importance of understanding efficiency trade offs, can make parameter selection daunting.

Hence the desire for, and use of, various estimation tools.

The high level *what*

Broadly speaking, any (lattice) estimator takes as input some

$$\textit{parameters} + \textit{attacks} + \textit{attack models} + \textit{units of cost}$$

and outputs the 'cost of the attacks' in the specified units. For example

$$\textit{Kyber512} + \textit{primal uSVP} + \textit{GSA Intersect} + \textit{blocksize } \beta.$$

The high level *what*

Broadly speaking, any (lattice) estimator takes as input some

$$\textit{parameters} + \textit{attacks} + \textit{attack models} + \textit{units of cost}$$

and outputs the 'cost of the attacks' in the specified units. For example

$$\textit{Kyber512} + \textit{primal uSVP} + \textit{GSA Intersect} + \textit{blocksize}\ \beta.$$

One then iterates through the parameter space to find acceptable parameters such that the cost of attacks is sufficiently high.

The high level *what*

Different estimators aim for different levels of generality:

- lattice-estimator $\leftrightarrow$ high generality (many parameters, attacks, models),
- leaky-LWE-estimator $\leftrightarrow$ high specificity (some parameters, one attack in detail),
- NTRUFatigue-estimator $\leftrightarrow$ high specificity (some parameters, one attack in detail).

The lattice-estimator

An estimator[1] based on a paper [APS15] that systematised and improved the analysis of a large range of attacks against LWE.

[1] `github:malb/lattice-estimator`

The lattice-estimator

An estimator[1] based on a paper [APS15] that systematised and improved the analysis of a large range of attacks against LWE.

PROMETHEUS members are involved in its maintenance and improvement (e.g. recent MATZOV [MAT22] cost model).

[1] `github:malb/lattice-estimator`

The lattice-estimator

An estimator[1] based on a paper [APS15] that systematised and improved the analysis of a large range of attacks against LWE.

PROMETHEUS members are involved in its maintenance and improvement (e.g. recent MATZOV [MAT22] cost model).

The aim is to capture as many attacks and improvements as possible and automate their cost estimation against a wide range of popular parameters, e.g. dimension, modulus, secret and error distributions etc…

[1] `github:malb/lattice-estimator`

The leaky-LWE-estimator

An estimator[2] based on a paper [DDGR20] with PROMETHEUS authors. It was created and is maintained by the same authors.

[2] `github:lducas/leaky-LWE-Estimator`

The leaky-LWE-estimator

An estimator[2] based on a paper [DDGR20] with PROMETHEUS authors. It was created and is maintained by the same authors.

So called because its main function is the integration of leaks (i.e. side channel information) into the primal uSVP attack.

[2] `github:lducas/leaky-LWE-Estimator`

The leaky-LWE-estimator

An estimator[2] based on a paper [DDGR20] with PROMETHEUS authors. It was created and is maintained by the same authors.

So called because its main function is the integration of leaks (i.e. side channel information) into the primal uSVP attack.

It improved our understanding of probabilistic aspects of this attack by considering distributions of projected vectors, not their mean lengths.

[2] `github:lducas/leaky-LWE-Estimator`

The NTRUFatigue-estimator

An estimator[3] based on a paper [DvW21] with a PROMETHEUS author.

[3] `github:WvanWoerden/NTRUFatigue`

The NTRUFatigue-estimator

An estimator[3] based on a paper [DvW21] with a PROMETHEUS author.

The works [ABD16, CJL16, KF17] show that large moduli q weaken NTRU schemes. Initial experiments focussed on low power lattice reduction and *large* q.

[3] `github:WvanWoerden/NTRUFatigue`

The NTRUFatigue-estimator

An estimator[3] based on a paper [DvW21] with a PROMETHEUS author.

The works [ABD16, CJL16, KF17] show that large moduli q weaken NTRU schemes. Initial experiments focussed on low power lattice reduction and *large* q.

This work concretises the size of q required for these attacks to function, and shows how lattice reduction functions on such instances. The authors give a estimator that determines when these effects begin to appear.

[3] `github:WvanWoerden/NTRUFatigue`

Use cases

A non exhaustive list of how these estimators have been used:

- NIST candidates: KYBER, SABER, FRODO, DILITHIUM,
- PROMETHEUS research: to estimate the security of signatures based on new Gaussian samplers over modules [BEP+21],
- non PROMETHEUS research:
  - to estimate LSH based improvements to MitM attacks on ternary LWE [KM21],
  - in FHE design and standardisation [ACC+18, BIP+22],
  - in hardware design and certification.

Conclusion

When are these tools for you? Whenever any subset of the following apply:

- you have designed a scheme based on LWE or NTRU,
- you want to understand how lattice attacks behave against concrete parameter choices for it,
- you want to know which attacks to consider (non automatically) in more detail,
- you want to understand the (lattice reduction based) implications of certain kinds of side channels,
- you want to rule out attacks against too large moduli.

Martin R. Albrecht, Shi Bai, and Léo Ducas.
A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 153–178. Springer, Heidelberg, August 2016.

Martin Albrecht, Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Shai Halevi, Jeffrey Hoffstein, Kim Laine, Kristin Lauter, Satya Lokam, Daniele Micciancio, Dustin Moody, Travis Morrison, Amit Sahai, and Vinod Vaikuntanathan.
Homomorphic encryption security standard.
Technical report, HomomorphicEncryption.org, Toronto, Canada, November 2018.

Martin R. Albrecht, Rachel Player, and Sam Scott.
On the concrete hardness of learning with errors.
Journal of Mathematical Cryptology, 9(3):169–203, 2015.

Pauline Bert, Gautier Eberhart, Lucas Prabel, Adeline Roux-Langlois, and Mohamed Sabt.

Implementation of lattice trapdoors on modules and applications.
In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021*, pages 195–214. Springer, Heidelberg, 2021.

Charlotte Bonte, Ilia Iliashenko, Jeongeun Park, Hilder V. L. Pereira, and Nigel P. Smart.
FINAL: Faster FHE instantiated with NTRU and LWE.
Cryptology ePrint Archive, Report 2022/074, 2022.
https://eprint.iacr.org/2022/074.

Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee.
An algorithm for ntru problems and cryptanalysis of the ggh multilinear map without a low-level encoding of zero.
LMS Journal of Computation and Mathematics, 19(A):255–266, 2016.

Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi.
LWE with side information: Attacks and concrete security estimation.
In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 329–358, Springer, Heidelberg, August 2020.

Léo Ducas and Wessel P. J. van Woerden.
NTRU fatigue: How stretched is overstretched?
In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part IV*, volume 13093 of *LNCS*, pages 3–32. Springer, Heidelberg, December 2021.

Paul Kirchner and Pierre-Alain Fouque.
Revisiting lattice attacks on overstretched NTRU parameters.
In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 3–26. Springer, Heidelberg, April / May 2017.

Elena Kirshanova and Alexander May.
How to find ternary lwe keys using locality sensitive hashing.
In *Cryptography and Coding: 18th IMA International Conference, IMACC 2021, Virtual Event, December 14–15, 2021, Proceedings*, pages 247–264, Berlin, Heidelberg, 2021. Springer-Verlag.

MATZOV.
Report on the Security of LWE: Improved Dual Lattice Attack, April 2022.