Introduction to lattice-based postquantum Cryptography

#ProyectosCiber

Sergi Simón Balcells

2025/04/01

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Acknowledgements

Esta investigación resulta del Proyecto Estratégico 'Avances en criptografía post-cuántica aplicados al desarrollo de un sistema de cupones' (C039/24), fruto del convenio de colaboración suscrito entre el Instituto Nacional de Ciberseguridad (INCIBE) y la Universidad de Lleida. Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation).

Outline

Lattice

Let $B = \{b_1, b_2, \ldots, b_m\}$, be a set of linear independent vectors on $\mathcal{R}^n$. Then:

$$L(B) = \{\sum_i a_i b_i | a_i \in \mathbb{Z}\}$$

is called a lattice generated by B. B is the base.
Note that B can be seen as a matrix $B = (b_1, b_2, \ldots, b_m)$ so:

$$L(B) = \{Ba | a \in \mathbb{Z}^n\}$$

Short Vector Problem

$$Ba = \lambda(L)$$

Where $\lambda(L)$ is the smallest vector and and a is a non-zero vector. This problem is NP-hard [Ajtai, 1996].

Short Integer Solution

Solve:

$$As = 0$$

Or more generaly:

$$As = v$$

Where $||s||$ is small.
The average case on this problem translates to a hard case of SVP.
Ajtai proved this and used it as a one-time-hash protocol.

A Ring Approach

For this problem to be hard, it needs large key sizes.
FrodoKEM [Alkim et al., 2023] uses up to 22kB just for the public key.
So, we change the base Ring from $\mathbb{Z}_p$ to $\mathcal{R} = \mathbb{Z}_q[x]/f(x)$ [Micciancio, 2007, Lyubashevsky et al., 2013a, Lyubashevsky et al., 2013b].

A Ring Approach

For this problem to be hard, it needs large key sizes.
FrodoKEM [Alkim et al., 2023] uses up to 22kB just for the public key.
So, we change the base Ring from $\mathbb{Z}_p$ to $\mathcal{R} = \mathbb{Z}_q[x]/f(x)$ [Micciancio, 2007, Lyubashevsky et al., 2013a, Lyubashevsky et al., 2013b]. To collapse a vector, we use the coefficient between $\frac{-q}{2}$ to $\frac{q}{2}$

Limitations of Ring Approach

The huge adventage with Rings is the computational gains of NTT multiplications.
They add constraints to the key that limit the security parameters harshly.
One way to solve it is to construct a matrix of smaller ring elements, but it is not always possible.

Outline

The Ring

The Ring on Falcon [et al., 2020] is

$$\mathcal{R} = Z_q[x]/\phi$$

Where $\phi = x^n + 1$, n is a power of 2 and $q = kn + 1$ and is prime. This lets the NTT to have an optimal performance.

The trapdoor

Falcon creates a polynomial:

$$fG - gF = q \ (mod \ \phi)$$

And constructs:

$$h = gf^{-1}$$

The public key is $A = \left[\begin{array}{c|c} 1 & h \end{array} \right]$
The secret basis is an orthogonal basis:

$$B = \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array} \right]$$

The idea

The idea is to solve $As' = v$ for some large s', and then use notion orthogonal basis to create a similar vector of s' s.t. $A(s' - Bw) = v$ and $||s' - Bw||_2$ is small.

Problems

The creation of s is random, so given the same vector it can output different solutions (s_1, s_2 s.t. $As_i = v$).
With enough of these solutions one can create an orthogonal basis.
There are two solutions on this:

- De-randomizing
- Adding your own random element.

Falcon uses the second, so it signs $As = H(m||r)$

Outline

LWE variant

We base our security on [Regev, 2009]:

$$As + e = b$$

Is hard to solve for vectors s and e with small norm.
As before, using rings provide better speed-ups with smaller key-sizes, but they are more sensible to the error distribution.

LWE variant

We base our security on [Regev, 2009]:

$$As + e = b$$

Is hard to solve for vectors s and e with small norm.
As before, using rings provide better speed-ups with smaller key-sizes, but they are more sensible to the error distribution.
Intuition:

$$(A \; I_n \; -b) \cdot \begin{pmatrix} s \\ e \\ 1 \end{pmatrix} = 0 \pmod{q}$$

Rounding elements

We round the elements if that are close to 0 to 0:

$$\lfloor x \rceil = \begin{cases} 0 & \text{if } -\frac{q}{4} \leq x < \frac{q}{4} \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

Security errors and how to avoid them

The error must be equivalent to a continuous spherical Guassian distribution of $r \geq 2$ [Peikert, 2016].
In discrete terms is better to use a Centered Binomial Distribution of parameter n. This corresponds to $2n$ toss coins ($n = 2$):

$$\sum a_i - \sum b_i = a_0 + a_1 - b_0 - b_1$$

This is easier to derandomize.

Security errors and how to avoid them

The error must be equivalent to a continuous spherical Guassian distribution of $r \geq 2$ [Peikert, 2016].
In discrete terms is better to use a Centered Binomial Distribution of parameter n. This corresponds to $2n$ toss coins ($n = 2$):

$$\sum a_i - \sum b_i = a_0 + a_1 - b_0 - b_1$$

This is easier to derandomize.
There is an estimator [Albrecht et al., 2015] to check the security bits of a protocol.

Outline

A gentle introduction to Kyber

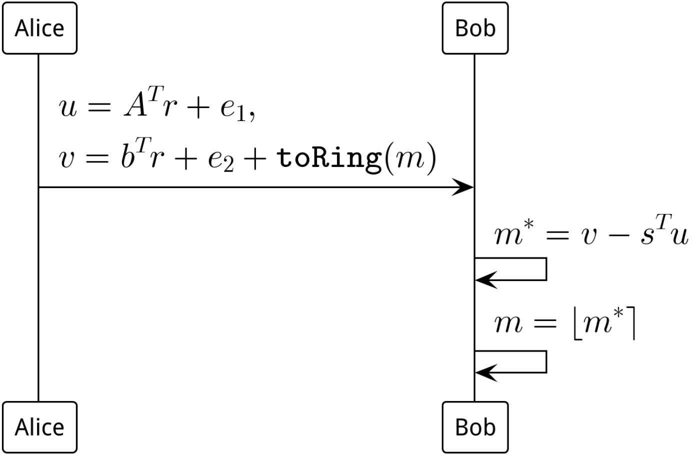

Figure: Activity diagram of Kyber [et al., 2018]

Why?

$$
\begin{aligned}
m^* &= v - s^T u \\
m^* &= b^T r + e_2 + m' - s^T(A^T r + e_1) \\
m^* &= (As + e)^T r + e_2 + m' - s^T A^T r - s^T e_1 \\
m^* &= s^T A^T r + e^T r + e_2 + m' - s^T A^T r - s^T e_1 \\
m^* &= m' + e'
\end{aligned} \tag{2}
$$

And rounding just deletes the error with a probability of failure of 2^{-128}

A gentle introduction to Dilithium

Signature creation [Ducas et al., 2017]:

1. $w = \lfloor Ay \rceil$
2. $c = H(m||w)$, $c \in \mathcal{R}$ «and small».
3. $z = y + cs$ and perform rejection sampling.

The signature is $\sigma = (z, c)$

A gentle introduction to Dilithium

Signature creation [Ducas et al., 2017]:

1. $w = \lfloor Ay \rceil$
2. $c = H(m||w)$, $c \in \mathcal{R}$ «and small».
3. $z = y + cs$ and perform rejection sampling.

The signature is $\sigma = (z, c)$
Check signature:

$$w' = \lfloor Az - bc \rceil$$

$$c' = H(m||w')$$

Then check:

$$c = c'$$

Outline

Example of a Non-Interactive Zero Knowledge Proof

Given the system [Lyubashevsky and Nguyen, 2022]:

$$\begin{aligned} B_0 r_0 &= As - B_1 r_1 \\ e &= E r_1 \end{aligned}$$

1. Generate y_0 y_1 small such as:

$$\begin{aligned} w &= Ay_0 - B_1 y_1 \\ e' &= Ey_1 \end{aligned}$$

2. Compute a challenge $c = \mathcal{H}(w, e')$ where $c \in \mathcal{R}$
3. Compute:

$$\begin{aligned} z_0 &= y_0 + cs \\ z_1 &= y_1 + cr_1 \end{aligned}$$

4. Perform a rejection sampling algorithm on z, so the secret cannot be retrieved.

NIZK acceptance

Check:

$$\begin{aligned} w + cB_0 r_0 &= Az_0 - B_1 z_1 \\ e' + ce &= Ez_1 \end{aligned}$$

And all $||z_i|| \leq \beta$.

References I

Thanks for your attention

Ajtai, M. (1996).
Generating hard instances of lattice problems.
Quaderni di Matematica, 13:1–32.
Preliminary version in STOC 1996.

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

Alkim, E., Bos, J. W., Ducas, L., Glabush, L., Longa, P., Mironov, I., Naehrig, M., Nikolaenko, V., Peikert, C., Raghunathan, A., Stebila, D., Easterbrook, K., and LaMacchia, B. (2023).
Frodokem: Learning with errors key encapsulation preliminary standardization proposal.
Technical report, FrodoKEM Team.

References II

Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehlé, D. (2017).
CRYSTALS – Dilithium: Digital signatures from module lattices.
Cryptology ePrint Archive, Paper 2017/633.

et al., J. B. (2018).
CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM.
In *IEEE European Symposium on Security and Privacy*, pages 353–367, London, UK.

et al., P.-A. F. (2020).
FALCON: Fast-fourier lattice-based compact signatures over NTRU.
`https://falcon-sign.info/`.
(accessed on 15 February 2025).

References III

Lyubashevsky, V. and Nguyen, N. K. (2022).
Bloom: bimodal lattice one-out-of-many proofs and applications.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 95–125. Springer.

Lyubashevsky, V., Peikert, C., and Regev, O. (2013a).
On ideal lattices and learning with errors over rings.
Journal of the ACM, 60(6):43:1–43:35.
Preliminary version in Eurocrypt 2010.

Lyubashevsky, V., Peikert, C., and Regev, O. (2013b).
A toolkit for ring-LWE cryptography.
In Johansson, T. and Nguyen, P. Q., editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 35–54. Springer, Heidelberg.

References IV

Micciancio, D. (2007).
Generalized compact knapsacks, cyclic lattices, and efficient one-way functions.
Computational Complexity, 16:365–411.

Peikert, C. (2016).
How (not) to instantiate ring-lwe.
In *International Conference on Security and Cryptography for Networks*, pages 411–430. Springer.

Regev, O. (2009).
On lattices, learning with errors, random linear codes, and cryptography.
Journal of the ACM, 56(6):1–40.
Preliminary version in STOC 2005.