INFO-F514
Protocols, cryptanalysis and mathematical cryptology
Plan

Mickael Kovel, Dan Adewuyi, Djonfang Tchuangue Vitaly, Peetroons Simon, Preda Patrick

February 22, 2025

1 Subject

Nowadays, the security of our data is a major concern. With the rise of quantum computers, the security of our data is at risk. We need to find new ways to encrypt our data. Moreover, we need to be able to perform operations on encrypted data. This is where homomorphic encryption comes in. As seen in the course, lattice-based encryption is a good candidate homomorphic encryption, and it turns out that it is also a good candidate for post-quantum encryption. In this project, we will study lattice-based encryption and its applications.

2 Plan

We plan to study :

- Why do we need post quantum and homomorphic encryption ? (Mickael)
- What is lattice scheme encryption ? (Patrick)
- Why is it a good candidate for post quantum encryption and homomorphic encryption ? (Mickael)
- How does it work ? (Patrick)
- What applications can we find for this encryption ? (Simon)
- Implement some examples of lattice scheme encryption to compare with the results of the paper.(Dan)

3 Sources

- Post-Quantum Lattice-Based Cryptography Implementations: A Survey [1]
- A Survey on Homomorphic Encryption Schemes: Theory and Implementation [2]
- ML Confidential: Machine Learning on Encrypted Data [3]
- Fully homomorphic encryption using ideal lattices [4]

References

[1] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations: A survey. *ACM Comput. Surv.*, 51(6), January 2019.

[2] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv.*, 51(4), July 2018.

[3] Thore Graepel, Kristin Lauter, and Michael Naehrig. Ml confidential: Machine learning on encrypted data. pages 1–21, 2013.

[4] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery.