Politecnico di Torino

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

MATHEMATICAL SCIENCES

DM 630/Telsy - Post-Quantum Security Aspects of Fully Homomorphic Encryption

Funded By	TELSY SPA [P.iva/CF:00737690016] MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584]
Supervisor	BAZZANELLA DANILO - danilo.bazzanella@polito.it
Contact	MORGARI GUGLIELMO - guglielmo.morgari@polito.it
Context of the research activity	The main cryptographic techniques used today allow users to protect data-at-rest or data-in-transit, but security is not guaranteed when we consider data-in-use. In fact, to be able to fully leverage external computing resources such as Cloud Service Providers, users must give them access to cleartext data, compromising data privacy. There is hence the need for Fully Homomorphic Encryption (FHE) schemes, that allow to arbitrarily process data while encrypted, guaranteeing their confidentiality. Progetto finanziato dal PNRR a valere sul DM 630/2024 - CUP E14D24002470004
	The research program aims at the study and development of cryptographic schemes in the field of Fully Homomorphic Encryption (FHE). A fundamental step towards the analysis of the current state-of-the-art will be the study of the mathematical problems, such as the Learning With Error problem, that constitute the security of most FHE schemes (such as TFHE [1] and CKKS [2]), but that are also at the basis of many Post-Quantum Cryptography (PQC) schemes [3]. The work done in further investigating the security assumptions of such problems could prove to be extremely useful both for FHE and PQC schemes, helping in guaranteeing the security of the cryptosystems even with respect to an adversary in possession of a Cryptographically Relevant Quantum Computer. Apart from analyzing the mathematical problems that guarantee the security of FHE and PQC schemes, the candidate will focus on the state-of-the-art of Fully Homomorphic Encryption, studying the main FHE schemes that have been proposed since 2009, when Craig Gentry's seminal work [4][5] proved that FHE was possible. In particular, the analysis will focus on the mathematical description of the schemes and their security (specifically in the PQC context), together with implementation aspects such as performance, complexity and resistance against known attacks. In order to do so, the

Objectives	candidate will also focus on the study of the main cryptographic libraries and tools that are currently used to implement Fully Homomorphic Encryption schemes. Another objective is to overcome the main shortcomings of FHE, mostly related to the very high computational overhead, especially when compared with cleartext operations. To better understand the requirements and constraints that FHE schemes should satisfy, the research activity will also include an in-depth analysis of the main use case scenarios where FHE could help in improving users' privacy while allowing them to leverage the computational resources of Cloud environments. In particular, the research program aims at identifying the main application scenarios where the security properties of FHE could become fundamental to guarantee compliance with privacy regulations (e.g., GDPR) and allow secure collaboration among different entities, without any risks for the confidentiality of the exchanged data. Some examples of use case scenarios for which the use of FHE could be transformative are Cloud platforms, training and inference for Machine Learning models and supply chain. A particular focus will be put on the analysis of the impact that a Cryptographically Relevant Quantum Computer will have on the above-mentioned scenarios. Building on the knowledge derived from this analysis, the research program aims at improving the existing schemes or developing new cryptosystems that can conjugate strong quantum resistant security with high performance, fostering the adoption of FHE schemes in the considered use case scenarios. The research project could also include the implementation of the proposed cryptosystems on different platforms, so to allow for more precise analyses of their performance and security. The activities of this research program will be carried out in close collaboration with Telsy, the Competence Centre for Cryptography and Cybersecurity within the TIM-Telecom Italia group, with more than 50 years of experience in the field of the design and implementation of cryptography algorithms and protocols. The candidate will be able to leverage Telsy's vast knowledge in both theoretical and implementation aspects of cryptography in order to reach the main objectives of the present research project. The relationship with the company will allow the candidate to spend one year of the PhD program in Telsy's offices, closely collaborating with Telsy Cryptography Research Group. References [1] Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2020). TFHE: fast fully homomorphic encryption over the torus. Journal of Cryptology, 33(1), 34-91. [2] Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In Advances in Cryptology –ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23 (pp. 409-437). Springer International Publishing. [3] https://csrc.nist.gov/projects/post-quantum-cryptography [4] C. Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st ACM Symposium on Theory of Computing – STOC 2009, pages 169–178. ACM, 2009. [5] C. Gentry. Toward basing fully homomorphic encryption on worst-case hardness. In T. Rabin, editor, Advances in Cryptology - CRYPTO 2010, volume 6223 of Lecture Notes in Computer Science, pages 116–137. Springer, 2010.

	The candidate should have a background in Mathematics or Computer

Skills and competencies for the development of the activity	Science relevant to the research activity. Additional preference requirements are familiarity with cryptographic schemes, Algebra, Number Theory and knowledge of the mathematical foundations of novel cryptographic techniques such as Fully Homomorphic Encryption and Post Quantum Cryptography. Nice-to-have: programming skills and knowledge of implementation aspects of cryptographic primitives.