Expression of interest

Contact details

Country	TURKEY
Name of the organisation	SABANCI UNIVERSITY
Name of the contact	Erkay SAVAS
Phone	+90 216 483 9501
Email	erkays@sabanciuniv.edu

Short description of the organisation/researcher/research group
Provide a short description of the equipment available, the relations with the industry, the profile of the main researchers

Established in 1996, Sabanci University (SU) in Istanbul, Turkey ranks among the highly rated research institutions in Turkey. The University employs more than 700 staff members and teaches to 4100 undergraduate and 1100 graduate students. SU is consistently ranked among the top three universities in Turkey and is currently ranked 44 in the Times Higher Education Young University Rankings. According to the Entrepreneurial and Innovative University Index of the Scientific and Technological Research Council of Turkey (TUBITAK), SU has been internationally recognized as one of the most innovative and research-oriented universities in Turkey.

At the national level, SU has received the highest number of EU funded projects per faculty member, taking part in 20 FP6 projects, 53 FP7 projects including 37 Marie Curie Grants, 12 Cooperation Projects and 4 Capacities Projects. In H2020 SU has been involved in 13 funded projects with a total partner budget of 1,9 M €. SU also has a commendable performance in the EU funded education programs, with 5 Jean Monnet European Modules, 3 Jean Monnet Chairs ad personam and 1 Jean Monnet Centre of Excellence. These European grants constitute about 18% of the SU's total budget for research. In Horizon 2021, Sabancı University has received 7,9 Million Euro EU contribution with its 40 funded projects. In terms of Collaborative projects SU has 27 projects with a total budget of 4 Million euro.

SU is the pioneering university of Turkey in the areas of software testing, cybersecurity, and cryptography. Both the Software Engineering Research Group (SUSOFT) and the Cryptography and Information Security (CISEC) Group of Sabancı University have a wide range of research and development expertise in software engineering, cryptographic security, and cyber security areas. Both groups have conducted and been involved in several privately and publicly funded projects and co-authored publications in the areas of software engineering, software testing, data-driven dynamic program analysis, static program analysis, software/system security, applied cryptography, IoT and Wireless System Security, cryptographic engineering, privacy-enhanced technologies, cyber incident detection and remediation, security in networked-systems.

Prof. Erkay Savaş is an expert in the fields of cryptography, data and communication security, privacy in biometrics, trusted computing, security and privacy in data mining applications, embedded systems security, and distributed systems. He is the director of the **Cryptography and Information Security Group (CISec)** of Sabanci University. He published many articles (**scholar**) in cryptographic engineering and applications of security and cryptography at prestigious international journals and proceedings of conferences and workshops including IEEE Transactions on Computers, IEEE Proceedings Computers and Digital Techniques, Data and Knowledge Engineering, Cryptographic Hardware and Embedded Systems. He is a member of IEEE, ACM, the IEEE Computer Society, and the International Association of Cryptologic Research (IACR).

Specific skills and proposed activities related to the topic
Indicate the specific skills and competence in relation with « HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography ” topic

- **Prof. Savas** can directly contribute to the following expected outputs of the projects:

- Measuring, assessing and standardizing/certifying future-proof cryptography

Prof. Savas can collaborate with researchers who have expertise in quantum algorithms that can be used to attack post-quantum cryptographic primitives to assess the feasibility and practicality of such attacks in terms of computation power, memory and other resources. This way, he can contribute to choosing the correct security parameters for a given cryptographic algorithm family such as key length, which provides sufficient security against quantum and classical computer attacks. He can provide highly accurate assessment of the implementation budget of future-proof cryptography in terms of hardware footprint and other resources, which is one of the determining factors in the standardization process.

- Addressing gaps between the theoretical possibilities offered by quantum resistant cryptography and its practical implementations

Prof. Savas can develop algorithms, techniques, methods, and hardware architectures for secure, lightweight and efficient implementations of post-quantum cryptography algorithms. These endeavors serve to measure and asses the feasibility of using quantum resistant cryptography algorithms in a wide range of applications with different requirements and constraints such as high speed, low power, and area efficient. He can also develop techniques to protect the implementations against powerful attacks such as various types of side-channel and fault attacks. He will develop test infrastructure to test the actual strength of the implementations against these attacks.

- Quantum resistant cryptographic primitives and protocols encompassed in security solutions

He can devise security solutions using quantum-resistant cryptographic primitives and protocols that can realize not only classical security services such as

confidentiality, integrity, authentication, and non-repudiation but also advanced security properties such as forward secrecy and plausible deniability, which are increasingly sought after in messaging applications. His expertise in lattice-based homomorphic encryption algorithms, which are also quantum resistant, will be instrumental for other upcoming popular applications in the area of privacy enhancing technologies.

- Solutions and methods that could be used to migrate from current cryptography towards future-proof cryptography

Prof. Savas will develop a migration strategy that consists of two phases. In the first phase, he envisions a transition to hybrid systems, in which both classical and quantum resistant cryptographic primitives are used. The envisioned hybrid cryptographic solutions are compromised only when both classical and quantum resistant primitives are broken. The second transition phase, which is the migration to security solutions using only quantum resistant cryptographic primitives, can start only when the latter primitives reach cryptographic maturity that is on par with the current strength of the classical cryptographic primitives against classical computer attacks. A clear and detailed plan is needed for smooth migration as there may exist aggravated security risks that can be managed with careful planning.

- Preparedness for secure information exchange and processing in the advent of large-scale quantum attacks

Secure, fast and efficient implementations of quantum resistant cryptographic primitives and protocols and clear and well-documented plan for the migration to future-proof cryptography are two important imperatives for protecting information exchange and processing against large-scale quantum attacks. Also, lessons and experience gained from the actual deployment of quantum-resistant cryptography in real-world use case scenarios and all germane challenges in the process are also needed for the said preparedness. Prof. Savas can engage and collaborate with one of the largest manufacturers of household appliances in Turkey and Europe for the deployment of quantum resistant cryptography in IoT use case scenario. Such large-scale deployment in resource-constrained devices will provide unique set of best practices for the deployment in the other areas and enhance our level of preparedness against quantum attacks.

References

Previous research projects on the national/international level
Related articles

Project acronym / starting date	**Main objectives**	**Main activities**	**Role in the project**

Twinning towards excellence for Privacy Enhancing Technologies leveraging Homomorphic Encryption / HORIZON-WIDERA-2021-ACCESS-03-01 – Twinning / 2022- …	The enCRYPTON project is to increase the innovation capacity of SÜ and enhance the consortium's scientific quality and research excellence within PET.	Data privacy management, identity management (personal privacy) and data that is commercially sensitive or related to national security are huge concerns and it is important for organisations to safeguard their data from hackers. Organisations might be keen to share data but want to restrict whom they are sharing information with and what information they want to share	PI
Implementations of Lattice-Based Cryptographic Arithmetic Blocks and Their Utilization in Homomorphic Encryption Applications / TÜBİTAK 118E725 / 2019-…	Lattice-based next-generation cryptographic building blocks and advanced cryptographic algorithms built on top of them, and studies have been carried out on applications.	In homomorphic encryption, an operation is performed on the encrypted data and the result is obtained in encrypted form. Precise and confidential data is encrypted in this way, unauthorized access to them will be prevented and the beneficial use of the data will be increased by making the desired operations on the encrypted data securely.	PI
Secure and Privacy-Preserving Management and Processing of Big Data using NoSQL Data Stores, TÜBİTAK 113E537, 2014-2016.	Security and privacy during the management and processing of big data A number of techniques, methods, algorithms and protocols have been studied that protect/increase	Authorized users, according to their authorization, can access, modify and process remote big data. The proposed system The most important difference is that while all these operations are being done, big data and related metadata/index data are always remains encrypted, it is kept encrypted in any case in a semi-trusted environment.	PI

Related articles

1. K Derya, AC Mert, E Öztürk, and E Savaş (2022) "CoHA-NTT: A Configurable Hardware Accelerator for NTT-based Polynomial Multiplication", Microprocessors and Microsystems, 89, 1044-51.
2. F Yarman, AC Mert, E Öztürk and E Savaş (2021) "A hardware accelerator for polynomial multiplication operation of CRYSTALS-KYBER PQC scheme", Design,

Automation & Test in Europe Conference & Exhibition, https://eprint.iacr.org/2021/485
3. L. Karaçay, E. Savaş, H. Alptekin, (2020) “Intrusion Detection Over Encrypted Network Data”, The Computer Journal, Volume 63, Issue 4, April 2020, Pages 604–619, https://doi.org/10.1093/comjnl/bxz111
4. AC Mert, Öztürk, E. and Savaş, E. (2020) "FPGA implementation of a run-time configurable NTT-based polynomial multiplication hardware", Microprocessors and Microsystems, Vol.78. https://doi.org/10.1016/j.micpro.2020.103219
5. AC Mert, E Karabulut, E Öztürk, E Savaş, M Becchi, and A Aysu, (2020) “A flexible and scalable NTT hardware: applications from homomorphically encrypted deep learning to post-quantum cryptography” Design, Automation & Test in Europe Conference & Exhibition (DATE), 346-351, 10.23919/DATE48585.2020.9116470
6. C. Mert, E. Öztürk and E. Savaş, "Design and Implementation of Encryption/ Decryption Architectures for BFV Homomorphic Encryption Scheme," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 353-362, Feb. 2020, doi: 10.1109/TVLSI.2019.2943127