Title: Post-quantum secure cryptographic schemes (FTP20)

Participant name: Panayiota Smyrli

Educational Institution: CYNET

Keywords: Post-quantum cryptography, code-based cryptosystems, computational syndrome decoding problem, quantum resistant assumptions, random linear codes.

Short Biography / Short Introduction of the Idea:

Panayiota is a PhD candidate in Post-Quantum Cryptography and Cyber Security Analyst at CYNET-CSIRT. Her research interests focus on cognitive areas of Cryptography and Network Security, as well as their applications in Computer Science and Telecommunications. The actualization of doctoral studies in this interdisciplinary field, stemmed from her postgraduate training and predominantly her M.Sc. thesis that concerned the study of code-based public key cryptosystems.

More precisely, she is actively involved in state-of-the-art techniques and she has been dedicated to further investigate the resilience of code-based cryptosystems, in light of the existence of quantum algorithms and new ones that will be developed. This is the main objective of her research, which by using techniques from Number/Coding/Lattice Theory, Algebra and other related areas, will lead to new constructions, with more effective ways of decoding, smaller key sizes and larger security margins.

Short Introduction of the Idea:

Recent advancements in quantum computing have brought about fundamental challenges to cryptography. The security of many classical cryptographic schemes, such as the digital signature algorithm (DSA), the Diffie-Hellman (DH) key exchange protocol, and their elliptic curve variants, relies on the hardness of the well-known discrete logarithm problem over cyclic groups in elliptic curves over finite fields. Furthermore, the security of RSA-based cryptosystems relies critically on the difficulty of factoring large numbers. Thanks to Shor's quantum factoring algorithm and the progressing maturity of quantum computing, these asymmetric cryptographic systems are now known to be vulnerable to attack by sufficiently powerful quantum computers. The fact that the currently available security protocols and mechanisms critically depend on the above cryptographic schemes, necessitates the design of new cryptographic primitives in the post-quantum era that rely on quantum-resistant hardness assumptions. Post-quantum schemes that have been proposed in the literature can be classified as lattice-based, code-based, hash-based, multivariate-based, and isogeny-based.

Especially, for some modified code-based constructions, such as the McEliece and Niederreiter encryption schemes, not only has it been impossible to design efficient quantum algorithms thus far, but there are also serious indications demonstrating that it would not be possible to use powerful techniques, such as quantum Fourier sampling, in the foreseeable future. This renders code-based cryptography to one of the most promising research fields in post-quantum cryptography.

The security of essentially all code-based cryptographic constructions relies on the conjectured intractability of the Computational Syndrome Decoding (CSD) problem for random linear codes. The CSD problem is one of the most fundamental combinatorial problems in the field of coding theory. Besides its relevance to the security of code-based cryptographic constructions, the average-case hardness of the CSD problem or equivalently the hardness of decoding random linear codes has been of profound importance in coding theory, in general. This sufficiently motivates the main objective of this work. Closely related to decoding random linear codes is the Learning Parity with Noise (LPN) problem and its generalization to codes over a larger field, the so-called Learning Parity with Errors (LWE) problem.