Università Politecnica delle Marche

Scuola di Dottorato in Scienze dell'Ingegneria

RESEARCH SEMINARS

Thursday 1 December 2022, 11:30 a.m.
Information Engineering Department (DII) library (q. 165)
Università Politecnica delle Marche

On a link between Code-Based and Multivariate-Based Cryptosystems

Dr. Alessio Meneghetti
Università di Trento

Abstract
The two most known algebraic problems underlying code-based and multivariate based cryptographic schemes are respectively the Maximum Likelihood Decoding Problem (MLD) and the Multivariate Quadratic Problem (MQ). Both were proved to be computationally hard problems: in particular, MLD has been proven to be NP-complete in 1978 by Berlekamp, McEliece and van Tilborg, while MQ has been proven NP-hard in 1979 by Garey and Johnson.
In 1977, Berman and Hartmanis formalised the concept of polynomial-time reduction, and then they formulated a conjecture on the equivalence between NP-complete problems. A related problem is the construction of explicit reductions between NP-hard problems.
In this talk we present an explicit polynomial-time map between MLD and MQ from which it is possible to derive the equivalence of the two problems, and therefore the possibility of studying code-based cryptosystems via methods from commutative algebra and vice-versa.

Towards a Post-Quantum OTS Scheme using QC-LDPC Codes

Mr. Giovanni Tognolini
Università di Trento

Abstract
We present a novel post-quantum code-based digital signature algorithm whose security is based on the difficulty of decoding Quasi-Cyclic codes in systematic form, and whose trapdoor relies on the knowledge of a hidden Quasi-Cyclic Low-Density-Parity-Check (QC-LDPC) code. The utilization of Quasi-Cyclic (QC) codes allows us to balance between security and key size, while the LDPC property lighten the encoding complexity, thus the signing algorithm complexity, significantly.
In this talk we present the scheme, prove its correctness and discuss possible vulnerabilities related to the utilisation of the scheme for multiple signatures.

All interested people are invited to participate

For further information please contact Prof. Marco Baldi (m.baldi@univpm.it)