UNIVERSITÀ POLITECNICA DELLE MARCHE

Dipartimento Ingegneria Informazione

Seminar Announcement

Wednesday May 7, 14:30
Engineering building, room 140/3

Error-correcting codes as a Swiss knife: information theory, telecommunications, magic tricks, post-quantum crypto...

Jean-Christophe Deneuville
Ecole Nationale de l'Aviation Civile

From its genesis to more recent applications such as post-quantum cryptography, this lecture traces the winding path of coding theory. We will go over the information-theoretic notions introduced by Shannon almost 80 years ago, and give a few examples of codes and decoding algorithms. Ubiquitous, we will mention their use in telecommunication, computers, ... but also in some magic tricks. Back to serious topics, we will see that some problems in coding theory are particularly difficult, which we will use to build cryptographic primitives, McEliece's scheme (1978) in particular. After having covered its security as well as its comparison to other schemes, we'll give an in-depth presentation of the HQC scheme, recently chosen by the US NIST institute for standardization. We will conclude this lecture with some open research problems concerning codes, cryptography and cryptography based on error-correcting codes.

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

Supported by the Italian Ministry of University and Research (MUR) under the "Quantum-safe cryptographic tools for the protection of national data and information technology assets" (QSAFEIT) project - No. FISA 2022-00618 (CUP I33C24000520001), Grant Assignment Decree no. 15461 adopted on 02.08.2024, funded by MUR under the Italian Fund for Applied Sciences (FISA), year 2022, "Information and Communication Technology" area.