Institut
Grand-Ducal
Section des Sciences

Scientific communication session

'Cryptography: From Ancient Ciphers to the Post-Quantum Era'

Prof. Jean-Sébastien CORON, University of Luxembourg

November 28 2024

- **University of Luxembourg, Belval**
- **Maison des Nombres, room MNO 1.040**
- **18h30-20h00, in English**
- **Open to the large public**
- **No registration necessary**

Jean-Sébastien Coron is a former student of the Ecole Normale Supérieure in France. He is professor in computer science at the University of Luxembourg, where he is leading the Applied Crypto Group (ACG) in the Computer Science department. His research interests include fully-homomorphic encryption, and side-channel attacks and countermeasures.

Abstract

This talk provides an introduction to cryptography, tracing its evolution from early techniques to modern developments in the post-quantum era. We will explore early cryptographic methods like mono-alphabetic ciphers and the one-time pad, before transitioning to classical cryptography with a focus on block ciphers like DES and AES. The session will also cover public-key cryptography, which secures today's internet, highlighting RSA encryption and RSA-based digital signatures. Finally, we will mention the emerging challenge of quantum computing and the ongoing efforts to develop post-quantum cryptographic solutions.

With the finacial support of :

Luxembourg National Research Fund

With the support of :

uni.lu FACULTY OF SCIENCE, TECHNOLOGY AND MEDICINE