DE CIFRIS TRENDS IN MODERN CRYPTOGRAPHY

THE FRENCH MAGISTERIUM

Trends Autumn 2024

ORGANIZERS (University of Trento and De Cifris):
Massimiliano Sala and Alessio Meneghetti

Lessons (20 recorded videos on Our YouTube Channel):

The French Magisterium

Algebraic Cryptanalysis
Side-Channel Attacks
Symmetric Cryptography
Lightweight Cryptography
Post-quantum Cryptography
Homomorphic Encryption
Multi-Party Computation in the Head
and much more …
(see next page)

Certificate

Online course with certificate (with exam)

For more information

https://www.decifris.it/trends24
alessio.meneghetti@unitn.it

To sign up:

send an email to trends@decifris.it
within 1st September 2024

UNIVERSITÀ DI TRENTO
Dipartimento di Matematica

Lecturing:

9th September - 30th November 2024

DE CIFRIS TRENDS IN MODERN CRYPTOGRAPHY
THE FRENCH MAGISTERIUM

Twenty leading professors and researchers will show us the top of French cryptographic research.

- *Magali Bardet (University of Rouen, France)*
  Polynomial System Solving and Application to Algebraic **Cryptanalysis**
- *Sonia Belaid (Crypto-expert, Paris, France)*
  Side-Channel **Attacks** and Masking Countermeasures
- *Jean-Francois Biasse (Center for Cryptographic Research, USF, USA)*
  The Code Equivalence Problem and its Applications to Cryptography
- *Christina Boura (University of Versailles, France)*
  Tools for **cryptanalysis** of symmetric primitives
- *Sébastien Canard (Telecom Paris- Saclay, France)*
  Cryptography for anonymity and accountability
- *Anne Canteaut (INRIA Paris, France)*
  Lightweight symmetric primitives
- *Claude Carlet (Universities of Bergen and Paris 8, France)*
  The Almost Perfect Nonlinearity of Substitution Boxes and its Consequences;
- *Léo Ducas (Centrum Wiskunde Informatica (CWI), Amsterdam, Netherlands)*
  Lattice-based Cryptography (I)
- *Philippe Gaborit (University of Limoges, France)*
  Code-based Cryptography with Rank Metric
- *Louis Goubin (University of Versailles, France)*
  Diving into Multivariate Cryptography
- *Adeline Roux-Langlois (GREYC, CNRS, Unicaen, Ensicaen, Caen, France)*
  Hardness of the Module Learning With Errors Problem
- *Alice Pellet-Mary (University of Bordeaux, France)*
  Lattice-based Cryptography (II)
- *Sihem Mesnager (Universities of Paris VIII and Sorbonne North, France)*
  Algebraic aspects in designing cryptographic functions in symmetric cryptography
- *Pierrick Meaux (University of Luxembourg, Luxembourg)*
  Hybrid Homomorphic Encryption
- *Ludovic Perret (University of Paris VII, France)*
  The Transition to Post-Quantum Cryptography
- *Léo Perrin (INRIA Paris, France)*
  Symmetric Techniques for Advanced Protocols: Design Strategies, and **Cryptanalysis**
- *Damien Stehlé (ENS Lyon, France)*
  Fully Homomorphic Encryption
- *Serge Vaudenay (EPFL Switzerland)*
  Anonymous Tokens
- *Damien Vergnaud (Sorbonne University, France)*
  Multi-Party Computation in the Head: Techniques and Applications
- *Giles Zémor (University of Bordeaux, France)*
  The Alekhnovich cryptosystem: code-based cryptography with security proofs

We are indebted to Prof. *Sihem Mesnager* for her excellent management.