UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

DIPARTIMENTO DI
INFORMATICA, SISTEMISTICA E
COMUNICAZIONE

Viale Sarca, 336
20126 Milano

SEMINAR ANNOUNCEMENT

Wednesday, 4th December 2024

at 10:00 am
Room "Sala Seminari" - Abacus Building (U14)

Are Cellular Automata of any use to Cryptography?

Speaker
Dr Luca Mariot
University of Twente (The Netherlands)

Abstract
During the past 40 years, Cellular Automata (CA) have been extensively used in cryptographic applications, including pseudorandom number generation and symmetric primitives. However, most of the research seems to be published in non-cryptographic venues, which raises a legitimate question: are CA of any relevance to cryptographers nowadays? This talk recollects the experience of the speaker while doing research in CA-based cryptography for the past 10 years, identifying some common pitfalls in this field along with some recommendations for future research. The talk also focuses on the observation that researchers working in the CA and cryptography communities often tackle similar problems, although under different terminologies. Hopefully, acknowledging and discussing this fact could help bridging the two research communities, and open up possibilities for future cross-community collaborations.

Short bio
Luca Mariot is an assistant professor at the University of Twente, The Netherlands. His main research interests lie at the intersection of cryptography and artificial intelligence, specifically focusing on nature-inspired computational models and optimization techniques for designing cryptographic primitives. Previously, Luca was a postdoc researcher at Radboud University and TU Delft, the Netherlands, and at the University of Milano-Bicocca, Italy. He received his PhD in Computer Science under a double degree agreement, from the University of Milano-Bicocca and the Université Côte d'Azur, France. Up to now, Luca published more than 60 peer-reviewed papers in various journals and conferences related to cryptography and natural computing, and served in the program committees of more than ten conferences and workshops.