OIST OKINAWA INSTITUTE OF SCIENCE AND TECHNOLOGY
沖縄科学技術大学院大学

VISITING PROGRAM

TSVP TALK

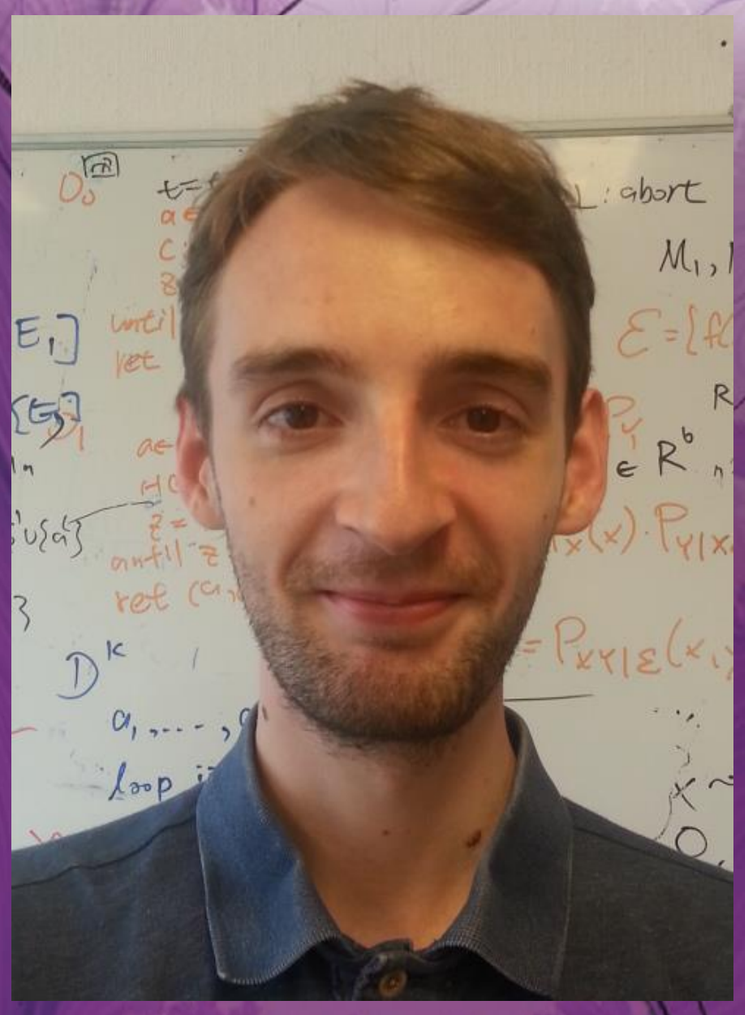
Quantum Cryptanalysis: An Algorithmic Perspective

2026 Thu. **Feb. 26**

11:00–12:00

HYBRID L5D23, ZOOM

For zoom and other details scan the QR code or visit oist.jp/visiting-program



Quantum computing is an enhanced model of computation, powered by dedicated devices which are still being actively developed. One of the scientific domains which is the most impacted by quantum computers - even the mere possibility of them - is cryptography. Indeed, the foundation of modern cryptography is computational hardness of well-studied mathematical problems, and quantum computers appear to be surprisingly good at solving some of them.

This talk will summarize how quantum algorithms reshape the security assumptions in cryptography, from Shor's algorithm - the most impactful one - and its most recent iterations, to Grover's algorithm - the most generic, with some peculiar other examples in-between.

The Inria Centre at Rennes University

André Schrottenloher

André Schrottenloher is a full-time researcher at the Inria Center at the University of Rennes, France. He completed his PhD thesis in 2021 at the Inria Center of Paris and was a post-doctoral researcher at CWI in Amsterdam between 2021 and 2022. His main research interest is the application of quantum algorithms to cryptanalysis, both in secret-key cryptography and public-key cryptography.

oist.jp/visiting-program

CONTACT Office of the Dean of Research tsvp@oist.jp