2 Best Papers EUROCRYPT 2024

Kongresssaal

Marc Joye and Gregor Leander

Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis

Itai Dinur

(paper #326)

Show abstract ›

PART 3: New Dimensions

SQIsignHD: New Dimensions in Cryptography

Pierrick Dartois, Antonin Leroux, Damien Robert, Benjamin Wesolowski

INRIA, IMB, DGA-MI, ENS de Lyon, CNRS, UMPA

Speaker(s): Pierrick Dartois

(paper #149)

Show abstract ›

AprèsSQI: Extra Fast Verification for SQIsign Using Extension-Field Signing

Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, Krijn Reijnders

University College London, NTNU, University of Regensburg, Radboud University Nijmegen

Speaker(s): Jonathan Komada Eriksen

(paper #86)

Show abstract ›

PART 3

New Dimensions

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

SQIsign2

A new algorithm to translate ideals to isogenies.

2020 | 2021 | 2022 | 2023 | 2024

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

SQIsignHD

Use the SIKE attacks! Represent the response as a **HD isogeny**. Required 4/8-dimensions.