3 Best Papers ASIACRYPT 2024?

Awarded Papers

Kongresssaal

Marc Joye and Gregor Leander

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

Speaker(s): Itai Dinur

(paper #326)

Show abstract ›

PART 4: 2D Future?

SQIsign2D-West: The Fast, the Small, and the Safer

Andrea Basso,Pierrick Dartois,Luca De Feo,Antonin Leroux,Luciano Maino,Giacomo Pope,Damien Robert, Benjamin Wesolowski

SQIsign2D-East

Kohei Nakagawa, Hiroshi Onuki

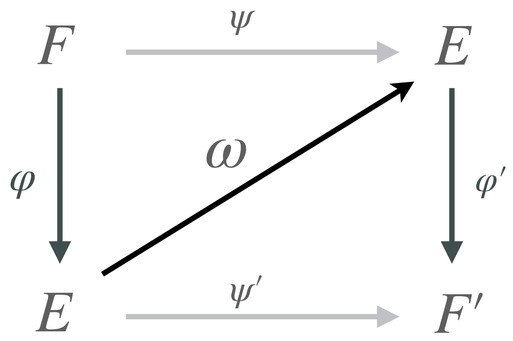
SQIPrime: a Dimension 2 Variant of SQIsignHD with Non-Smooth Challenge Isogenies

Max Duparc, Tako Boris Fouotsa

PART 4

2D Future

Nakagawa - Onuki trick (2023)



say we want to create such
a square, but we only have E
and some $\omega \in \mathrm{End}(E)$
of degree $q(2^a - q)$

we can find a suitable isogeny
$\varphi : F \to E$ using Kani!!!