

# Best Paper ASIACRYPT 2020

Best Paper award ⓘ 📅

YouTube

Chat

Chair: Shiho Moriai & Huaxiong Wang

Finding Collisions in a Quantum World: Quantum Black-Box Separation of Collision-Resistance and One-Wayness

[Show abstract ›](#)

# PART 1: SQIsign

New results on Gimli: full-permutation distinguishers and improved collisions

[Show abstract ›](#)

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras

Inria, France

Media: 📄

**SQISign: Compact Post-Quantum signatures from Quaternions and Isogenies**

[Show abstract ›](#)

Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, Benjamin Wesolowski

IBM Research, Zurich; Université Aix-Marseilles; DGA, Ecole Polytechnique; University of Birmingham; Université de

Bordeaux, CNRS

Media: 📄

# PART 1

## SQLsign

### SQLsign

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

2020

2021

2022

2023

2024