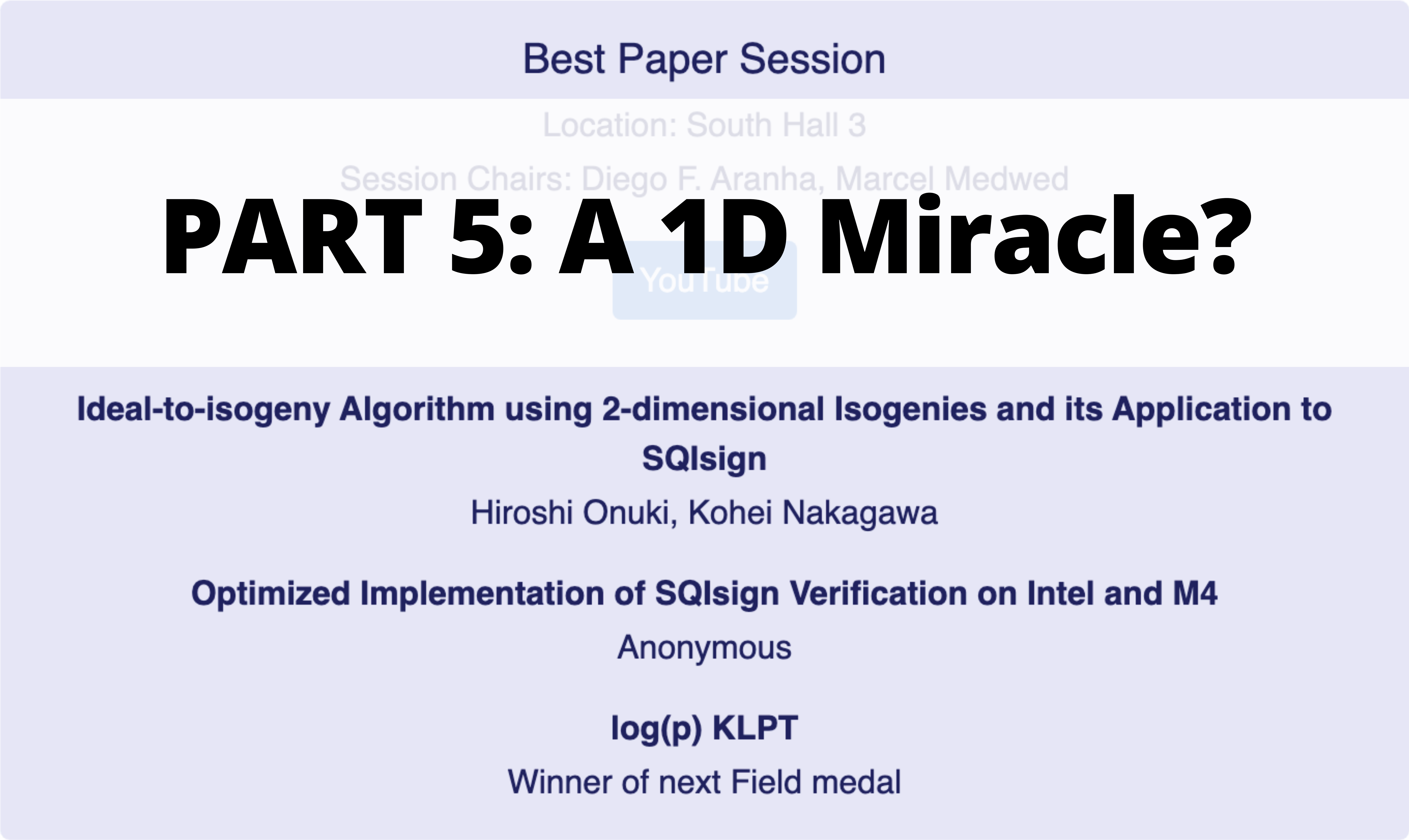
More Best Papers??

PART 5: A 1D Miracle?



Best Paper Session

Location: South Hall 3

Session Chairs: Diego F. Aranha, Marcel Medwed

Ideal-to-isogeny Algorithm using 2-dimensional Isogenies and its Application to SQIsign

Hiroshi Onuki, Kohei Nakagawa

Optimized Implementation of SQIsign Verification on Intel and M4

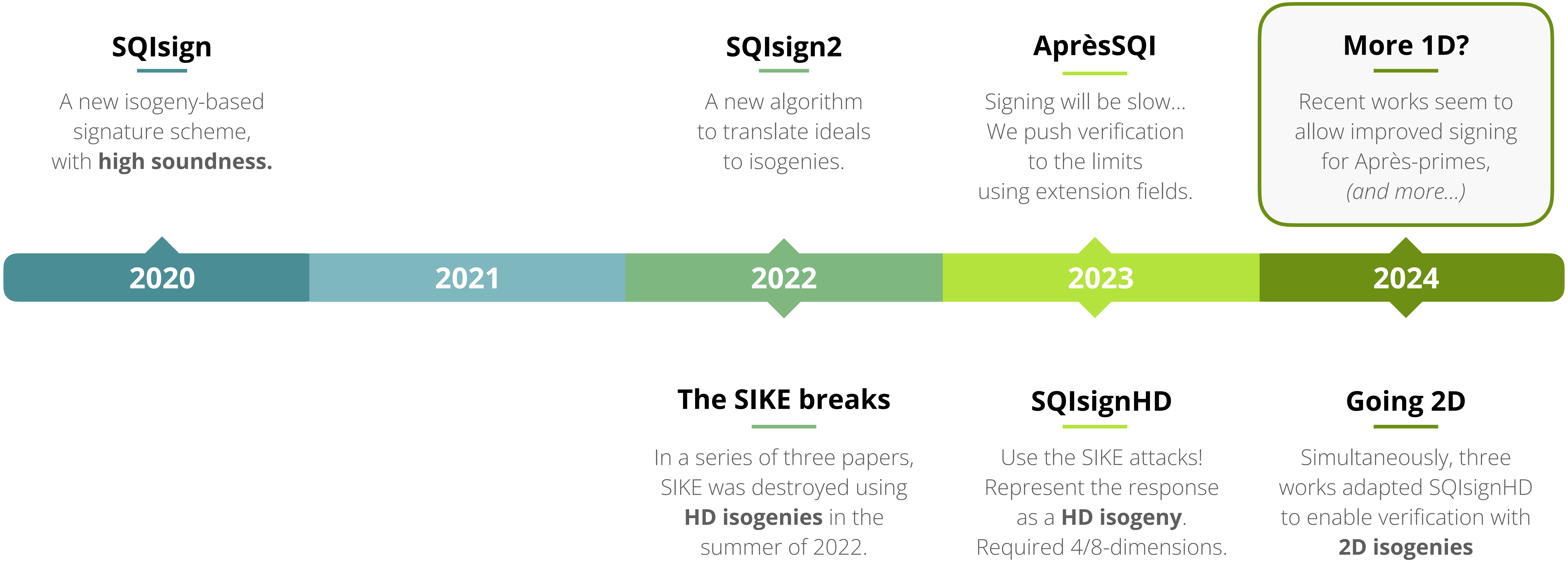
Anonymous

log(p) KLPT

Winner of next Field medal

PART 5

A 1D Miracle?



SQIsign

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

2020

2021

SQIsign2

A new algorithm to translate ideals to isogenies.

2022

The SIKE breaks

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

AprèsSQI

Signing will be slow... We push verification to the limits using extension fields.

2023

SQIsignHD

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

More 1D?

Recent works seem to allow improved signing for Après-primes, *(and more...)*

2024

Going 2D

Simultaneously, three works adapted SQIsignHD to enable verification with **2D isogenies**