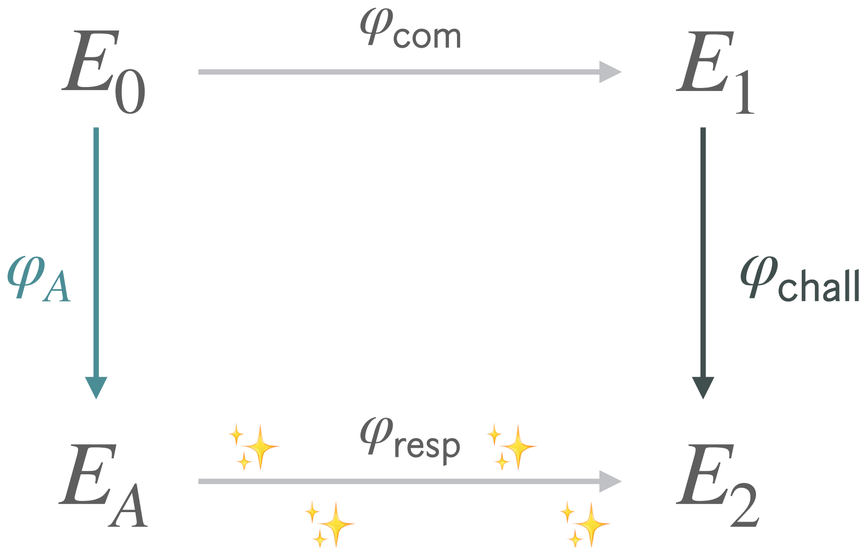
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✘ **signing is now even slower, using extension fields, takes literal seconds**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

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