

PART 5 A 1D Miracle?

Remember this slide?

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!



PART 5 A 1D Miracle?

Remember this slide?

1

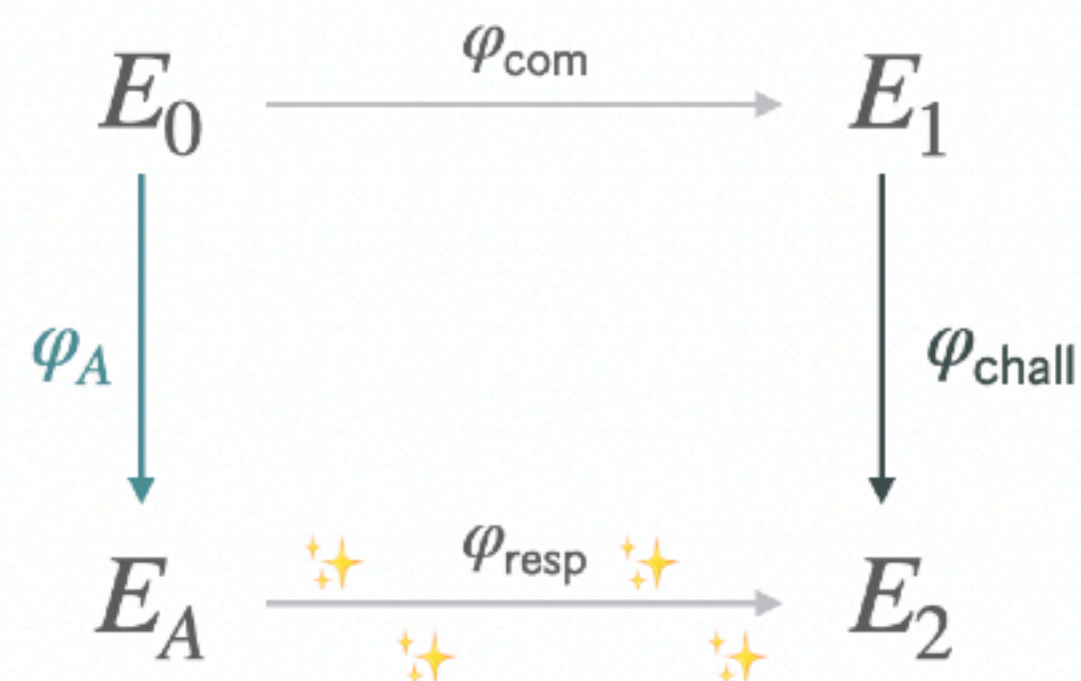
2024/778 shows
much more practical
signing procedure for 1D
using 2D-isogenies 🤖

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 now seems somewhat OK,
better than NIST SQIsign,
but not yet as fast as 2D-West,



faster
primes!



fewer
blocks!



FAST
verification!

Radboud University



Radboud University



[2024/778]: Hiroshi Onuki, Kohei Nakagawa “*Ideal-to-isogeny algorithm
using 2-dimensional isogenies and its application to SQIsign*”