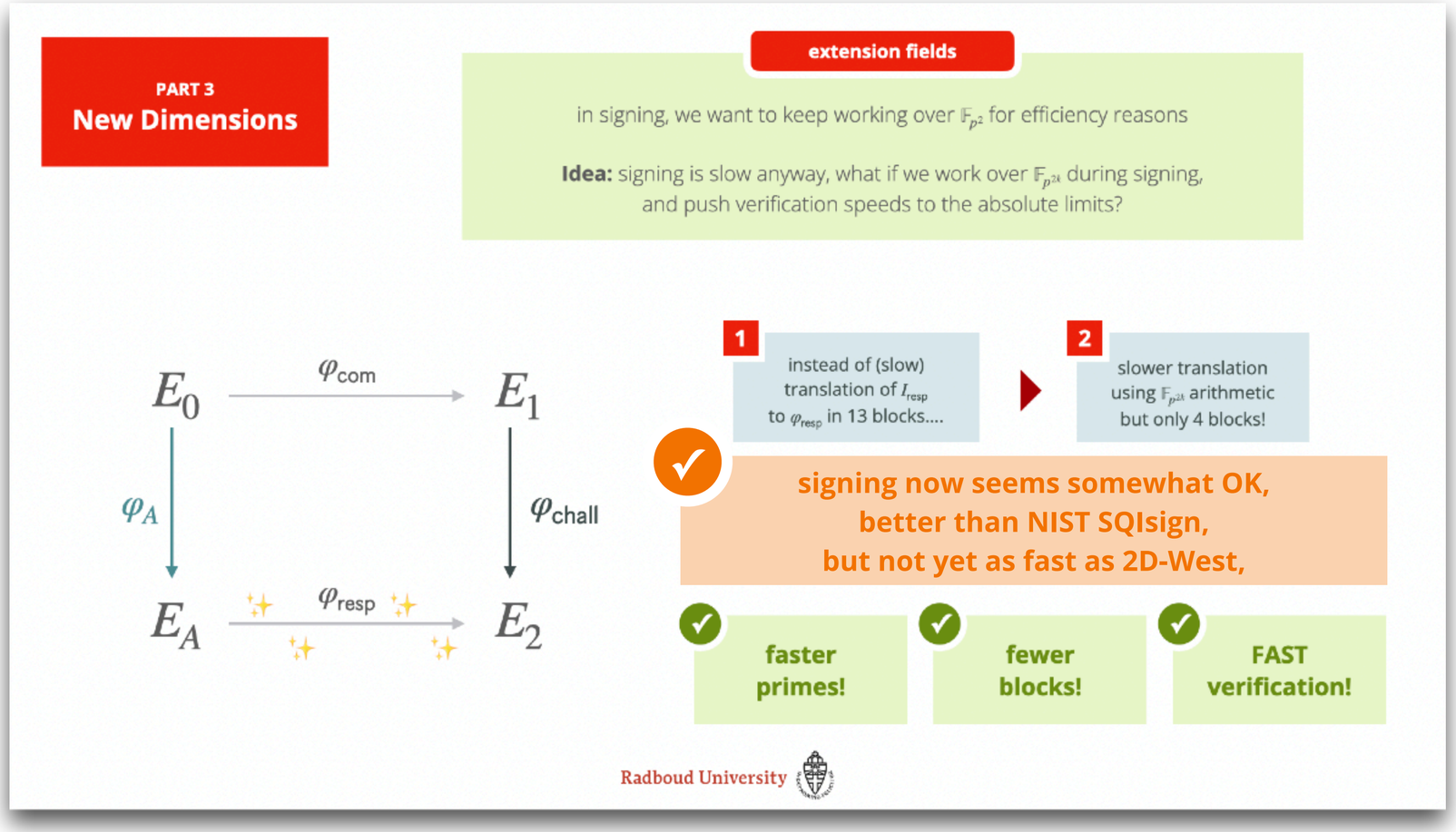
PART 5

A 1D Miracle?

Remember this slide?



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

2. Ongoing work shows highly-optimised verification for 1D verification “very likely” outperforms 2D verification

3. However, we need a “miracle" in new techniques for 1D to get better signing times than SQIsign2D

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

CONCLUSION

2D SQIsign is the “way to go” for now!

1D SQIsign is not dead! However, requires a breakthrough to achieve similar results

Want best paper awards? Do SQIsign research.