Hack the Web3.0 : SDK3 for Web3

ZKP Tools in the Nano

Renaud Dubois

Ledger
Innovation Team

July 5, 2022

STARKs		SNARKs
	VS	
Computational integrity		Privacy-enhancing
Post quantum, No trusted Setup		Asymptotic complexities ++
Delegation, Layer 2		SSI, transaction hiding
Power function based Hashs		Pairings

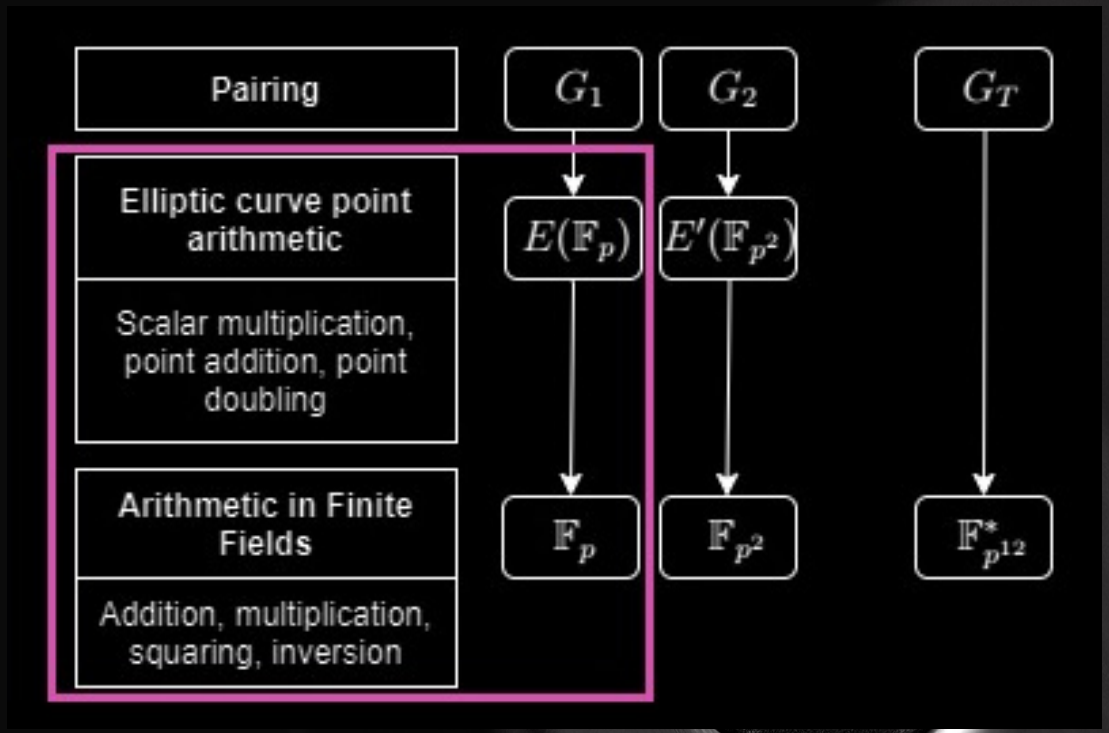
STARKs		SNARKs
	VS	
Computational integrity		Privacy-enhancing
Post quantum, No trusted Setup		Asymptotic complexities ++
Delegation, Layer 2		SSI, transaction hiding
Power function based Hashs		Pairings

Snarks are fun because they used Pairings. And Pairings are cool.

Zero Kowledge Proofs

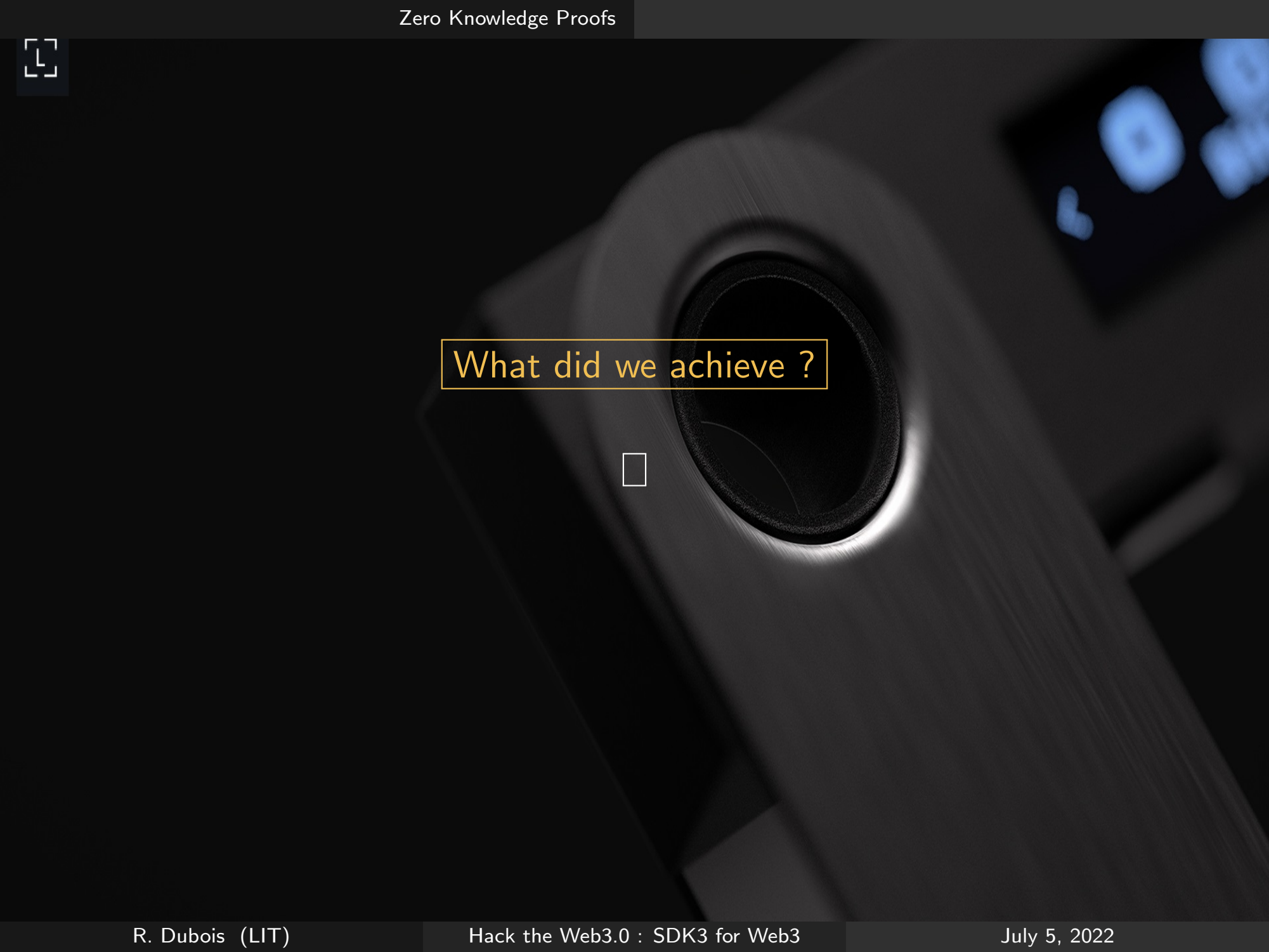
- Pairings enable Commitments, Efficient signatures, Zk-snarks, Anonymous Credentials (SSI)
- Ledger direct examples : Linkable Signatures for Anonymous airdrop (**device ID**), Ring signature (**endorsement**), Strongly Verifiable SS (**Protect**), **Decentralized Identifiers**.
- More info :
  - `https://github.com/rdubois-crypto/PrivacyProtocols/blob/main/report/Privacy.pdf`

All of this provides futurist SSI and DIds systems, and endpoint needs to implement Pairings for efficiency.



The Initial Hack Objective

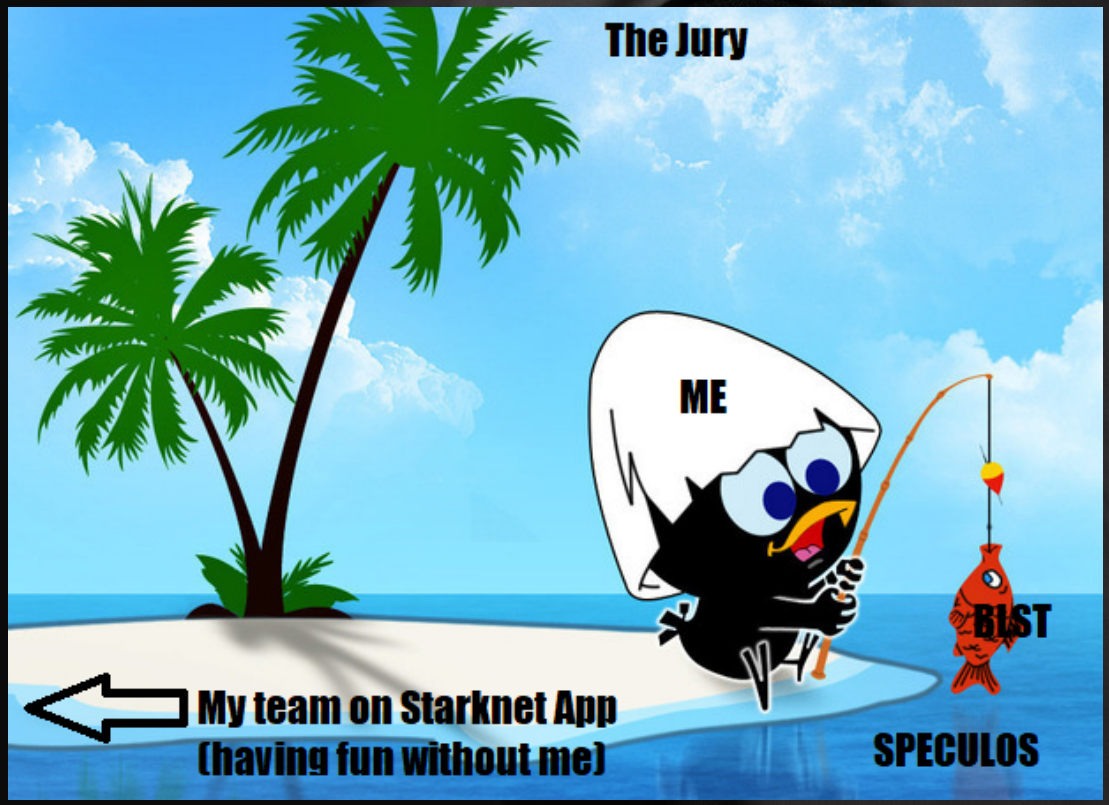
- Strip modular arithmetic from Open Source (blst library)
- Accelerate using bolos calls (available in pink square on figure)
- `cx_err_t cy_pairing_asn1(cx_curve_t curve, uint8_t *P1, size_t P1_len, uint8_t *P2, size_t P2_len, uint8_t *e, size_t e_len);`
- Push the result as a "Package" for external ZKP developpers



What did we achieve ?

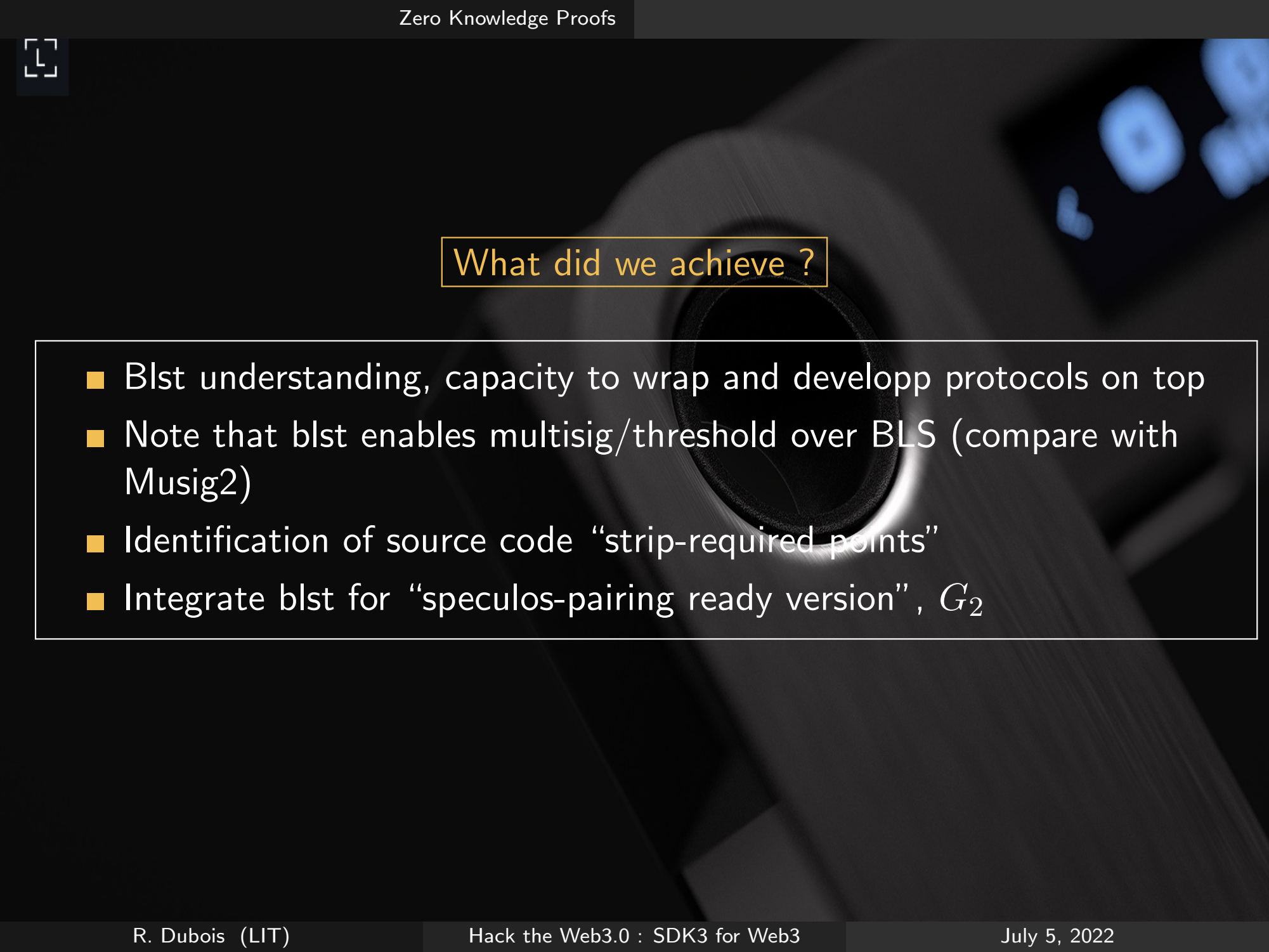
What did we achieve ?

Not that much !



No $BLS12\_381\_G_2$ API in sdk2, no Montgomery handling yet in speculos

`https://github.com/rdubois-crypto/hackthew3`



What did we achieve ?

- Blst understanding, capacity to wrap and developp protocols on top
- Note that blst enables multisig/threshold over BLS (compare with Musig2)
- Identification of source code "strip-required points"
- Integrate blst for "speculos-pairing ready version", G_2

What's Next ?

- Make target (Nano) integration
- Overwrap blst and bolos into unified APIs (on top of blst, libECC, bolos and libsec256k1) join work with ANSSI, CryptoNext, THALES. `https://github.com/rdubois-crypto/cylib`
- First use case : Groth Signature (widely used efficient sig for ZKP) `https://eprint.iacr.org/2015/824.pdf`
- More info :
  - `https://github.com/rdubois-crypto/PrivacyProtocols/blob/main/report/Privacy.pdf`

Questions ?