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

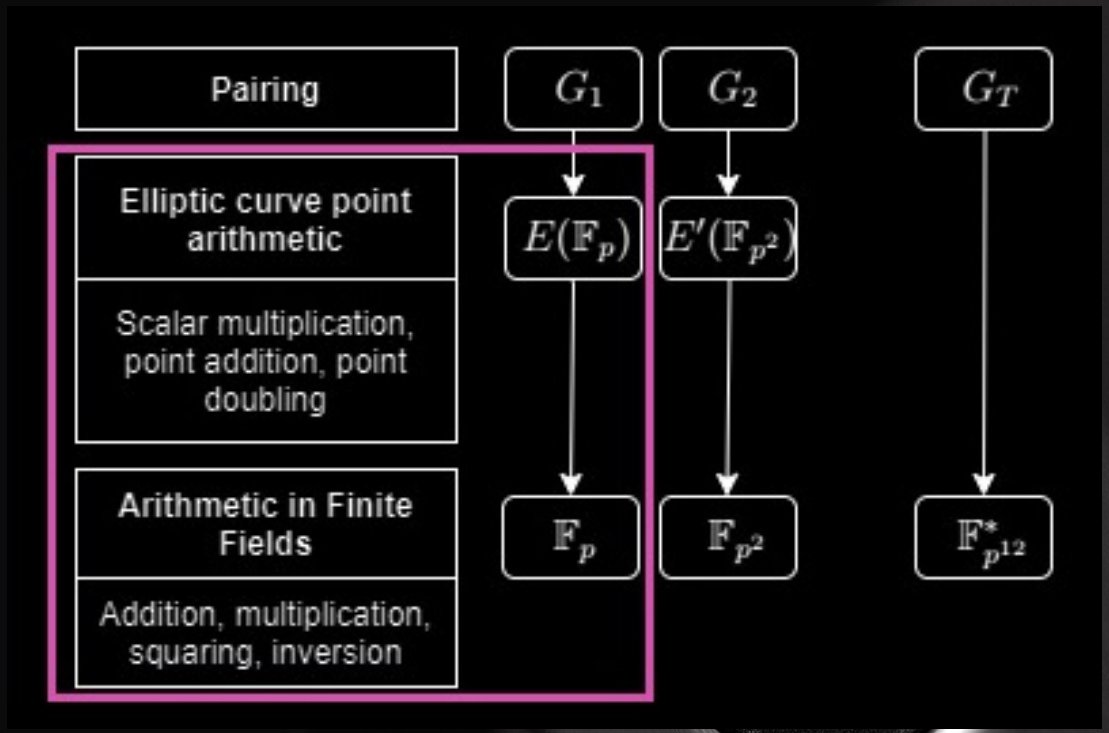
STARKs		SNARKs
	VS	
Computational integrity		Privacy-enhancing
Post quantum, No trusted Setup		Asymptotic complexities ++
Delegation, Layer 2		SSI, transaction hiding

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

Zero Kowledge Proofs

- Pairings enable Zk-snarks, Commitments, Efficient signatures
- 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`

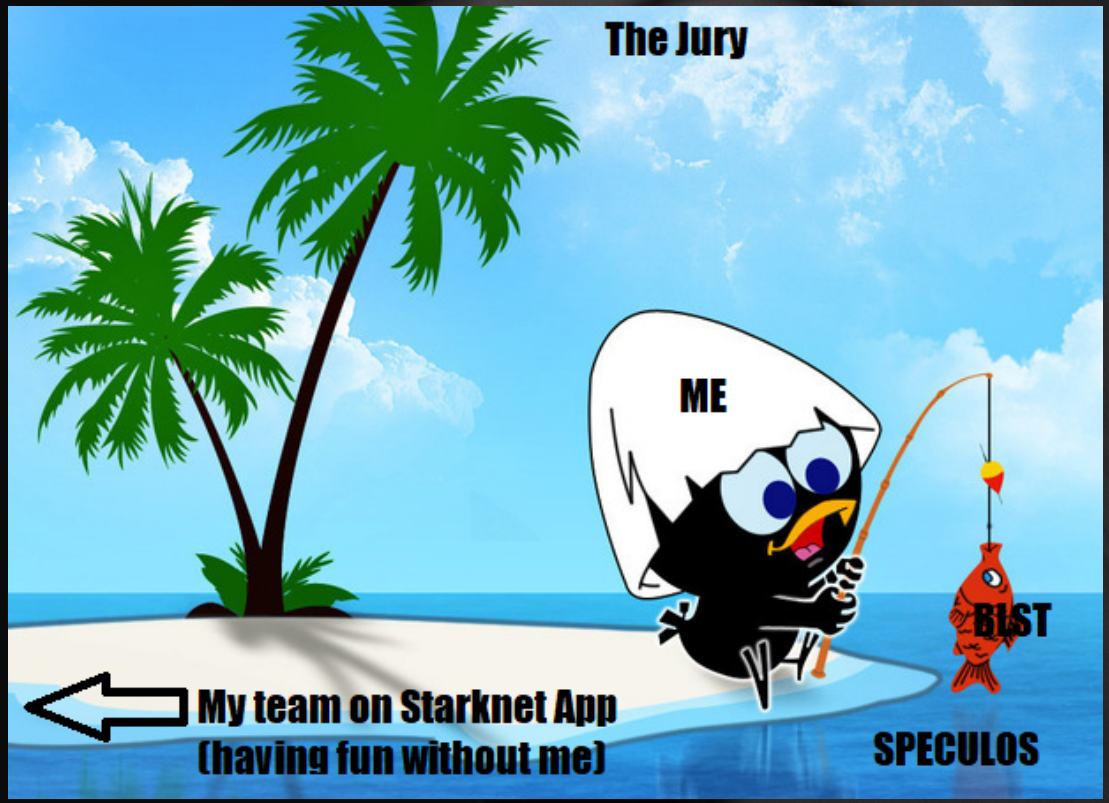
All of this provides futurist SSI and DIds systems, and endpoint needs to implement Pairings for efficiency.



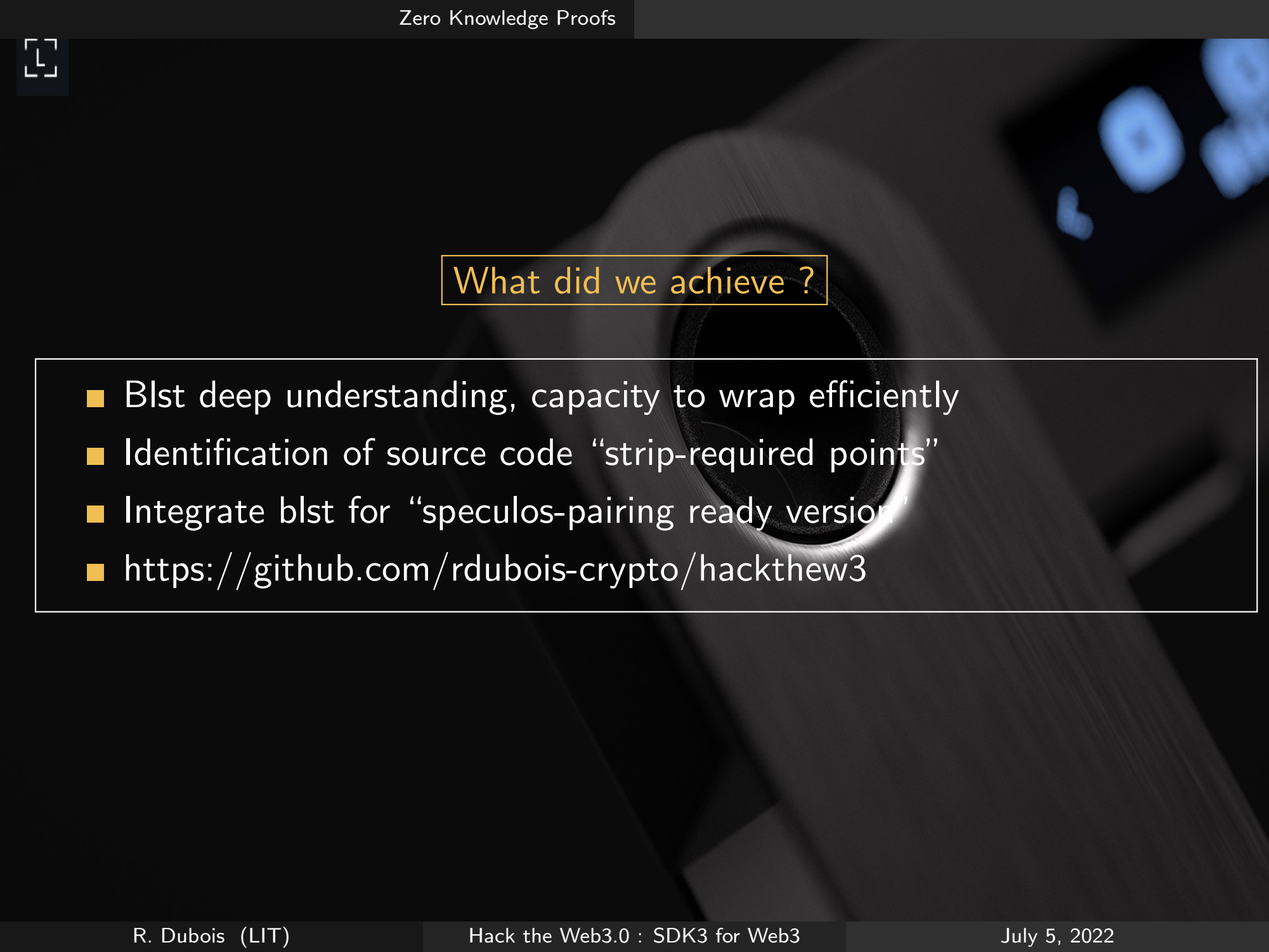
The Initial Hack Objective

- Strip modular arithmetic from Open Source (blst library)
- Accelerate using bolos calls (available in pink square on figure)
- Push the result as a "Package" that external developpers can use for ZKP integration on Nano.
- https://github.com/rdubois-crypto/hackthew3

What did we achieve ?



Not much : alone, no Montgomery handling yet in speculos



What did we achieve ?

- Blst deep understanding, capacity to wrap efficiently
- Identification of source code “strip-required points”
- Integrate blst for “speculos-pairing ready version”
- https://github.com/rdubois-crypto/hackthew3

Questions ?