aPlonK: Aggregated *PlonK* from Multi-Polynomial Commitment Schemes

Miguel Ambrona, Marc Beunardeau, Anne-Laure Schmitt, Raphaël R. Toledo

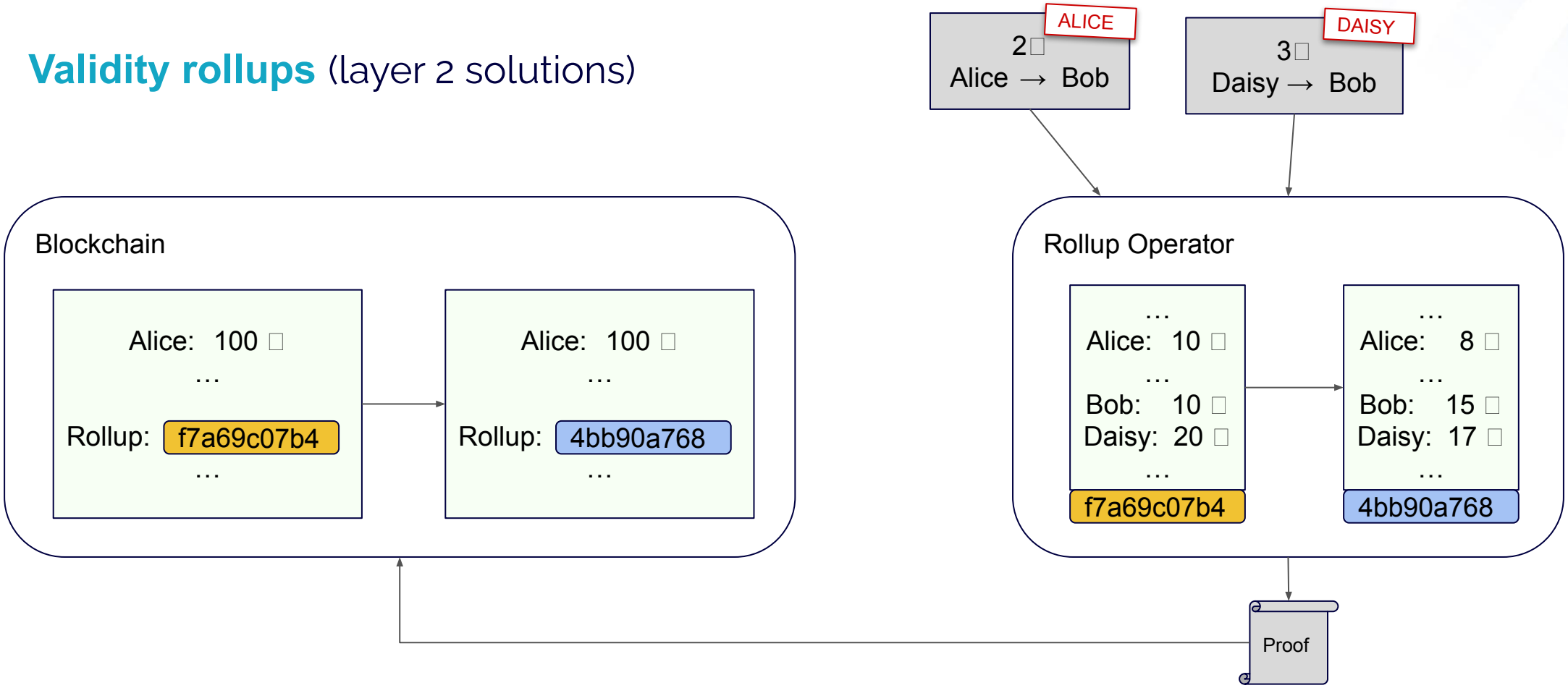
nomadic labs

Tezos

Blockchain scalability

SNARKs $\exists w : R(x, w) = 1$

Validity rollups (layer 2 solutions)



Challenges

- **Verifying** the **proof** faster than verifying transactions
- **Prover complexity** is O(n log n)

Possible solutions

- **Recursion** (a transition is valid from a state for which a similar proof exists)
- **IVC** and **PCD** (move parts of the SNARK verifier outside of the circuit)

~~Cycles of elliptic curves~~ ~~Non-native operations~~

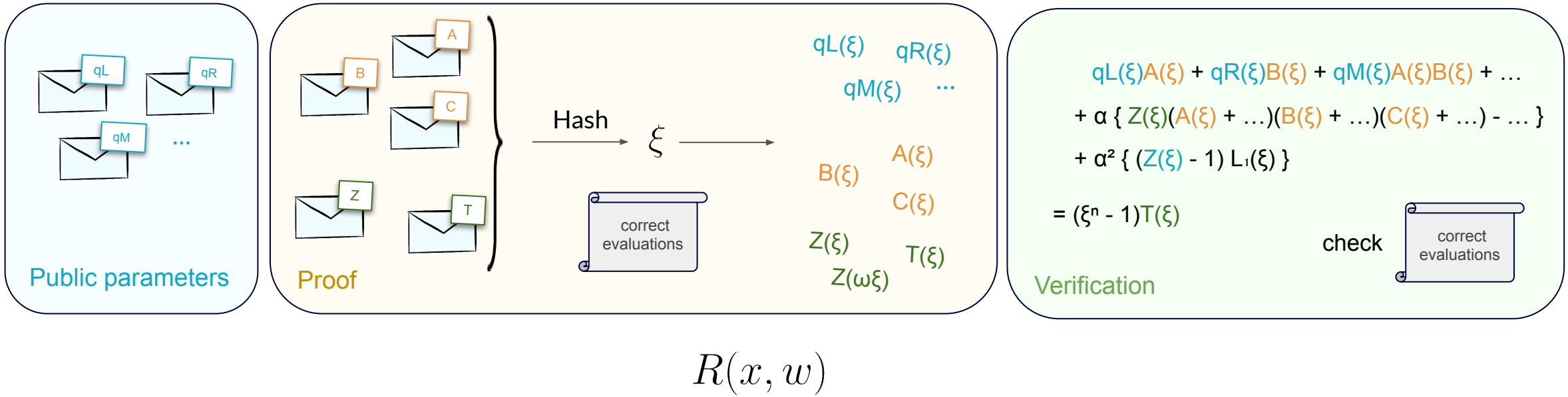
Proof aggregation for PlonK (following SnarkPack GMN21)

PlonK

Polynomial Commitments

Proof: f inside ✉ evaluates to v on z

PlonK

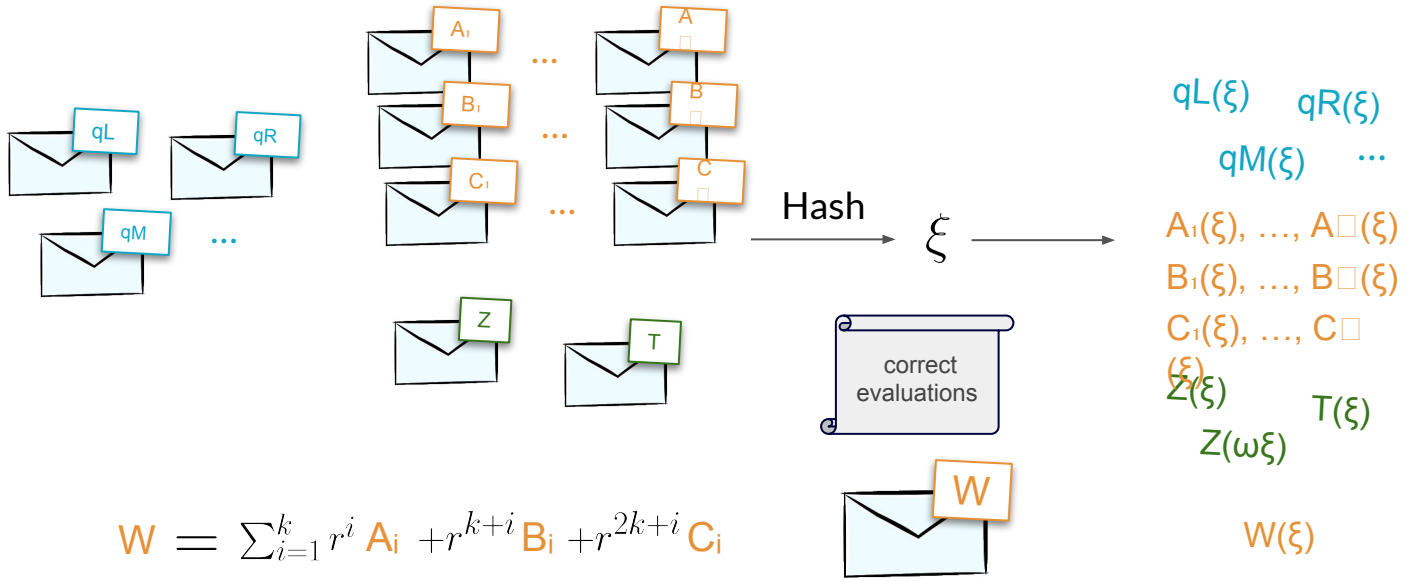


$$R(x, w)$$

PlonK

[AC:KZG10]

$$\sum_{i=1}^{k} r^i \underset{\mathbb{G}_1}{A_i} = \sum_{i=1}^{k} r^i A_i$$



$$W = \sum_{i=1}^{k} r^i A_i + r^{k+i} B_i + r^{2k+i} C_i$$

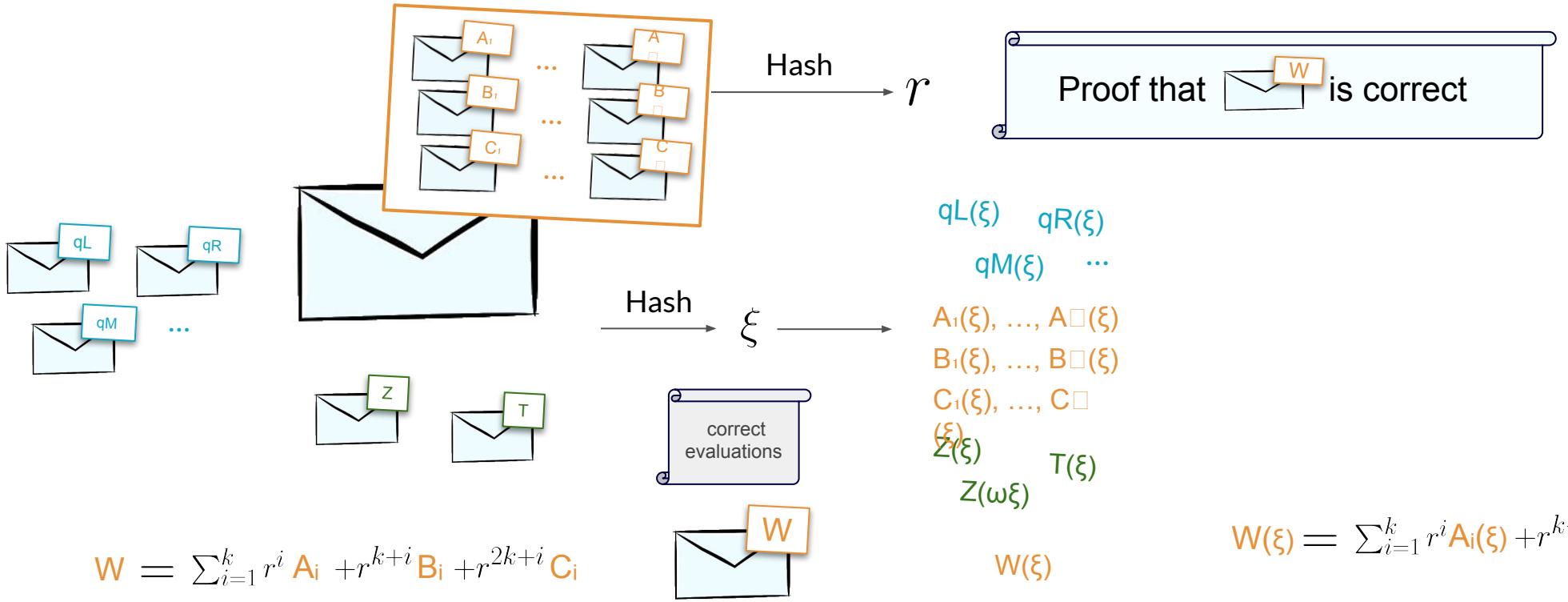
$$W(\xi) = \sum_{i=1}^{k} r^i A_i(\xi) + r^{k+i} B_i(\xi) + r^{2k+i} C_i(\xi)$$

PlonK (aggregation)

[AC:BMMTV21] [FC:GMN21]

$$e(A_i, [\tau]_2) \cdots e(A_\square, [\tau^k]_2) \cdot e(B_i, [\tau^{k+1}]_2) \cdots e(C_\square, [\tau^{3k}]_2)$$

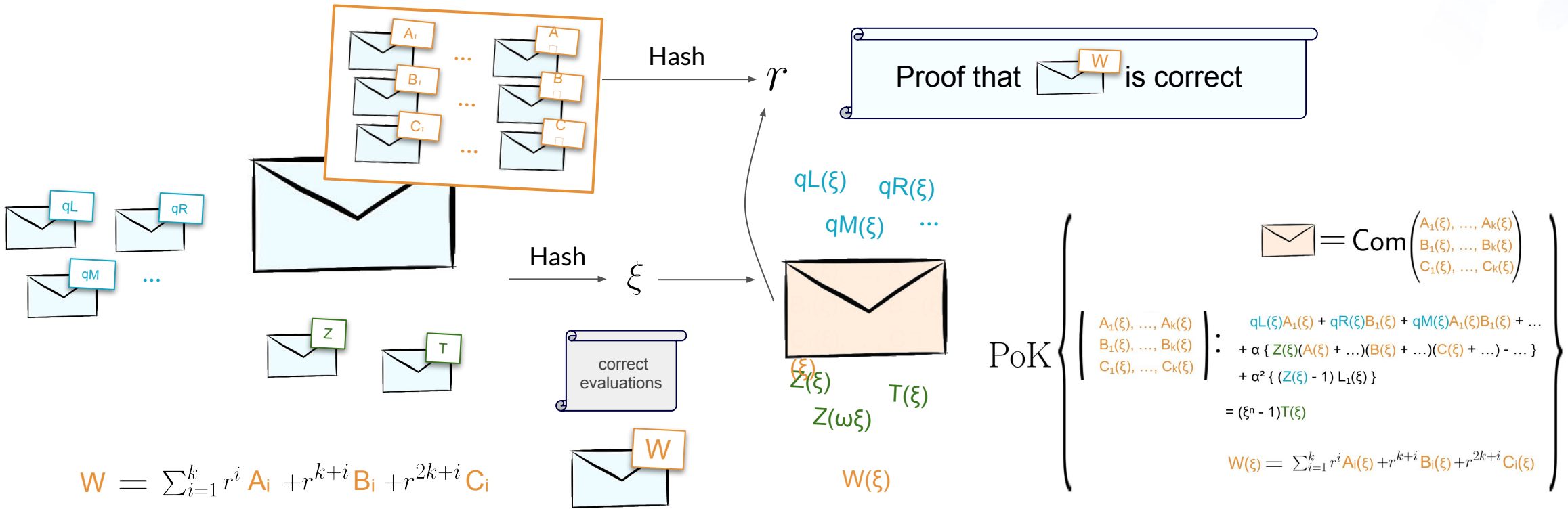
~~$$e(A, [\bar{\tau}]_2) \cdots e(\cdot, [\bar{\tau}^{k}]_2) \cdot e(B, [\bar{\tau}^{k+1}]_2) \cdots e(\cdot, [\bar{\tau}^{3k}]_2)$$~~



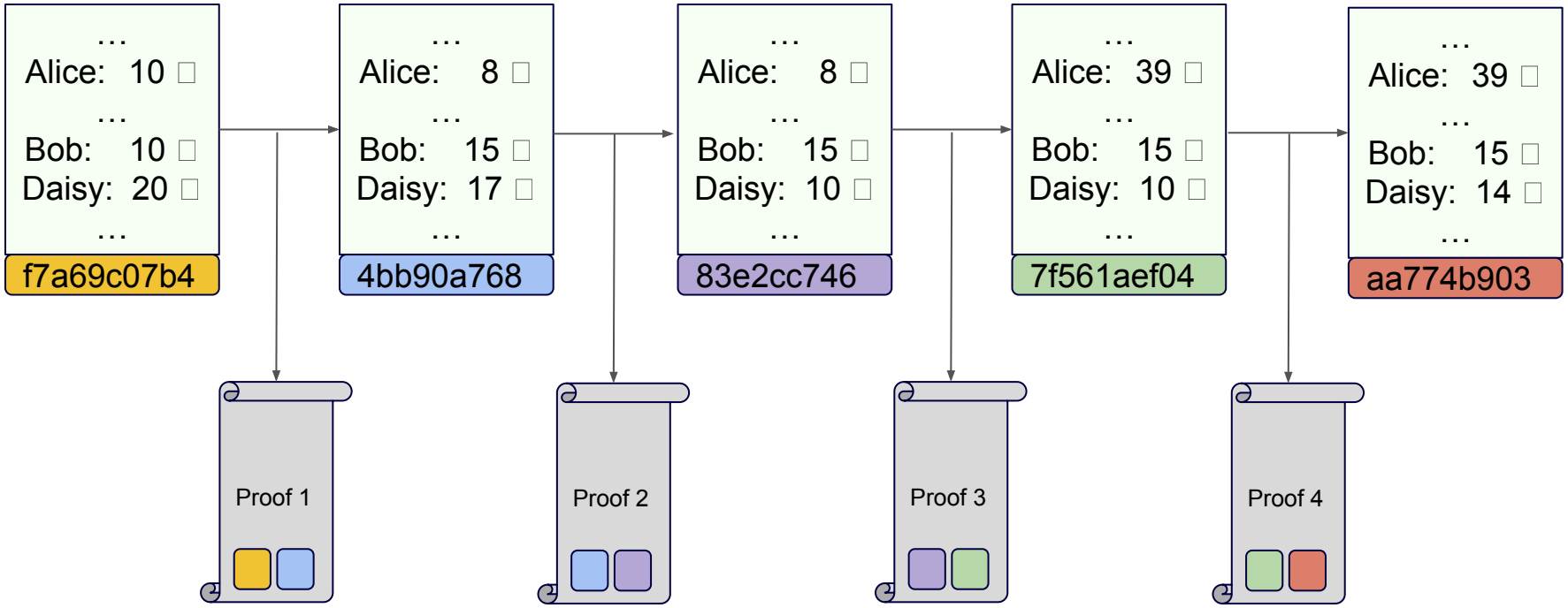
$$W = \sum_{i=1}^{k} r^i A_i + r^{k+i} B_i + r^{2k+i} C_i$$

$$W(\xi) = \sum_{i=1}^{k} r^i A_i(\xi) + r^{k+i} B_i(\xi) + r^{2k+i} C_i(\xi)$$

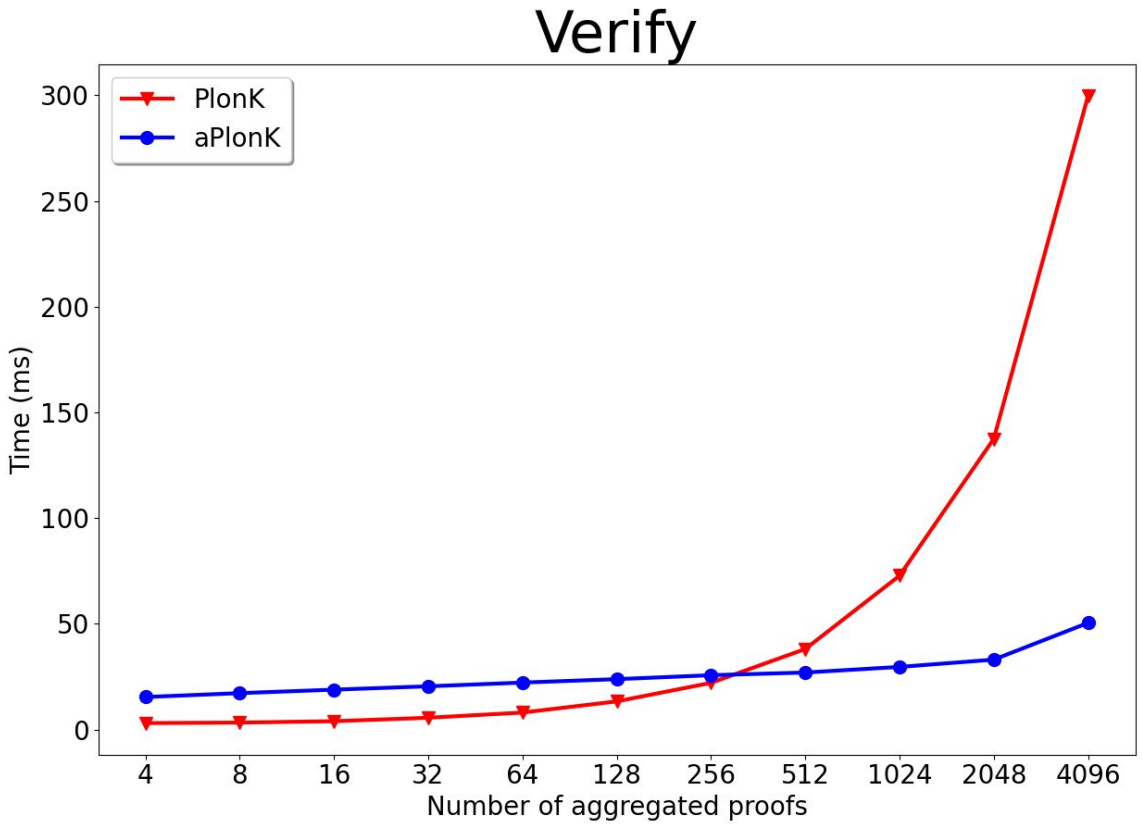
PlonK (aggregation)

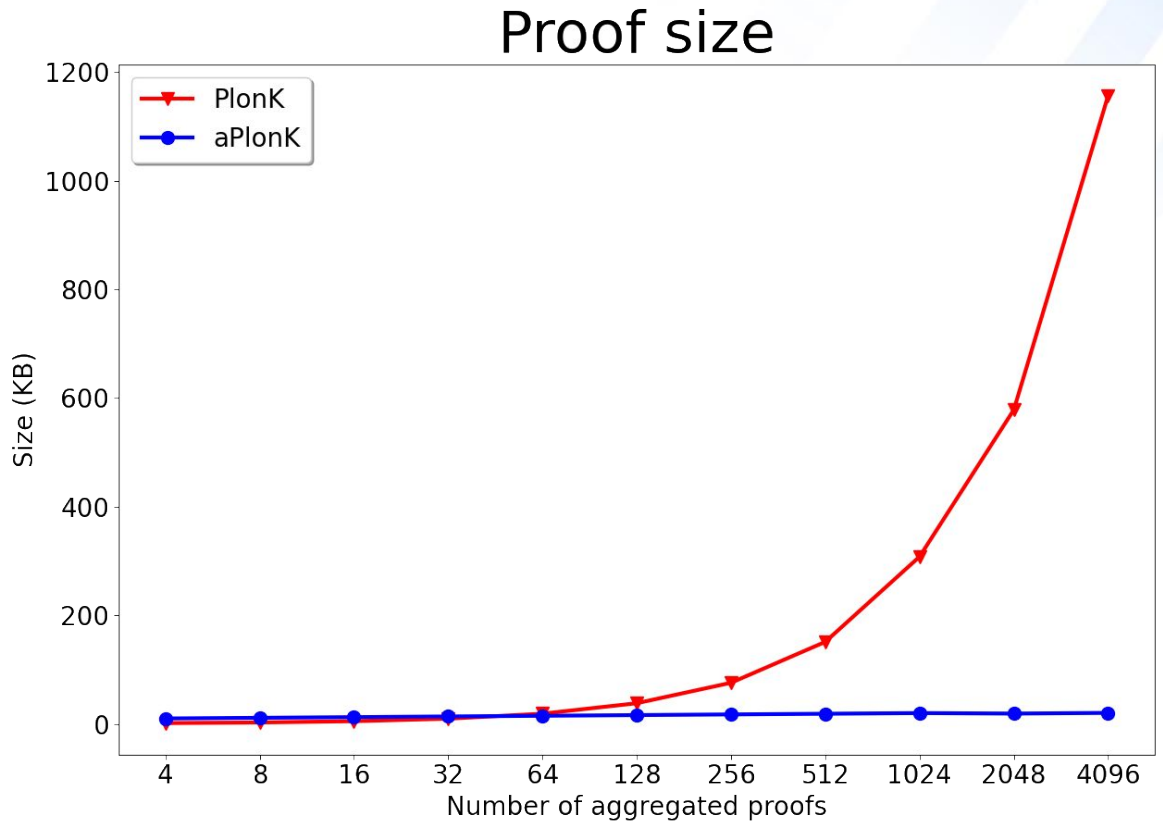


Hiding public inputs

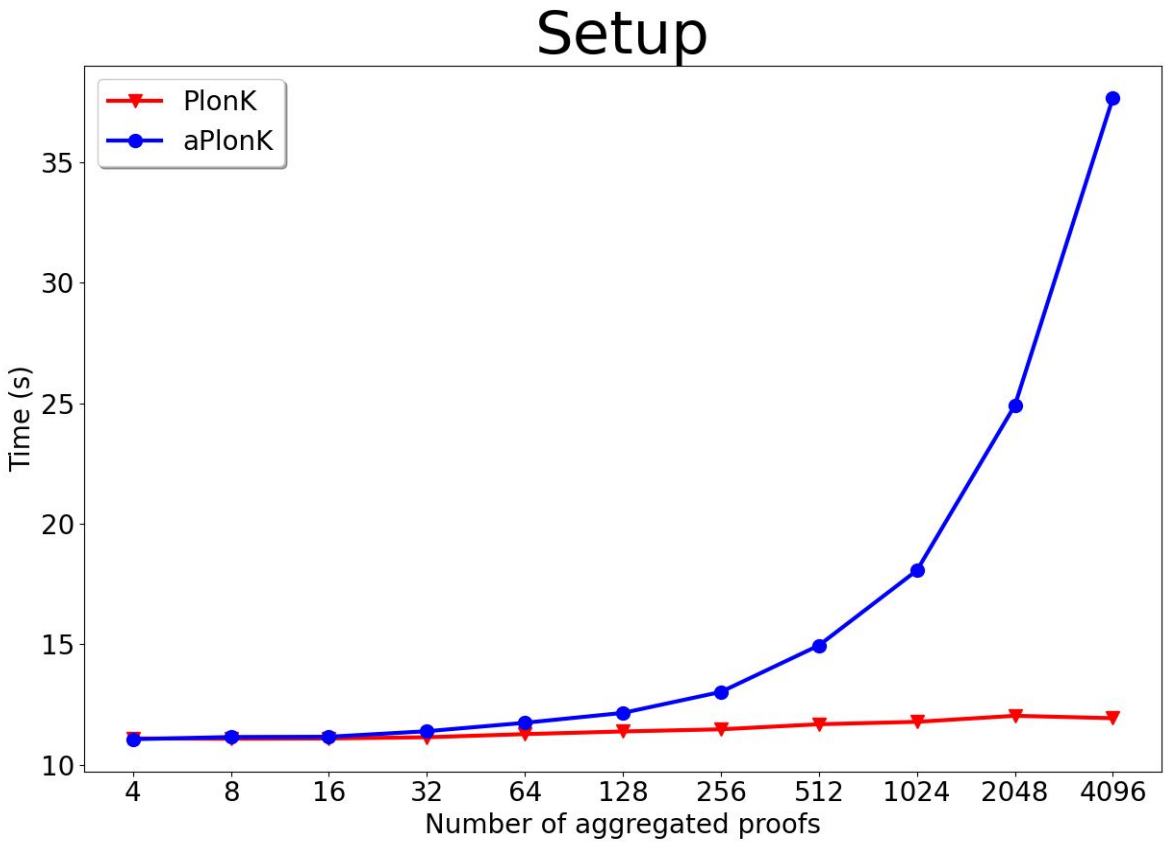


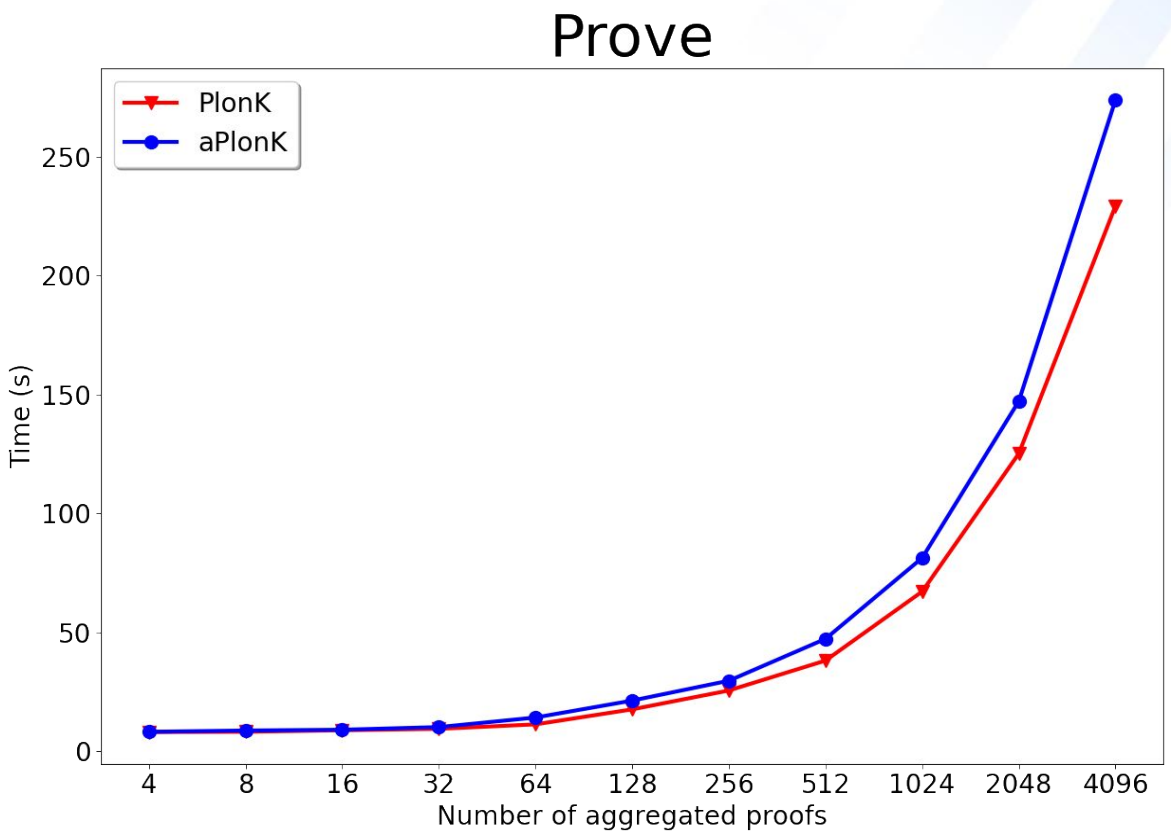
Experiments





Experiments





Conclusion

- **Proof aggregation** for PlonK
- Notion of **Multi-Polynomial Commitment** Schemes
- **Meta-verification** (hiding public inputs)
- Involve **committed data** in **PlonK** statements **efficiently**
- **Implementation:** https://gitlab.com/nomadic-labs/cryptography/aplonk

Team: https://research-development.nomadic-labs.com/files/cryptography.html

Thank you!