Exploring the Interplay of Cryptographic Accumulators and Zero-Knowledge Proofs

Anaïs Barthoulot

University of Montpellier, LIRMM

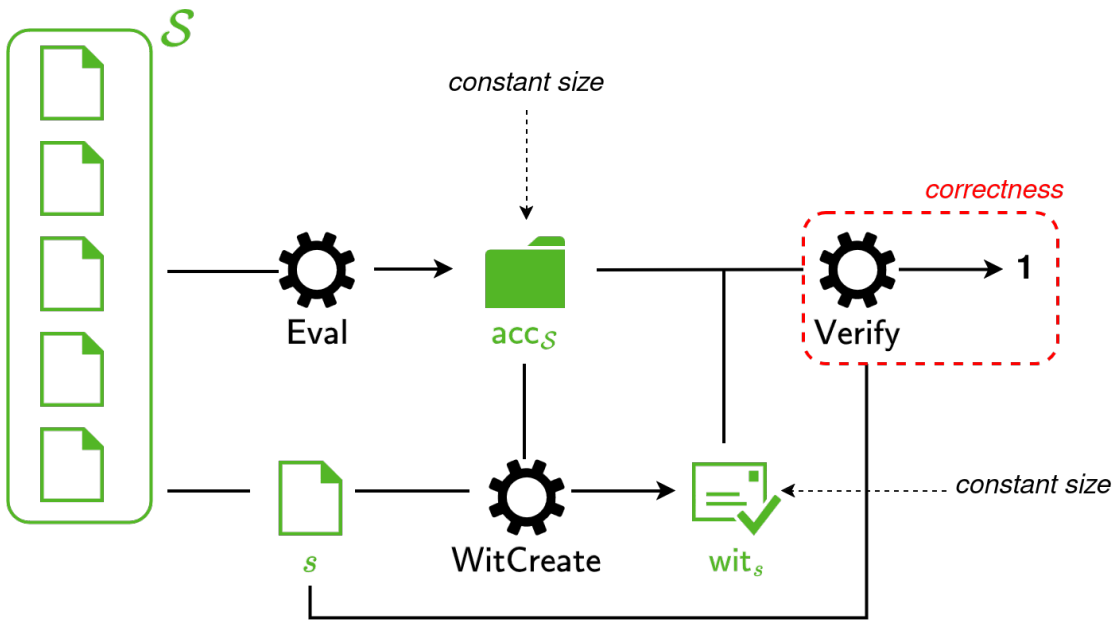
Foundations and Applications of Zero-Knowledge Proofs

4th September 2024

(Asymmetric) Cryptographic Accumulators

Definition (simplified) [1] [2]

- $\mathsf{Setup}(\lambda) \rightarrow \mathsf{pk}, \mathsf{sk}$
- $\mathsf{Eval}(\mathsf{pk}, (\mathsf{sk},)\ \mathcal{S}) \rightarrow \mathsf{acc}_{\mathcal{S}}$
- $\mathsf{WitCreate}(\mathsf{pk}, (\mathsf{sk},)\ \mathsf{acc}_{\mathcal{S}}, \mathcal{S}, s) \rightarrow \mathsf{wit}_s$
- $\mathsf{Verify}(\mathsf{pk}, \mathsf{acc}_{\mathcal{S}}, s, \mathsf{wit}_s) \rightarrow 0/1$



[1] One-way accumulators: A decentralized alternative to digital signatures, Benaloh and de Mare,EUROCRYPT 1993

[2] Revisiting Cryptographic Accumulators, Additional Properties and Relations to other Primitives, Derler, Hanser, and Slamanig CT-RSA 2015

Accumulator Security Properties

In Brief

- Lots of properties such as

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge*

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Zero-knowledge accumulator

- Accumulated value and witnesses leak *nothing* about the underlying set, not even the size of the set

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Zero-knowledge accumulator

- Accumulated value and witnesses leak *nothing* about the underlying set, not even the size of the set

$\rightarrow$ **Not considered in this talk**

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Zero-knowledge accumulator

- Accumulated value and witnesses leak *nothing* about the underlying set, not even the size of the set

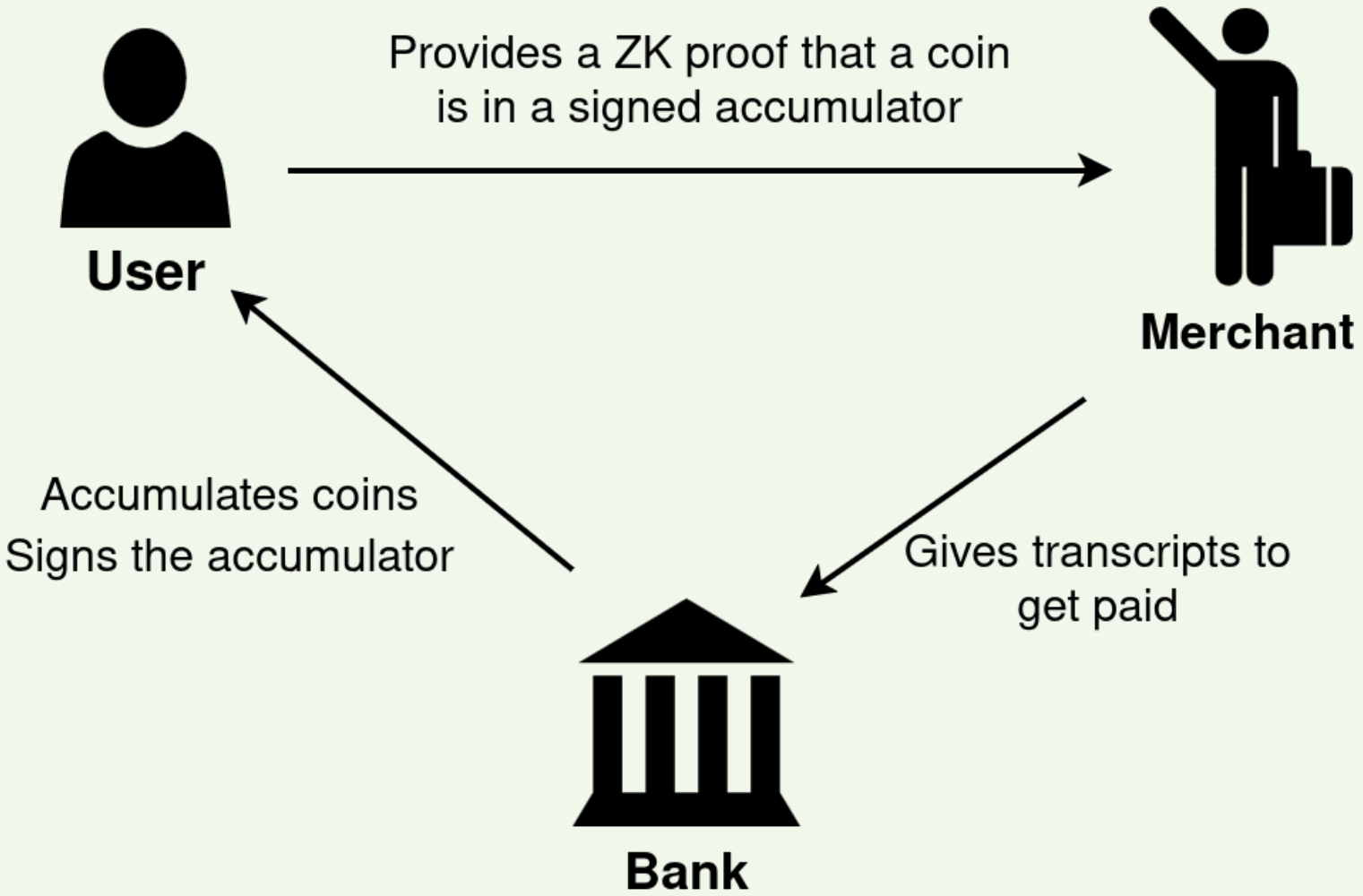
$\rightarrow$ **Not considered in this talk**

Accumulator with **zero-knowledge proofs of knowledge**

- Prove membership of an element, while keeping the element hidden

Accumulators and ZK Proofs: Example of Application

E-Cash



Other applications: anonymous credentials, ...

Interplay of Accumulators and ZK Proofs

- **Efficiently Provable**: combined with a commitment scheme
  example: RSA-based accumulators and Pedersen commitments[3]

[3] Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, Camenisch and Lysyanskaya, Crypto 2002

Interplay of Accumulators and ZK Proofs

- **Efficiently Provable**: combined with a commitment scheme
  example: RSA-based accumulators and Pedersen commitments[3]

- **SNARK-friendly**: verification done with (zk) SNARKs
  example: Merkle trees, RSA-based accumulators [4]

[3] Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, Camenisch and Lysyanskaya, Crypto 2002

[4] Scaling Verifiable Computation Using Efficient Set Accumulators, Ozdemir, Wahby, Whitehat, Boneh, SEC 2020

Interplay of Accumulators and ZK Proofs

- **Efficiently Provable**: combined with a commitment scheme
  example: RSA-based accumulators and Pedersen commitments[3]
- **SNARK-friendly**: verification done with (zk) SNARKs
  example: Merkle trees, RSA-based accumulators [4]
- **Determinantal Accumulators**: designed to construct special NIZK proofs [5]

[3] Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, Camenisch and Lysyanskaya, Crypto 2002

[4] Scaling Verifiable Computation Using Efficient Set Accumulators, Ozdemir, Wahby, Whitehat, Boneh, SEC 2020

[5] Set (Non-)Membership NIZKs from Determinantal Accumulators, Lipmaa and Parisella, Latincrypt 2023

Key Takeaways

- **Combining ZK Proofs and Accumulators**
  - Enhances privacy of accumulators
  - Applied in E-Cash, anonymous credentials, and blockchain technologies

Active Research Area