# Interview presentation

Stefano Trevisani

December 2, 2022

Università degli Studi di Udine

Alpen Adria Universität Klagenfurt

# ZK-SNARKs, what?

*Zero-Knowledge Succinct Non-interactive ARgument of Knowledge*:

- A multidisciplinary topic: math, complexity, cryptography[1].
- Prover wants to prove a statement, might be dishonest!
- Verifier wants to verify the proof, might be curious!
- Prover does not want to disclose secrets: **Zero-Knowledge**.
- Verifier does not want to waste time: **Succinct** proof.
- Prover proves once and for all: **Non-interactive**.
- Parties are "not too powerful": **ARgument of Knowledge**.

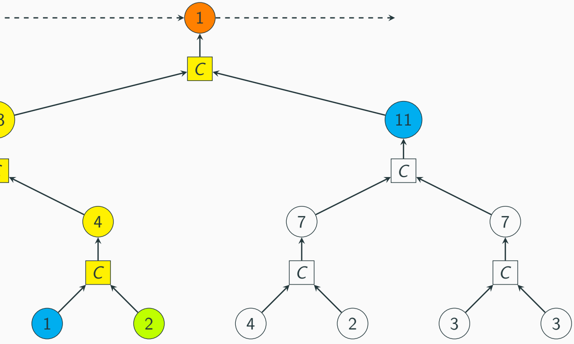
[1] A few milestones: [GMR89, Sha92, Dam93, Mic00, GGPR12, Gro16].

# ZK-SNARKs, why?

Many useful applications! For example:

- Cloud computing [PGHR13].
- Households figuring out their bills privately.
- **Anonymous transactions on the blockchain** [BSCG+14].

# The Blockchain

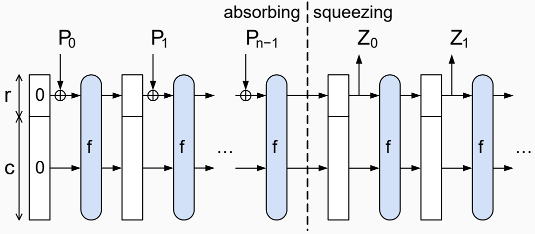



- Groups of transactions are leaves of a *Merkle tree* [Mer88].
- Bottom-up computation using a **compression function**.
- The root contains the *commitment* (among other data).
- Verify a commitment following the *authentication path*.

# Compression functions

One-way compression functions (OWCF):

- Many (e.g. 2) inputs and few (e.g. 1) outputs.
- Easy to compute, but hard to invert (and find collisions).
- Usually derived from one-way permutations.
- Standard designs (SHA [Dan15]) work over *boolean fields*.
- Davies-Meyer [Pre05], sponge [BDPVA07]...



# ZK-SNARK and compression functions

SHA is very fast natively, but what about in ZK-SNARK?

- Efficient ZK-SNARKs over prime fields $\mathbb{F}_p$ [GGPR12].
- Input-output relationship as bi-linear constraints (R1CS) [BSCTV13].
- One multiplication $=$ one constraint.
- What about SHA-256? 25000+ constraints!
- Can we do better?

# MiMC

Minimal Multiplicative Complexity (MiMC) hash function [AGR$^+$16]:

- Extremely simple: *round function* is $x^3 + c^2$.
- Many rounds to be secure against *algebraic attacks*.
- MiMCHash-256: 640 constraints.
- Can we do better?

[2]Warning: might not be a permutation!

Many improvements in the last years, POSEIDON [GKR$^+$21][3]:

- Partial *substitution-permutation network* (SPN) rounds.
- Full SPN for classic attacks (linear, differential. . . ).
- Partial SPN for algebraic attacks (interpolation, Gröbner. . . ).
- POSEIDON-256: 276 constraints.
- Can we do better?

[3] See also: [GHR$^+$22, BBC$^+$22, AABS$^+$19].

# Arion

Our design Arion [RST23]:

- Builds on the GTDS algebraic framework [RS22].
- Two variants: Arion and $\alpha$-Arion.
- $\alpha$-ArionHash-256: 76 constraints.

# Comparisons

`libsnark`: used by ZCash [BSCG+14] for its blockchain.

We used it to implement:

- Several primitives designed for ZK-SNARK, including ours.
- A self-parametrizing Merkle tree.
- A new mode of hash, the Augmented Binary tRee [ABR21].

Proof generation times for MT commitments over 256-bit prime fields

| Tree height | $\alpha$-ArionHash | Griffin | Poseidon |
|---|---|---|---|
| 4 | 73 ms | 88 ms | 186 ms |
| 8 | 145 ms | 181 ms | 386 ms |
| 16 | 278 ms | 338 ms | 745 ms |
| 32 | 509 ms | 622 ms | 1422 ms |

# $\mathcal{T}$he $\mathcal{E}$nd

*Thank you for your attention!*

Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec.
**Design of symmetric-key primitives for advanced cryptographic protocols.**
Cryptology ePrint Archive, Paper 2019/426, 2019.
https://eprint.iacr.org/2019/426.

Elena Andreeva, Rishiraj Bhattacharyya, and Arnab Roy.
**Compactness of hashing modes and efficiency beyond merkle tree.**
Cryptology ePrint Archive, Paper 2021/573, 2021.
https://eprint.iacr.org/2021/573.

Martin Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen.
**Mimc: Efficient encryption and cryptographic hashing with minimal multiplicative complexity.**
In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, pages 191–219, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems.
**New design techniques for efficient arithmetization-oriented hash functions:anemoi permutations and jive compression mode.**
Cryptology ePrint Archive, Paper 2022/840, 2022.
https://eprint.iacr.org/2022/840.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
**Sponge functions.**
In *ECRYPT hash workshop*, volume 2007, 2007.

Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza.
**Zerocash: Decentralized anonymous payments from bitcoin.**
In *2014 IEEE Symposium on Security and Privacy*, pages 459–474, 2014.

Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza.
**Succinct non-interactive zero knowledge for a von neumann architecture.**
Cryptology ePrint Archive, Paper 2013/879, 2013.
https://eprint.iacr.org/2013/879.

Ivan Damgård.
**Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with preprocessing.**
In Rainer A. Rueppel, editor, *Advances in Cryptology — EUROCRYPT' 92*, pages 341–355, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

Quynh H. Dang.
**Secure Hash Standard.**
National Institute of Standards and Technology, Jul 2015.

Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova.
**Quadratic span programs and succinct nizks without pcps.**
Cryptology ePrint Archive, Paper 2012/215, 2012.
https://eprint.iacr.org/2012/215.

Lorenzo Grassi, Yongling Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang.
**A new feistel approach meets fluid-spn: Griffin for zero-knowledge applications.**
*IACR Cryptol. ePrint Arch.*, 2022:403, 2022.

Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger.
**Poseidon: A new hash function for zero-knowledge proof systems.**
In *USENIX Security Symposium*, 2021.

Shafi Goldwasser, Silvio Micali, and Charles Rackoff.
**The knowledge complexity of interactive proof systems.**
*SIAM Journal on Computing*, 18(1):186–208, 1989.

Jens Groth.
**On the size of pairing-based non-interactive arguments.**
Cryptology ePrint Archive, Paper 2016/260, 2016.
`https://eprint.iacr.org/2016/260`.

Ralph C. Merkle.
**A digital signature based on a conventional encryption function.**
In Carl Pomerance, editor, *Advances in Cryptology — CRYPTO '87*, pages 369–378, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg.

Silvio Micali.
**Computationally sound proofs.**
*SIAM J. Comput.*, 30(4):1253–1298, oct 2000.

Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova.
**Pinocchio: Nearly practical verifiable computation.**
Cryptology ePrint Archive, Paper 2013/279, 2013.
`https://eprint.iacr.org/2013/279`.

Bart Preneel.
**Davies–Meyer Hash Function, pages 136–136.**
Springer US, Boston, MA, 2005.

Arnab Roy and Matthias Steiner.
**Generalized triangular dynamical system: An algebraic system for constructing cryptographic permutations over finite fields, 2022.**

Arnab Roy, Matthias Steiner, and Stefano Trevisani.
**Arion: Arithmetization-oriented permutation and hashing from generalized triangular dynamical systems.**

Undergoing submission, 2023.

Adi Shamir.
**Ip = pspace.**
*J. ACM*, 39(4):869–877, oct 1992.