Algebraic Hashes Initiative

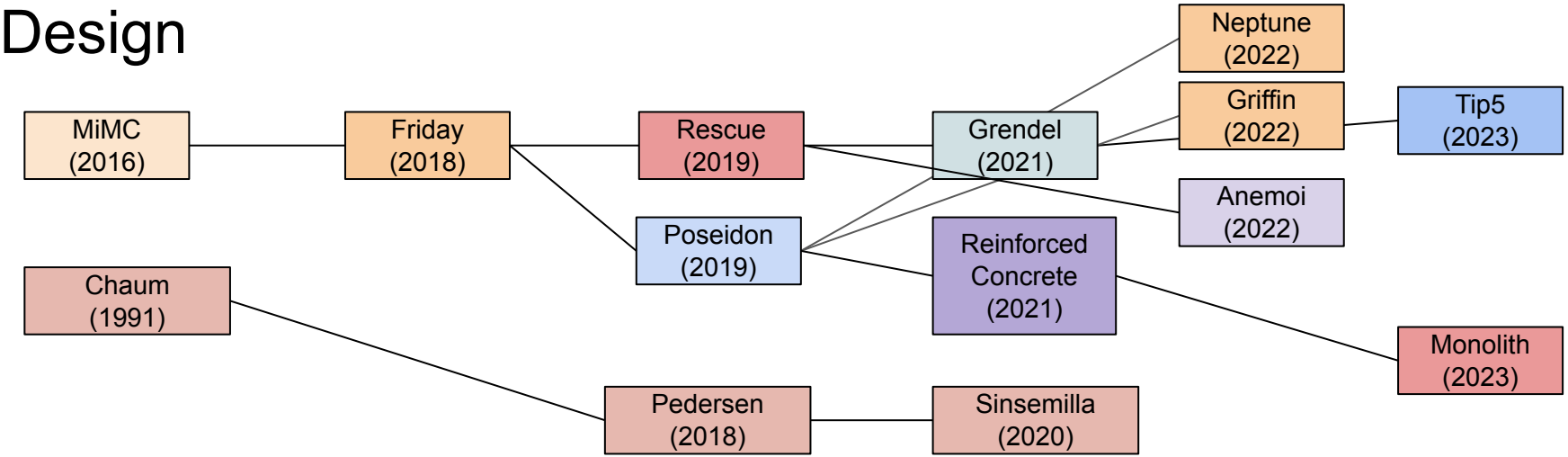
Dmitry Khovratovich, Ethereum Foundation

New hash designs

With development of IVC, we need hash functions that are efficient in circuits:

- Merkle tree opening proofs
- Fiat-Shamir-transformed protocols
- Compression in recursive SNARKs
- Provenance proofs

Design


MiMC (2016)
Friday (2018)
Rescue (2019)
Grendel (2021)
Neptune (2022)
Griffin (2022)
Tip5 (2023)
Anemoi (2022)
Poseidon (2019)
Reinforced Concrete (2021)
Chaum (1991)
Monolith (2023)
Pedersen (2018)
Sinsemilla (2020)

New hash designs in Ethereum

The new designs are already used in many Ethereum applications and may be found useful in the Ethereum core protocol as well (signature aggregation, threshold constructions, storage proofs, etc.)

Limits of confidence

Ethereum Community (and EF in particular) still lacks confidence in new designs:

- No standards (IETF, ISO, NIST)
- Big variety
- Easy of misuse
- Relatively little public scrutiny comp. to AES/SHA-⅔
- Reliance on shaky algebraic assumptions

Algebraic Hashes Initiative

Ethereum Foundation plans to support analysis and design of symmetric primitives aimed for “ZK” world

Algebraic Hashes Initiative

Goals:

- Get more confidence in the most popular designs
- Be able to recommend concrete schemes for certain usecases
- Make hashing the security and/or performance bottlenecks no more
- Have backup solutions for the case of sudden cryptography or quantum attack.

Algebraic Hashes Initiative: step 1

Bounties:

- Build on 2021-22 bounty program
- Craft reduced versions of most interesting schemes
- Award growing with target strength and supplementary material

Feedback needed:

- Give us weakened versions
- Any fairness issue
- Comments on rules

Algebraic Hashes Initiative: step 2

Research awards:

- Best paper awards
- Several categories (attacks, designs, implementations, bounds)
- Targeting young researchers as well

Feedback needed:

- Classes
- Bonuses
- Any issues that prevent your PhD students working on this

Algebraic Hashes Initiative: step 3

Research wishlist:

- Interest in a wide class of papers (Groebner basis, heavily modified variants, incremental results) that are often rejected from conferences

Feedback needed:

- Suggestions

Algebraic Hashes Initiative: step 4

New meetings:

- Support and organize research retreats in the “good old” SHA-3 fashion
- Working groups
- Final reports

Feedback needed:

- Dates
- Topics
- Locations
- People

Algebraic Hashes Initiative: step 5

Conferences:

- Somehow support conferences and journals of our profile
- Ask for special entries in call for papers

Feedback needed:

- What we can ask
- How we can motivate
- What conference organizers need/like

Algebraic Hashes Initiative: step 6

Standardization:

- Motivate creation of new standards for widely used designs

Feedback needed:

- Suggestions

Algebraic Hashes Initiative: summary

- Bounties
- Paper awards
- Research wishlist
- New meetings
- Conference support
- Standardization

Anything else?

- We may not have resources for everything but we can prioritize
- Comments are welcome