Survey of MPC- and ZK-friendly Symmetric Cryptography

Christian Rechberger

May 10, 2026

TU Graz and TACEO

Symmetric Crypto for (MPC, ZK) Researchers and Practitioners

- This is about the art and science to create new hardness assumptions
- No unconditional proofs, no underlying hardness assumptions
- Proofs may rule out certain classes of attacks, but eventually this is (as almst all of cryptography anyhow) a cat-and-mouse game of attacks and defenses
- Symmetric Cryptography = Math + Mess
  (often more mess than elsewhere in crypto)

MPC, ZK, MPC+ZK, for Symmetric Cryptographers (1/2)

- "ZK": Checking integrity/Signing/Authenticating computation on data
  (instead of checking/signing/authenticating data)
- "MPC": Encrypting computation on data
  (instead of encrypting data)
- "MPC+ZK": question to the audience

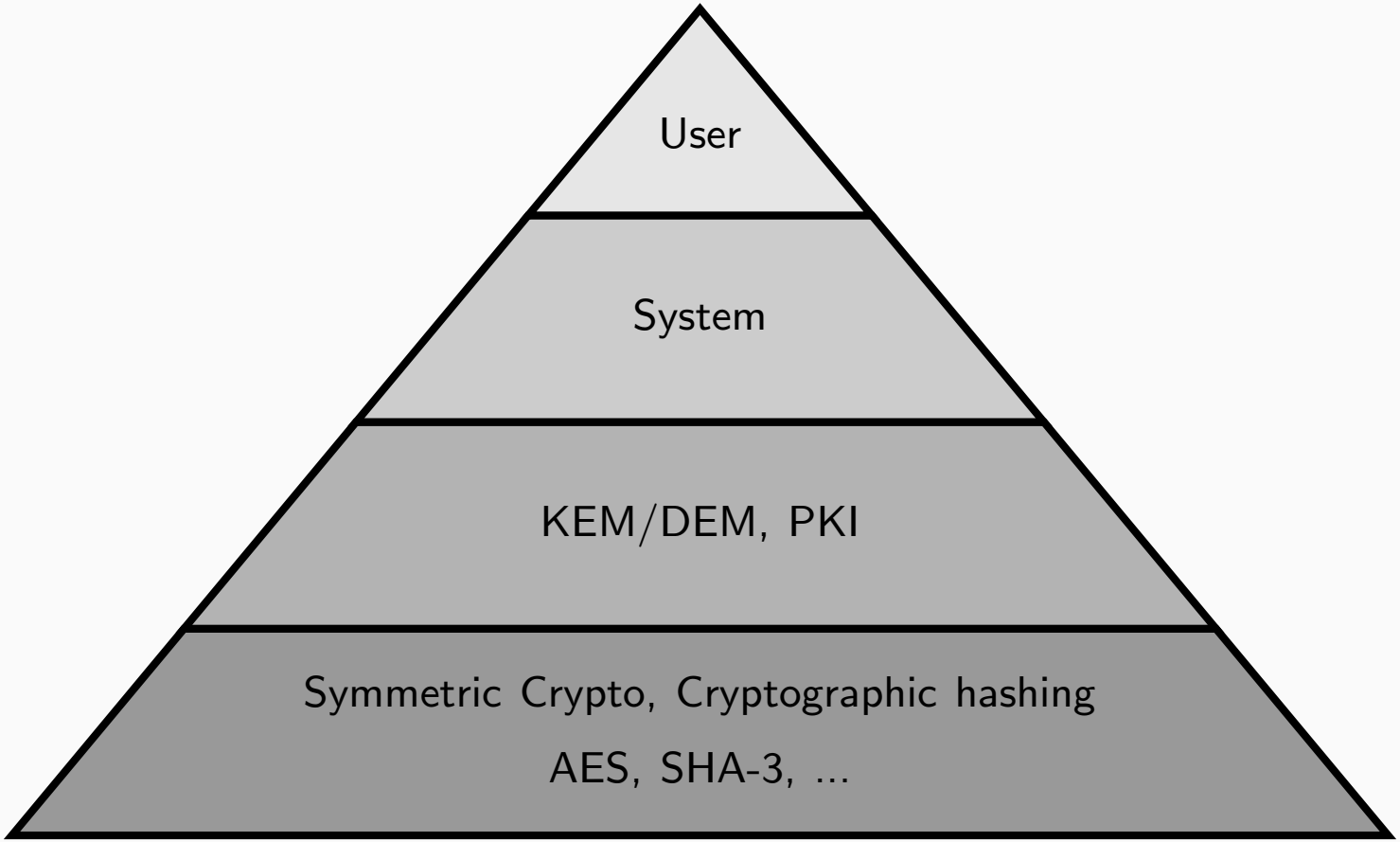
MPC, ZK, MPC+ZK, for Symmetric Cryptographers (2/2)

- Very fast moving field, esp. on practical aspects of "ZK" in the last 5 years.
- Work on practical aspects of "MPC" is also accelerating and finding larger and larger classes applications.
- The *combination* of both technologies is the most recent trend.
- Not all innovations are formally published! Blogs, HackMD pages, github repos are other relevant sources.

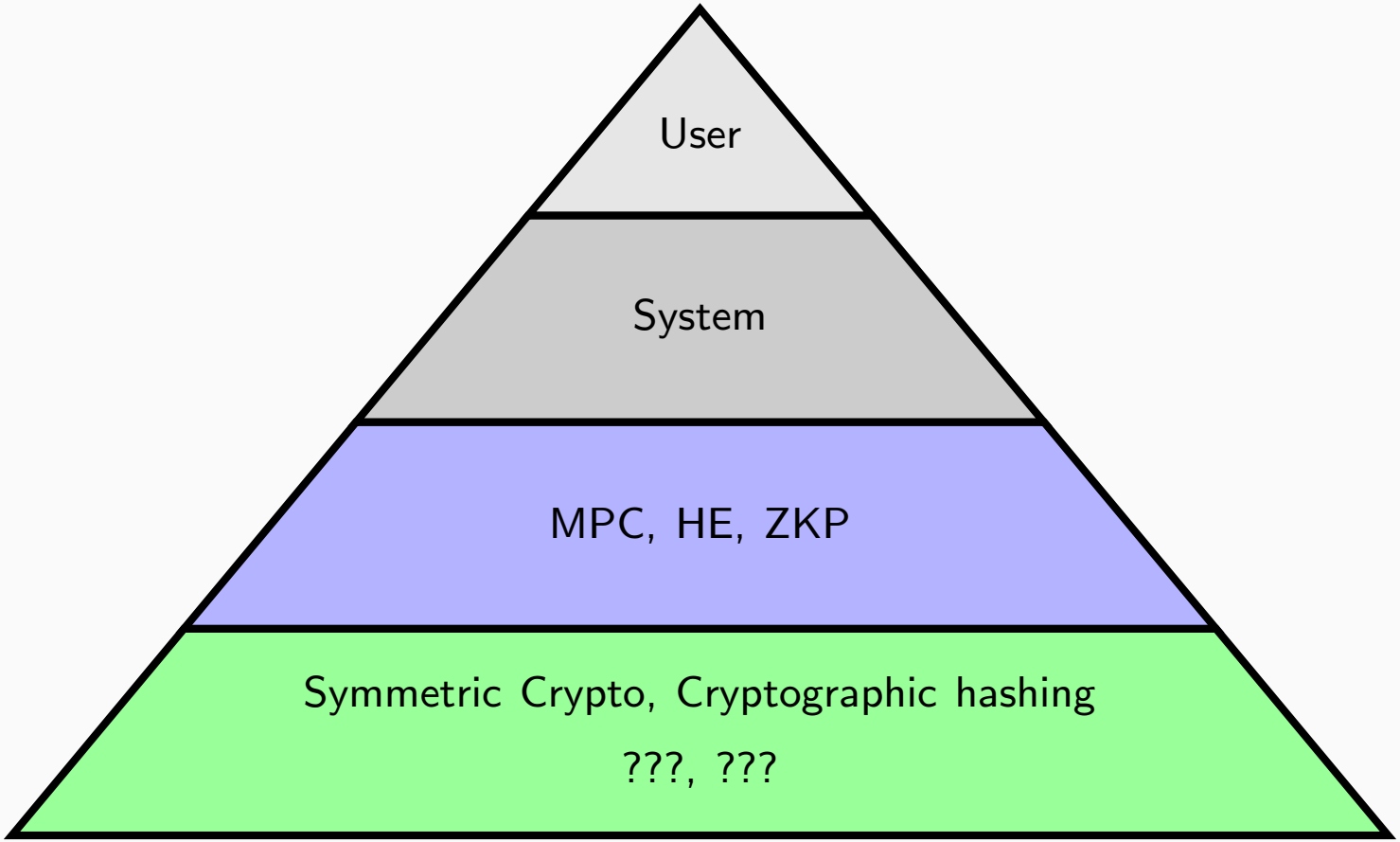
Wait, where is FHE in this?

- Technically, can be seen as an umbrella terms for a class of techniques to do MPC, next to others such as secret sharing, or garbled circuits
- sub-techniques: BGV/BFV, CKKS, TFHE all have distinct demands
- To keep things simpler, FHE-friendly and Garbled-circuit-friendly symmetric crypto and is out of scope for this talk

Role of symmetric-key crypto and hashing in systems



Role of symmetric-key crypto and hashing in systems



Implementation environments for symmetric cryptography

Efficiently provide confidentiality, authenticity, integrity

- until 1980s: dedicated machines, hardware implementing DES, LFSR-based approaches
- since 1990s: software implementations become more relevant in addition to hardware, see e.g. AES
- since 2010s: another boost for software-environments due to virtualization
- also since 2010s: programmable cryptography is becoming increasingly practical

New cryptographic functionalities are new applications of symmetric cryptography

- FHE: Reducing ciphertext expansion, OPRFs, ...
- MPC: Distributed databases, private set intersection, data analytics, OPRFs, public-key signature schemes
- ZKP: Use-cases of zero-knowledge proofs:
  - Set Membership Proofs ("I know a private key of one of the public keys of this Merkle tree")
  - Data Commitments ("Here is the Merkle tree of the execution trace of my program, I can open it at any point").
  - Outsourced Computation, "proof everything"

A Zoo of MPC/ZK-friendly concretely-efficient symmetric crypto

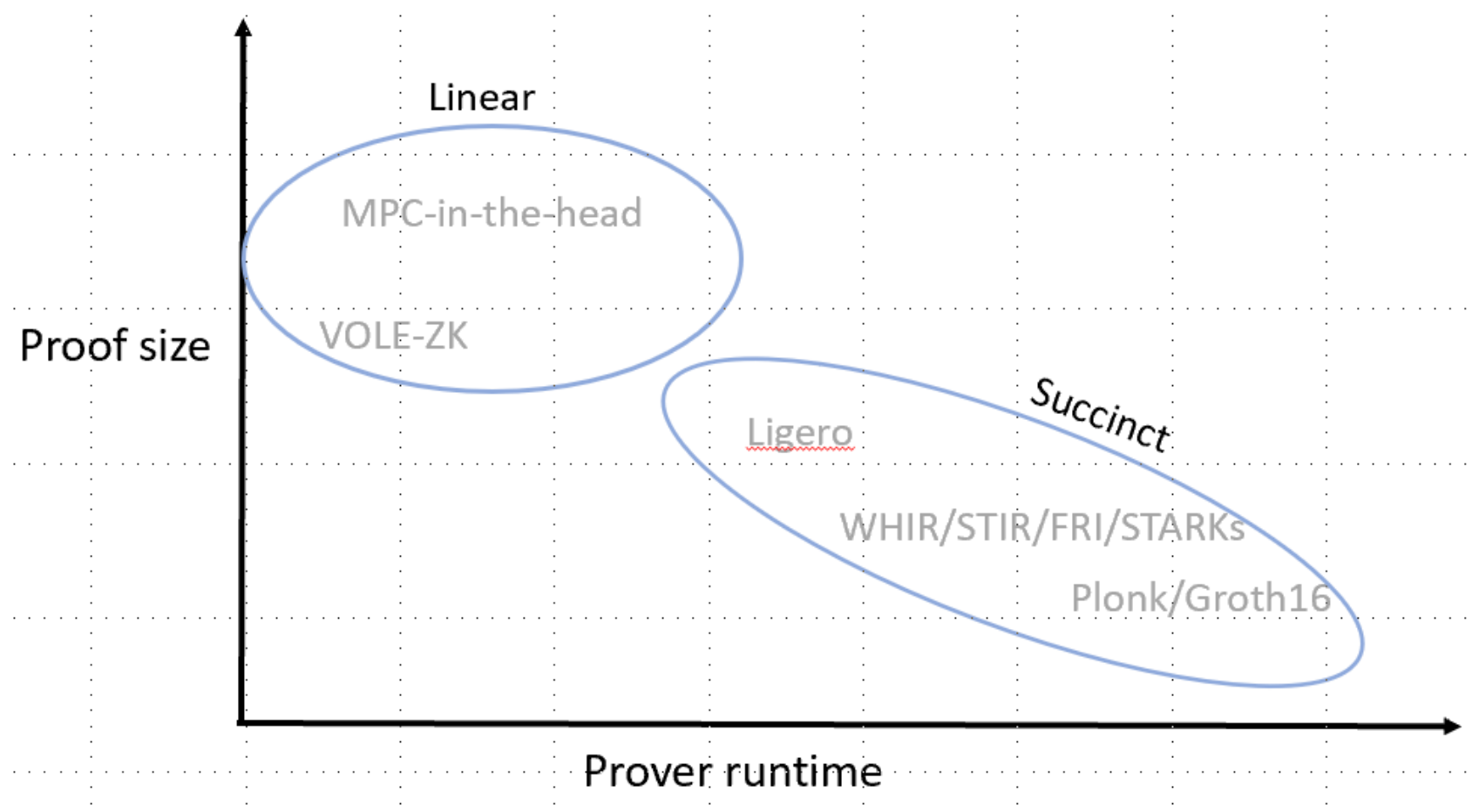
2015: 2	[Can+18; Alb+15]
2016: 2	[Gra+16; Alb+16]
2017: -	
2018: 2	[Bon+18; AD18]
2019: 4	[Alb+19; Aly+20; Gra+20; Gra+21]
2020: 1	[SAD20]
2021: 6	[Dob+21; Din+21; Sze21; Gra+22a; Dob+22; Gra+22b]
2022: 5	[Bou+23; AMT22; Gra+23b; Gra+23a; Ash+22]
2023: 6	[RST23; AKM23; Gra+24b; GKS23; Sze+23; Sal23]
2024: 3	[Ash+24; Gra+24a; AT24]
2025: 4	[Bal+25; Ha+25; Bou+25; Gra+26]

source: mostly IACR eprint, plus selection from IEEE Access, ToSC, arxiv

Included, but quite different: Signatures via MPC-in-the-head, VOLE-in-the-head

- 2017-2022: First NIST standardization process
  - Finalist Picnic based on MPCitH and LowMC
  - SPHINCS+ (hash based) was selected instead.
- since 2023: Additional signatures process at NIST
  - Lots of MPCitH-based submissions
  - Submission FAEST based on VOLEitH and AES (with Rain as a potential alternative OWF)

Families of ZK Proofs



The ZK-friendly Hash Function Zoo

Type 1

"low degree only"

- Low-degree

$$y = x^d$$

- Fast in Plain
- Many rounds
- Often more constraints
- MiMC(16), GMiMC (19), Poseidon (19), Neptune (21), Poseidon2 (23), Poseidon2b(25)

The ZK-friendly Hash Function Zoo

Type 1

"low degree only"

- Low-degree

$$y = x^d$$

- Fast in Plain
- Many rounds
- Often more constraints
- MiMC(16), GMiMC (19), Poseidon (19), Neptune (21), Poseidon2 (23), Poseidon2b(25)

Type 2

"non-procedural", "fluid"

- Low-degree equiv.

$$y = x^{1/d} \Rightarrow x = y^d$$

- Slow in Plain
- Fewer rounds
- Fewer constraints
- Friday(18), Vision(19), *Rescue* (19), Grendel(21), Rain(21), AIM(22), Griffin (22), Anemoi (22), Arion(23)

The ZK-friendly Hash Function Zoo

Type 1

"low degree only"

- Low-degree

$$y = x^d$$

- Fast in Plain
- Many rounds
- Often more constraints
- MiMC(16), GMiMC (19), Poseidon (19), Neptune (21), Poseidon2 (23), Poseidon2b(25)

Type 2

"non-procedural", "fluid"

- Low-degree equiv.

$$y = x^{1/d} \Rightarrow x = y^d$$

- Slow in Plain
- Fewer rounds
- Fewer constraints
- Friday(18), Vision(19), *Rescue* (19), Grendel(21), Rain(21), AIM(22), Griffin (22), Anemoi (22), Arion(23)

Type 3

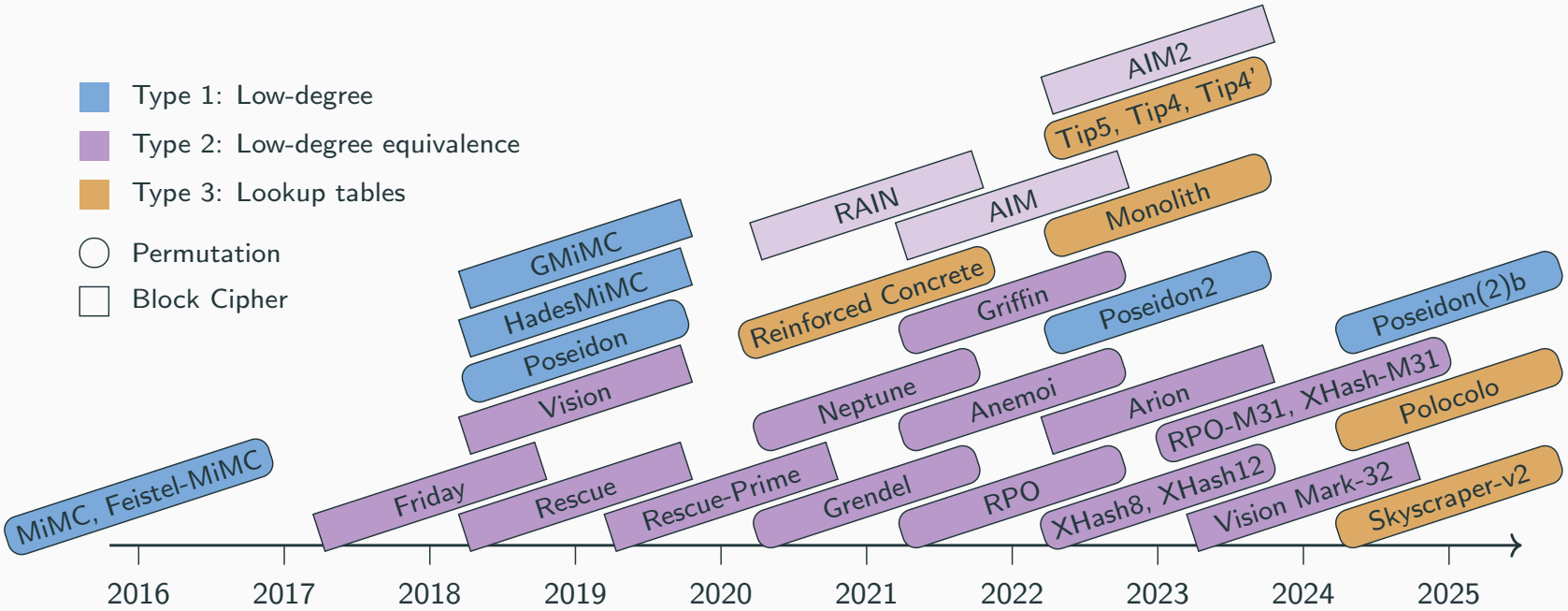
"lookups"

- Lookup tables

$$y = T[x]$$

- Very fast in Plain
- Even fewer rounds
- Constraints depend on proof system
- `Reinforced Concrete` (21), Tip5/Tip4 (23), `Monolith` (23), Skyscraper-v2(25), Polocolo (25)

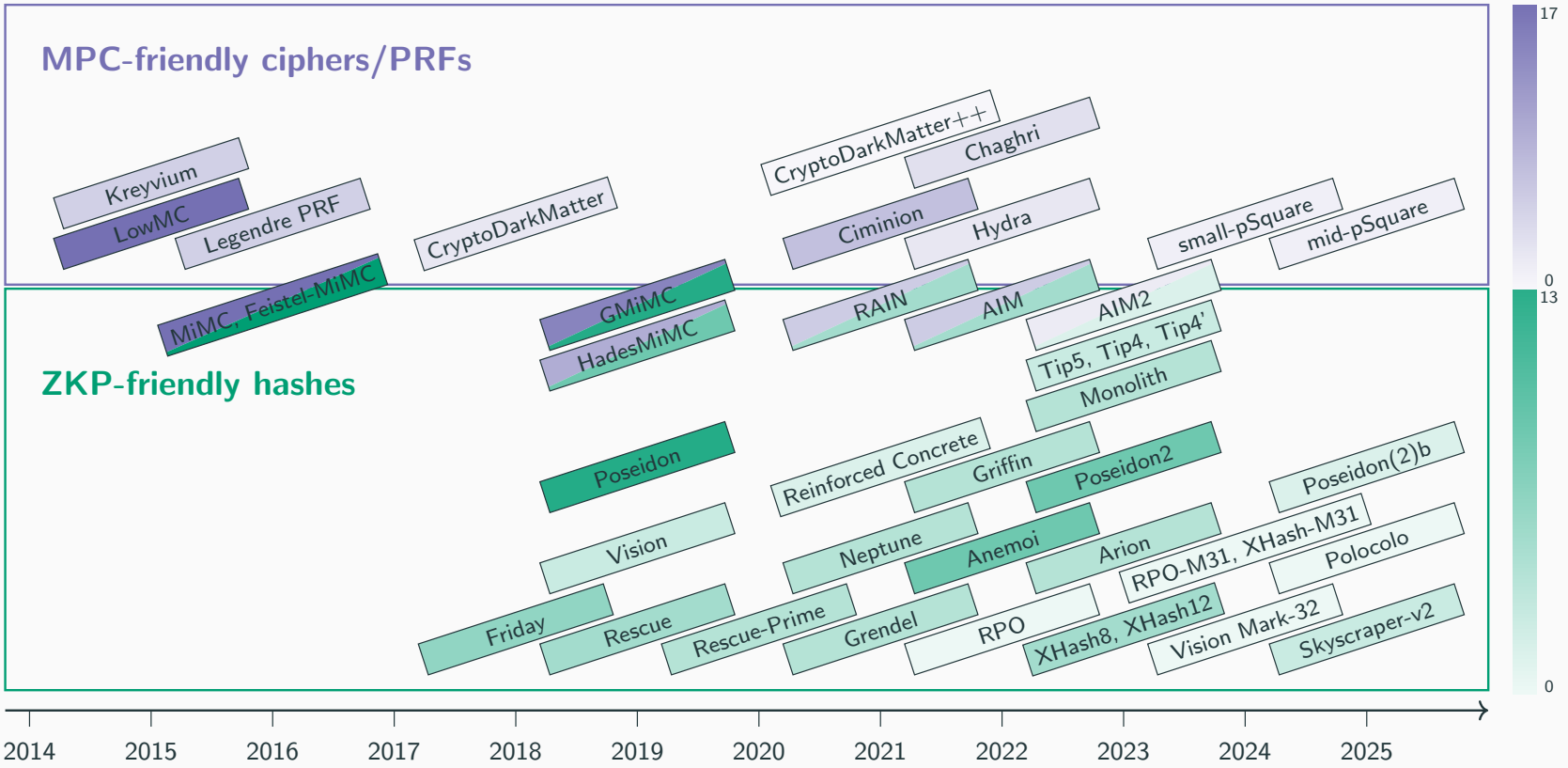
The ZK-friendly Hash Function Zoo



The MPC/Sharing-friendly Symmetric Crypto Zoo

- 2015: LowMC
- 2016: MiMC, LegendrePRF
- 2018: CryptoDarkMatter
- 2019: GMiMC
- 2020: HadesMiMC
- 2021: Ciminion, "CryptoDarkMatter++"
- 2022: Rain, AIM
- 2023: Hydra
- ongoing: GenLowMC (new: lookup aligned, dynamic generation of MPC circuit)

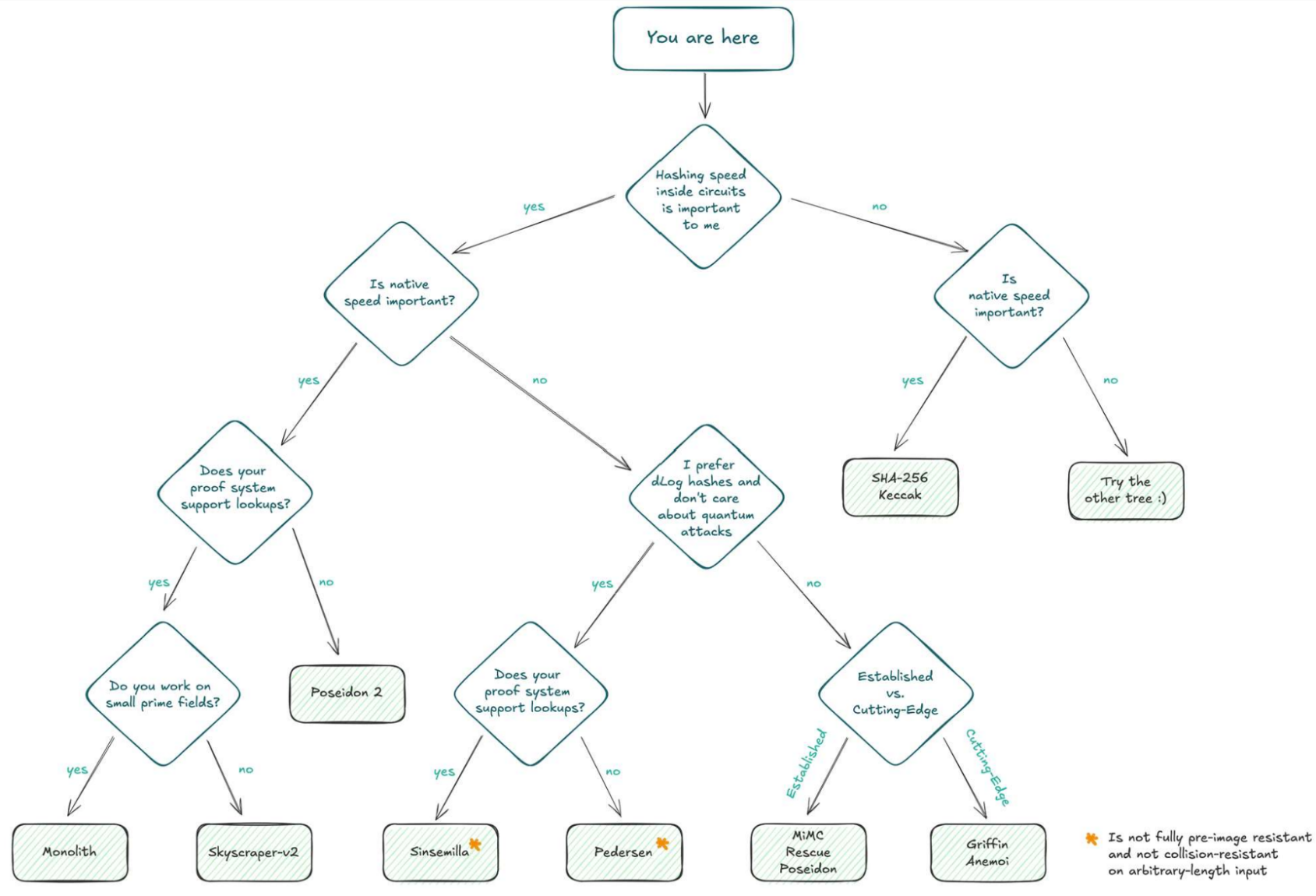
Cryptanalysis



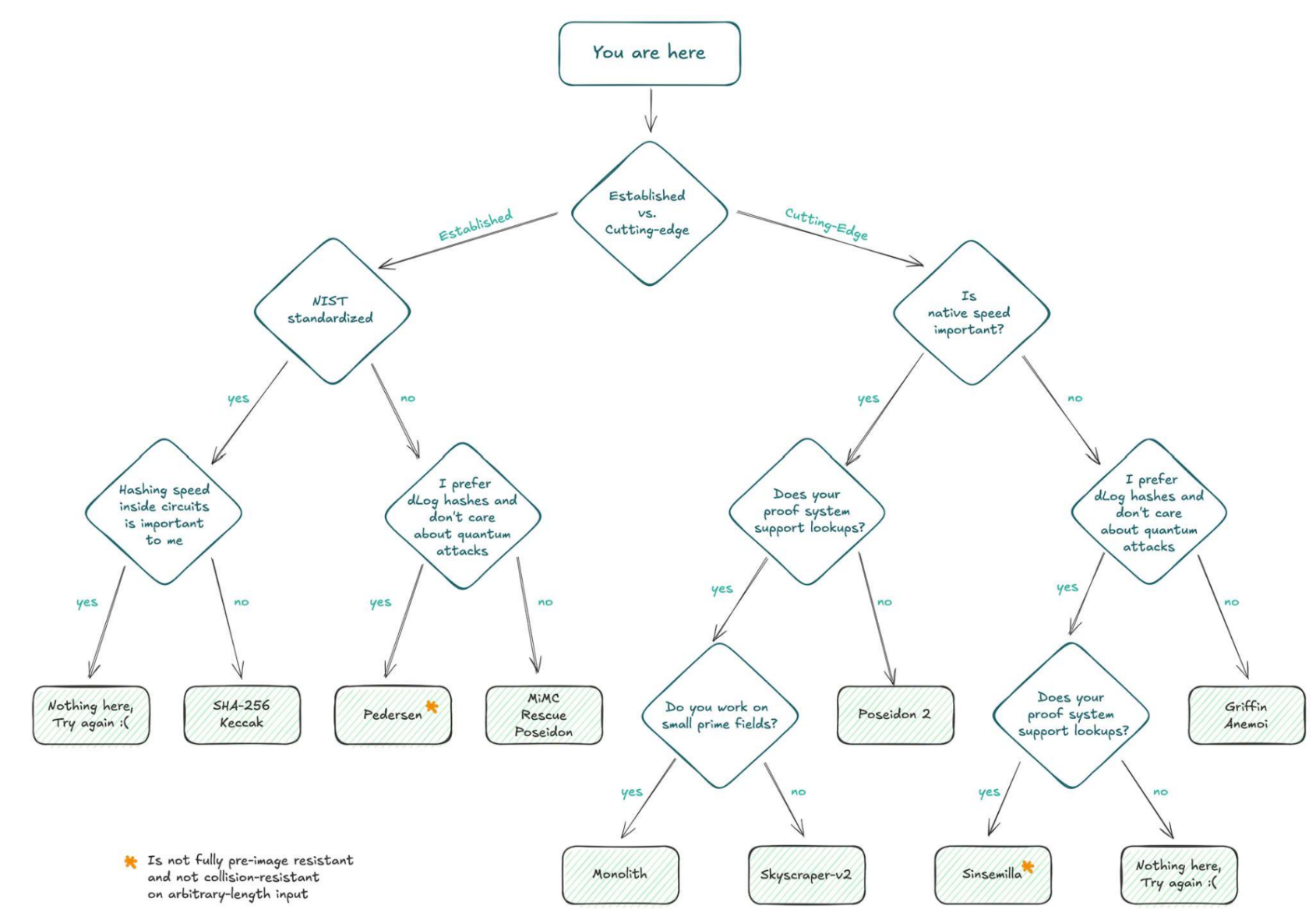
Cryptanalysis bounties/challenges/...

- Picnic/LowMC: Three rounds of challenges since 2020-2023:
  - winners: Subhadeep Banik, Khashayar Barooti, Serge Vaudenay, Hailun Yan, F. Betül Durak, Itai Dinur
  - `https://lowmcchallenge.github.io/`
- ZKProofs-friendly hashes, 2021-2022:
  - winners: Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, Léo Perrin
  - `https://www.zkhashbounties.info/`
- Ongoing: Poseidon cryptanalysis initiative (2024-2026)
  - winners (so far): Aurelien Boeuf, Antoine Bak, Augustin Bariant, Maël Hostettler, Guilhem Jazeron, Giuseppe Vitto, William Borgeaud, Ziyu Zhao, Jintai Ding, Simon-Philipp Merz, À̀lex Rodríguez
  - `https://www.poseidon-initiative.info/`
  - New challenges to be announced very soon (TM). Total sum around 1M.

How to choose? (1/2)



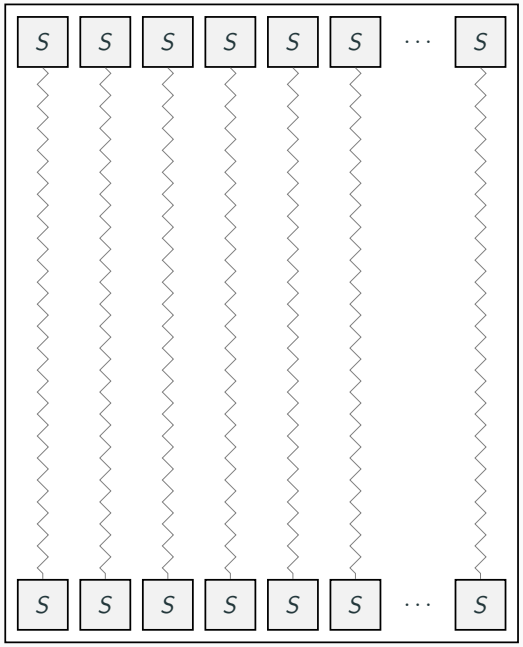
How to choose? (2/2)



S-Box sizes, over time. A selection

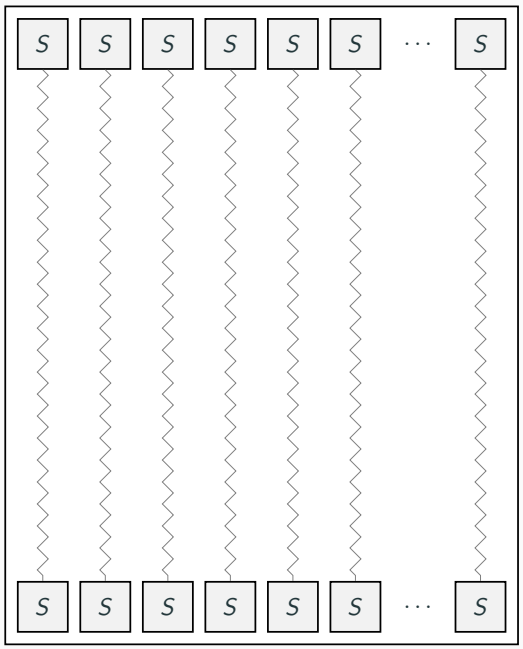
- mid 1970s, 6to4-bit: DES S-box just fits on a Chip
- mid 1990s, 8to8-bit: e.g. Rijndael/AES, attractive for good performance in both HW and SW
- since 2000, smaller, more "lightweight" S-boxes
  - 3to3-bit (e.g. Printcipher, LowMC)
  - 4to4-bit (e.g. Noekeon, Present, Klein, Prince)
  - 5to5-bit (e.g. Keccak, Ascon)
- since 2015, big and huge "S-boxes"
  - n to n-bit, elements in GF(2^n)
    - for n from 100 to 1000 (e.g. MiMC, Rain)
  - n to n-bit, elements in GF(p)
    - for n from 128 to $\geq$1000 (e.g. MiMC)
    - for n from 17 to 63 (e.g. Pasta)
    - for n from 8 to 256 (most in the ZK-friendly Zoo)

How to arrange the S-Boxes? SPNs with Partial Nonlinear Layers

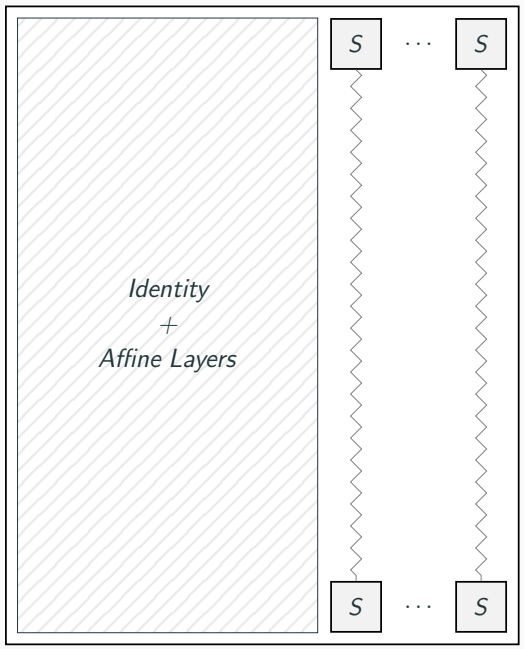


SPN
(e.g., SHARK in
1996)

How to arrange the S-Boxes? SPNs with Partial Nonlinear Layers

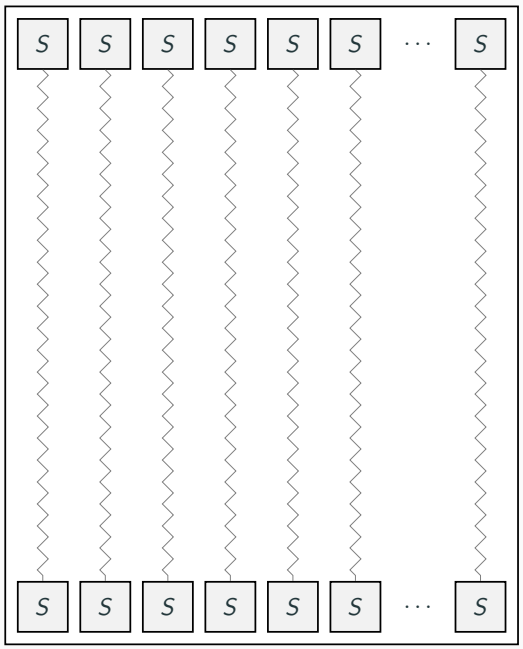


SPN
(e.g., SHARK in 1996)

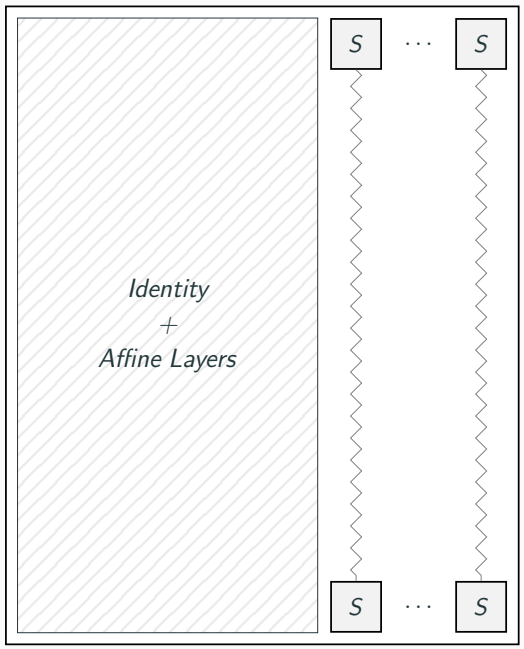


P-SPN since 2010
(e.g., ARMADILLO, Zorro, LowMC)

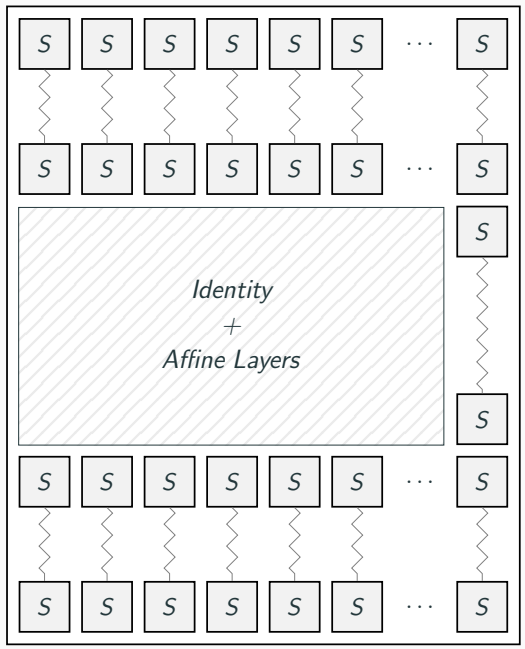
How to arrange the S-Boxes? SPNs with Partial Nonlinear Layers



SPN
(e.g., SHARK in 1996)



P-SPN since 2010
(e.g., ARMADILLO, Zorro, LowMC)



Hades
(e.g., HadesMiMC, Poseidon)

Thoughts on "Theory" vs. "Practice"

- Provable Security?
  - Modes of operation: do proofs carry over from F_2 to F_p?
  - SPN vs. Partial-SPN: First positive results by Guo, Standaert, Wang, Wang, Yu (FSE 22)
    - Stronger model, like indifferentiability?
  - "ZK-friendly" compression? New work by Andreeva, Bhattacharyya, Roy, Trevisani (CSF 24)
- "Asymptotic analysis" / "asymptotic designs".
  - Input: blocksize, security level
  - Output: concrete design with security claim
  - Some designs allow for it, e.g. HPC, LowMC, MiMC, Poseidon, ...
  - Pros: Flexibility
  - Cons: Less focused cryptanalysis.

Wanted

1) Consolidate spezialization tree of candidate hashes
2) A concretely efficient primitive for *Low-depth hashing*
   - ZK-friendly and simultaneously MPC-friendly
3) Generalization of results to non-binary/arbitrary fields
   - Proofs
   - Cryptanalysis techniques
4) Rings as underlying object instead of fields?

Standardization and Investments

NIST is organizing a Threshold Cryptography Process (two workshops in the last 2 years)
ZKproof.org community standard

- Large investments by governments
  - US DARPA, 100Ms of USD
  - EU Framework Programs
  - Asia?
- Even larger private investments
  - closer to 1B, early focus mostly on "ZK", now more activity in MPC incl. FHE

Conclusions

- Lots of exciting new developments in "high functionality cryptography" - some are likely here to stay
- Industry interest is growing
- Demand for standards to support interoperability and increase trust
- Lots of exciting research for design and analysis of symmetric crypto and hashing
- Even if you don't care about use-cases, super nice excuse to do new math, new symmetric crypto

Survey of MPC- and ZK-friendly Symmetric Cryptography

Christian Rechberger

May 10, 2026

TU Graz and TACEO

Bibliography i

Tomer Ashur and Siemen Dhooghe. *MARVELlous: a STARK-Friendly Family of Cryptographic Primitives*. IACR Cryptology ePrint Archive, Paper 2018/1098. 2018. URL: https://eprint.iacr.org/2018/1098.

Tomer Ashur, Al Kindi, and Mohammad Mahzoun. *XHash8 and XHash12: Efficient STARK-friendly Hash Functions*. IACR Cryptology ePrint Archive, Paper 2023/1045. 2023. URL: https://eprint.iacr.org/2023/1045.

Bibliography ii

Martin R. Albrecht et al. “Ciphers for MPC and FHE”. In: *EUROCRYPT 2015*. Vol. 9056. LNCS. Springer, 2015, pp. 430–454. DOI: 10.1007/978-3-662-46800-5_17. URL: https://eprint.iacr.org/2016/687.

Martin R. Albrecht et al. “MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity”. In: *ASIACRYPT 2016*. Vol. 10031. LNCS. 2016, pp. 191–219. DOI: 10.1007/978-3-662-53887-6_7. URL: https://eprint.iacr.org/2016/492.

Bibliography iii

Martin R. Albrecht et al. “Feistel Structures for MPC, and More”. In: *ESORICS 2019*. Vol. 11736. LNCS. Springer, 2019, pp. 151–171. DOI: 10.1007/978-3-030-29962-0_8. URL: https://eprint.iacr.org/2019/397.

Abdelrahaman Aly et al. “Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols”. In: *IACR Transactions on Symmetric Cryptology* 2020.3 (2020), pp. 1–45. DOI: 10.13154/tosc.v2020.i3.1-45. URL: https://eprint.iacr.org/2019/426.

Bibliography iv

Tomer Ashur, Mohammad Mahzoun, and Dilara Toprakhisar. "Chaghri – A FHE-friendly Block Cipher". In: *CCS 2022*. ACM, 2022, pp. 139–150. DOI: 10.1145/3548606.3559364. URL: https://eprint.iacr.org/2022/592.

Tomer Ashur et al. *Rescue-Prime Optimized*. IACR Cryptology ePrint Archive, Paper 2022/1577. 2022. URL: https://eprint.iacr.org/2022/1577.

Tomer Ashur et al. *Vision Mark-32: ZK-Friendly Hash Function Over Binary Tower Fields*. IACR Cryptology ePrint Archive, Paper 2024/633. 2024. URL: https://eprint.iacr.org/2024/633.

Bibliography v

Tomer Ashur and Sundas Tariq. *RPO-M31 and XHash-M31: Efficient Hash Functions for Circle STARKs*. IACR Cryptology ePrint Archive, Paper 2024/1635. 2024. URL: https://eprint.iacr.org/2024/1635.

Brieuc Balon et al. "mid-pSquare: Leveraging the Strong Side-Channel Security of Prime-Field Masking in Software". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.4 (2025), pp. 486–519. DOI: 10.46586/tches.v2025.i4.486-519. URL: https://eprint.iacr.org/2025/519.

Bibliography vi

Dan Boneh et al. “Exploring Crypto Dark Matter: – New Simple PRF Candidates and Their Applications”. In: *TCC 2018*. Vol. 11240. LNCS. Springer, 2018, pp. 699–729. DOI: 10.1007/978-3-030-03810-6_25. URL: https://eprint.iacr.org/2018/1218.

Bibliography vii

Clémence Bouvier et al. “New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode”. In: *CRYPTO 2023*. Vol. 14083. LNCS. Springer, 2023, pp. 507–539. DOI: 10.1007/978-3-031-38548-3_17. URL: https://eprint.iacr.org/2022/840.

Bibliography viii

Clémence Bouvier et al. “Skyscraper: Fast Hashing on Big Primes”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.2 (2025), pp. 743–780. DOI: 10.46586/tches.v2025.i2.743-780. URL: https://eprint.iacr.org/2025/058.

Anne Canteaut et al. “Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression”. In: *Journal of Cryptology* 31.3 (2018), pp. 885–916. DOI: 10.1007/s00145-017-9273-9. URL: https://eprint.iacr.org/2015/113.

Bibliography ix

Itai Dinur et al. “MPC-Friendly Symmetric Cryptography from Alternating Moduli: Candidates, Protocols, and Applications”. In: *CRYPTO 2021*. Vol. 12828. LNCS. Springer, 2021, pp. 517–547. DOI: 10.1007/978-3-030-84259-8_18. URL: https://eprint.iacr.org/2021/885.

Christoph Dobraunig et al. “Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields”. In: *EUROCRYPT 2021*. Vol. 12697. LNCS. Springer, 2021, pp. 3–34. DOI: 10.1007/978-3-030-77886-6_1. URL: https://eprint.iacr.org/2021/267.

Bibliography x

Christoph Dobraunig et al. “Shorter Signatures Based on Tailor-Made Minimalist Symmetric-Key Crypto”. In: *CCS 2022*. ACM, 2022, pp. 843–857. DOI: 10.1145/3548606.3559353. URL: https://eprint.iacr.org/2021/692.

Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. “Poseidon2: A Faster Version of the Poseidon Hash Function”. In: *AFRICACRYPT 2023*. Vol. 14064. LNCS. Springer, 2023, pp. 177–203. DOI: 10.1007/978-3-031-37679-5_8. URL: https://eprint.iacr.org/2023/323.

Lorenzo Grassi et al. “MPC-Friendly Symmetric Key Primitives”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. ACM, 2016, pp. 430–443. DOI: 10.1145/2976749.2978332. URL: https://eprint.iacr.org/2016/542.

Lorenzo Grassi et al. “On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy”. In: *EUROCRYPT 2020*. Vol. 12106. LNCS. Springer, 2020, pp. 674–704. DOI: 10.1007/978-3-030-45724-2_23. URL: https://eprint.iacr.org/2019/1107.

Lorenzo Grassi et al. “Poseidon: A New Hash Function for Zero-Knowledge Proof Systems”. In: *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*. USENIX Association, 2021, pp. 519–535. URL: https://eprint.iacr.org/2019/458.

Lorenzo Grassi et al. “Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over Fnp Application to Poseidon”. In: *IACR Transactions on Symmetric Cryptology* 2022.3 (2022), pp. 20–72. DOI: 10.46586/tosc.v2022.i3.20-72. URL: https://eprint.iacr.org/2021/1695.

Lorenzo Grassi et al. “Reinforced Concrete: A Fast Hash Function for Verifiable Computation”. In: *CCS 2022*. ACM, 2022, pp. 1323–1335. DOI: 10.1145/3548606.3560686. URL: https://eprint.iacr.org/2021/1038.

Bibliography xiv

Lorenzo Grassi et al. “From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications”. In: *EUROCRYPT 2023*. Vol. 14007. LNCS. Springer, 2023, pp. 255–286. DOI: 10.1007/978-3-031-30634-1_9. URL: https://eprint.iacr.org/2022/342.

Lorenzo Grassi et al. “Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications”. In: *CRYPTO 2023*. Vol. 14083. LNCS. Springer, 2023, pp. 573–606. DOI: 10.1007/978-3-031-38548-3_19. URL: https://eprint.iacr.org/2022/403.

Lorenzo Grassi et al. “Generalized Feistel Ciphers for Efficient Prime Field Masking”. In: *EUROCRYPT 2024*. Vol. 14653. LNCS. Springer, 2024, pp. 188–220. DOI: 10.1007/978-3-031-58734-4_7. URL: https://eprint.iacr.org/2024/431.

Lorenzo Grassi et al. “Monolith: Circuit-Friendly Hash Functions with New Nonlinear Layers for Fast and Constant-Time Implementations”. In: *IACR Transactions on Symmetric Cryptology* 2024.3 (2024), pp. 44–83. DOI: 10.46586/tosc.v2024.i3.44-83. URL: https://eprint.iacr.org/2023/1025.

Lorenzo Grassi et al. “Poseidon(2)b: Binary Field Versions of Poseidon/Poseidon2”. In: *IACR Communications in Cryptology* 2.4 (2026), p. 15. DOI: 10.62056/a66ce0zn4. URL: https://eprint.iacr.org/2025/1893.

Jincheol Ha et al. “Polocolo: A ZK-Friendly Hash Function Based on S-Boxes Using Power Residues”. In: *EUROCRYPT 2025*. Vol. 15604. LNCS. Springer, 2025, pp. 303–332. DOI: 10.1007/978-3-031-91134-7_11. URL: https://eprint.iacr.org/2025/926.

Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani. "Arion: Arithmetization-Oriented Permutation and Hashing from Generalized Triangular Dynamical Systems". In: *CoRR* abs/2303.04639 (2023). DOI: 10.48550/arxiv.2303.04639. arXiv: 2303.04639.

Alan Szepieniec, Tomer Ashur, and Siemen Dhooghe. *Rescue-Prime: a Standard Specification (SoK)*. IACR Cryptology ePrint Archive, Paper 2020/1143. 2020. URL: https://eprint.iacr.org/2020/1143.

Robin Salen. *Two additional instantiations from the Tip5 hash function construction*. 2023. URL: https://toposware.com/paper_tip5.pdf.

Alan Szepieniec et al. *The Tip5 Hash Function for Recursive STARKs*. IACR Cryptology ePrint Archive, Paper 2023/107. 2023. URL: https://eprint.iacr.org/2023/107.

Alan Szepieniec. *On the Use of the Legendre Symbol in Symmetric Cipher Design*. IACR Cryptology ePrint Archive, Paper 2021/984. 2021. URL: https://eprint.iacr.org/2021/984.