From Farfalle to MEGAFONO via CIMINION: The PRF HYDRA for MPC Applications

Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, **Roman Walch**

25.04.2023

SCIENCE
PASSION
TECHNOLOGY

Domain Specific Symmetric Primitives

- Modern cryptographic protocols
  - MPC: Multiple parties jointly compute a function on private input
  - HE: Compute on encrypted data
  - ZKP: Proof validity of statements without leaking witnesses
- Symmetric Primitives are useful in these protocols
- ... but have different design criteria:
  - Prime fields
  - Minimizing multiplicative complexity/depth

⇒ Many new primitives designed

Domain Specific Symmetric Primitives

- Modern cryptographic protocols
  - MPC: Multiple parties jointly compute a function on private input
  - HE: Compute on encrypted data
  - ZKP: Proof validity of statements without leaking witnesses
- Symmetric Primitives are useful in these protocols
- ... but have different design criteria:
  - Prime fields
  - Minimizing multiplicative complexity/depth

$\Rightarrow$ Many new primitives designed

Symmetric Primitives for MPC

- Use cases:
  - Encryption/decryption with unknown key
    - Key-Management: Software HSM via MPC
    - Suspending expensive MPC computations
    - Transferring data into/out of delegated MPC computations

  $\Rightarrow$ Symmetric key is secret shared in MPC
- Cost target: Mainly minimizing number of multiplications
- MiMC, GMiMC, HadesMiMC, *Rescue*, Ciminion, ...

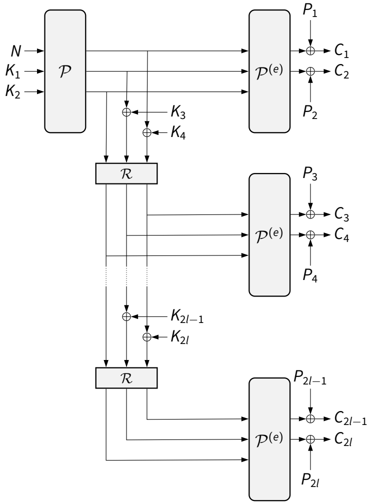
Symmetric Primitives for MPC

- Use cases:
  - Encryption/decryption with unknown key
    - Key-Management: Software HSM via MPC
    - Suspending expensive MPC computations
    - Transferring data into/out of delegated MPC computations

  $\Rightarrow$ Symmetric key is secret shared in MPC
- Cost target: Mainly minimizing number of multiplications
- MiMC, GMiMC, HadesMiMC, *Rescue*, Ciminion, ...

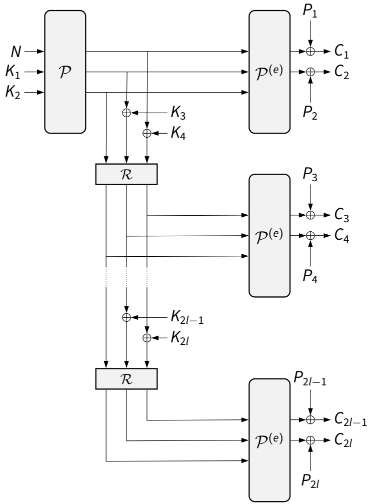
CIMINION (Eurocrypt 2021)

- Based on a modified Farfalle [BDH+17]
  - Expensive Permutation $\mathcal{P}$
  - Cheaper Permutation $\mathcal{P}^{(e)}$
    - Fast for encrypting large data
- Problem:
  - Round keys K_i created by expensive hash function instantiated with $\mathcal{P}$
  - Only efficient in MPC if key schedule can be discarded
  - Not the case in many use cases!



CIMINION (Eurocrypt 2021)

- Based on a modified Farfalle [BDH+17]
  - Expensive Permutation $\mathcal{P}$
  - Cheaper Permutation $\mathcal{P}^{(e)}$
    - Fast for encrypting large data
- Problem:
  - Round keys K_i created by expensive hash function instantiated with $\mathcal{P}$
  - Only efficient in MPC if key schedule can be discarded
  - Not the case in many use cases!

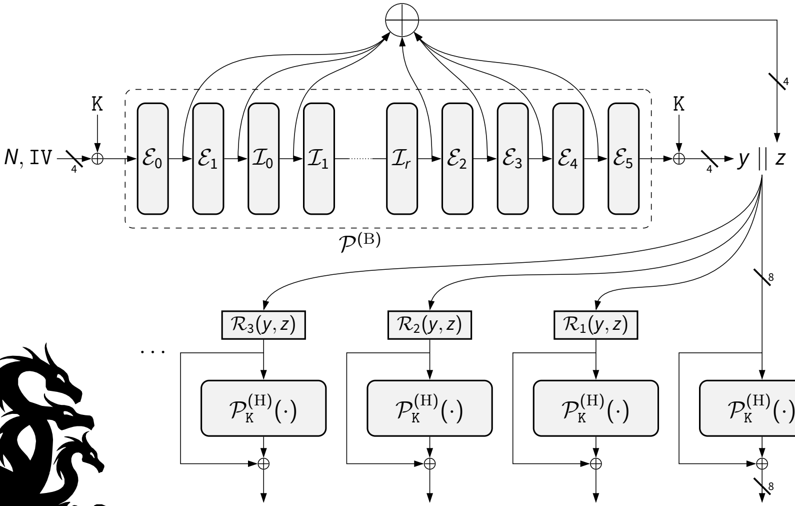


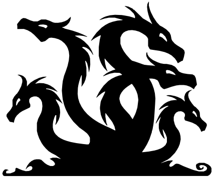
Goals and Contribution

- Goal:
  - MPC-friendly cipher as efficient as CIMINION
  - ... without expensive key schedule
- Contribution:
  - MEGAFONO design strategy
  - Efficient instantiation: The PRF HYDRA
    - Extendable output, used as stream cipher

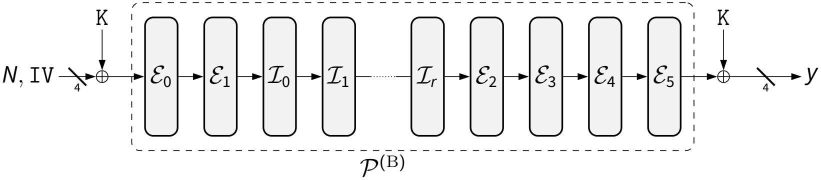
Hydra: A Megafono based PRF

MEGAFONO and the PRF Hydra



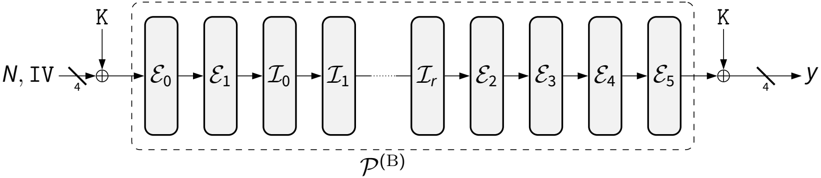


The body of MEGAFONO/HYDRA



- Even-Mansour construction [EM97]
  - If $\mathcal{P}^{(B)}$ is PRP, attacker cannot know/control y
  - Allows cheaper and more efficient heads
- Cheaper Heads:
  - Cost of expensive body amortized for large data
  - Similar to CIMINION

The body of MEGAFONO/HYDRA



- Even-Mansour construction [EM97]
  - If $\mathcal{P}^{(B)}$ is PRP, attacker cannot know/control y
  - Allows cheaper and more efficient heads
- Cheaper Heads:
  - Cost of expensive body amortized for large data
  - Similar to CIMINION

Transitions to the Heads of MEGAFONO/HYDRA

- Unpredictable y already prevents many statistical attacks in Heads
  - Main concern of heads: Algebraic attacks
  - Strongest vector: Gröbner basis
  - Cost depends on degree and number of variables
- In CIMINION
  - Additional independent variables created by expensive key schedule
  - Key schedule instantiated as sponge with $\mathcal{P}^{(B)}$

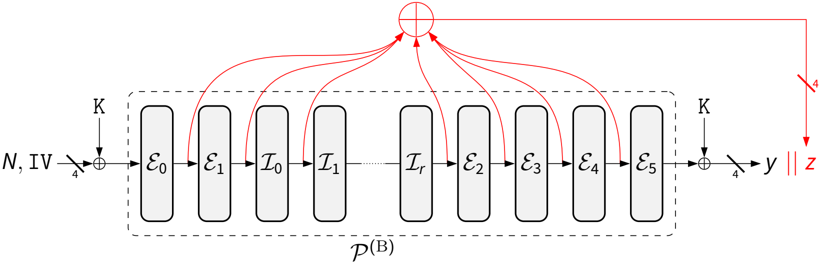
  $\Rightarrow$ Allows efficient $\mathcal{P}^{(e)}$ with low-degree round functions

Transitions to the Heads of MEGAFONO/HYDRA

- Unpredictable y already prevents many statistical attacks in Heads
  - Main concern of heads: Algebraic attacks
  - Strongest vector: Gröbner basis
  - Cost depends on degree and number of variables
- In CIMINION
  - Additional independent variables created by expensive key schedule
  - Key schedule instantiated as sponge with $\mathcal{P}^{(B)}$

$\Rightarrow$ Allows efficient $\mathcal{P}^{(e)}$ with low-degree round functions

The body of MEGAFONO/HYDRA (cont.)



- New idea in MEGAFONO:
  - Create new variables z from intermediate results for free!
- Expensive relations between z, K, and y

$\Rightarrow$ Attacker forced to treat z as new variable

$\Rightarrow$ More variables as in CIMINION, but without key schedule

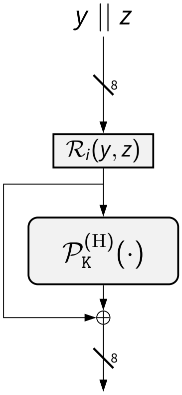
The Heads of MEGAFONO/HYDRA

- Main concern: Algebraic attacks
  - Goal: Prevent inversion and cheap equation systems without K, y, or z
- Keyed permutation $\mathcal{P}_{\mathrm{K}}^{(\mathrm{H})}$ reintroduces K
- Combining multiple heads can cancel out y, z

  $\Rightarrow$ Prevented by feed forward!

$\Rightarrow$ No truncation necessary to prevent inversion

  - More throughput compared to CIMINION
- Non-linear rolling function $\mathcal{R}_i$

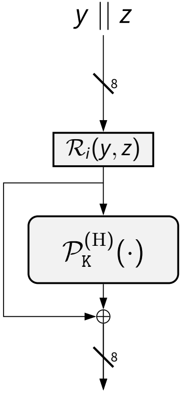


The Heads of MEGAFONO/HYDRA

- Main concern: Algebraic attacks
  - Goal: Prevent inversion and cheap equation systems without K, y, or z
- Keyed permutation $\mathcal{P}_{\mathrm{K}}^{(\mathrm{H})}$ reintroduces K
- Combining multiple heads can cancel out y, z

  $\Rightarrow$ Prevented by feed forward!

$\Rightarrow$ No truncation necessary to prevent inversion
  - More throughput compared to CIMINION
- Non-linear rolling function $\mathcal{R}_i$



Hydra: Concrete Instantiation

Hydra: Instantiation

- Body instantiated as Hades [GLR+20]
  - External rounds prevent statistical attacks via wide trail design strategy
    - Cheap MDS matrix and power maps $x \mapsto x^d$
  - Internal rounds prevent algebraic attacks
    - Generalized Lai-Massey construction [LM90]

$$\text{Variants of} \quad y_i = x_i + \left(\sum_h (-1)^h \cdot x_h \right)^2$$

    - Less multiplications than power maps for same degree
    - Cheap matrix to prevent invariant subspace trail
- Heads instantiated similar to internal rounds
- Rolling function also based on generalized Lai-Massey

HYDRA: Instantiation

- Body instantiated as HADES [GLR+20]
  - External rounds prevent statistical attacks via wide trail design strategy
    - Cheap MDS matrix and power maps $x \mapsto x^d$
  - Internal rounds prevent algebraic attacks
    - Generalized Lai-Massey construction [LM90]

$$\text{Variants of} \quad y_i = x_i + \left(\sum_h (-1)^h \cdot x_h \right)^2$$

    - Less multiplications than power maps for same degree
    - Cheap matrix to prevent invariant subspace trail
- Heads instantiated similar to internal rounds
- Rolling function also based on generalized Lai-Massey

HYDRA: Instantiation

- Body instantiated as HADES [GLR+20]
  - External rounds prevent statistical attacks via wide trail design strategy
    - Cheap MDS matrix and power maps $x \mapsto x^d$
  - Internal rounds prevent algebraic attacks
    - Generalized Lai-Massey construction [LM90]

$$\text{Variants of} \quad y_i = x_i + \left(\sum_h (-1)^h \cdot x_h \right)^2$$

    - Less multiplications than power maps for same degree
    - Cheap matrix to prevent invariant subspace trail
- Heads instantiated similar to internal rounds
- Rolling function also based on generalized Lai-Massey

Number of Rounds for 128 bit Prime

- 6 external rounds in Body
  - 8 multiplications per round
  - Same as HadesMiMC [GLR+20]
- 42 internal rounds in Body
  - 2 multiplications per round
  - Strongest attack: Interpolation attack
  - 71 in HadesMiMC with same number of multiplications
- 39 rounds in Heads
  - 1 multiplication per round
  - Strongest attack: Gröbner Basis when attacking two heads

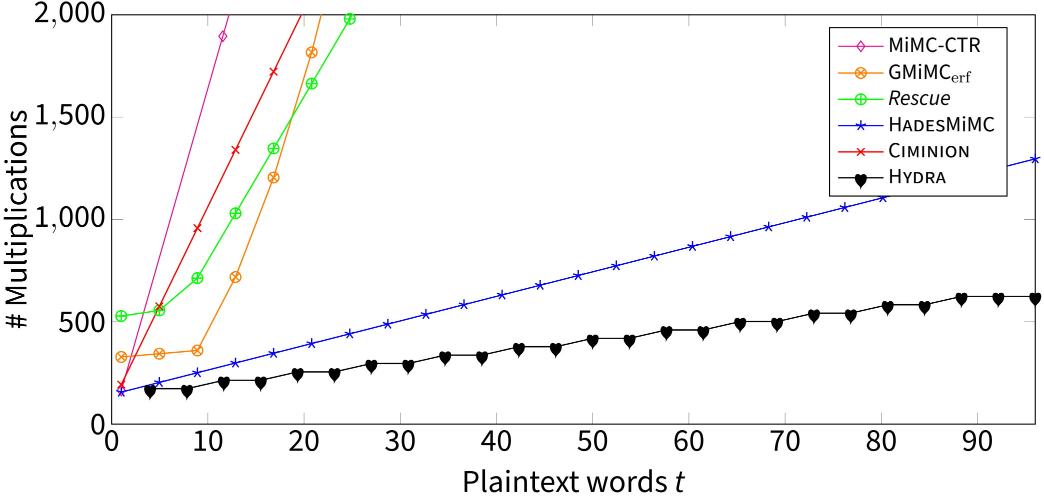
Number of Rounds for 128 bit Prime

- 6 external rounds in Body
  - 8 multiplications per round
  - Same as HADESMiMC [GLR+20]
- 42 internal rounds in Body
  - 2 multiplications per round
  - Strongest attack: Interpolation attack
  - 71 in HADESMiMC with same number of multiplications
- 39 rounds in Heads
  - 1 multiplication per round
  - Strongest attack: Gröbner Basis when attacking two heads

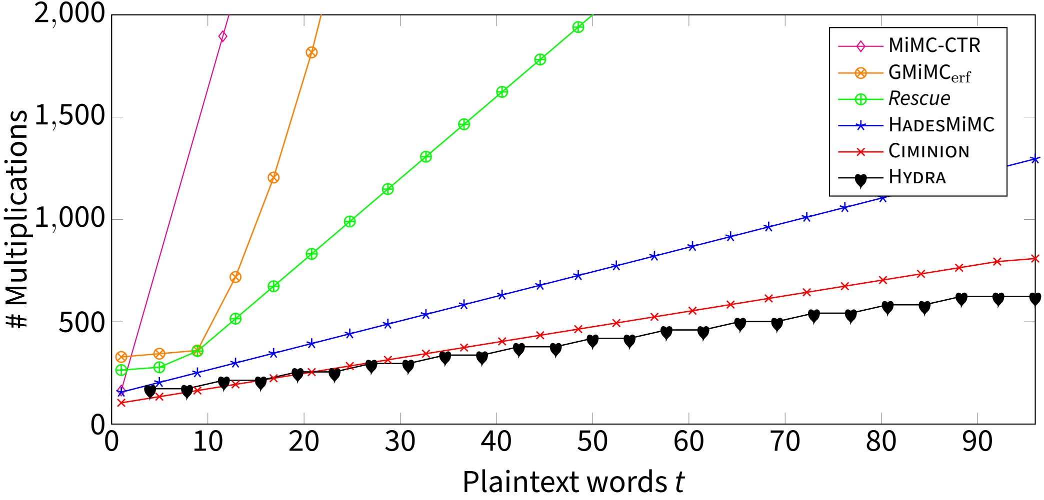
Number of Rounds for 128 bit Prime

- 6 external rounds in Body
  - 8 multiplications per round
  - Same as HadesMiMC [GLR+20]
- 42 internal rounds in Body
  - 2 multiplications per round
  - Strongest attack: Interpolation attack
  - 71 in HadesMiMC with same number of multiplications
- 39 rounds in Heads
  - 1 multiplication per round
  - Strongest attack: Gröbner Basis when attacking two heads

Multiplicative Complexity – With Key Schedules



Multiplicative Complexity – Without Key Schedules



Benchmarks

- In paper: Benchmarks using the MP-SPDZ library
  - SPDZ, 2 parties, LAN, offline + online phase
  - Encrypting *t* plaintext words with secret shared key
- Confirm expectation from previous slides
  - Hydra significantly outperforms other ciphers
  - Only Ciminion (without key schedule) is slightly faster for small *t*
- Implementation Framework:
  - `https://extgit.iaik.tugraz.at/krypto/mpc-zoo`

Summary

- MEGAFONO
  - New Farfalle based design strategy
- HYDRA:
  - Efficient and secure variant of Farfalle/CIMINION without key schedule
  - Minimized multiplicative complexity
  - Most efficient PRF in MPC
- Paper with extensive security analysis and benchmarks
  - https://eprint.iacr.org/2022/342.pdf
- Any further security analysis is welcome ☺

Questions

SCIENCE
PASSION
TECHNOLOGY

From Farfalle to MEGAFONO via CIMINION: The PRF HYDRA for MPC Applications

Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, **Roman Walch**

25.04.2023

Bibliography I

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. **Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols**. IACR Trans. Symmetric Cryptol. 2020.3 (2020), pp. 1–45.

[AGP+19] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. **Feistel Structures for MPC, and More**. ESORICS (2). Vol. 11736. Lecture Notes in Computer Science. Springer, 2019, pp. 151–171.

[AGR+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. **MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity**. ASIACRYPT (1). Vol. 10031. Lecture Notes in Computer Science. 2016, pp. 191–219.

[BDH+17] Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. **Farfalle: parallel permutation-based cryptography**. IACR Trans. Symmetric Cryptol. 2017.4 (2017), pp. 1–38.

Bibliography II

[DGGK21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. **Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields.** EUROCRYPT (2). Vol. 12697. Lecture Notes in Computer Science. Springer, 2021, pp. 3–34.

[EM97] Shimon Even and Yishay Mansour. **A Construction of a Cipher from a Single Pseudorandom Permutation.** J. Cryptol. 10.3 (1997), pp. 151–162.

[GLR+20] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. **On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy.** EUROCRYPT (2). Vol. 12106. Lecture Notes in Computer Science. Springer, 2020, pp. 674–704.

[LM90] Xuejia Lai and James L. Massey. **A Proposal for a New Block Encryption Standard.** EUROCRYPT. Vol. 473. Lecture Notes in Computer Science. Springer, 1990, pp. 389–404.