SCIENCE
PASSION
TECHNOLOGY

On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy

Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, **Markus Schofnegger**

Eurocrypt 2020

The Current Situation

- General-purpose ciphers for “traditional” use cases
  - E.g., for pure encryption AES is fine
- But: Many new use cases recently (MPC, STARKs, FHE, ...)
- They benefit from certain properties
  - E.g., multiplication count, multiplication depth
  - Working directly over $\mathbb{F}_p$ for large p
- Existing constructions not well-suited for many of these use cases

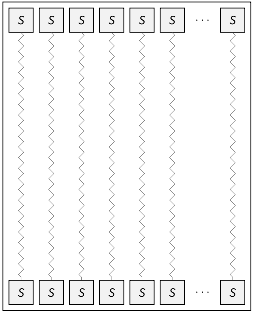
The Current Situation

- General-purpose ciphers for “traditional” use cases
  - E.g., for pure encryption AES is fine
- But: Many new use cases recently (MPC, STARKs, FHE, ...)
- They benefit from certain properties
  - E.g., multiplication count, multiplication depth
  - Working directly over $\mathbb{F}_p$ for large p
- Existing constructions not well-suited for many of these use cases

The Current Situation

- General-purpose ciphers for “traditional” use cases
  - E.g., for pure encryption AES is fine
- But: Many new use cases recently (MPC, STARKs, FHE, …)
- They benefit from certain properties
  - E.g., multiplication count, multiplication depth
  - Working directly over $\mathbb{F}_p$ for large p
- Existing constructions not well-suited for many of these use cases

SPNs with Partial Nonlinear Layers

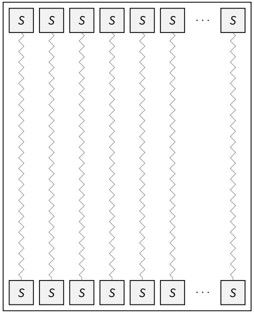


SPN
(e.g., SHARK in 1996)

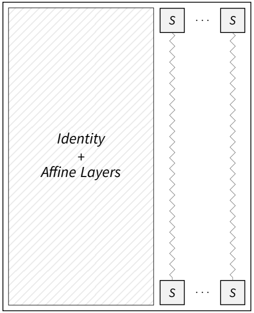
P-SPN
(e.g., Zorro in 2013 and LowMC in 2015)

HADES
(e.g., HADESMiMC)

≫ SPNs with Partial Nonlinear Layers



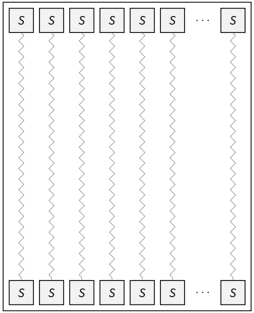
SPN
(e.g., SHARK in 1996)



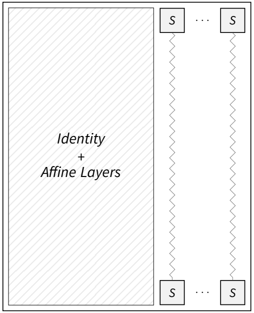
P-SPN
(e.g., `Zorro` in 2013 and LowMC in 2015)

HADES
(e.g., HADESMiMC)

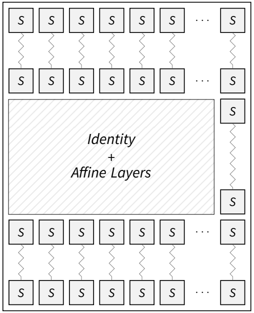
SPNs with Partial Nonlinear Layers



SPN
(e.g., SHARK in 1996)



P-SPN
(e.g., `Zorro` in 2013 and LowMC in 2015)



HADES
(e.g., HADESMiMC)

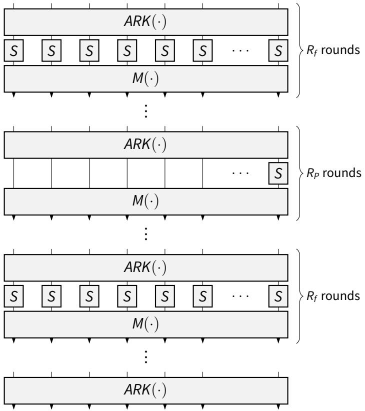
The HADES Design Strategy

Hades in a Nutshell

- Rounds with full nonlinear layers
  - At the beginning and at the end
  - Wide trail strategy for protection against diff./lin. attacks
  - Conjectured security and analysis for other stat. attacks
- Rounds with partial nonlinear layers
  - In the middle
  - Increase the degrees in a "cheaper" way
  - Used against algebraic attacks

Hades in a Nutshell cont.

- S-box size n, number of S-boxes in full rounds t
- Design is very flexible
  - Choose n and t almost freely
- Optimizations for many partial rounds [DKP+19]
- Reference implementations available[1]



[1] https://extgit.iaik.tugraz.at/krypto/hadesmimc/

Concrete Instantiation and Cryptanalysis

Concrete Instantiation

- Details
  - Field: $\mathbb{F}_p$, where $p \approx 2^{128}$
  - One S-box $f(x) = x^3$ in the partial rounds
  - Cauchy matrix with specific starting sequence
- Inverse is expensive, but for our setting we only need the encryption direction!

Concrete Instantiation

- Details
  - Field: $\mathbb{F}_p$, where $p \approx 2^{128}$
  - One S-box $f(x) = x^3$ in the partial rounds
  - Cauchy matrix with specific starting sequence
- Inverse is expensive, but for our setting we only need the encryption direction!

Cryptanalysis

- Two security levels
  - State size security: $\approx t \cdot \log_2(p)$ bits
  - S-box size security: $\approx \log_2(p)$ bits
- Focus on small security level for multi-party computation (MPC) use case
  - Elements and multipliers in $\mathbb{F}_p$, where $p \approx 2^{128}$
  - Key size $\approx$ 128 bits
  - Data $\leqslant \sqrt{p}$

Goal of HADES – The MPC Use Case

Goal of HADES – The MPC Use Case

- Setting: Secret-sharing-based MPC system (MP-SPDZ framework[2])
- Cost metric – roughly speaking:
  - Linear and affine functions: Almost free
  - Nonlinear functions: Expensive
- Multiplication requires communication between parties
  - Total number of multiplication is a good estimate for the complexity
- Small number of multiplications is crucial to reduce communication overhead

[2] https://github.com/data61/MP-SPDZ

Goal of HADES – The MPC Use Case

- Setting: Secret-sharing-based MPC system (MP-SPDZ framework[2])
- Cost metric – roughly speaking:
  - Linear and affine functions: Almost free
  - Nonlinear functions: Expensive
- Multiplication requires communication between parties
  - Total number of multiplication is a good estimate for the complexity
- Small number of multiplications is crucial to reduce communication overhead

[2] https://github.com/data61/MP-SPDZ

Benchmark of HadesMiMC (and Others) in MPC Setting cont.

Cipher	Online			Runtime	
	Lat.(ms)	$\mathbb{F}_p$/s	Comm./$\mathbb{F}_p$	$\mathbb{F}_p$/s	Comm./$\mathbb{F}_p$
HadesMiMC$_2$	3.85	117358	**1.90**	**261**	**266**
MiMC$_2$	**3.53**	79728	3.50	192	366
Rescue $_2$	5.54	23464	6.10	70	971
HadesMiMC$_4$	1.90	185160	**1.14**	**526**	**133.2**
MiMC$_4$	1.69	83876	3.50	192	366
Rescue $_4$	**1.25**	46890	3.08	136	485
HadesMiMC$_{32}$	**0.32**	258610	**0.39**	**1098**	**60.8**
MiMC$_{32}$	0.34	87831	3.5	192	366
Rescue $_{32}$	0.42	57695	1.93	274	243

The tests are done over LAN for $t \in \{2, 4, 32\}$, the total size is $N = 128 \cdot t$ bits, and MiMC is used in counter mode. The security level of *Rescue* is higher.

Open Problems and Future Work

- More use cases
  - HADES strategy used for STARKAD and POSEIDON [GKK+19]
- Improve understanding of higher-order differential attacks over $\mathbb{F}_p$
- Cryptanalytic differences between full rounds and partial rounds
  - Properties of the linear layer (see [KR20], [BCD+20], [GRS20])

Thanks!

References I

[BCD+20] Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer. **Out of Oddity - New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems.** IACR Cryptology ePrint Archive 2020 (2020), p. 188.

[DKP+19] Itai Dinur, Daniel Kales, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. **Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC.** EUROCRYPT (1). Vol. 11476. Lecture Notes in Computer Science. Springer, 2019, pp. 343–372.

[GKK+19] Lorenzo Grassi, Daniel Kales, Dmitry Khovratovich, Arnab Roy, Christian Rechberger, and Markus Schofnegger. **Starkad and Poseidon: New Hash Functions for Zero Knowledge Proof Systems.** IACR Cryptology ePrint Archive 2019 (2019), p. 458.

References II

[GRS20] Lorenzo Grassi, Christian Rechberger, and Markus Schofnegger. **Weak Linear Layers in Word-Oriented Partial SPN and HADES-Like Ciphers.** IACR Cryptology ePrint Archive 2020 (2020), p. 500.

[KR20] Nathan Keller and Asaf Rosemarin. **Mind the Middle Layer: The HADES Design Strategy Revisited.** IACR Cryptology ePrint Archive 2020 (2020), p. 179.