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

Where We Are

- General-purpose ciphers used for many use cases
  - 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 primitives not well-suited for many of these use cases
- Idea: Design something which is good in these scenarios

Where We Are

- General-purpose ciphers used for many use cases
  - 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 primitives not well-suited for many of these use cases
- Idea: Design something which is good in these scenarios

Where We Are

- General-purpose ciphers used for many use cases
  - 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 primitives not well-suited for many of these use cases
- Idea: Design something which is good in these scenarios

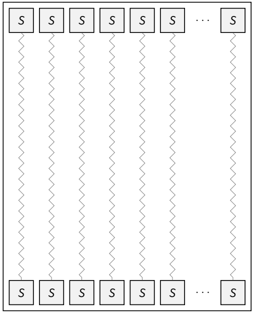
Where We Are cont.

- This idea is in general not extremely new...
- LowMC [ARS+15] from 2015 designed to minimize number of multiplications in $\mathbb{F}_2$
- However, the security of P-SPNs (including LowMC) is not easy to analyze
- Hence:
  - Can we build something that is easier to analyze?
  - Can we also use this approach to optimize the number of multiplications (and other metrics)?

Where We Are cont.

- This idea is in general not extremely new...
- LowMC [ARS+15] from 2015 designed to minimize number of multiplications in $\mathbb{F}_2$
- However, the security of P-SPNs (including LowMC) is not easy to analyze
- Hence:
  - Can we build something that is easier to analyze?
  - Can we also use this approach to optimize the number of multiplications (and other metrics)?

≈ SPNs with Partial Nonlinear Layers

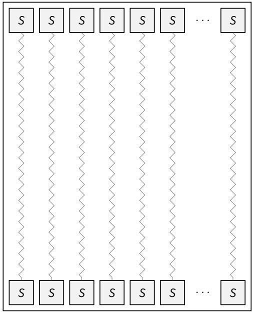


SPN
(e.g., SHARK in 1996)

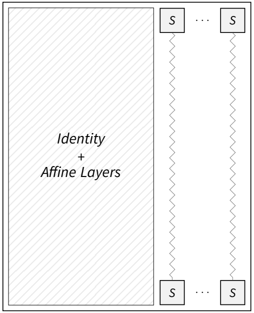
P-SPN
(e.g., Zorro in 2013 and LowMC in 2015)

HADES
(e.g., HADESMiMC)

≈ SPNs with Partial Nonlinear Layers



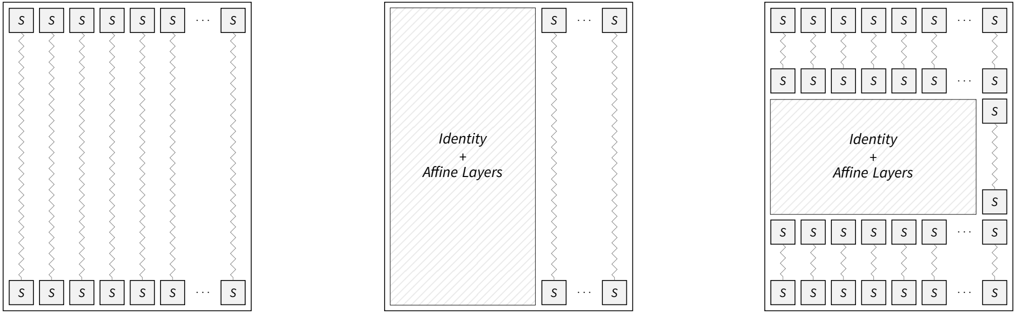
SPN
(e.g., SHARK in 1996)



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)

Why are we doing this?

- Partial SPNs like LowMC difficult to analyze from a statistical point of view
  - This is also true for Feistel networks, e.g. GMiMC [AGP+19] (indeed, GMiMC is currently being investigated)
- We would like to use well-known techniques
- One possibility is the *wide trail strategy*, originally used for the AES
  - Idea: Use this strategy to protect HADES constructions against differential and linear attacks
  - Problem: Needs full nonlinear layers (expensive...)

Why are we doing this?

- Partial SPNs like LowMC difficult to analyze from a statistical point of view
  - This is also true for Feistel networks, e.g. GMiMC [AGP+19] (indeed, GMiMC is currently being investigated)
- We would like to use well-known techniques
- One possibility is the *wide trail strategy*, originally used for the AES
  - Idea: Use this strategy to protect HADES constructions against differential and linear attacks
  - Problem: Needs full nonlinear layers (expensive...)

The HADES Design Strategy

Wide Trail Strategy for HADES – The Full Nonlinear Layer

- Used against some statistical attacks
- Linear layer? Branch number of the matrix?
  - Goal: Minimize number of (nonconstant) multiplications
  - Multiplications with fixed constants cheap in our setting
  - Use the “best” matrix from a statistical point of view: MDS
- Full rounds against statistical attacks

Wide Trail Strategy for HADES – The Full Nonlinear Layer

- Used against some statistical attacks
- Linear layer? Branch number of the matrix?
  - Goal: Minimize number of (nonconstant) multiplications
  - Multiplications with fixed constants cheap in our setting
  - Use the “best” matrix from a statistical point of view: MDS
- Full rounds against statistical attacks

Wide Trail Strategy for HADES – The Full Nonlinear Layer

- Used against some statistical attacks
- Linear layer? Branch number of the matrix?
  - Goal: Minimize number of (nonconstant) multiplications
  - Multiplications with fixed constants cheap in our setting
  - Use the “best” matrix from a statistical point of view: MDS
- Full rounds against statistical attacks

Raising the Degrees – The Partial Nonlinear Layer

- Differential and linear attacks: Solved by MDS
  - Conjectured security against other statistical attacks
- Algebraic attacks
  - Our use cases benefit from a “simple” algebraic structure
  - ... this makes algebraic attacks more powerful
- Degree likely rises in the same way during full and partial rounds
- We (mainly) use partial rounds to gain security against algebraic attacks
  - They contain only one S-box $\rightarrow$ not that expensive in our setting
  - However: We may need many partial rounds (depending on p)

Raising the Degrees – The Partial Nonlinear Layer

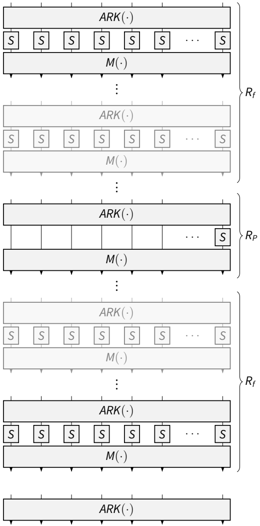
- Differential and linear attacks: Solved by MDS
  - Conjectured security against other statistical attacks
- Algebraic attacks
  - Our use cases benefit from a “simple” algebraic structure
  - ... this makes algebraic attacks more powerful
- Degree likely rises in the same way during full and partial rounds
- We (mainly) use partial rounds to gain security against algebraic attacks
  - They contain only one S-box $\rightarrow$ not that expensive in our setting
  - However: We may need many partial rounds (depending on p)

Raising the Degrees – The Partial Nonlinear Layer

- Differential and linear attacks: Solved by MDS
  - Conjectured security against other statistical attacks
- Algebraic attacks
  - Our use cases benefit from a "simple" algebraic structure
  - ... this makes algebraic attacks more powerful
- Degree likely rises in the same way during full and partial rounds
- We (mainly) use partial rounds to gain security against algebraic attacks
  - They contain only one S-box $\rightarrow$ not that expensive in our setting
  - However: We may need many partial rounds (depending on p)

Construction of HADES – Combining Everything

- Symmetry: Same number R_f of rounds with full S-box layers at the beginning and end ($R_F = 2 \cdot R_f$)
- R_P rounds with partial S-box layers in the middle
- Adjust for different metrics (e.g., depth)
- S-box size n, number of S-boxes in full rounds t
- Many partial rounds: Make use of optimizations [DKP+19]



Construction of HADES – Combining Everything cont.

- Design is very parameterizable
  - Number of cells t can be (almost) freely chosen
  - S-box size n can be (almost) freely chosen
  - State size $N = n \cdot t$
  - Nice! But cryptanalysis gets harder...
- Cryptanalysis for specific instantiations over $\mathbb{F}_p$
  - $\log_2(p) \approx n$

Concrete Instantiation and Cryptanalysis

Concrete Instantiation

- Details
  - Field: $\mathbb{F}_p$, where $p \approx 2^{128}$
  - One S-box in the partial rounds
  - S-box: $f(x) = x^3$
  - Cauchy matrix with specific starting sequence (more details in the paper)
- 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 in the partial rounds
  - S-box: $f(x) = x^3$
  - Cauchy matrix with specific starting sequence (more details in the paper)
- 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 ≈ 128 bits
  - Data $\leqslant \sqrt{p}$

Cryptanalysis cont.

- Statistical attacks
  - Recall: Wide trail strategy and MDS matrix for security against differential and linear attacks
  - We also estimate the complexity of other stat. attacks
- Algebraic attacks
  - Interpolation attacks
  - GCD attacks, Gröbner basis attacks and various strategies
  - Higher-order differential attacks
- More details in the paper

Cryptanalysis cont.

- Statistical attacks
  - Recall: Wide trail strategy and MDS matrix for security against differential and linear attacks
  - We also estimate the complexity of other stat. attacks
- Algebraic attacks
  - Interpolation attacks
  - GCD attacks, Gröbner basis attacks and various strategies
  - Higher-order differential attacks
- More details in the paper

Goal of HADES – The MPC Use Case

Goal of HADES – The MPC Use Case

- Large application area
- Our setting: secret-sharing-based MPC system
  - Data shared as elements of $\mathbb{F}_p$
  - Transfer data by evaluating block cipher calls on this data
  - Traditional algorithms like AES not efficient
- Avoid having many ciphertexts per stored share in the system
  - Single block cipher evaluation for multiple shares
- Compare with similar constructions (e.g., MiMC, *Rescue*)

Goal of HADES – The MPC Use Case cont.

- 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
- Additions are free, but cost can still be influenced
  - Impact on computational cost if there are many

Goal of HADES – The MPC Use Case cont.

- 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
- Additions are free, but cost can still be influenced
  - Impact on computational cost if there are many

Goal of HADES – The MPC Use Case cont.

- 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
- Additions are free, but cost can still be influenced
  - Impact on computational cost if there are many

Goal of HADES – The MPC Use Case cont.

- Small number of multiplications is crucial to reduce communication overhead
  - Depth can also be important
- Different tradeoffs and round numbers

Some Instances of HadesMiMC

Text Size $\log_2 p \times t$	Security κ	S-Box Size $(\log_2 p)$	#S-Box (t)	Rounds R_F (Full S-Box)	Rounds R_P (Partial S-Box)
256	128	128	2	6	71
256	256	128	2	12	76
512	128	128	4	6	71
512	512	128	4	12	76
1024	128	128	8	6	71
1024	1024	128	8	16	72
2048	128	128	16	6	71
2048	2048	128	16	20	69
4096	128	128	32	6	71
4096	4096	128	32	24	66

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]
- More cryptanalysis
  - Improve understanding of higher-order differential attacks over $\mathbb{F}_p$
  - Cryptanalytic differences between full rounds and partial rounds
  - Better tradeoffs possible?
  - Properties of the linear layer...

Properties of the Linear Layer

- Linear layer: Multiplication with an MDS matrix M
- Some problems for specific Cauchy generation methods and $\mathbb{F}_{2^n}$
  - For $t = 2^k$, the matrix M^2 is a multiple of the identity matrix
  - Then $\exists \mathcal{S} \subseteq (\mathbb{F}_{2^n})^t$ such that $\mathcal{S}$ is invariant for the partial rounds and no S-boxes are active in these rounds
  - This does not work over $\mathbb{F}_p$, HadesMiMC is not affected!
- More details are given in [KR20] and [BCD+20] (for generic t)
- Possible solution: Change Cauchy matrix generation sequence (see [KR20])
- New results for arbitrary matrices and $\mathbb{F}_p$ [GRS20]

Properties of the Linear Layer

- Linear layer: Multiplication with an MDS matrix M
- Some problems for specific Cauchy generation methods and $\mathbb{F}_{2^n}$
  - For $t = 2^k$, the matrix M^2 is a multiple of the identity matrix
  - Then $\exists \mathcal{S} \subseteq (\mathbb{F}_{2^n})^t$ such that $\mathcal{S}$ is invariant for the partial rounds and no S-boxes are active in these rounds
  - This does not work over $\mathbb{F}_p$, HadesMiMC is not affected!
- More details are given in [KR20] and [BCD+20] (for generic t)
- Possible solution: Change Cauchy matrix generation sequence (see [KR20])
- New results for arbitrary matrices and $\mathbb{F}_p$ [GRS20]

Properties of the Linear Layer

- Linear layer: Multiplication with an MDS matrix M
- Some problems for specific Cauchy generation methods and $\mathbb{F}_{2^n}$
  - For $t = 2^k$, the matrix M^2 is a multiple of the identity matrix
  - Then $\exists \mathcal{S} \subseteq (\mathbb{F}_{2^n})^t$ such that $\mathcal{S}$ is invariant for the partial rounds and no S-boxes are active in these rounds
  - This does not work over $\mathbb{F}_p$, HADESMiMC is not affected!
- More details are given in [KR20] and [BCD+20] (for generic t)
- Possible solution: Change Cauchy matrix generation sequence (see [KR20])
- New results for arbitrary matrices and $\mathbb{F}_p$ [GRS20]

Thank you!

References I

[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.

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. **Ciphers for MPC and FHE.** EUROCRYPT (1). Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 430–454.

[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.

References II

[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.

[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.