Symmetric-Key Encryption Schemes for Multi-Party Computation (MPC) Application

Lorenzo Grassi

December 2020

Radboud University

Motivation: Research of New Designs

Motivated by progress in practical applications of

- secure multi-party computation (MPC)
- fully homomorphic encryption (FHE)
- zero-knowledge proofs (ZK)
- ...

where

- *primitives from symmetric cryptography instantiated in* $(\mathbb{F}_{2^n})^t$ *and/or* $(\mathbb{F}_p)^t$ *are needed*;
- *performance of symmetric-key algorithms influences the protocols efficiency.*

Multi-Party Computation (MPC)

Jointly evaluate a function on private inputs s.t. *no party can learn anything more than the output of the function*:

- *input:* parties P_i with (private) input x_i;
- *output:* jointly compute a (known) function $y = f(x_1, ..., x_n)$ s.t. *correctness* and *privacy* are guaranteed.

Roughly speaking:

$$f(x_1, ..., x_n) \text{ “}\equiv\text{” } \mathrm{Dec}\Big(f'(\mathrm{Enc}(x_1), ..., \mathrm{Enc}(x_n))\Big)$$

where $\mathrm{Enc}(x)$ “$\equiv$” $(E'_{pk}(k), E''_k(x))$.

Roughly Speaking:

- Linear/Affine functions: *almost free*
- Non-linear functions: *expensive*

MPC (joint evaluation of a function in individually known but globally secret inputs):

- shared data are (often) elements of a finite field $(\mathbb{F}_p)^t$ for **large** p (e.g., $p \approx 2^{64}, 2^{128}$);
- multiplications require communications between the parties $\Rightarrow$ *total number of multiplications is a good estimate of the complexity of an MPC protocol*;
- additions for free, but other metrics influence the cost (namely, number of offline & online communication rounds).

Linearly Sharing MPC Scheme: Cost Metrics

Roughly Speaking:

- Linear/Affine functions: *almost free*
- Non-linear functions: *expensive*

MPC (joint evaluation of a function in individually known but globally secret inputs):

- shared data are (often) elements of a finite field $(\mathbb{F}_p)^t$ for **large** p (e.g., $p \approx 2^{64}, 2^{128}$);
- multiplications require communications between the parties $\Rightarrow$ *total number of multiplications is a good estimate of the complexity of an MPC protocol*;
- additions for free, but other metrics influence the cost (namely, number of offline & online communication rounds).

Linearly Sharing MPC Scheme: Cost Metrics

Roughly Speaking:

- Linear/Affine functions: *almost free*
- Non-linear functions: *expensive*

MPC (joint evaluation of a function in individually known but globally secret inputs):

- shared data are (often) elements of a finite field $(\mathbb{F}_p)^t$ for **large** p (e.g., $p \approx 2^{64}, 2^{128}$);
- multiplications require communications between the parties $\Rightarrow$ *total number of multiplications is a good estimate of the complexity of an MPC protocol*;
- additions for free, but other metrics influence the cost (namely, number of offline & online communication rounds).

“New” Schemes: Which Differences?

In “traditional” Ciphers/Hash Functions (e.g., AES, Keccak, ...), there is a good balance between the number of linear and non-linear operations (since they have approximately the same cost in Hardware/Software implementations).

In these new schemes:

- the number of non-linear operations is usually much smaller than the number of linear operations;
- the size of the S-Box does “not” influence the performance $\rightarrow$ “huge” S-Box (e.g., over $\mathbb{F}_{2^n}$ or $\mathbb{F}_p$ for $n \approx 128$ or $p \approx 2^{128}$);
- *simple algebraic representation*: “new” algebraic attacks become much more powerful than “traditional” statistical attacks.

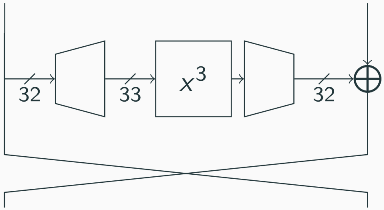
Table of Contents

MiMC

An old design: KN cipher

Knudsen-Nyberg cipher [NK95]:

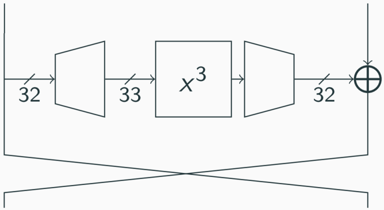
- 64-bit block cipher using Feistel mode of operation



- Broken with Interpolation Attack (algebraic) [JK97]
- This design was abandoned – recent textbook [KR11] even states that it's an example of how *NOT* to design a cipher

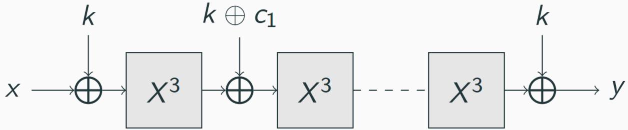
Knudsen-Nyberg cipher [NK95]:

- 64-bit block cipher using Feistel mode of operation



- Broken with Interpolation Attack (algebraic) [JK97]
- This design was abandoned – recent textbook [KR11] even states that it's an example of how *NOT* to design a cipher

MiMC block cipher [AGR+16]: MiMC-n/n and MiMC-p/p



$(x \mapsto x^3$ is a permutation **iff** $n = 2n' + 1$ odd and $p \equiv_3 2)$

MiMC block cipher: Number of Rounds

Large number of rounds:

$$\lceil n \cdot \log_3 2 \rceil \approx 0.64 \cdot n \qquad \text{or} \qquad \lceil \log_3 p \rceil$$

(where $p \approx 2^n$)

E.g., for $p \approx 2^{128}$:

- AES: 10 rounds and ≈ 960 (MPC) multiplications (no look-up table in MPC!!!);
- MiMC: 81 rounds and 162 (MPC) multiplications.

(Remember: AES works over $(\mathbb{F}_{2^8})^{16}$ so conversion from/to $\mathbb{F}_p$ takes place!)

Interpolation Attack [JK97]

Goal: construct a polynomial corresponding to the encryption function without knowledge of the secret key. E.g., given plaintexts and ciphertexts (x_i, y_i), use Lagrange's Formula:

$$P(x) = \sum_{i=0}^{d} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

Such polynomial can then be used for a forgery attack or/and a key-recovery attack.

If the degree is "maximum" (as in the case of a random permutation), then cost of the attack $\approx$ cost of brute force attack:

- the degree of 1-round MiMC is 3: hence, 3^r after r rounds;
- for a security level of $\log_2 p$ bits: $3^r \approx p$ implies $r \approx \log_3(p)$.

Interpolation Attack [JK97]

Goal: construct a polynomial corresponding to the encryption function without knowledge of the secret key. E.g., given plaintexts and ciphertexts (x_i, y_i), use Lagrange's Formula:

$$P(x) = \sum_{i=0}^{d} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

Such polynomial can then be used for a forgery attack or/and a key-recovery attack.

If the degree is "maximum" (as in the case of a random permutation), then cost of the attack $\approx$ cost of brute force attack:

- the degree of 1-round MiMC is 3: hence, 3^r after r rounds;
- for a security level of $\log_2 p$ bits: $3^r \approx p$ implies $r \approx \log_3(p)$.

Experimental Results – MiMC in MPC Applications

Table: Two-party performance of different PRFs in a Local Area Network (*LAN*) – "op(s)" $\equiv$ operation(s):

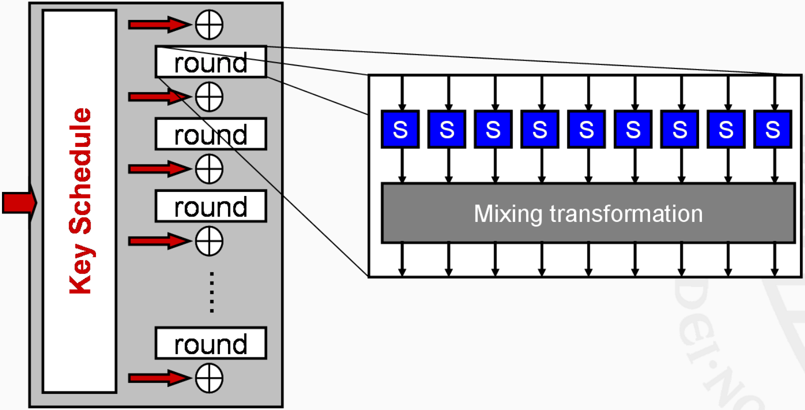
PRF	**Latency** (ms/op)	**Throughput** (ops/s)	**Preproc** (ops/ms)
AES [DR02]	7.713	530	5.097
LowMC [ARS+15]	4.302	591	2.562
MiMC	5.889	*6388*	33.575

where

- latency: the *best running time of a single cipher evaluation* (by running sequential single-threaded executions of it);
- throughput: the encryption rate given in the *number of field elements that can be encrypted in parallel per second* (by running multiple executions using different threads).

From SPN to Hades

SPN Ciphers


Key Schedule
round
round
round
round
S
S
S
S
S
S
S
S
S
Mixing transformation

Partial-SPN Ciphers

Move from a full S-Box layer

$$\mathcal{S} : x = [x_1 \| x_2 \| ... \| x_t] \in \mathbb{F}^t \to \mathcal{S}(x) = [S(x_1) \| S(x_2) \| ... \| S(x_t)]$$

to a Partial S-Box layer, e.g.

$$\mathcal{S} : x = [x_1 \| x_2 \| ... \| x_t] \in \mathbb{F}^t \to \mathcal{S}(x) = [S(x_1) \| x_2 \| ... \| x_t]$$

Question:

can we guarantee security and at the same time reduce the total number of non-linear operations w.r.t. a SPN cipher?

Note: we do "not" care about the number of linear operations (which obviously increases by increasing the number of rounds!)

Partial-SPN Ciphers

Move from a full S-Box layer

$$\mathcal{S} : x = [x_1 \| x_2 \| \ldots \| x_t] \in \mathbb{F}^t \to \mathcal{S}(x) = [S(x_1) \| S(x_2) \| \ldots \| S(x_t)]$$

to a Partial S-Box layer, e.g.

$$\mathcal{S} : x = [x_1 \| x_2 \| \ldots \| x_t] \in \mathbb{F}^t \to \mathcal{S}(x) = [S(x_1) \| x_2 \| \ldots \| x_t]$$

Question:

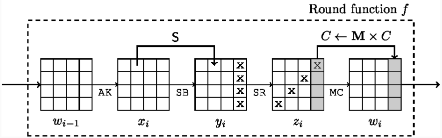
can we guarantee security and at the same time reduce the total number of non-linear operations w.r.t. a SPN cipher?

Note: we do "not" care about the number of linear operations (which obviously increases by increasing the number of rounds!)

Zorro

Zorro [GGN+13] (proposed for Masking):

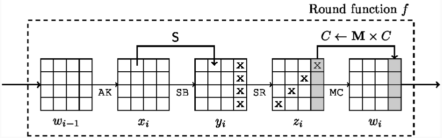
- 24-round AES: only 4 S-Boxes (in the first row) are applied in each round;



- Less S-Boxes than for AES: $24 \cdot 4 = 96 < 160 = 16 \cdot 10$;
- Broken by statistical attacks:
  (1) "wide-trail' design strategy [DR01] does not apply any-more: ad-hoc security argument by the designers;
  (2) using the same (AES) MixLayer in each round introduces weakness (in P-SPN)!

Zorro [GGN+13] (proposed for Masking):

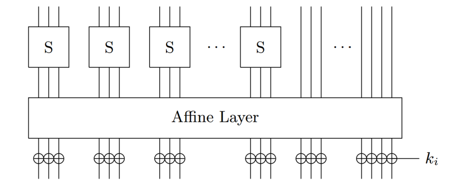
- 24-round AES: only 4 S-Boxes (in the first row) are applied in each round;



- Less S-Boxes than for AES: $24 \cdot 4 = 96 < 160 = 16 \cdot 10$;
- Broken by statistical attacks:
  (1) "wide-trail' design strategy [DR01] does not apply any-more: ad-hoc security argument by the designers;
  (2) using the same (AES) MixLayer in each round introduces weakness (in P-SPN)!

LowMC [ARS+15] (proposed for MPC/FHE/ZK):

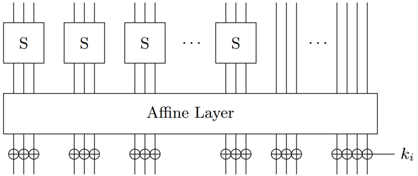
- a random **different** (invertible) affine layer over $\mathbb{F}_2^{n\times n}$ is applied at each round



- Disadvantages:
  (1) proposed solution could be quite expensive, both computationally and memory-wise;
  (2) security analysis could become more complicated
- First version broken by algebraic attacks

LowMC [ARS+15] (proposed for MPC/FHE/ZK):

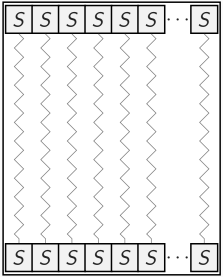
- a random **different** (invertible) affine layer over $\mathbb{F}_2^{n\times n}$ is applied at each round



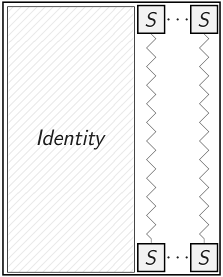
- Disadvantages:
  (1) proposed solution could be quite expensive, both computationally and memory-wise;
  (2) security analysis could become more complicated
- First version broken by algebraic attacks

"Hades" Strategy

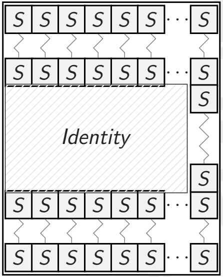
How to reduce number of non-linear operations & guarantee security with simple/elegant argument?



(a) SPN



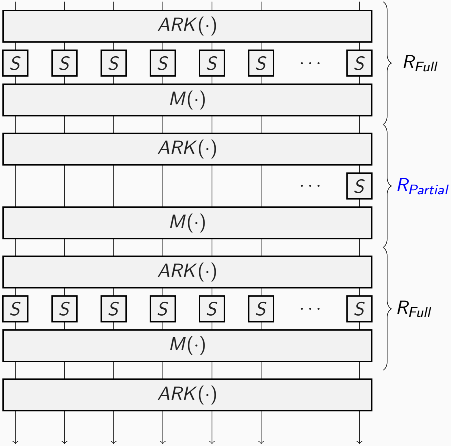
(b) P-SPN



(c) *"Hades" strategy*

HadesMiMC

From SHARK [RDP+96] to HadesMiMC



HadesMiMC defined over $(\mathbb{F}_p)^t$ (similar for $(\mathbb{F}_{2^n})^t$):

- Cube S-Box: $S(x) = x^3$ – invertible iff $\gcd(p-1, 3) = 1$;
- MixLayer: multiplication via MDS matrix (e.g., Cauchy matrix – assuming $t + 1 < p$);
- Affine key schedule: $k_i = M^i \cdot k + c_i$;
- *Efficient Implementation*: only for rounds with partial S-Box layer, MixLayer implemented via an equivalent matrix of the form

$$\begin{bmatrix} x_0 & y_1 & y_2 & \dots & y_{t-1} \\ z_1 & 1 & 0 & \dots & 0 \\ z_2 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ z_{t-1} & 0 & 0 & \dots & 1 \end{bmatrix}$$

Number of Rounds & Security Analysis

Number of rounds $R_F + R_P = 2 \cdot R_f + R_P$: depends both on p, t and on the security level:

- exploit rounds with full S-Box layer (together with Wide-Trail design strategy [DR01]) to guarantee security against statistical attacks;
- exploit rounds with partial S-Box layer in order to increase the degree;
- security against algebraic attacks (in particular, Grobner basis attacks) depend both on the rounds with full and partial S-Box layer!

Number of Rounds

Find the best ratio between R_F and R_P that guarantees security and minimizes the metric cost!

Text Size $\log_2 p \times t$	**Security** κ	**Word Size** ($\log_2 p$)	**# Words** (t)	**Rounds** $\mathrm{R_F}$ (Full S-Box)	**Rounds** $\mathrm{R_P}$ (Partial S-Box)
128	128	8	16	10	4
128	128	16	8	8	10
256	128	128	2	6	71
256	256	128	2	12	76
1 024	128	128	8	6	71
1 024	1 024	128	8	16	72
1 024	1 024	128	8	14	79

Experimental Results – MPC

Two-party performance of CTR-MiMC [AGR+16], HadesMiMC and Rescue [AAB+19] over a *LAN* over $t = 2, 4$ and 32 blocks (*total size* $\approx 128 \times t$ bits):

	Online Cost			**(Entire) Runtime**	
	Latency ($ms/\mathbb{F}_p$)	*Throughput* ($\mathbb{F}_p/s$)	*Communication* per $\mathbb{F}_p$	*Throughput* ($\mathbb{F}_p/s$)	*Communication* per $\mathbb{F}_p$
HadesMiMC_2	3.85	**117 358**	**1.90**	**261**	**266**
MiMC_2	**3.53**	79 728	3.50	192	366
$\textit{Rescue}_2$	5.54	23 464	6.10	70	971
HadesMiMC_4	1.90	**185 160**	**1.14**	**526**	**133.2**
MiMC_4	1.69	83 876	3.50	192	366
$\textit{Rescue}_4$	**1.25**	46 890	3.08	136	485
HadesMiMC_{32}	**0.32**	**258 610**	**0.39**	**1 098**	**60.8**
MiMC_{32}	0.34	87 831	3.5	192	366
$\textit{Rescue}_{32}$	0.42	57 695	1.93	274	243

(GMiMC_{erf} [AGP+19] broken – *Rescue* has largest security margin!)

Key-Recovery Attack on Full MiMC-n/n

Given a function $F : \mathbb{F}_{2^N} \to \mathbb{F}_{2^N}$

$$F(x) = \phi_0 \oplus \bigoplus_{i=1}^{d} \phi_i \cdot x^i \qquad \text{(where } \phi_d \neq 0\text{)},$$

it admits an equivalent representation over $\mathbb{F}_2^N$, namely $F \equiv (F_0, ..., F_{N-1})$ where $F_i : \mathbb{F}_2^N \to \mathbb{F}_2$:

$$F_i(x_0, x_1, ..., x_{N-1}) = \bigoplus_{u=(u_0,...,u_{N-1})\in\mathbb{F}_2^N} \varphi(u) \cdot x_0^{u_0} \cdot ... \cdot x_{N-1}^{u_{N-1}}$$

In the following:

- $d \equiv$ degree of F over $\mathbb{F}_{2^N}$
- $\delta \equiv$ *algebraic* degree of F over $\mathbb{F}_2^N$

where $\delta(F) = \max_{0\leq i\leq 2^N-1}\{hw(i)\,|\,\phi_i \neq 0\}$.

Given a function $F : \mathbb{F}_{2^N} \to \mathbb{F}_{2^N}$

$$F(x) = \phi_0 \oplus \bigoplus_{i=1}^{d} \phi_i \cdot x^i \qquad \text{(where } \phi_d \neq 0\text{)},$$

it admits an equivalent representation over $\mathbb{F}_2^N$, namely $F \equiv (F_0, \dots, F_{N-1})$ where $F_i : \mathbb{F}_2^N \to \mathbb{F}_2$:

$$F_i(x_0, x_1, \dots, x_{N-1}) = \bigoplus_{u=(u_0,\dots,u_{N-1})\in\mathbb{F}_2^N} \varphi(u) \cdot x_0^{u_0} \cdot \dots \cdot x_{N-1}^{u_{N-1}}$$

In the following:

- $d \equiv$ degree of F over $\mathbb{F}_{2^N}$
- $\delta \equiv$ *algebraic* degree of F over $\mathbb{F}_2^N$

where $\delta(F) = \max_{0\leq i\leq 2^N-1}\{hw(i) \,|\, \phi_i \neq 0\}$.

Higher-Order Differential Attack

Given a a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ under a fixed secret key k, **higher-order differential cryptanalysis** [Knu94] exploits the fact that

for any vector subspace $V \subseteq \mathbb{F}_2^n$ with dimension greater than the algebraic degree of E_k:

$$\dim(V) \geq \deg(E_k) + 1$$

and for any (fixed) element $v \in \mathbb{F}_2^n$:

$$\bigoplus_{x \in V \oplus v} x = \bigoplus_{x \in V \oplus v} E_k(x) = 0.$$

Problem: estimate the algebraic degree of $E_k(\cdot)$!

Given a a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ under a fixed secret key k, **higher-order differential cryptanalysis** [Knu94] exploits the fact that

> *for any vector subspace $V \subseteq \mathbb{F}_2^n$ with dimension greater than the algebraic degree of E_k:*
>
> $$\dim(V) \geq \deg(E_k) + 1$$
>
> *and for any (fixed) element $v \in \mathbb{F}_2^n$:*
>
> $$\bigoplus_{x \in V \oplus v} x = \bigoplus_{x \in V \oplus v} E_k(x) = 0.$$

Problem: estimate the algebraic degree of $E_k(\cdot)$!

Trivial Estimation of the Growth of the Degree

The degree of the composition of two functions $F \circ G(\cdot)$ is always upper bounded by

$$\deg(G \circ F(\cdot)) \leq \deg(F) \cdot \deg(G).$$

Given a SPN cipher $(\mathbb{F}_{2^n})^t \to (\mathbb{F}_{2^n})^t$ with round functions defined as

$$R(\cdot) = k \oplus M \circ [\underbrace{S\|...\|S\|S}_{\equiv t \text{ S-Boxes}}](\cdot)$$

where $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ has algebraic degree $\delta \geq 2$, then the degree of $E_k(\cdot)$ after R rounds is *upper bounded* by δ^R. Thus, **at least**

$$\log_\delta(n \cdot t - 1) \equiv \log_\delta(N - 1) \textbf{ rounds}$$

are **necessary** to reach maximum degree.

Trivial Estimation of the Growth of the Degree

The degree of the composition of two functions $F \circ G(\cdot)$ is always upper bounded by

$$\deg(G \circ F(\cdot)) \leq \deg(F) \cdot \deg(G).$$

Given a SPN cipher $(\mathbb{F}_{2^n})^t \to (\mathbb{F}_{2^n})^t$ with round functions defined as

$$R(\cdot) = k \oplus M \circ [\underbrace{S\|...\|S\|S}_{\equiv t \text{ S-Boxes}}](\cdot)$$

where $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ has algebraic degree $\delta \geq 2$, then the degree of $E_k(\cdot)$ after R rounds is *upper bounded* by δ^R. Thus, **at least**

$$\log_\delta(n \cdot t - 1) \equiv \log_\delta(N - 1) \textbf{ rounds}$$

are **necessary** to reach maximum degree.

Estimation from [BCD11]

Theorem (C. Boura, A. Canteaut, C. De Cannière – FSE'11)
Let F be a function from $\mathbb{F}_2^N$ to $\mathbb{F}_2^N$ corresponding to the concatenation of t smaller S-Boxes $S_1, \ldots, S_t$ defined over $\mathbb{F}_2^n$. Then, for any function G from $\mathbb{F}_2^N$ to $\mathbb{F}_2^N$, we have

$$\deg(G \circ F(\cdot)) \leq \min\left\{\deg(F) \cdot \deg(G), N - \frac{N - \deg(G)}{\gamma}\right\},$$

where

$$\gamma = \max_{i=1,\ldots,n-1} \frac{n-i}{n-\delta_i} \leq n-2$$

where δ_i is the maximum degree of the product of any i coordinates of any of the smaller S-Boxes

Comparison btw [BCD11] and Trivial Estimation

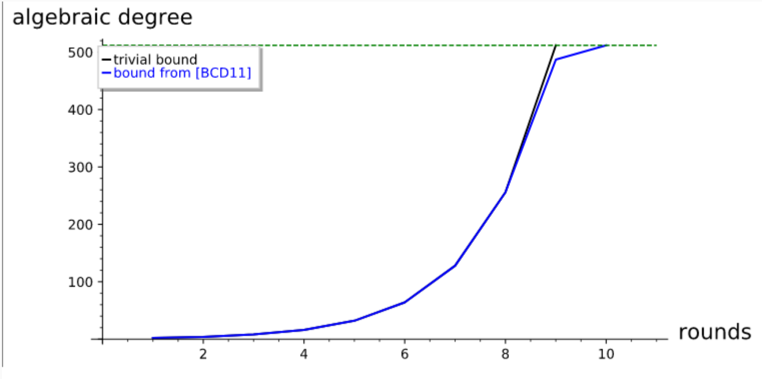


Figure: Different *upper bounds* of the growth of the algebraic degree of a typical SPN cipher (with cubic S-Box) over $(\mathbb{F}_{2^{19}})^{27}$

Theorem ([EGL+20])
Consider an iterated Even-Mansour cipher $EM_k^r(\cdot) : \mathbb{F}_{2^N} \to \mathbb{F}_{2^N}$

$$EM_k^r(\cdot) := k^r \oplus (...R(k^1 \oplus R(k^0 \oplus \cdot))...)$$

of $r \geq 1$ *rounds, where* $R(\cdot)$ *is a polynomial of degree* $d \geq 3$*:*

$$R(x) = \rho_0 \oplus \bigoplus_{i=1}^{d} \rho_i \cdot x^i \qquad \text{(where } \rho_d \neq 0\text{).}$$

The algebraic degree (= degree over $\mathbb{F}_2^N$*) after* r *rounds is upper bounded by*

$$\lfloor \log_2(d^r + 1) \rfloor.$$

Consider an *iterated Even-Mansour* cipher $EM_k^r(\cdot) : \mathbb{F}_{2^N} \to \mathbb{F}_{2^N}$

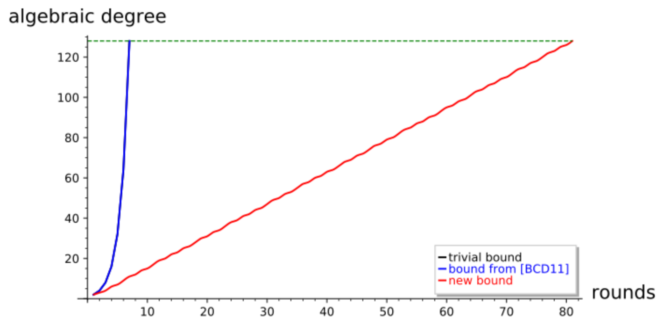
$$EM_k^r(\cdot) := k^r \oplus (\ldots R(k^1 \oplus R(k^0 \oplus \cdot))\ldots)$$

of $r \geq 1$ rounds, where – as before – $R(\cdot)$ is a polynomial of degree $d \geq 3$.

The minimum number of rounds **necessary** to prevent a (secret-key) high-order differential distinguisher is given by

$$\left\lceil \log_d \left(2^{N-1} - 1\right) \right\rceil \approx (N-1) \cdot \log_d(2).$$

Concrete Results on MiMC-N/N



First secret-key zero-sum distinguisher for $\lceil \log_3(2^{N-1} - 1) \rceil$ rounds (out of $\lceil N \cdot \log_3(2) \rceil$):

- **security margin: 1 or 2 rounds (depending on N)**

Theoretical & Practical Results for MiMC

n	$\mathcal{R}$ (our estimation)	$\mathcal{R}^{[BCD11]}$	Practical $\mathcal{R}$
5	3	3	4
7	4	3	5
9	6	4	6
11	7	4	7
13	8	4	9
15	9	4	10
17	11	5	11
33	21	6	21
65	41	7	-
129	81	8	-
257	162	9	-

$R \equiv$ necessary number of rounds to prevent zero-sum .

Theorem ([BC13])
Let f be a permutation over $\mathbb{F}_2^N$. Then, $\deg(f^{-1}) = N - 1$ *if and only if* $\deg(f) = N - 1$.

Chosen-Ciphertext Key-Recovery Attack:

$$\text{plaintexts} \xrightarrow[\text{Key-Recovery}]{R(\cdot) \text{ or } R^2(\cdot)} \textit{zero-sum} \xleftarrow[\text{Distinguisher}]{R^{-r}(\cdot)} \text{ciphertexts}$$

- set up a system of (low-degree) algebraic equations for the first 1/2 round(s);
- solve them to find the key.

Total cost of the attack: 2^{n-1} chosen ciphertexts & $\approx 2^{n-\log_2(n)+1}$ encryptions.

Theorem ([BC13])
Let f be a permutation over $\mathbb{F}_2^N$. Then, $\deg(f^{-1}) = N - 1$ if and only if $\deg(f) = N - 1$.

Chosen-Ciphertext Key-Recovery Attack:

$$\text{plaintexts} \xrightarrow[\text{Key-Recovery}]{R(\cdot) \text{ or } R^2(\cdot)} \textit{zero-sum} \xleftarrow[\text{Distinguisher}]{R^{-r}(\cdot)} \text{ciphertexts}$$

- set up a system of (low-degree) algebraic equations for the first 1/2 round(s);
- solve them to find the key.

Total cost of the attack: 2^{n-1} chosen ciphertexts & $\approx 2^{n-\log_2(n)+1}$ encryptions.

Key-Recovery Attack: New Number of Rounds

In order to provide security, new number of rounds for MiMC over $\mathbb{F}_{2^n}$:

$$\lceil n \cdot \log_3(2) \rceil + \underbrace{\lceil \log_3(2n \cdot \log_3(2)) \rceil}_{\text{new term!}}$$

(e.g., for $n = 129$: 5 more rounds – from 82 to 87).

- No change for the prime case! (the previous attack works only over a binary field)
- Cryptanalysis is never finished: We can only guarantee security against **KNOWN** attacks!!! It is always possible that new attacks are discovered and a scheme (including AES & SHA-3) is broken!!

Key-Recovery Attack: New Number of Rounds

In order to provide security, new number of rounds for MiMC over $\mathbb{F}_{2^n}$:

$$\lceil n \cdot \log_3(2) \rceil + \underbrace{\lceil \log_3(2n \cdot \log_3(2)) \rceil}_{\text{new term!}}$$

(e.g., for $n = 129$: 5 more rounds – from 82 to 87).

- No change for the prime case! (the previous attack works only over a binary field)
- Cryptanalysis is never finished: We can only guarantee security against **KNOWN** attacks!!! It is always possible that new attacks are discovered and a scheme (including AES & SHA-3) is broken!!

Open Problems

Open Problems

As every new construction, more cryptanalysis is necessary:

- improve attacks based on higher-order differentials over $\mathbb{F}_{2^n}$: is it possible to estimate the growth of the degree for generic SPN/Feistel schemes with big S-Boxes?
- what about other attacks that work better/differently over $\mathbb{F}_p$ than over $\mathbb{F}_{2^n}$? How does the value of p influence the possibility to set up an attack (e.g., is there any attack that performs better for $p \approx 2^n \pm \varepsilon$ or not)?

Is it possible to design a scheme with better performances w.r.t. the current ones present in the literature?

Thanks for your attention!

Questions?

Comments?

Proof (1/2)

Let $\mathfrak{D}_r \equiv \mathfrak{D}$ be the degree of $EM_k^r(\cdot) = \bigoplus_{i=0}^{\mathfrak{D}} \varepsilon_i \cdot x^i$ after r rounds. Given a subspace $\mathcal{V} \subseteq \mathbb{F}_{2^N}$ of dimension $N-1$, then

$$\bigoplus_{x \in \mathcal{V} \oplus v} E_k(x) = \bigoplus_{x \in \mathcal{V} \oplus v} \left(\bigoplus_{i=0}^{\mathfrak{D}} \varepsilon_i \cdot x^i \right) = \bigoplus_{i=0}^{\mathfrak{D}} \varepsilon_i \left(\bigoplus_{x \in \mathcal{V} \oplus v} x^i \right) = 0$$

if $deg(x \mapsto x^i) \equiv hw(i) \leq N-2$ for each $i = 0, ..., d$.

Necessary condition to prevent a (secret-key) high-order differential distinguisher:

$E_k(\cdot)$ must contain at least one monomial x^i with $hw(i) \geq N-1$.

Proof (1/2)

Let $\mathfrak{D}_r \equiv \mathfrak{D}$ be the degree of $EM_k^r(\cdot) = \bigoplus_{i=0}^{\mathfrak{D}} \varepsilon_i \cdot x^i$ after r rounds.
Given a subspace $\mathcal{V} \subseteq \mathbb{F}_{2^N}$ of dimension $N-1$, then

$$\bigoplus_{x \in \mathcal{V} \oplus v} E_k(x) = \bigoplus_{x \in \mathcal{V} \oplus v} \left(\bigoplus_{i=0}^{\mathfrak{D}} \varepsilon_i \cdot x^i \right) = \bigoplus_{i=0}^{\mathfrak{D}} \varepsilon_i \left(\bigoplus_{x \in \mathcal{V} \oplus v} x^i \right) = 0$$

if $deg(x \mapsto x^i) \equiv hw(i) \leq N-2$ for each $i = 0, ..., d$.

Necessary condition to prevent a (secret-key) high-order differential distinguisher:

$E_k(\cdot)$ *must contain at least one monomial* x^i *with* $hw(i) \geq N-1$.

Proof (2/2)

Since

- the smallest i s.t. $hw(i) \geq N - 1$ is $i = 2^{N-1} - 1$
- the degree of $EM_k^r(\cdot)$ is upper bounded by $\mathfrak{D}_r \leq d^r$

it follows that the minimum number of rounds $\mathcal{R}$ to prevent such attack must satisfy

$$d^{\mathcal{R}} \geq 2^{N-1} - 1 \quad \Longrightarrow \quad \mathcal{R} \geq \log_d(2^{N-1} - 1).$$

[AAB+19] A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec

Efficient Symmetric Primitives for Advanced Cryptographic Protocols (A Marvellous Contribution).

IACR Cryptology ePrint Archive 2019

[AGP+19] M. R. Albrecht, L. Grassi, L. Perrin, S. Ramacher, C. Rechberger, D. Rotaru, A. Roy and M. Schofnegger

Feistel Structures for MPC, and more.

ESORICS 2019

[AGR+16] M.R. Albrecht, L. Grassi, C. Rechberger, A. Roy and T. Tiessen

MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity.

ASIACRYPT 2016

[ARS+15] M.R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen and M. Zohner

Ciphers for MPC and FHE.

EUROCRYPT 2015

[BC13] C. Boura, A. Canteaut and C. De Canniere

On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$.

IEEE Trans. Inf. Theory 2013

[BS91] E. Biham and A. Shamir

Differential Cryptanalysis of DES-like Cryptosystems.

J. Cryptology 1991

[BCD+20] T. Beyne, A. Canteaut, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo and F. Wiemer

Out of Oddity - New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems.

Crypto 2020

[BCD11] C. Boura, A. Canteaut and C. De Canniere

Higher-Order Differential Properties of Keccak and Luffa.

FSE 2011

[DR01] J. Daemen and V. Rijmen

The Wide Trail Design Strategy.

IMACC 2001

[DR02] J. Daemen and V. Rijmen

The Design of Rijndael: AES - The Advanced Encryption Standard.

Springer 2002

[EGL+20] M. Eichlseder, L. Grassi, R. Luftenegger, M. Oygarden, C. Rechberger, M. Schofnegger and Q. Wang

An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC.

Asiacrypt 2020

[GGN+13] B. Gérard, V, Grosso, M. Naya-Plasencia and F. Standaert

Block Ciphers That Are Easier to Mask: How Far Can We Go?

CHES 2013

[GKR+19] L. Grassi, D. Khovratovich, A. Roy, C. Rechberger and M. Schofnegger

Starkad and Poseidon: New Hash Functions for Zero Knowledge Proof Systems

IACR Cryptology ePrint Archive 2019

[GLR+20] L. Grassi, R. Lueftenegger, C. Rechberger, D. Rotaru and M. Schofnegger

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

EUROCRYPT 2020

[GRR+16] L. Grassi, C. Rechberger, D. Rotaru, P. Scholl and N.P. Smart

MPC-Friendly Symmetric Key Primitives

CCS 2016

T. Jakobsen, L.R. Knudsen

The interpolation attack on block ciphers,

FSE 1997

L.R. Knudsen
Truncated and Higher Order Differentials.
FSE 1994

L.R. Knudsen and M. Robshaw
The Block Cipher Companion.
Book – Springer 2011

References x

N. Keller and A. Rosemarin

Mind the Middle Layer: The HADES Design Strategy Revisited.

IACR Cryptology ePrint Archive 2020

K. Nyberg and L.R. Knudsen

Provable Security Against a Differential Attack.

J. Cryptology 1995

V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers and E. De Win

The Cipher SHARK

FSE 1996