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

Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander,
Gaëtan Leurent, Léo Perrin, María Naya Plasencia, Yu Sasaki,
Yosuke Todo, Friedrich Wiemer

Crypto 2020 - August 2020

Symmetric primitives optimized for a specific cost metric

- **FHE-friendly encryption:** Low-MC [Albrecht et al. 15], Flip [Méaux et al. 16], Kreyvium [Canteaut et al. 16], Rasta [Dobraunig et al. 18]...
- **MPC-friendly block ciphers:** MiMC [Albrecht et al. 16] and its variants
- **Primitives dedicated to new integrity proof systems (STARKs, SNARKs, Bulletproof)**: hash functions specified as sequences of low-degree polynomials or low-degree rational maps over a finite field.

Older examples:

Cradic [Knudsen Nyberg 92], Misty [Matsui 97].

SNARK-friendly and STARK-friendly primitives

Performance.

- the size of the polynomial relations representing the execution trace over a large finite field should be minimized.
- finite fields of odd characteristic, especially prime fields, are suitable.

Security.

- algebraic attacks based on Gröbner basis [Albrecht et al. 19]...
- all other cryptanalytic techniques.

Focus on STARK-friendly primitives

StarkWare challenges `https://starkware.co/hash-challenge/`

Keyed permutations.

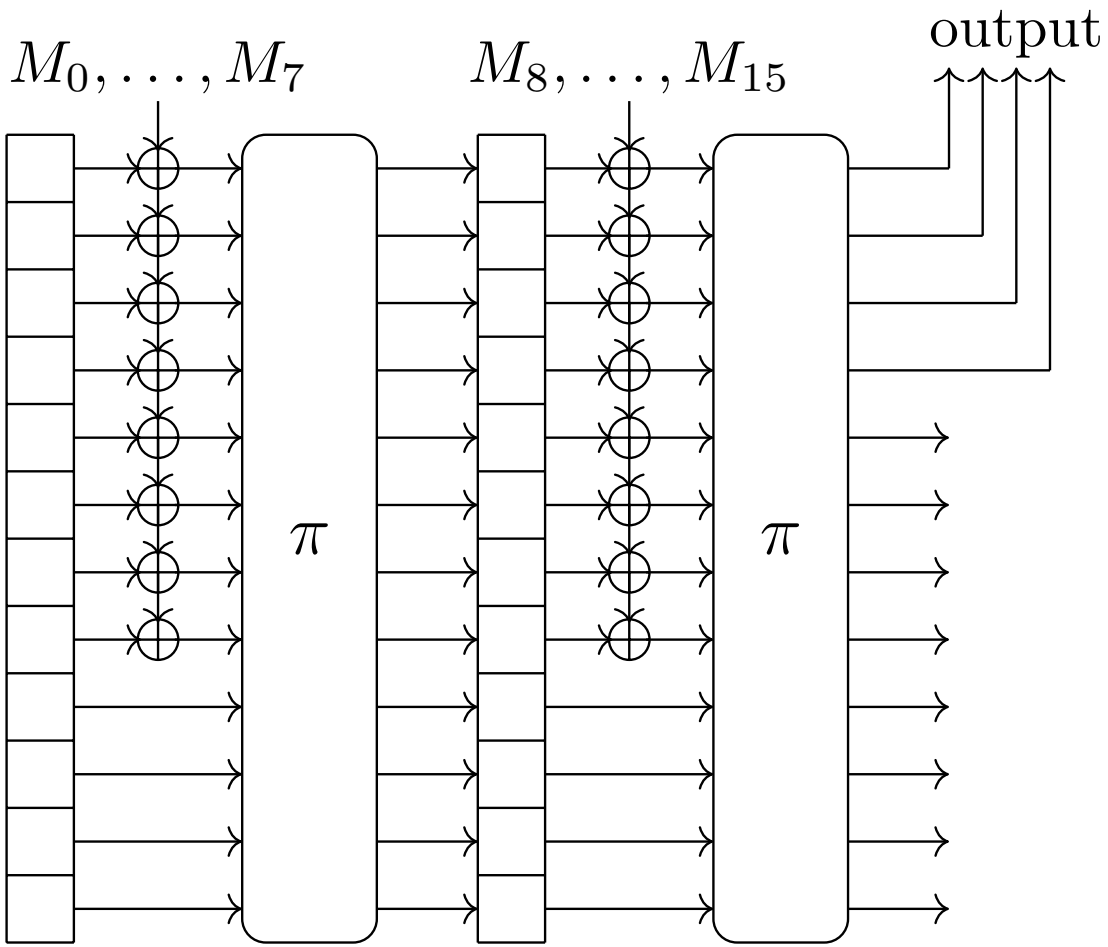
- GMiMC i.e. $\text{GMiMC}_{\text{erf}}$ over $\mathbb{F}_p$ [Albrecht et al. 19]
- HadesMiMC permutation: Starkad ($\mathbb{F}_{2^m}$) and Poseidon ($\mathbb{F}_p$) [Grassi et al. 19]

Hash functions.

sponges using one of the previous functions as inner permutation.

Sponge construction

Sponge construction with blocksize t and capacity c.



Parameters

Security level	$\log_2 q$	q (prime)	q (binary)	c	t	Variant
128 bits	64	$2^{61} + 20 \times 2^{32} + 1$	2^{63}	4	12	128-d
	128	$2^{125} + 266 \times 2^{64} + 1$	2^{125}	2	4	128-a
				2	12	128-c
	256	$2^{253} + 2^{199} + 1$	2^{255}	1	3	128-b
				1	11	128-e
256 bits	128	$2^{125} + 266 \times 2^{64} + 1$	2^{125}	4	8	256-a
				4	14	256-b

Keypoints

- generalization of attacks to fields of any characteristic.
- use of the specific algebraic structure to improve classical attacks.

Outline

- Integral attacks over fields of any characteristic
- Integral distinguishers on the full GMiMC
- Algebraically-controlled differential attacks on GMiMC

Integral attacks over $\mathbb{F}_q$

When $q = 2^m$.

For any $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, for any (affine) subspace $V \subset \mathbb{F}_2^m$ with $\deg(F) < |V| - 1$,

$$\sum_{x \in V} F(x) = 0.$$

Integral attacks over $\mathbb{F}_q$

When $q = 2^m$.

For any $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, for any (affine) subspace $V \subset \mathbb{F}_2^m$ with $\deg(F) < |V| - 1$,

$$\sum_{x \in V} F(x) = 0.$$

Because, for $V = b + \langle a_1, \ldots, a_v \rangle$,

$$D_{a_1} D_{a_2} \ldots D_{a_v} F(b) = \sum_{x \in V} F(x)$$

Not valid in odd characteric.

But for any q

For any exponent k with $0 \le k < q-1$,

$$\sum_{x \in \mathbb{F}_q} x^k = 0$$

General result.

For any $F : \mathbb{F}_q \to \mathbb{F}_q$ with $\deg(F) < q-1$,

$$\sum_{x \in \mathbb{F}_q} F(x) = 0 \ .$$

However, this only works when an input is saturated

For any $F : \mathbb{F}_q \to \mathbb{F}_q$ with $\deg(F) < q - 1$,

$$\sum_{x \in \mathbb{F}_q} F(x) = 0 \ .$$

Less general than the property over $\mathbb{F}_{2^m}$:

For any (affine) subspace $V \subset \mathbb{F}_2^m$ such that $\deg(F) < |V| - 1$,

$$\sum_{x \in V} F(x) = 0.$$

Using multiplicative subgroups

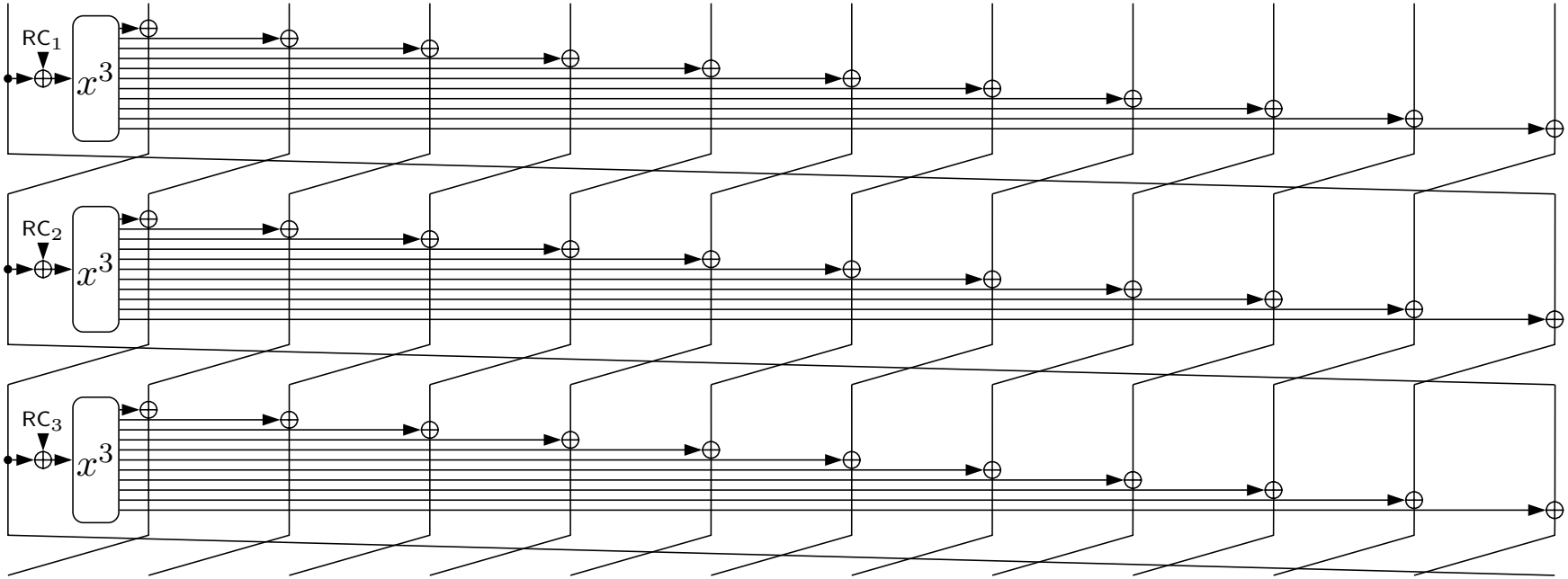
Let G be a multiplicative subgroup of $\mathbb{F}_q^\times$.

For any $F : \mathbb{F}_q \to \mathbb{F}_q$ such that $\deg(F) < |G|$,

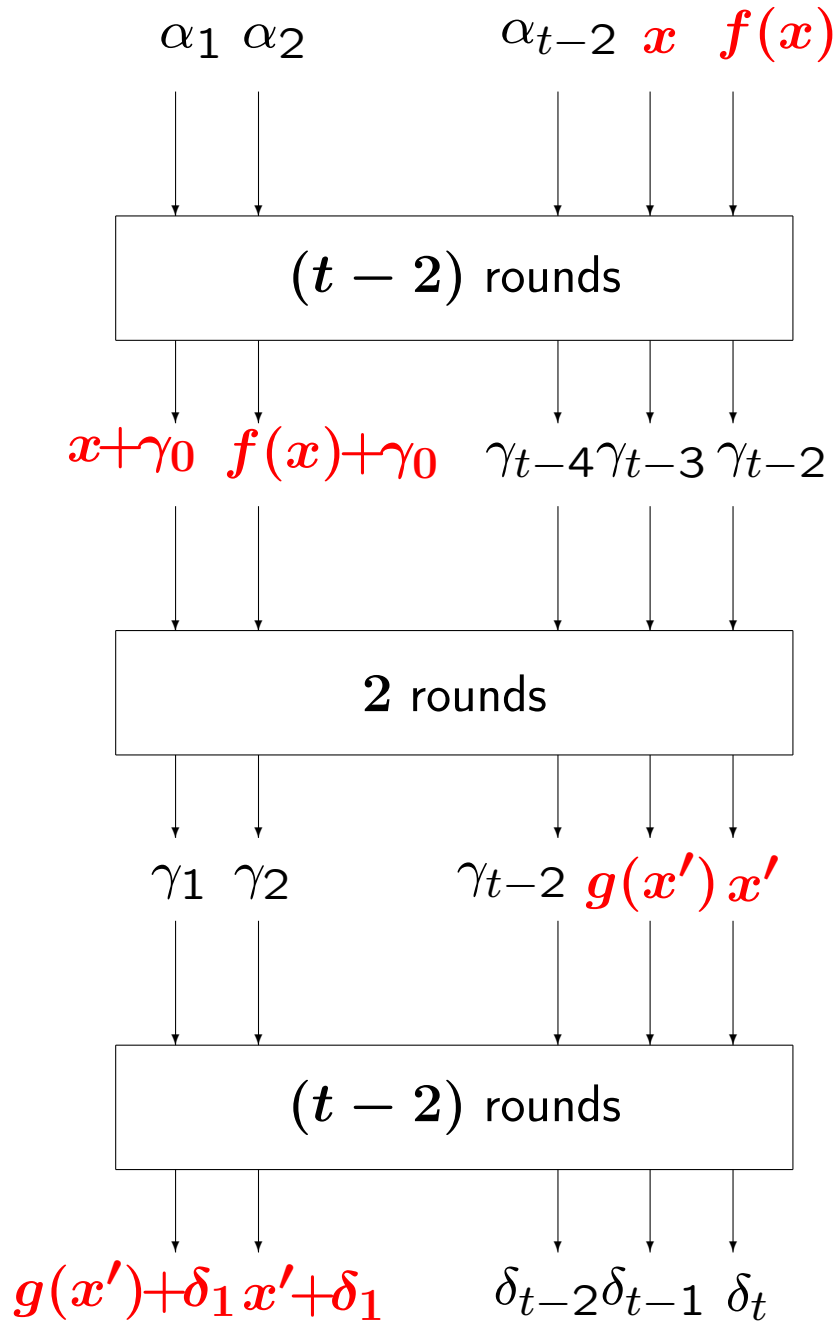
$$\sum_{x \in G} F(x) = F(0) \cdot |G| \ .$$

Integral attacks on GMiMC

GMiMC with 101 rounds



A differential property on $(2t-2)$ rounds



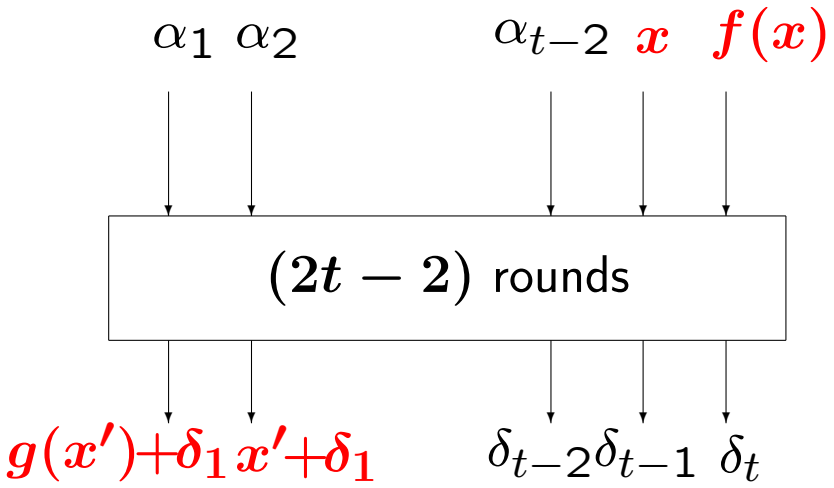
$x \in \mathbb{F}_q$

$\deg f = 3$

$x' \in \mathbb{F}_q$

$\deg g = 3$

A differential property on $(2t-2)$ rounds



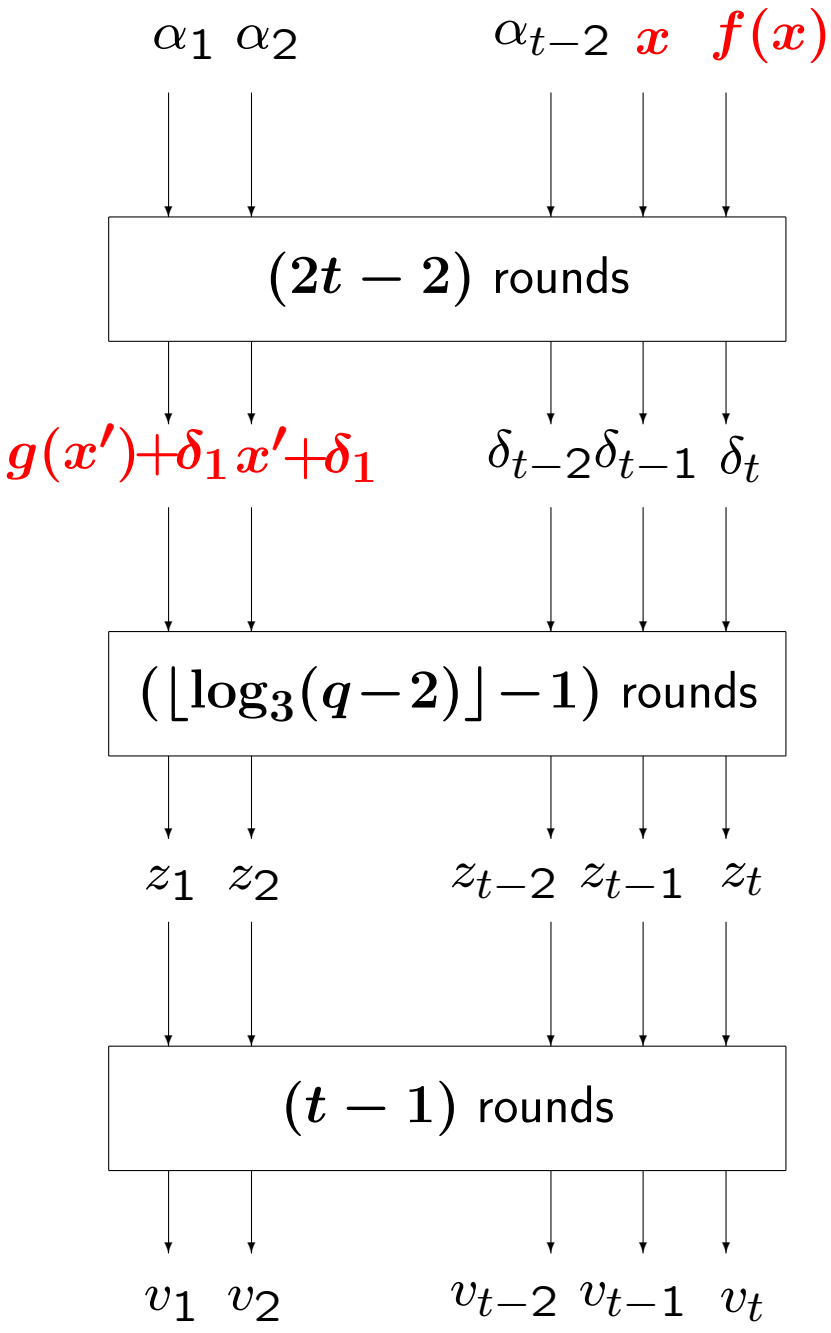
$x \in \mathbb{F}_q$

$\deg f = 3$

$x' \in \mathbb{F}_q$

$\deg g = 3$

Integral distinguisher on GMiMC



$x \in \mathbb{F}_q$

$\deg f = 3$

$x' \in \mathbb{F}_q$

$\deg g = 3$

$\deg_x z_i = 3^{r+1} < q-1$

for $r \leq \lfloor \log_3(q-2) \rfloor - 1$

$\sum_{i=2}^{t} v_i - (t-2)v_1$

is a linear combination of the z_i

Integral distinguisher on GMiMC

With complexity q.

After $3t - 4 + \lfloor \log_3(q-2) \rfloor$ rounds,

$$\sum_{i=2}^{t} v_i - (t-2)v_1$$

is a polynomial of degree at most $(q-2)$ in x.

$\Rightarrow$ It sums to 0 when x varies in $\mathbb{F}_q$.

$\log_2 q$	t	Full nb of rounds	Nb of rounds of the distinguisher
61	12	101	70
125	4	166	86
125	12	182	110
253	3	326	–
253	11	342	–

Integral distinguisher on GMiMC using multiplicative subgroups

For $q = 2^{253} + 2^{199} + 1$.

After $3t - 4 + \lfloor \log_3(|G| - 1) \rfloor$ rounds,

$$\sum_{i=2}^{t} v_i - (t-2)v_1$$

is a polynomial of degree at most $(|G| - 1)$ in x.

$\Rightarrow$ It sums to 0 when x varies in G.

$\log_2 q$	t	Full nb of rounds	Nb of rounds of the distinguisher
61	12	101	70
125	4	166	86
125	12	182	110
253	3	326	85 with $\lvert G\rvert = 2^{128}$
253	11	342	109 with $\lvert G\rvert = 2^{128}$

Zero-sum distinguisher on GMiMC

With a multiplicative subgroup G.

After $4t - 6 + 2\lfloor \log_3(|G| - 1) \rfloor$ rounds,

$$\sum_{i=1}^{t-1} u_i - (t-2)u_t \quad \text{and} \quad \sum_{i=2}^{t} v_i - (t-2)v_1$$

sum to 0 when x varies in G.

$\log_2 q$	t	Full nb of rounds	Nb of rounds of the ZS	$\lvert G \rvert$
61	12	101	118	q
61	12	101	102	$2^{33} \cdot 167 \cdot 211 \simeq 2^{48}$
125	4	166	166	q
125	12	182	198	q
253	3	326	166	2^{128}
253	11	342	198	2^{128}

Algebraically-controlled differential attacks on GMiMC

Algebraically-controlled differential attacks

Idea:

use algebraic techniques to efficiently find hash function inputs that satisfy a differential characteristic (avoid expensive probabilistic cost)

Method:

represent the conditions of differential transitions as (efficiently solvable) algebraic equations

Application to GMiMC:

- exploit algebraic structure to penetrate deep into internal state
- attack almost entirely algebraic — differential transitions too expensive to bypass probabilistically

Results:

- basic method on $3t - 2$ rounds of permutation
- extend to more rounds and attack the hash function (e.g., practical 40-round collision on GMiMC-128-d)

Application to GMiMC

Differential characteristic:

Δ_0, Δ_0' arbitrary non-zero differences

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}} (\Delta_0' + \Delta_1, \Delta_1, \ldots, \Delta_1, \Delta_0) \qquad \Delta_0 \xrightarrow{S} \Delta_1$$

$$\xrightarrow{\mathcal{R}} (\Delta_1 + \Delta_1', \ldots, \Delta_1 + \Delta_1', \Delta_0 + \Delta_1', \Delta_0' + \Delta_1) \qquad \Delta_0' + \Delta_1 \xrightarrow{S} \Delta_1'$$

Application to GMiMC

Differential characteristic:

$\boldsymbol{\Delta_0}, \boldsymbol{\Delta_0'}$ arbitrary non-zero differences

$$(\boldsymbol{\Delta_0}, \boldsymbol{\Delta_0'}, 0, \ldots, 0) \xrightarrow{\mathcal{R}} (\boldsymbol{\Delta_0'}+\boldsymbol{\Delta_1}, \boldsymbol{\Delta_1}, \ldots, \boldsymbol{\Delta_1}, \boldsymbol{\Delta_0}) \qquad \boldsymbol{\Delta_0} \xrightarrow{S} \boldsymbol{\Delta_1}$$

$$\xrightarrow{\mathcal{R}} (\boldsymbol{\Delta_1}+\boldsymbol{\Delta_1'}, \ldots, \boldsymbol{\Delta_1}+\boldsymbol{\Delta_1'}, \boldsymbol{\Delta_0}+\boldsymbol{\Delta_1'}, \boldsymbol{\Delta_0'}+\boldsymbol{\Delta_1}) \quad \boldsymbol{\Delta_0'}+\boldsymbol{\Delta_1} \xrightarrow{S} \boldsymbol{\Delta_1'}$$

If $\boldsymbol{\Delta_1} + \boldsymbol{\Delta_1'} = 0$, we get an iterative differential characteristic

$$(\boldsymbol{\Delta_0}, \boldsymbol{\Delta_0'}, 0, \ldots, 0) \xrightarrow{\mathcal{R}^t} (\boldsymbol{\Delta_0} - \boldsymbol{\Delta_1}, \boldsymbol{\Delta_0'} + \boldsymbol{\Delta_1}, 0, \ldots, 0)$$

Application to GMiMC

Differential characteristic:

Δ_0, Δ_0' arbitrary non-zero differences

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}} (\Delta_0' + \Delta_1, \Delta_1, \ldots, \Delta_1, \Delta_0) \qquad \Delta_0 \xrightarrow{S} \Delta_1$$

$$\xrightarrow{\mathcal{R}} (\Delta_1 + \Delta_1', \ldots, \Delta_1 + \Delta_1', \Delta_0 + \Delta_1', \Delta_0' + \Delta_1) \qquad \Delta_0' + \Delta_1 \xrightarrow{S} \Delta_1'$$

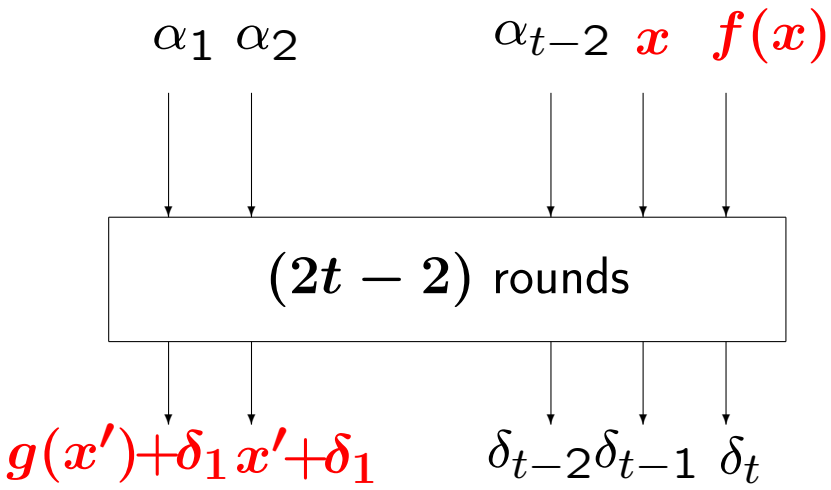
If $\Delta_1 + \Delta_1' = 0$, we get an iterative differential characteristic

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}^t} (\Delta_0 - \Delta_1, \Delta_0' + \Delta_1, 0, \ldots, 0)$$

$\Delta_1 + \Delta_1' = 0$ occurs with probability $\approx 1/q$

Condition $\Delta_1 + \Delta_1' = 0$ is viewed as an equation on values

A differential property on $(2t-2)$ rounds



$x \in \mathbb{F}_q$

$\deg f = 3$

$x' \in \mathbb{F}_q$

$\deg g = 3$

Satisfying $(3t-2)$ rounds

Satisfying $(2t-2)$ rounds with special states values:

$$X_0 = (\alpha_1, \ldots, \alpha_{t-2}, x, f(x)) \xrightarrow{\mathcal{R}^{2t-2}} X_{2t-2} = (g(x') + \delta_1, x' + \delta_1, \delta_3, \ldots, \delta_t)$$

$$Y_0 = (\alpha_1, \ldots, \alpha_{t-2}, y, f(y)) \xrightarrow{\mathcal{R}^{2t-2}} Y_{2t-2} = (g(y') + \delta_1, y' + \delta_1, \delta_3, \ldots, \delta_t)$$

Therefore

$$X_{2t-2} - Y_{2t-2} = (g(x') - g(y'), x' - y', 0, \ldots, 0)$$

Satisfying $(3t-2)$ rounds

Satisfying $(2t-2)$ rounds with special states values:

$$X_0 = (\alpha_1, \ldots, \alpha_{t-2}, x, f(x)) \xrightarrow{\mathcal{R}^{2t-2}} X_{2t-2} = (g(x') + \delta_1, x' + \delta_1, \delta_3, \ldots, \delta_t)$$
$$Y_0 = (\alpha_1, \ldots, \alpha_{t-2}, y, f(y)) \xrightarrow{\mathcal{R}^{2t-2}} Y_{2t-2} = (g(y') + \delta_1, y' + \delta_1, \delta_3, \ldots, \delta_t)$$

Therefore

$$X_{2t-2} - Y_{2t-2} = (g(x') - g(y'), x' - y', 0, \ldots, 0)$$

Adding t rounds with the differential characteristic

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}^t} (\Delta_0 - \Delta_1, \Delta_0' + \Delta_1, 0, \ldots, 0)$$

Satisfying $(3t-2)$ rounds

Satisfying $(2t-2)$ rounds with special states values:

$$X_0 = (\alpha_1, \ldots, \alpha_{t-2}, x, f(x)) \xrightarrow{\mathcal{R}^{2t-2}} X_{2t-2} = (g(x') + \delta_1, x' + \delta_1, \delta_3, \ldots, \delta_t)$$
$$Y_0 = (\alpha_1, \ldots, \alpha_{t-2}, y, f(y)) \xrightarrow{\mathcal{R}^{2t-2}} Y_{2t-2} = (g(y') + \delta_1, y' + \delta_1, \delta_3, \ldots, \delta_t)$$

Therefore

$$X_{2t-2} - Y_{2t-2} = (g(x') - g(y'), x' - y', 0, \ldots, 0)$$

Adding t rounds with the differential characteristic

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}^t} (\Delta_0 - \Delta_1, \Delta_0' + \Delta_1, 0, \ldots, 0)$$

The differential transition after $(3t-2)$ rounds is assured if $\Delta_2(x,y) + \Delta_2'(x,y) = 0$

Degree of the equation?

Satisfying $(3t-2)$ rounds

Satisfying $(2t-2)$ rounds with special states values:

$$X_0 = (\alpha_1, \ldots, \alpha_{t-2}, x, f(x)) \xrightarrow{\mathcal{R}^{2t-2}} X_{2t-2} = (g(x') + \delta_1, x' + \delta_1, \delta_3, \ldots, \delta_t)$$
$$Y_0 = (\alpha_1, \ldots, \alpha_{t-2}, y, f(y)) \xrightarrow{\mathcal{R}^{2t-2}} Y_{2t-2} = (g(y') + \delta_1, y' + \delta_1, \delta_3, \ldots, \delta_t)$$

Therefore

$$X_{2t-2} - Y_{2t-2} = (g(x') - g(y'), x' - y', 0, \ldots, 0)$$

Adding t rounds with the differential characteristic

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}^t} (\Delta_0 - \Delta_1, \Delta_0' + \Delta_1, 0, \ldots, 0)$$

The differential transition after $(3t-2)$ rounds is assured if $\Delta_2(x,y) + \Delta_2'(x,y) = 0$

Degree of the equation

$$\xrightarrow{\mathcal{R}^{2t-2}} \deg g = 3 \xrightarrow{\mathcal{R}} \deg = 3^2 \xrightarrow{\mathcal{R}} \deg = 3^3 = 27$$

Satisfying $(3t-2)$ rounds

Satisfying $(2t-2)$ rounds with special states values:

$$X_0 = (\alpha_1, \ldots, \alpha_{t-2}, x, f(x)) \xrightarrow{\mathcal{R}^{2t-2}} X_{2t-2} = (g(x') + \delta_1, x' + \delta_1, \delta_3, \ldots, \delta_t)$$
$$Y_0 = (\alpha_1, \ldots, \alpha_{t-2}, y, f(y)) \xrightarrow{\mathcal{R}^{2t-2}} Y_{2t-2} = (g(y') + \delta_1, y' + \delta_1, \delta_3, \ldots, \delta_t)$$

Therefore

$$X_{2t-2} - Y_{2t-2} = (g(x') - g(y'), x' - y', 0, \ldots, 0)$$

Adding t rounds with the differential characteristic

$$(\Delta_0, \Delta_0', 0, \ldots, 0) \xrightarrow{\mathcal{R}^t} (\Delta_0 - \Delta_1, \Delta_0' + \Delta_1, 0, \ldots, 0)$$

The differential transition after $(3t-2)$ rounds is assured if $\Delta_2(x,y) + \Delta_2'(x,y) = 0$

Degree **only** $3^3 = 27$

Set $y =$ **const** and solve for x (factor polynomial)

Conclusions

	Rounds		Type	Rounds	Cost
GMiMC (128 bits)	101	permutation	integral distinguisher	70	2^{61}
			ZS distinguisher	102	$\mathbf{2^{48}}$
			diff. distinguisher	66	practical
		hash function	collisions	40	practical
			collisions	52	2^{83}
HadesMiMC (128 bits)	8+40	permutation	ZS distinguisher	6+45	2^{61}
GMiMC (256 bits)	186	permutation	integral distinguisher	116	2^{125}
			ZS distinguisher	206	$\mathbf{2^{125}}$
HadesMiMC (256 bits)	8+83	permutation	ZS distinguisher	6+87	2^{125}
		hash function*	preimages	8+any	$\mathbf{2^{160}}$

Need for new tools for analyzing primitives over fields of odd characteristic.

Special thanks to StarkWare Industries and to the Ethereum Foundation