Security of Poseidon hash function against linear and differential attacks with respect to field operations

Lyudmila Kovalchuk[1,2]

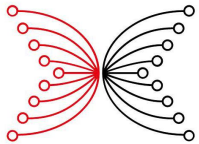
Joint work with Mariia Rodinko[1,3], Roman Oliynykov[1,3]

{lyudmila.kovalchuk, mariia.rodinko, roman.oliynykov}@iohk.io

[1] Input Output HK, Hong Kong

[2] National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

[3] V.N. Karazin Kharkiv National University, Kharkiv, Ukraine



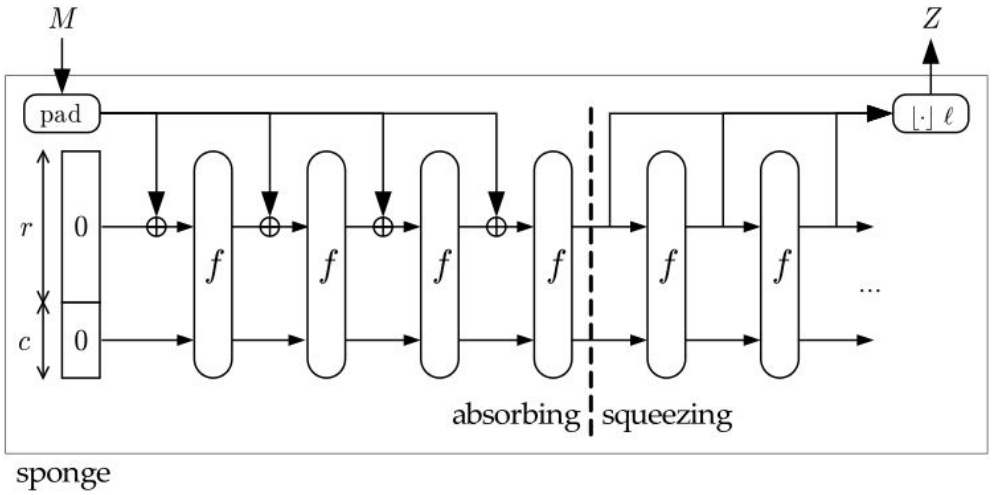
INPUT | OUTPUT

CECC 2020

Terms and definitions

- SNARK – Succinct Non-interactive ARguments of Knowledge.
- Constraints – special equations, used in SNARK.
- *HadesMiMC* (2019) – block cipher, optimal for using in SNARK (with small number constraints per bit).
- *In 2019 new strategy HadesMiMC appeared which crucial points are:*
  - to reduce the number of s-boxes;
  - to reduce the number of constraints.
- Hash-function Poseidon: “Hades inside SPONGE”; is optimal for using in SNARK: up to 0.18 constraints per bit, which is about 8 times smaller than for the Pederson hash-function.

Sponge and Hades constructions



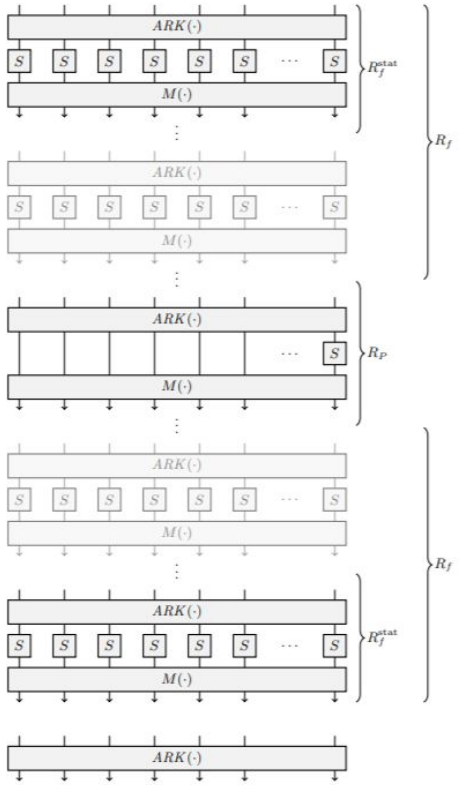


Figure 1. Sponge (left) and Hades (right) constructions

Formalization of HadesMiMC (I)

Let p be a large prime, l is its bit length, $l \approx \log p$. In our case $l \approx 753$.

We define a bijection $s : F_p \to F_p$ as $s(x) = x^u \bmod p$, where $(u, p-1) = 1$, or as

$$s(x) = \begin{cases} x^{-1} \bmod p, \; if \;\; x \neq 0; \\ 0, \; otherwise. \end{cases}$$

Formalization of HadesMiMC (II)

For some $t \in N$ let us define values $x, C \in \left(F_p\right)^t$ as $x = \left(x_t, ..., x_1\right)$, $C = \left(c_t, ..., c_1\right)$, where $x_i, c_i \in F_p$, $i = \overline{1,t}$.

Let us define two mappings: $S^{full} : \left(F_p\right)^t \to \left(F_p\right)^t$ and $S^{part} : \left(F_p\right)^t \to \left(F_p\right)^t$ as

$$S^{full}(x) = \left(s(x_t), ..., s(x_1)\right), \qquad S^{part}(x) = \left(x_t, ...x_2, s(x_1)\right). \tag{1}$$

Finally, let us define MDS-matrix $A : \left(F_p\right)^t \to \left(F_p\right)^t$ of the size $t \times t$.

Formalization of HadesMiMC (III)

Let us define the round functions for permutation HadesMiMC. They are of two types: round function with full s-box layer, which is defined as $f_C^{full} : (F_p)^t \to (F_p)^t$, where for arbitrary $C \in (F_p)^t$:

$$f_C^{full}(x) = A \circ S^{full}(x * C), \tag{2}$$

and round function with partial s-box layer, which is defined as $f_C^{part} : (F_p)^t \to (F_p)^t$, where for arbitrary $C \in (F_p)^t$:

$$f_C^{part}(x) = A \circ S^{part}(x * C), \tag{3}$$

where $x * C = (x_t + c_t, ..., x_1 + c_1)$ and "+" is field addition (addition modulo p).

Formalization of HadesMiMC (IV)

Definition 1: HadesMiMC-like block cipher (or permutation) with parameters p, t, u, r_{full}, and r_{part} is the family of permutations $H_C^{(p,t,u,r_{full},r_{part})} : (F_p)^t \to (F_p)^t$ parameterized by $C = (C_1, \ldots, C_{2r_{full}+r_{part}})$, $C_i \in (F_p)^t$, which is defined as

$$H_C^{(p,t,u,r_{full},r_{part})}(x) = f^{full}_{C_{2r_{full}+r_{part}}} \circ \ldots \circ f^{full}_{C_{r_{full}+r_{part}+1}} \circ f^{part}_{C_{2r_{full}+r_{part}}} \circ \ldots \circ f^{part}_{C_{r_{full}+1}} \circ f^{full}_{C_{r_{full}}} \circ \ldots \circ f^{full}_{C_1}(x). \quad (4)$$

If parameters p, t, u, r_{full}, and r_{part} are set, we will write H_C, for simplicity.

Main remarks to [1, 2] about security estimations against differential and linear cryptanalysis

Differential cryptanalysis. The main result which expresses security of cipher with parameter of s-box, branch number of linear operator and a number of rounds is correct only in the case of sequential full rounds. It should be further improved for HadesMiMC because there are partial rounds between two sets of full rounds.

Linear cryptanalysis. The main results given in [1,2] are correct in case of ”classical” linear cryptanalysis; SPN-structures based on operations in prime fields require further analysis.

Security Against Differential Cryptanalysis (I)

Proposition 1: HadesMiMC-like block cipher (4) is Markov cipher.

Proposition 2 (easily derived from [3]): for HadesMiMC-like cipher, its security against differential cryptanalysis is upper estimated with the value Δ^b, where

$$\Delta = \max_{\alpha,\beta \in F_p^*} \frac{1}{p} \sum_{x \in F_p} \delta\left(s\left(x+\alpha\right) - s\left(x\right), \beta\right),$$

"+" and "-" are field addition and subtraction, b is the number of active s-boxes in all rounds.

Proposition 3 ([4]): the number of active s-boxes in 2 sequential rounds with round function (2) is not less than branch number $br\left(A\right)$.

Security Against Differential Cryptanalysis (II)

Proposition 4 (obvious): the number of active s-boxes in all rounds of (4) isn't less than the number of active s-boxes in rounds with full s-box layer.

Proposition 5 (corollary of Prop. 2 and Prop. 3): the number of active s-boxes in (4) isn't less than

$$2(t+1)\cdot\left[\frac{r_{full}}{2}\right]. \qquad (6)$$

Proposition 6: i) let $s(x)=x^u \bmod p$ and $(p-1,u)=1$. Then $\Delta \le \frac{u-1}{p}$.

ii) let $s(x)=x^{-1} \bmod p$. Then $\Delta \le \frac{4}{p}$.

Proposition 7: let r_{full} is even, $s(x)=x^u \bmod p$ or $s(x)=x^{-1} \bmod p$ and $A:(F_p)^t \to (F_p)^t$ is MDS matrix of the size $t \times t$. Then security estimations of the block cipher (4) against differential cryptanalysis is upper estimated with the value

$$\Delta^b=\left(\frac{u-1}{p}\right)^{(t+1)\cdot r_{full}} \quad \text{or} \quad \Delta^b=\left(\frac{4}{p}\right)^{(t+1)\cdot r_{full}}.$$

Security Against Linear Cryptanalysis

Proposition 8: security estimations of the block cipher (4) against linear cryptanalysis is upper estimated with the value

$$\max_{\chi,\rho\in\hat{F}_p} ELP^E(\chi,\rho) \le L^b,$$

$$L = L(s) = \max_{\chi,\rho\in\hat{F}_p} \left| \frac{1}{p} \sum_{x\in F_p} \left(\overline{\chi}(x), \rho(s(x)) \right) \right|^2$$

where χ and ρ are additive characters of F_p (characters of additive group of this field).

Proposition 9: let $s(x) = x^u \bmod p$, $u \in \mathbf{N}$. Then $L(s) \le \dfrac{(u-1)^2}{p}$.

Proposition 10: let $s(x) = \begin{cases} x^{-1} \bmod p, \; if \;\; x \ne 0; \\ 0, \; else. \end{cases}$. Then $L(s) \le \dfrac{16}{p}$.

A number of rounds

The number of full rounds for HadesMiMC can be easily found from inequality

$$\left(\frac{(u-1)^2}{p}\right)^{(t+1)\cdot r_{full}} \leq 2^{-2N}.$$

For example, if $l(p)=750$, $t=3$, $u=13$ we get $r_{full} \geq 2$.

Similar inequality also holds for inverse s-boxes.

But for reasons of symmetry it is recommended two full rounds on the beginning and two at the end of SPN.

References

1. Lorenzo Grassi and Reinhard Lüftenegger and Christian Rechberger and Dragos Rotaru and Markus Schofnegger.: *On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. Cryptology ePrint Archive*, 2019.

2. Lorenzo Grassi, Daniel Kales, Dmitry Khovratovich, Arnab Roy, Christian Rechberger, and Markus Schofnegger: *Poseidon and Starkad: New Hash Functions for Zero Knowledge Proof Systems*, 2019.

3. Serge Vaudenay: On the security of CS-cipher, 2001. Elektronnyi resurs. – [Rezhym dostupu]: https://link.springer.com/content/pdf/10.1007%2F3-540-48519-8_19.pdf

4. Douglas R. Stinson, Stafford Tavares: *Selected Areas in Cryptography: 7th Annual International Workshop*, 2003. Elektronnyi resurs. – [Rezhym dostupu]: https://books.google.com.ua/books?id=F3CqCAAAQBAJ&dq=Kanda,+Knudsen+(branch+number)&hl=ru&source=gbs_navlinks_s.html.