DOI 10.1007/s10559-021-00352-y
*Cybernetics and Systems Analysis, Vol. 57, No. 2, March, 2021*

# SECURITY OF THE POSEIDON HASH FUNCTION AGAINST NON-BINARY DIFFERENTIAL AND LINEAR ATTACKS*

**L. Kovalchuk,[1] R. Oliynykov,[2] and M. Rodinko[3]**

UDC 681.3.06:006.354

**Abstract.** *In the paper, we construct security estimations of Poseidon hash function against non-binary linear and differential attacks. We adduce the general parameters for the Poseidon hash function that allow using this hash function in recurrent SNARK-proofs based on MNT-4 and MNT-6 triplets. We also analyse how to choose S-boxes for such function for this choice to be optimal from the point of view of the number of constraints and security. We show how many full rounds are sufficient to guarantee security of such hash function against non-binary linear and differential attacks. We also calculate the number of constraints per bit achieved in the proposed realizations and demonstrate a considerable gain as compared to the Pedersen hash function.*

**Keywords:** *SNARK, constraints, Poseidon hash function, non-binary linear and differential cryptanalysis.*

## INTRODUCTION

One of the most important problems arising in construction of SNARK-proofs and STARK-proofs [1–3] is reduction of the number of constraints describing algorithms in the respective SNARK-system. The construction of such proofs begins with the fact that a certain transformation (for example, a hash function) should be described as a system of certain equations of many variables over a finite field whose left-hand side contains a polynomial of many second-degree variables, and the right-hand side contains a polynomial of many variables of the first degree. These equations are called constraints, and their complexity determines the complexity of constructing the appropriate SNARK-proof. Most often SNARK-proofs are used to prove knowledge of the pre-image of some hash function. Therefore, the hash functions used in such blockchains should be designed so that they can be described by as few constraints as possible.

One of the first hash functions convenient for constructing SNARK-proofs was the Pedersen hash function [4, p. 134]. It is based on operations in a group of points of an elliptic curve, which, in turn, can be reduced to operations in the corresponding finite field. Since constraints are polynomials just over such a field, the number of constraints required to specify such a hash function is ten times less than for "classical" hash functions that operate with byte and bit operations (about 1.68 constraints per 1 bit of input). This number of constraints is quite acceptable but the question of reducing it still remains relevant. The Poseidon hash function proposed in [5] appeared to be quite a good construction with respect to the number of constraints. For this function, the number of constraints is up to 15 times smaller than for the Pedersen hash function. Utilization of this function in SNARK-systems requires provision of a full substantiation of its security against

*This work was partially supported by the National Research Foundation of Ukraine under Grant 2020.01/0351.

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," Kyiv, Ukraine, and IOHK, Hong Kong, *lusi.kovalchuk@gmail.com*. [2]V. N. Karazin Kharkiv National University, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine, and IOHK, Hong Kong, *roliynykov@gmail.com*. [3]V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, and IOHK, Hong Kong, *m.rodinko@gmail.com*. Translated from Kibernetyka ta Systemnyi Analiz, No. 2, March–April, 2021, pp. 115–127. Original article submitted October 19, 2020.

 1060-0396/21/5702-0268 

the main applicable cryptographic attacks. The Poseidon hash function is based upon the SPONGE construction [6] that uses the HADES block cipher algorithm [7] as the inner permutation. For this reason, the main part of the security substantiation for the Poseidon hash function is to show that the HADES algorithm is indistinguishable from a random permutation [5, 6]. The authors of the HADES algorithm, and later the authors of the Poseidon hash function adduced very detailed substantiations for security of these constructions against some class of attacks they called "algebraic attacks." However, for these algorithms, substantiation of security against linear and differential cryptoanalysis attacks was to a large extent empirical and requires further analysis to achieve a strict formal substantiation. For example, in substantiation of the algorithm security against linear attacks, the authors considered coordinate functions of S-boxes demonstrating that in fact they analyzed its security against classical linear attacks. However, as shown in [8, 9], for non-binary ciphers it is necessary to analyze security specifically against non-binary linear cryptoanalysis, as both the key adder and the linear layer use operations in the prime field instead of binary operations. The similar situation takes place with respect to the differential cryptanalysis.

The purpose of this paper is to obtain security estimates of Poseidon hash function against non-binary linear and differential attacks, show how many full rounds would be sufficient to guarantee security of such hash function against these attacks, and adduce the general parameters for the Poseidon hash function that allows using this hash function in recurrent SNARK-proofs.

## 1. MATHEMATICAL MODEL OF THE POSEIDON

The Poseidon hash function [5] uses SPONGE construction [6] with a permutation named HadesMiMC [7] inside it (see Fig. 1).

Three parameters describe this construction: capacity $c$, rate $r$, and permutation length $N$, where $N = c + r$. From some practical consideration, we are interested in the case where $N = 3[\log p]$, $c = 2[\log p]$, and $r = [\log p]$, where prime $p$ is of special form, which provides compatibility with triplets MNT-4 or MNT-6 in CODA (now MINA) [10, 11]. Any permutation or block cipher may be used inside SPONGE. The authors of [7] suggested to use HadesMiMC as the permutation that needs the least number of constraints per bit, when used in SNARK-systems. HadesMiMC may be considered as a block cipher whose round functions are different in different rounds. The main idea of HadesMiMC is to use rounds with full number of S-boxes and rounds with partial number of S-boxes (for example, only 1 S-box). The general scheme of Hades is given in Fig. 2 (this figure is taken from [7] with all its designations, which are wide used for block ciphers). Such construction allows reducing the number of constraints, while preserving security level against different (statistical and algebraic) attacks.

Now we describe the mathematical model of the permutation HadesMiMC on which Poseidon is based.

Let $p$ be a large prime, $l$ be its bit length, $l \approx \log p$.

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

For some $t \in N$ define values $x, C \in (F_p)^t$ as $x = (x_t, \ldots, x_1)$, $C = (c_t, \ldots, c_1)$, where $x_i, c_i \in F_p$, $i = \overline{1, t}$. For $x \in (F_p)^t$ define two mappings: $S^{\text{full}}: (F_p)^t \to (F_p)^t$ and $S^{\text{part}}: (F_p)^t \to (F_p)^t$ as

$$S^{\text{full}}(x) = (s(x_t), \ldots, s(x_1)), \; S^{\text{part}}(x) = (x_t, \ldots, x_2, s(x_1)). \tag{1}$$

Finally, define a $t \times t$ MDS-matrix $A: (F_p)^t \to (F_p)^t$.

Define the round functions for the permutation HadesMiMC. They are of two types: the round function with a full S-box layer that is defined as $f_C^{\text{full}}: (F_p)^t \to (F_p)^t$, where for arbitrary $C \in (F_p)^t$:

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

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

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

where $x * C = (x_t + c_t, \ldots, x_1 + c_1)$ and "+" is field addition (addition modulo $p$) and $S^{\text{full}}$, $S^{\text{part}}$ were defined in (1).

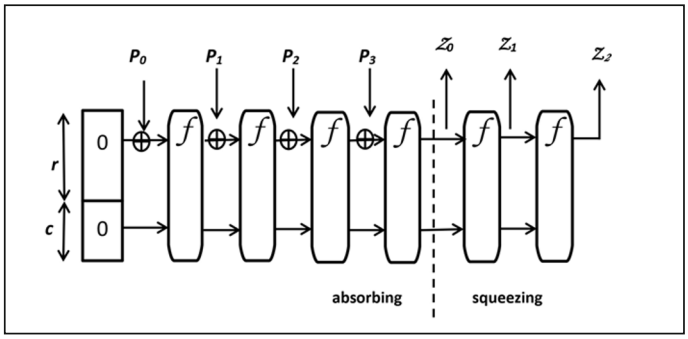


Fig. 1. SPONGE construction.

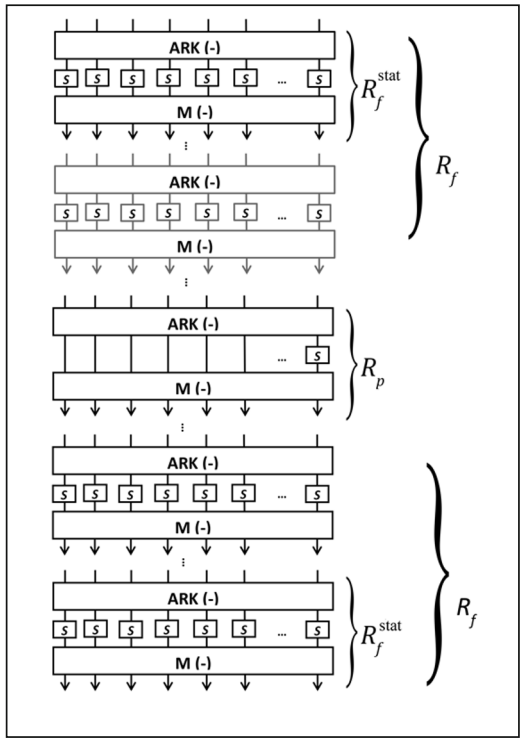


Fig. 2. HadesMiMC.

**Definition 1.** A HadesMiMC-like permutation with parameters $p$, $t$, $u$, $r_{\text{full}}$, and $r_{\text{part}}$ is the family of permutations $H_{\boldsymbol{C}}^{(p,t,u,r_{\text{full}},r_{\text{part}})}:(F_p)^t \to (F_p)^t$ parameterized by the set of round constants $\boldsymbol{C}=(C_1,\ldots,C_{2r_{\text{full}}+r_{\text{part}}})$, $C_i \in (F_p)^t$ that are defined as

$$H_{\boldsymbol{C}}^{(p,t,u,r_{\text{full}},r_{\text{part}})}(x)=f_{C_{2r_{\text{full}}+r_{\text{part}}}}^{\text{full}}\circ\ldots\circ f_{C_{r_{\text{full}}+r_{\text{part}}+1}}^{\text{full}}\circ f_{C_{2r_{\text{full}}+r_{\text{part}}}}^{\text{part}}\circ\ldots\circ f_{C_{r_{\text{full}}+1}}^{\text{part}}\circ f_{C_{r_{\text{full}}}}^{\text{full}}\circ f_{C_1}^{\text{full}}(x). \quad (4)$$

If parameters $p$, $t$, $u$, $r_{\text{full}}$, and $r_{\text{part}}$ are set, we will write $H_{\boldsymbol{C}}$, for simplicity.

**Note.** The transformation (4) means that, for fixed set of constraints $\boldsymbol{C}=(C_1,\ldots,C_{2r_{\text{full}}+r_{\text{part}}})$, we first apply functions $f_{C_1}^{\text{full}},\ldots,f_{C_{r_{\text{full}}}}^{\text{full}}$, i.e., functions of the type (2) with a full S-box layer and with corresponding "round keys" $C_1,\ldots,C_{r_{\text{full}}}$, and they are the first $r_{\text{full}}$ rounds of the transformation. Then we apply functions of the type (3) with a partial S-box layer during $r_{\text{part}}$ round and with corresponding "round keys;" and then again apply $r_{\text{full}}$ rounds with functions of the type (2).

## 2. CRYPTOGRAPHICAL SECURITY OF THE POSEIDON

**2.1. Security in the Random Oracle Model.** Security of SPONGE construction depends mostly on the security of its internal permutation, HadesMiMC in our case. So we will pay a lot of attention to security of HadesMiMC. It was proven in [12] that if an internal permutation is modeled as a randomly chosen permutation, then the SPONGE function is indistinguishable from the random oracle up to $2^{c/2}$ calls to it.

For some practical aspects, it is convenient to set $c=2l(p)$, so the maximal security level of the SPONGE construction is $l(p)$. It means that we should prove that the security level of the internal permutation is also no less than $l(p)$. But we will use stronger requirement to find the number of rounds of the permutation.

In what follows, under security estimations against differential and linear cryptanalysis of block cipher we will understand the maximum of average (on keys) probabilities of its differential and linear characteristics, respectively.

**2.2. Security Against Linear and Differential Attacks.** In this chapter we construct, rigorously proved, security estimates for HadesMiMC against these two types of statistical attacks. Note that to construct estimates against differential attacks, we mostly use known results or their generalizations. But to construct the similar estimates against linear attacks, we had to prove a few non-trivial statements on sums of characters of the additive group of the finite field.

**2.2.1. Security Estimates of Non-Binary Cipher HadesMiMC Against Differential Cryptanalysis.** To construct security estimates against differential cryptanalysis, we consider HadesMiMC as a block cipher. Further we use the following results.

**Definition 2** [13]. The block cipher $E$ with the round function

$$f: M \times K \to M$$

(where $M$ is an Abelian group w.r.t. some operation "*," 0 is its neutral element) is called a Markov cipher w.r.t. "*" if $\forall x,\ \alpha,\ \beta \in M$:

$$\frac{1}{|K|}\sum_{k\in K}\delta(f(k, x*\alpha)*f(k,x)^{-1}, \beta) = \frac{1}{|K|}\sum_{k\in K}\delta(f(k,\alpha)*f(k,0)^{-1}, \beta)\ , \tag{5}$$

where $\delta$ is the Kronecker delta: $\delta(x, y) = \begin{cases} 1 & \text{if } x = y, \\ 0, & \text{else}. \end{cases}$

**Note.** This definition can be easily generalized for the case where the round functions are different.

**Definition 3** [14]. The branch number of the $t \times t$ matrix $A: (F_p)^t \to (F_p)^t$ is

$$br(A) = \min_{x\in(F_p)^t\setminus(0,\dots,0)}\{wt(Ax) + wt(x)\},$$

where $wt$ is the Hamming weight.

Note that if $A$ is an MDS-matrix, then its branch number is maximal possible (for its size) and is equal to $br(A) = t+1$. For example, in our case, $t = 3$ and $br(A) = 4$.

**Proposition 1.** The block cipher (4) is a Markov cipher.

This proposition may be proven directly, by checking (5) for its round functions.

**Proposition 2** (easily derived from [15]). For the Markov cipher (4), its security against differential cryptanalysis is upper estimated with the value $\Delta^b$, where

$$\Delta = \max_{\alpha,\beta\in F_p^*}\frac{1}{p}\sum_{x\in F_p}\delta(s(x+\alpha)-s(x), \beta), \tag{6}$$

"+" is the field addition and $b$ is the number of active S-boxes in all rounds.

**Proposition 3** [14]. The number of active S-boxes in 2 sequential rounds with the round function (2) is no less than $br(A)$.

In the case if $A$ is a $t \times t$ MDS-matrix, $br(A) = +1$ and, according to Proposition 3, the number of active S-boxes in 2 sequential rounds with full S-box layer is no less than $t+1$. But if there are several rounds, each with only one S-box, between two rounds with a full S-box layer, we cannot state anything about the number of active S-boxes in these rounds, except that this number is no less than the number of rounds. It should be noted that the authors of [5] did not take this detail into account when constructing security estimates against linear and differential cryptanalysis, and, as a result, incorrect estimates were obtained.

**Proposition 4** (obvious). The number of active S-boxes in all rounds of (4) is no less than the number of active S-boxes in rounds with a full S-box layer.

**Proposition 5** (corollary of Prop. 2 and Prop. 3). The number $b$ of active S-boxes in (4) is no less than

$$b \geq 2(t+1)\cdot\left\lceil\frac{r_{\text{full}}}{2}\right\rceil, \tag{7}$$

and, if $r_{\text{full}}$ is even, is no less than

$$b \geq (t+1) r_{\text{full}}.$$

**Note.** The inequality (7) implies that it is more efficient to have an even value $r_{\text{full}}$, because one extra round that makes $r_{\text{full}}$ odd does not increase the value in (7). So, in what follows, we will choose $r_{\text{full}}$ to be even.

In this chapter, we construct security estimates for HadesMiMC-like permutations with two types of S-boxes: power functions and inverse S-boxes. Before proving the main results, we will need the following auxiliary statement about parameters (6).

**Proposition 6** [16].

1. Let $s(x) = x^u \bmod p$, where $(u, p-1) = 1$. Then $\Delta \leq \dfrac{(u-1)}{p}$.

2. Let $s(x) = \begin{cases} x^{-1} \bmod p \text{ if } x \neq 0; \\ 0, \text{ else.} \end{cases}$ Then $\Delta \leq \dfrac{4}{p}$.

**THEOREM 1.** 1. Let $r_{\text{full}}$ be even, $s(x) = x^u \bmod p$, $A : (F_p)^t \to (F_p)^t$ be a $t \times t$ MDS matrix. Then the security estimate of the block cipher (4) against differential cryptanalysis is upper bounded with the value

$$\left( \frac{u-1}{p} \right)^{(t+1) r_{\text{full}}}. \tag{8}$$

2. Let $r_{\text{full}}$ be even, $s(x) = x^{-1} \bmod p$, $A : (F_p)^t \to (F_p)^t$ be a $t \times t$ MDS matrix. Then security estimate of the block cipher (4) against differential cryptanalysis is upper bounded with the value

$$\left( \frac{4}{p} \right)^{(t+1) r_{\text{full}}}.$$

**Proof.** It is obvious using Propositions 1–6 and the fact that in this case $\left\lceil \dfrac{r_{\text{full}}}{2} \right\rceil + \left\lceil \dfrac{r_{\text{full}}}{2} \right\rceil = r_{\text{full}}$. □

Usually a block cipher is considered to be practically secure against differential cryptanalysis if its security estimate is no more than $2^{-N}$, where $N$ is its block size. But in our case, as we showed in 2.1, the maximal security level of SPONGE construction is $l(p) \approx \log p$. So, the weaker requirement may be formulated as

$$\Delta^b < 2^{-\log p}.$$

However, we will use a stronger requirement. Moreover, to increase the security and make it closer to the theoretical one, we require

$$\Delta^b < 2^{-2N},$$

which means

$$\left( \frac{u-1}{p} \right)^{(t+1) r_{\text{full}}} < 2^{-2N} \quad \text{or} \quad \left( \frac{4}{p} \right)^{(t+1) r_{\text{full}}} < 2^{-2N}, \tag{9}$$

using statements 1 and 2 of Theorem 1 for powered and inverse S-boxes, respectively. Also in [5] the authors proposed to add two extra full rounds, just for any case. But adding two full rounds (one at the beginning, and one at the end) makes $r_{\text{full}}$ odd and does not increase security. So, if we decide to add some extra rounds, we should add them in such a way that $r_{\text{full}}$ is even (i.e., when adding additional rounds we should provide even parity of $r_{\text{full}}$).

As we can see from (9), a permutation with power S-boxes with $u > 5$ requires more rounds than with inverse ones, for the same level of security. In the next chapter, we will discuss a type of S-boxes that is preferable from different points of view.

**2.2.2. Security Estimates of Non-Binary Cipher HadesMiMC Against Linear Cryptanalysis.** According to [9], the parameters that characterize practical security of a block cipher against linear attacks, essentially depend on the structure of this cipher, and first of all, on the operation in the key adder. Thus, the practical security estimate (with

respect to the field addition in $F_p$) of a cipher $E$ against linear cryptanalysis is the value

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

where $b$ is the number of active S-boxes and the parameter $L$ depends on the S-box (see Definition 15 and explanation on p. 25 in [9]):

$$L = L(s) = \max_{\chi,\rho\in\hat{F}_p} \left| \frac{1}{p} \sum_{x\in F_p} (\overline{\chi}(x), \rho(s(x))) \right|^2, \tag{10}$$

where $\chi$ and $\rho$ are additive characters of $F_p$ (characters of the additive group of this field).

The value $b$ is the same as for the differential cryptanalysis, i.e., it is the number of all active S-boxes in the cipher. Using the same consideration as in 2.1, we get $b = (t+1)r_{\text{full}}$ if $r_{\text{full}}$ is even (we consider only this case).

**Proposition 7.**

1. Let $s(x) = x^u \bmod p$, where $(u, p-1) = 1$. Then $L(s) \le \dfrac{(u-1)^2}{p}$.
2. Let $s(x) = \begin{cases} x^{-1} \bmod p \text{ if } x \ne 0; \\ 0, \text{ else.} \end{cases}$ Then $L(s) \le \dfrac{16}{p}$.

**Proof.**

1. First, let us estimate the value

$$\sum_{x\in F_p} (\overline{\chi}(x)\rho(s(x))) = \sum_{x\in F_p} (\overline{\chi}(x)\rho(x^{13})). \tag{11}$$

Note that the group $(F_p,+)$ is cyclic (with the generator $g = 1$), so the corresponding group of characters $(\hat{F}_p, \times)$ is also cyclic. Let $\psi$ be the generator of $(\hat{F}_p, \times)$. Then any element from this group, particularly characters $\overline{\chi}$ and $\rho$, can be represented as

$$\overline{\chi} = \psi^{\alpha},\ \rho = \psi^{\beta},$$

for some appropriate $0 \le \alpha, \beta \le p-1$.

Then

$$\overline{\chi}(x)\rho(x^{13}) = \psi(x)^{\alpha} \cdot \psi(x^{13})^{\beta} = \psi(\alpha x) \cdot \psi(\beta x^{13}) = \psi(\alpha x + \beta x^{13}), \tag{12}$$

using the fact that $\psi$ is a homomorphism.

Now we can rewrite (11) using (12) as

$$\sum_{x\in F_p} (\overline{\chi}(x)\rho(x^{13})) = \sum_{x\in F_p} \psi(\alpha x + \beta x^{13}). \tag{13}$$

Applying the Weil Theorem ([17], Theorem 5.38) to (13), we obtain

$$\sum_{x\in F_p} \psi(\alpha x + \beta x^{13}) \le (\deg(\alpha x + \beta x^{13}) - 1) \cdot \sqrt{p} = 12\sqrt{p}. \tag{14}$$

After application of (11)–(14) to (10), we obtain

$$L = L(s) = \max_{\chi,\rho\in\hat{F}_p} \left| \frac{1}{p} \sum_{x\in F_p} (\overline{\chi}(x), \rho(s(x))) \right|^2 = \max_{\alpha,\beta} \left| \frac{1}{p} \sum_{x\in F_p} \psi(\alpha x + \beta x^{13}) \right|^2 \le \left| \frac{1}{p} \cdot 12 \cdot \sqrt{p} \right|^2 = \frac{144}{p}.$$

2. First, let us estimate the value

$$\sum_{x\in F_p}(\bar{\chi}(x)\rho(s(x))) = \sum_{x\in F_p^*}(\bar{\chi}(x)\rho(x^{-1}))+1. \tag{15}$$

Note that the group $(F_p,+)$ is cyclic (with the generator $g=1$), so the corresponding group of characters $(\hat{F}_p,\times)$ is also cyclic. Let $\psi$ be the generator of $(\hat{F}_p,\times)$. Then any element from this group, particularly characters $\bar{\chi}$ and $\rho$, can be represented as

$$\bar{\chi}=\psi^{\alpha},\ \rho=\psi^{\beta},$$

for some appropriate $0\le\alpha,\beta\le p-1$.

Then

$$\bar{\chi}(x)\rho(x^{-1})=\psi(x)^{\alpha}\cdot\psi(x^{-1})^{\beta}=\psi(\alpha x)\cdot\psi(\beta x^{-1})=\psi(\alpha x+\beta x^{-1}), \tag{16}$$

using the fact that $\psi$ is a homomorphism.

Now we can rearrange (15) using (16) as

$$\sum_{x\in F_p}(\bar{\chi}(x)\rho(x^{-1})) = \sum_{x\in F_p^*}\psi(\alpha x+\beta x^{-1}). \tag{17}$$

Applying the theorem about the Kloosterman sum ([17], Theorem 1.5) to (17), we obtain

$$\sum_{x\in F_p^*}\psi(\alpha x+\beta x^{-1}) = 2\sum_{x_1,x_2\in F_p:\ x_1x_2=\alpha\beta}\psi(x_1+x_2)\le 2\cdot 2\cdot\sqrt{p}=4\sqrt{p}. \tag{18}$$

After application of (15)–(18) to (10), we obtain

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

$$=\max_{\alpha,\beta}\left|\frac{1}{p}\left(\sum_{x\in F_p^*}\psi(\alpha x+\beta x^{-1}+1)\right)\right|^2\approx\left|\frac{1}{p}\cdot 4\cdot\sqrt{p}\right|^2=\frac{16}{p}.\ \square$$

**THEOREM 2.** 1. Let $r_{\text{full}}$ be even, $s(x)=x^u \bmod p$, $A:(F_p)^t\to(F_p)^t$ be a $t\times t$ MDS matrix. Then the security estimate of the block cipher (4) against linear cryptanalysis is upper bounded with the value

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

2. Let $r_{\text{full}}$ be even, $s(x)=x^{-1} \bmod p$, $A:(F_p)^t\to(F_p)^t$ be a $t\times t$ MDS matrix. Then security estimate of the block cipher (4) against linear cryptanalysis is upper bounded with the value

$$\left(\frac{16}{p}\right)^{(t+1)r_{\text{full}}}.$$

**Proof.** It is obvious using Propositions 1–5, Proposition 7, and the fact that in this case $\left[\frac{r_{\text{full}}}{2}\right]+\left[\frac{r_{\text{full}}}{2}\right]=r_{\text{full}}$. $\square$

## 3. CHOICE OF S-BOXES

Choice of S-boxes should take into account the following aspects:

— the mapping $s: F_p \to F_p$ should be bijective, i.e., for a power S-box the requirement $(p-1, u) = 1$ should be met;

— for reasons of security against linear and differential cryptanalysis, the parameters $\Delta$ and $L$ (which depend only on the S-box) should be as small as possible;

— in terms of SNARKs implementation complexity, the number of constraints (which also depends only on the number and type of S-boxes) should be as small as possible.

Recall that for the inverse S-boxes, the parameters $\Delta$ and $L$ are estimated by the upper bound as $\Delta \le \frac{4}{p}$ and $L \le \frac{16}{p}$, and for the power ones — as $\Delta \le \frac{(u-1)}{p}$ and $L \le \frac{(u-1)^2}{p}$ (Propositions 6 and 7). So, for the power S-boxes, it makes sense to choose the parameter $u$ as $u = \min\{v \in N: (v, p-1) = 1\}$.

For the inverse S-boxes the parameters $\Delta$ and $L$ will be smaller than for the power ones if $u \ne 3$. So, in terms of the cryptographic security, the most appropriate are either inverse or cubic S-boxes if the latest ones define a bijective mapping. If $p-1$ is divided by 3, then inverse S-boxes have no competitors.

In terms of minimizing the number of constraints, inverse and power S-boxes with a small value of the parameter $u$ are also the most appropriate. Indeed, to describe an inverse S-box, 3 constraints are needed; to describe a cubic S-box — 2 constraints:

$$\begin{cases} x_1 x_1 = x_2; \\ x_1 x_2 = x_3, \end{cases}$$

to describe an S-box $s(x) = x^5 \bmod p$, 3 constraints are needed:

$$\begin{cases} x_1 x_1 = x_2; \\ x_2 x_2 = x_3; \\ x_1 x_3 = x_4, \end{cases}$$

etc., with an increase in the exponent $u$ the number of constraints grows approximately as $2 \log u$. So, if $p-1$ is divided by all relatively "small" prime 3, 5, 7, 11, …, then both the security requirements and the requirements for simplicity of implementation lead to the choice of inverse S-boxes.

However, on the other hand, implementation of an inverse S-box is costly since it requires execution of the Euclid's algorithm, which, in turn, requires the order of O(log $p$) divisions with a remainder. Therefore, when choosing an S-box, all factors must be taken into account and an acceptable compromise must be sought.

In the next Sec. 5, when calculating the algorithm parameters for specific values of the field characteristics, we will consider two options for choosing of S-boxes: inverse and power, with the smallest exponent providing bijection.

## 4. NUMBER OF ROUNDS WITH FULL AND PARTIAL S-BOX LAYERS AND FULL NUMBER OF CONSTRAINTS

Following [5, 7], we define the number of rounds with a full S-box layer, $r_{\text{full}}$, as the minimal number of rounds that guarantee security against differential and linear cryptanalysis (forward and backward). Then determine the number of rounds with a partial layer of S-boxes, based on considerations of the security against algebraic attacks.

As noted, the authors of [5] also recommend adding two rounds just in case. However, after adding two rounds (one at the beginning, one at the end), the value $r_{\text{full}}$ will become odd, i.e. adding two rounds will not increase the security against statistical attacks. If we add two rounds at the beginning and end, it will significantly increase the number of constraints. We do not see a reasonable need to increase the number of rounds with a full layer of S-boxes, especially in a situation where the number of constraints is critical.

The number of constraints per bit is determined as follows. The number of constraints required to specify one S-box must be multiplied by the number of all S-boxes, which is completely determined by the number of rounds of both types and their structure. Then the resulting value must be divided by the value $r$ that determines the length of the output on one iteration of the SPONGE construction.

## 5. NUMERICAL RESULTS FOR MNT-COMPATIBLE PARAMETERS

We calculated the number of rounds with a full layer of S-boxes for a prime field of characteristic $p$, where the bit length of the characteristic is equal to 753. As a prime field, we chose one of the fields for which triplets MNT-4 and MNT-6 are defined [11]. In rounds with a full layer of S-boxes, we will place 3 S-boxes, in rounds with a partial layer — one S-box. We define a linear operator as an MDS matrix of dimension $3\times 3$. In this case, the capacity $c = 2\cdot 752 = 1504$ and rate $r = 752$ if you use a byte representation. Power S-boxes were chosen as $s(x) = x^{13} \bmod p$, because of $\min\{v \in N : (v,\ p-1) = 1\} = 13$. For inverse S-boxes and power S-boxes of the form $s(x) = x^{13} \bmod p$, the number of rounds with a full layer of S-boxes is 4 (2 rounds at the beginning, 2 at the end, to eliminate the possibility of both attacks with the chosen plaintext and attacks with the chosen ciphertext). The number of rounds with a partial layer of S-boxes, according to (4.1) and (4.2) in [5], will be about 60. In this case, the number of constraints per bit is equal to 0.48 for power S-boxes and 0.29 for inverse S-boxes, which is 3.5–5.8 times less than the same indicator for the Pedersen function.

The number of full rounds for the Poseidon we find from the inequality

$$\left(\frac{144}{p}\right)^{4r_{\text{full}}} \le 2^{-2N} = 2^{-6p},$$

whence we obtain

$$r_{\text{full}} = \left\lfloor \frac{6\cdot 753}{4\cdot 745} \right\rfloor = 2,$$

i.e., we have two rounds with a full layer of S-boxes at the beginning and at the end of the algorithm.

The same number of rounds is enough to guarantee security against linear cryptanalysis.

Note than in case of adding 2 extra rounds (one to the beginning, one to the end) and 2 rounds to make $r_{\text{full}}$ even, we obtain

$$r_{\text{full}} = 4,$$

so the whole number of full rounds is 8.

## CONCLUSIONS

The paper contains the following results.

1. Security estimates were considered against non-binary linear and differential attacks. Let us note that construction of such estimates uses serious algebraic techniques, in particular, some properties of sums of characters for an additive group of the finite field, and properties of sums of such characters.

2. We adduce the general parameters for the Poseidon hash function that allows using this hash function in recurrent SNARK-proofs based on MNT-4 and MNT-6 triplets.

3. We analyzed how to choose S-boxes for such function, for this choice to be optimal from the point of view of the number of constraints and of security.

4. We showed how many full rounds would be sufficient to guarantee security of such hash function against non-binary linear and differential attacks.

5. We calculated the number of constraints per bit that is achieved in the proposed realization; a considerable gain was demonstrated, as compared to the Pedersen hash function.

We provided strict formal proofs for all listed results.

Following [5] and [7], we chose the round functions for random permutations and their parameters in the following way:

— the number of rounds with a full S-box layer is chosen as the minimal number that guarantees security against generalized differential and linear attacks;

— the number of rounds with a partial S-box layer is chosen as the minimal number that guarantees security against other attacks, called “algebraic” in [5, 7];

— S-BOXes are chosen as power functions in the field that set bijection in this field.

Considering specific features of the hash function application and the need for its compatibility with MNT-4 or MNT-6 triplets [10], we chose the following parameters of the round functions:

— a prime field $F_p$ where $p$ is a prime number that is used in MNT-4, of the length of 753 bits;

— exponent of the function describing the S-BOX was chosen so as from one side, to guarantee the required level of security against attacks, and from the other side, to minimize the number of constraints;

— one round with a full S-box layer contains three S-BOXes, and a round with a partial S-box layer contains one S-BOX.

Such selection of parameters in the case of the prime field with the characteristic bitlength of about 750 bits (MNT-fields, [11]) allows obtaining of the following characteristics of the hash function at the set security level of $\lambda = 128$ bits:

— 4 rounds with a full S-box layer (two rounds at the beginning and two at the end);

— about 60 rounds with a partial S-box layer;

— from 0.28 to 0.48 constraints per bit.

The results obtained show that the Poseidon hash function is secure against non-binary linear and differential attacks. Given the security level, we can choose parameters of this hash that guarantee its cryptographical security. An indisputable advantage of the hash function with such structure is its efficiency in utilization for SNARK-proofs. For completeness of our investigations, it should be noted that very similar results concerning differential and linear attacks on block ciphers with non-binary operations were obtained in [18–20]. But algorithms and transformations, considered in these works, were not SNARK-oriented, like HadesMiMC and Poseidon.

## REFERENCES


1. E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, “Scalable, transparent, and post-quantum secure computational integrity,” IACR Cryptology ePrint Archive (2018). URL: https://eprint.iacr.org/2018/046.pdf.
2. J. Groth, “On the size of pairing-based non-interactive arguments,” in: Proc. Advances in Cryptology — EUROCRYPT 2016 (May 8–12, 2016, Vienna, Austria), Vienna, LNCS, Vol. 9666, 305–326 (2016). https://doi.org/10.1007/978-3-662-49896-5_11.
3. B. Parno, J. Howell, C. Gentry, and M. Raykova, “Pinocchio: Nearly practical verifiable computation,” in: Proc. IEEE Symposium on Security and Privacy (May 19–22, 2013, Berkeley, CA, USA), Berkeley (2013), pp. 238–252. https://doi.org/10.1109/SP.2013.47.
4. D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, Zcash Protocol Specification: Version 2020.1.15 [Overwinter+Sapling+Blossom+Heartwood+Canopy], Tech. Rep., Electric Coin Company (2020). URL: https://github.com/zcash/zips/blob/master/protocol/protocol.pdf.
5. L. Grassi, D. Kales, 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). URL: https://eprint.iacr.org/2019/458.pdf.
6. G. Bertoni, D. Joan, P. Michaël, and V.A. Gilles, Cryptographic Sponge Functions (2011): URL: https://keccak.team/files/CSF-0.1.pdf.
7. L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru, and M. Schofnegger, “On a generalization of substitution-permutation networks: The HADES design strategy,” IACR Cryptology ePrint Archive (2019). URL: https://eprint.iacr.org/2019/1107.pdf.

8. M. A. Abdelraheem, M. Ågren, P. Beelen, and G. Leander, “On the distribution of linear biases: Three instructive examples,” in: Proc. Advances in Cryptology — CRYPTO 2012 (August 19–23, 2012, Santa Barbara, CA, USA), Santa Barbara, LNCS, Vol. 7417, 50–67 (2012). https://doi.org/ 10.1007/978-3-642-32009-5_4.
9. T. Baigneres, J. Stern, and S. Vaudenay, “Linear cryptanalysis of non binary ciphers,” in: Proc. 14th Intern. Workshop, SAC 2007 (August 16-17, 2007, Ottawa, Canada), Ottawa, LNCS, Vol. 4876, 84–211 (2007). https://doi.org/10.1007/978-3-540-77360-3_13.
10. A. Miyaji, M. Nakabayashi, and Sh. Takano, “New explicit conditions of elliptic curve traces for FR-reduction,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E84-A, No. 5, 1234–1243 (2001).URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.20.8113&rep=rep1&type=pdf.
11. “Constructing optimal pairing-friendly curves,” Coinlist [online]. URL: https://coinlist.co/build/coda/ pages/theory.
12. G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, “On the indifferentiability of the sponge construction,” in: Proc. Advances in Cryptology — EUROCRYPT 2008, (April 13-17, 2008, Istanbul, Turkey), Istanbul, LNCS, Vol. 4965, 181–197 (2008). https://doi.org/10.1007/978-3-540-78967-3_11.
13. X. Lai, J. L. Massey, and S. Murphy, “Markov ciphers and differential cryptanalysis,” in: Proc. Advances in Cryptology — EUROCRYPT’91 (April 8–11, 1991, Brighton, UK), Brighton, Vol. 547, 17–38 (1991). https://doi.org/10.1007/3-540-46416-6_2.
14. A. M. Youssef, S. Mister, and S. E. Tavares, “On the design of linear transformations for substitution permutation encryption networks,” Workshop on Selected Areas of Cryptography (SAC’96), Workshop Record (1997), pp. 40–48. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.17.1208&rep=rep1&type=pdf.
15. S. Vaudenay, “On the security of CS-cipher,” in: Proc. 6th Intern. Workshop, FSE’99 (March 24–26, 1999, Rome, Italy), Rome (1999), pp. 260–274. https://doi.org/10.1007/3-540-48519-8_19.
16. K. Nyberg, “Differentially uniform mappings for cryptography,” in: Proc. Advances in Cryptology — EUROCRYPT’93 (May 23–27, 1993, Lofthus, Norway), Lofthus, LNCS, Vol. 765, 55–64 (1994). https://doi.org/10.1007/3-540-48285-7_6.
17. R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press (1994). https://doi.org/10.1017/CBO9781139172769.
18. L. V. Kovalchuk, “Upper-bound estimation of the average probabilities of integer-valued differentials in the composition of key adder, substitution block, and shift operator,” Cybern. Syst. Analysis, Vol. 46, No. 6, 936–944 (2010). https://doi.org/10.1007/s10559-010-9274-2.
19. L. V. Kovalchuk and V. T. Bezditnyi, “Upper bounds for the average probabilities of difference characteristics of block ciphers with alternation of Markov transformations and generalized Markov transformations,” Cybern. Syst. Analysis, Vol. 50, No. 3, 386–393 (2014). https://doi.org/10.1007/s10559-014-9627-3.
20. A. N. Alekseychuk, L. V. Kovalchuk, A. S. Shevtsov, and S. V. Yakovliev, “Cryptographic properties of a new national encryption standard of Ukraine,” Cybern. Syst. Analysis, Vol. 52, No. 3, 351–366 (2016). https://doi.org/10.1007/s10559-016-9835-0.