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

Lorenzo Grassi[1,3](✉), Reinhard Lüftenegger[1](✉), Christian Rechberger[1], Dragos Rotaru[2,4], and Markus Schofnegger[1]

[1] IAIK, Graz University of Technology, Graz, Austria
L.Grassi@science.ru.nl, {reinhard.luftenegger, christian.rechberger,markus.schofnegger}@iaik.tugraz.at
[2] University of Bristol, Bristol, UK
[3] Know-Center, TU Graz, Graz, Austria
[4] imec-Cosic, Department of Electrical Engineering, KU Leuven, Leuven, Belgium
dragos.rotaru@esat.kuleuven.be

Abstract. Keyed and unkeyed cryptographic permutations often iterate simple round functions. Substitution-permutation networks (SPNs) are an approach that is popular since the mid 1990s. One of the new directions in the design of these round functions is to reduce the substitution (S-Box) layer from a full one to a partial one, uniformly distributed over all the rounds. LowMC and Zorro are examples of this approach.

A relevant freedom in the design space is to allow for a highly non-uniform distribution of S-Boxes. However, choosing rounds that are so different from each other is very rarely done, as it makes security analysis and implementation much harder.

We develop the design strategy Hades and an analysis framework for it, which despite this increased complexity allows for security arguments against many classes of attacks, similar to earlier simpler SPNs. The framework builds upon the wide trail design strategy, and it additionally allows for security arguments against algebraic attacks, which are much more of a concern when algebraically simple S-Boxes are used.

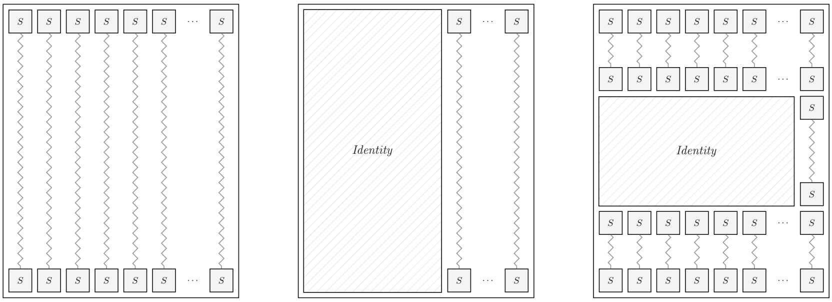
Subsequently, this is put into practice by concrete instances and benchmarks for a use case that generally benefits from a smaller number of S-Boxes and showcases the diversity of design options we support: A candidate cipher natively working with objects in GF(p), for securing data transfers with distributed databases using secure multiparty computation (MPC). Compared to the currently fastest design MiMC, we observe significant improvements in online bandwidth requirements and throughput with a simultaneous reduction of preprocessing effort, while having a comparable online latency.

Keywords: Hades strategy · Cryptographic permutations · Secure Multiparty Computation (MPC)

A. Canteaut and Y. Ishai (Eds.): EUROCRYPT 2020, LNCS 12106, pp. 674–704, 2020.
https://doi.org/10.1007/978-3-030-45724-2_23

1 Introduction

Starting out with a layer of local substitution boxes (S-Boxes), combining it with a global permutation box (sometimes merely wires, sometimes affine transformations), and iterating such a round a number of times is a major design approach in symmetric cryptography. The resulting constructions are often referred to as substitution-permutation networks (SPNs) and are used to instantiate block ciphers, permutations, pseudo-random functions (PRFs), one-way functions, hash functions, and various other constructions. The approach can be traced back to Shannon's confusion-diffusion paradigm. There is a huge amount of efficient designs that exploit this design strategy, including Rijndael/AES [20] which is perhaps the most important one. Theoretical aspects have been analyzed too, which include the asymptotic analysis by Miles and Viola [41], and more recent results in the provable security framework [16,26].



(a) SPN (b) P-SPN (c) Hades

Fig. 1. SP-Networks and Generalizations (P-SPNs and Hades).

Driven by various new application areas and settings, a variation of the SPN approach – the so-called partial substitution-permutation network (P-SPN) – has been proposed and investigated on the practical side [5,27]. The idea is to replace parts of the substitution layer with an identity mapping, leading to substantial practical advantages. A big caveat of this approach is that existing elegant approaches to rule out large classes of attacks via the so-called *wide trail strategy* [19] are no longer applicable and have to be replaced by more ad-hoc approaches, as discussed in more details in Sect. 1.1. We note that the well studied Feistel approach and its generalizations, when the round function is using S-Boxes, also have the property that only a part of the internal state is affected by S-Boxes in a given round.

Our Contribution in a Nutshell: We propose a new generalization of SPNs, which we call the "HADES" approach[1]. This is illustrated in Fig. 1. It *(1st)* restores the ability to apply the elegant wide trail strategy to rule out important classes of attacks, *(2nd)* is accompanied with a broad framework to rule out various other attack vectors for many relevant instantiation possibilities, and *(3rd)* is demonstrated to result in even better implementation characteristics in the same application domains P-SPNs have been introduced for.

We use the rest of the introduction to explain this further. In Sect. 1.1 we explain the difficulty of the security analysis of P-SPNs, in Sect. 1.2 we outline our alternative generalization of SPNs called HADES. A big part of the paper will then be spent on detailing the approach and its framework for the security analysis. On the practical side, in Sect. 1.4 we will discuss how applications which rely on properties like a small number of S-Boxes can benefit from this framework. A very recent and independent work [3] explores various generalized Feistel networks as a method benefiting similar settings. This nicely complements our paper, and we include this approach in our practical comparisons.

1.1 The Big Caveat: Security Analysis of P-SPNs

The wide trail strategy cannot guarantee security against all attacks in the literature. As a concrete example, algebraic attacks that exploit the low degree of the encryption or decryption function – like the interpolation attack [33] or the higher-order differential one [36] – are (almost) independent of the linear layer used in the round transformation[2], which is the crucial point of such a design strategy. In other words, especially in the case of a low-degree S-Box, the wide trail strategy is not sufficient by itself, and it must be combined with something else (e.g., increasing the number of rounds) to guarantee security against all known attacks.

Moreover, the "hidden" assumption of such a strategy is that each round contains a full S-Box layer. Even if this is a well accepted practice, there are various applications/contexts in which non-linear operations are much less expensive than linear ones. For example, this includes masking and practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) that use symmetric primitives.

A possible way to achieve a lower implementation cost is by designing a primitive minimizing the number of non-linear operations. To achieve this goal, possible strategies are looking for low-degree S-Boxes and/or exploiting SPN structures where not all the state goes through the S-Boxes in each round. This second approach has been proposed for the first time by Gérard *et al.* [27] at CHES 2013. Such partial non-linear SP networks – in which the non-linear operation is applied to only part of the state in every round – contain a wide range of possible concrete schemes that were not considered so far, some of which have

[1] Referring to Fig. 1 and 2, if one highlights the S-Boxes per round, the obtained picture resembles a "*bident*". In classical mythology, the bident is a weapon associated with Hades, the ruler of the underworld.

[2] We remark that a linear/affine function does in general not increase/change the degree.

performance advantages on certain platforms. A concrete instantiation of their methodology is Zorro [27], a 128-bit lightweight AES-like cipher which reduces the number of S-Boxes per round from 16 to only 4 (to compensate, the number of rounds has been increased to 24).

A similar approach has then been considered by Albrecht *et al.* [5] in the recent design of a family of block ciphers called LowMC proposed at Eurocrypt 2015. LowMC is a flexible block cipher based on an SPN structure and designed for MPC/FHE/ZK applications. It combines an incomplete S-Box layer with a strong linear layer to reduce the total number of AND gates.

How Risky Are Partial SP Networks? The wide trail strategy and tools that were developed in order to formally prove the security of block ciphers against standard differential and linear cryptanalysis do not apply to partial SP networks such as Zorro, and authors use heuristic arguments instead.

For the case of Zorro, the simple bounds on the number of active S-Boxes in linear and differential characteristics cannot be used due to the modified SubBytes operation. Even though the authors came up with a dedicated approach to show the security of their design, this turned out to be insufficient, as Wang *et al.* [46] found iterative differential and linear characteristics that were missed by the heuristic and used them to break full Zorro. An automated characteristic search tool and dedicated key-recovery algorithms for SP networks with partial non-linear layers have been presented in [8]. In there, the authors propose generic techniques for differential and linear cryptanalysis of SP networks with partial non-linear layers. Besides obtaining practical attacks on P-SPN ciphers, the authors concluded that even if "*the methodology of building PSP networks based on AES in a straightforward way is flawed, [...] the basic PSP network design methodology can potentially be reused in future secure designs*".

Similarly, the authors of LowMC chose the number of rounds in order to guarantee that no differential/linear characteristic can cover the whole cipher with *non-negligible probability.* However, they do not provide such strong security arguments against other attack vectors including algebraic attacks. As a result, the security of earlier versions of LowMC against algebraic attacks was found to be lower than expected [23,25], and full key-recovery attacks on LowMC have been set up. More recently, generalizations of impossible differential attacks have been found for some LowMC instances [43].

1.2 The Idea in a Nutshell – The HADES Strategy

Summarizing the current situation: The wide trail strategy is appealing due to its simplicity, but limited to differential and linear attacks, and does not work with partial S-Box layers. Additionally, when S-Boxes are chosen to have a low degree, other attacks vectors are more relevant anyhow. Designs of this type, like Zorro and LowMC, require a lot of ad-hoc analysis.

To address this issue we propose to start with a classical wide trail design, i.e., with a full S-Box layer (outer layer), and then add a part with full and/or partial S-Box layers in the middle. Even without the middle part, the outer layer in itself is supposed to give arguments against differential and linear attacks in exactly the same way the wide trail strategy does. At the same time, arguments against low-degree attacks can be obtained working on the middle layer. Since algebraic attacks exploit the small degree of the encryption/decryption function, the main role of this middle part is to achieve a high degree, with perhaps only few (e.g., one) S-Boxes per round. Depending on the cost metric of the target application one has in mind (e.g., minimizing the total number of non-linear operations), we show that the best solution is to choose the optimal ratio between the number of rounds with full S-Box layers and with partial S-Box layers in order to achieve both security and performance. We refer to this high-level approach as the "Hades" strategy and will be more concrete in the following.

1.3 Related Work – Designs with Different Round Functions

Almost all designs for block ciphers and permutations, not only those following the wide trail design strategy, use round functions that are very similar, differing often only in so-called round constants which break symmetries in order to prevent attacks like slide attacks. Notable exceptions to this are the AES finalist MARS, the lightweight cipher PRINCE [14] and the cipher *Rescue* [6], recently proposed for ZK-STARK proof system and MPC applications. MARS has whitening rounds with a different structure than the inner rounds with the idea to frustrate cryptanalytic attacks. A downside was perhaps that it also complicated cryptanalysis. PRINCE rounds differ in that the later half of the rounds is essentially the inverse of the first half of the rounds, and a special middle round is introduced. This allows to achieve a special property, namely that a circuit describing PRINCE computes its own inverse (when keyed in a particular way). Similar to PRINCE, each round of *Rescue* is composed of two steps, which are respectively a non-linear S-Box layer and its inverse (that is, $R(\cdot) = M' \circ S^{-1} \circ M \circ S(\cdot)$ for particular affine layers M, M'). Finally, we mention the cases of LowMC [5] and Rasta [24], for which different (independent and random) linear layers are used in each round. Due to their particular design strategies, this allows to maximize the amount of diffusion achieved by the linear layer. In none of these cases, however, the *amount* of non-linearity, and hence their cryptographic strength, differs over the rounds.

1.4 HadesMiMC: Concrete Instantiations for MPC Applications

We briefly outline the use cases in the following and discuss how our new design compares against the best-in-class.

MPC. There is a large application area around secure multi-party computation. The setting is a secret-sharing-based MPC system where data is often shared as elements of a finite field $\mathbb{F}_p$ for large p. In order to get data securely in and out of such a system, an efficient solution can be to directly evaluate a symmetric primitive within such an MPC system. Note that "traditional" PRFs such as AES are not efficient in this setting, since they are built for computational engines which work over data types that do not easily match the operations possible in the MPC engine. For example, AES is a byte-oriented cipher, which is hard to represent using arithmetic in $\mathbb{F}_p$. More details can be found in [32], where for the first time this setting was explicitly analyzed and where the authors concluded that among various other options MiMC [4] was competitive. After these initial works, several new primitives have been proposed for MPC applications, including GMiMC [3] (a generalization of MiMC based on Feistel networks), Jarvis and Friday [7], and *Rescue* and *Vision* [6]. GMiMC was recently broken [13] by exploiting its weak key schedule, and Gröbner basis attacks were found against Jarvis and Friday [2].

Concrete Instances. For our concrete instantiations of HadesMiMC, we borrow ideas from the pre-predecessor of AES, namely SHARK [44], an SPN design with a single large MDS layer covering the whole internal state. Concretely specified instances, both full and toy versions, together with their reference implementation, test vectors, and helper scripts are available online[3].

When benchmarking our new design HadesMiMC for MPC applications, we observe significant improvements in online bandwidth requirements and throughput with a simultaneous reduction of preprocessing effort with respect to MiMC and *Rescue*, while having a comparable online latency. The same holds also for the comparison between HadesMiMC and GMiMC, with the exception for the online throughput when the number of blocks is bigger than or equal to 16.

New Instances for Future Use Cases. HadesMiMC is a very parameterizable design approach: Given any block size and a cost metric that one aims to minimize, a concrete secure instantiation – hence, the best S-Box size and the best ratio between rounds with full S-Box and partial S-Box layers – can be created easily using our scripts. In fact we can already report on such usage: Variants of HadesMiMC have been proposed [29] for use cases of efficient proof systems like STARKs, SNARKs and Bulletproofs, for which they outperform competing designs, often by a large margin.

2 Description of the Hades Strategy

Block ciphers and cryptographic permutations are typically designed by iterating an efficiently implementable round function many times in the hope that the resulting composition behaves like a randomly drawn permutation. In general, the same round function is iterated enough times to make sure that any symmetries and structural properties that might exist in the round function vanish. In our case, instead of considering the same non-linear layer for all rounds, we propose to consider *a variable number of S-Boxes per round*, that is, to use different S-Box layers in the round functions.

Each round of a cipher based on Hades is composed of three steps:

1. *Add Round Key* – denoted by $ARK(\cdot)$;
2. *SubWords* – denoted by S-Box$(\cdot)$;
3. *MixLayer* – denoted by $M(\cdot)$.

[3] https://extgit.iaik.tugraz.at/krypto/hadesmimc.

A final round key addition is then performed, and the final MixLayer operation can be omitted (we sometimes include it in this description for simplicity):

$$\underbrace{ARK \rightarrow \text{ S-Box} \rightarrow M}_{1st\text{ round}} \rightarrow ... \rightarrow \underbrace{ARK \rightarrow \text{ S-Box} \rightarrow M}_{(R-1)\text{-}th\text{ round}} \rightarrow \underbrace{ARK \rightarrow \text{ S-Box}}_{R\text{-}th\text{ round}} \rightarrow ARK$$

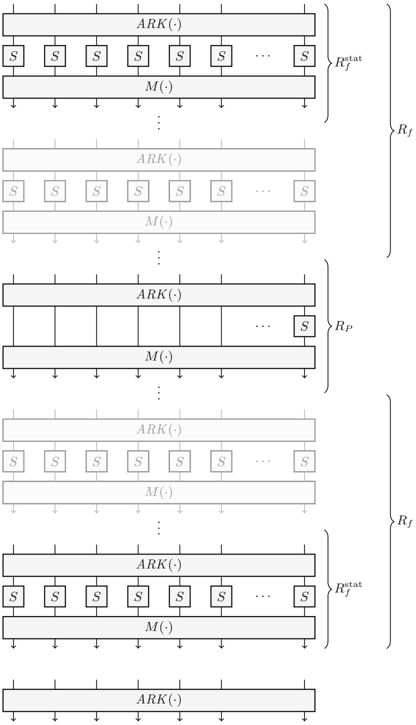


Fig. 2. Construction of Hades (the final matrix multiplication can be omitted).

The crucial property of Hades is that the number of S-Boxes per round is not the same for every round:

- a certain number of rounds – denoted by R_F – has a *full* S-Box layer, i.e., t S-Box functions;
- a certain number of rounds – denoted by R_P – has a *partial* S-Box layer, i.e., $1 \leq s < t$ S-Boxes and $(t - s)$ identity functions.

In the following, we only consider the case $s = 1$, that is, R_P rounds have a single S-Box per round and $t - 1$ identity functions. However, we remark that this construction can be easily generalized (e.g., like LowMC) allowing more than a single S-Box per round in the middle R_P rounds.

In more details, assume $R_F = 2 \cdot R_f$ is an even number. Then

- the first R_f rounds have a full S-Box layer,
- the middle R_P rounds have a partial S-Box layer (i.e., 1 S-Box per round),
- the last R_f rounds have a full S-Box layer.

Note that the rounds with a partial S-Box layer are "masked" by the rounds with a full S-Box layer, which means that an attacker should not (directly) take advantage of the rounds with a partial S-Box layer.

Crucial Points of the Hades Strategy. In the Hades design, R_f^{stat} rounds with full S-Box layers situated at the beginning and the end guarantee security against statistical attacks, yielding a total of $R_F^{\text{stat}} = 2 \cdot R_f^{\text{stat}}$ rounds with full S-Box layers. As we are going to show, they are sufficient in order to apply the wide trail strategy, even without the middle rounds with partial S-Box layers. Moreover, the choice to have the same number of rounds with full non-linear layers at the beginning and at the end aims to provide the same security with respect to chosen-plaintext and chosen-ciphertext attacks.

Security against all algebraic attacks is achieved working both with rounds $R_F = R_F^{\text{stat}} + R'_F \geq R_F^{\text{stat}}$ with full S-Box layers and rounds $R_P \geq 0$ with partial S-Box layers. The degree of the encryption/decryption function has a major impact on the cost of an algebraic attack. Even if one S-Box per round is potentially sufficient to increase this degree, other factors can have a crucial impact on the cost of such attacks too (e.g., a Gröbner basis attack also depends on the number of non-linear equations and variables).

Finally, another crucial point of our Hades strategy regards the possibility to choose among several possible combinations of rounds $(R_F \geq R_F^{\text{stat}}, R_P \geq 0)$ that provide the *same* security level. Namely, one can potentially decrease (resp. increase) the number of rounds with partial S-Box layers and add (resp. remove) $R'_F = 2 \cdot R'_f \geq 0$ rounds with full S-Box layers instead *without affecting the security level.* This freedom allows to choose the best combination of rounds (R_F, R_P) that minimizes a given cost metric. Roughly speaking, the idea is to find a balance between the approach in an SPN and a P-SPN cipher.

Choosing the Field and the Linear/Non-linear Layer. Our strategy does not pose any restriction/constriction on the choice of the field, on the linear layer, or on the choice of the S-Box. The idea is to consider a "traditional" SPN cipher – defined over $(\mathbb{F}_{q^n})^t$ for $q = 2$ or $q = p$ prime – based on the wide trail strategy, and then to replace a certain number of rounds with full S-Box layers with the same number of rounds with partial S-Box layers in order to reduce the number of non-linear operations, but without affecting the security. The Hades strategy has a considerable impact especially in the case of ciphers with low-degree S-Boxes, since in this case a large number of rounds is required to guarantee security against algebraic attacks.

3 The Keyed Permutation HadesMiMC

HadesMiMC is a construction for cryptographic permutations based on the strategy just proposed. It is obtained by applying the Hades strategy to the cipher SHARK [44] proposed by Rijmen *et al.* in 1996 and based on the wide trail strategy. Our design works with texts of $t \geq 2$ words[4] in $(\mathbb{F}_p, +, \times) \equiv (\text{GF}(p), +, \times)$, where p is a prime of size $p \approx 2^n \geq 11$ (namely, the smallest prime bigger than $2^3 = 8$) and where $+$ and $\times$ are resp. the addition and the multiplication in $\mathbb{F}_p$. In the following, N denotes $N := \lceil \log_2 p \rceil \cdot t$.

3.1 Specification of HadesMiMC

Each round $R_k(\cdot) : (\mathbb{F}_p)^t \to (\mathbb{F}_p)^t$ of HadesMiMC is defined as

$$R_k(\cdot) = k + M \times \mathcal{S}(\cdot),$$

where $k \in (\mathbb{F}_p)^t$ is the secret subkey, $M \in (\mathbb{F}_p)^{t \times t}$ is an invertible matrix that defines the linear layer, $\mathcal{S}(\cdot) : (\mathbb{F}_p)^t \to (\mathbb{F}_p)^t$ is the S-Box layer, defined as $\mathcal{S} = [S(\cdot), ..., S(\cdot)]$ for the rounds with full S-Box layers and as $\mathcal{S} = [S(\cdot), I(\cdot), ..., I(\cdot)]$ for the rounds with partial S-Box layers, where $S(\cdot) : \mathbb{F}_p \to \mathbb{F}_p$ is a non-linear S-Box and $I(\cdot)$ is the identity function.

The number of rounds $R = 2 \cdot R_f + R_P$ depends on the choice of the S-Box and of the parameters p and t. For the MPC applications we have in mind, we usually consider a large prime number (namely, $p \geq 2^{64}$, e.g. $p \approx 2^{128}$), and each round is composed of the following operations:

- the non-linear S-Box is defined as the *cube* one, namely S-Box$(x) = x^3$; we recall that x^3 is a permutation[5] in GF(p) if and only if $p \neq 1 \bmod 3$;
- as in SHARK, the MixLayer of HadesMiMC is defined by a multiplication with a fixed $t \times t$ MDS matrix.

Details about the MDS matrix, the key schedule, and the number of rounds are given in the following. Test vectors are provided in [30, App. A].

About the MDS Matrix. A $t \times t$ MDS matrix[6] M with elements in GF(p) exists if the condition $2t + 1 \leq p$ is satisfied (see [39] for details). Since there are several ways to construct an MDS matrix, we recall in [30, App. B] some concrete strategies proposed in the literature. We also provide a script that, given an input p and t, returns an MDS matrix.

Security Level κ and Key Schedule. For our goals, we define two security levels, respectively $\kappa = \log_2(p) \cdot t \approx n \cdot t = N$ and $\kappa = \log_2(p) \approx n$ (note that $n = \lceil \log_2(p) \rceil$ is the field size in bits).

Case: $\kappa = \log_2(p) \cdot t \approx N$. Let $k \in (\mathbb{F}_p)^t$ be the secret key of size $N \approx t \cdot \log_2(p)$ bits, and let $k = [k_0, k_1, ..., k_{t-1}]$ be its representation over $\mathbb{F}_p$ (namely,

[4] The case $t = 1$ corresponds to MiMC [4].

[5] More generally, a power map $x \mapsto x^\alpha$ is a permutation over $\mathbb{F}_p$ if and only if $\gcd(\alpha, p-1) \neq 1$ – see e.g. Hermite's criterion for more details.

[6] A matrix $M \in \mathbb{F}^{t \times t}$ is called a *Maximum Distance Separable* (MDS) matrix iff it has a branch number $\mathcal{B}(M)$ equal to $\mathcal{B}(M) = t + 1$. The branch number is defined as $\mathcal{B}(M) = \min_{x \in \mathbb{F}^t \setminus \{0\}} \{wt(x) + wt(M(x))\}$, where wt is the bundle weight in wide trail terminology. Equally, a matrix M is MDS iff every submatrix of M is non-singular.

$k_j \in \mathbb{F}_p$ for each $0 \leq j < t$). We define the i-th round key $k^{(i)}$ for $0 \leq i \leq R$ (where R is the number of rounds) as follows. For the first round $i = 0$, the subkey is simply given by the whitening key, that is, $k^{(0)} := k$. For the next rounds, the subkeys are defined by a linear key schedule as

$$\forall i = 1, ..., R: \quad k^{(i)} := \hat{M} \cdot k^{(i-1)} + RC^{(i)},$$

where $RC^{(i)} \neq 0$ are random round constants and $\hat{M}$ is an MDS matrix[7]. For the matrix $\hat{M}$ we require that $\hat{M}^i = \prod_{i=1}^{R} \hat{M}$ has no zero coefficient[8], where $1 \leq i \leq R$ and R is the total number of rounds. This condition implies that each word of each subkey $k^{(i)}$ (linearly) depends on all words of k. As a result, even if an attacker guesses a certain number of words of a subkey $k^{(i)}$, she does not have information about other subkeys (more precisely, she cannot deduce any words of other subkeys).

Case: $\kappa = \log_2(p) \approx n$ (for MPC Applications). Let $k' \in \mathbb{F}_p$ be the secret key of size $n \approx \log_2(p)$ bits. We define the subkeys as

$$\forall i = 0, ..., R: \quad k^{(i)} = [\underbrace{k', k', \cdots, k'}_{t \text{ times}}] \oplus RC^{(i)},$$

for random round constants $RC^{(i)}$.

Efficient Implementation and Decryption. Like for LowMC, the amount of operations required in each round with a partial non-linear layer can be reduced. Referring to the idea proposed in [22], in [30, App. C] we recall an equivalent representation of an SPN with partial non-linear layers that can be exploited for an efficient implementation of HadesMiMC.

Finally, we mention that – as for MiMC [4] – decryption is much more expensive than encryption (e.g., $x^{1/3} \equiv x^{(2p-1)/3}$ over $\mathbb{F}_p$). However, we emphasize that HadesMiMC has been proposed for applications where the decryption process (hence, computing the inverse) is not required. We therefore provide benchmark results only for the encryption function. If used for confidentiality, we suggest to use modes where the inverse is not needed (e.g., the counter (CTR) mode).

3.2 Design Considerations: Reviving "Old" Design Ideas

Why SHARK Among Many Others? Since in our practical applications (e.g., the MPC use case which we will mainly consider) the cost of linear operations is much lower than the cost of non-linear ones, we decided to focus on the most efficient linear layer (from the security point of view) to construct HadesMiMC, namely the one that provides the fastest diffusion at word level. This corresponds to a linear layer defined as a multiplication with an MDS matrix that involves the entire state, which is exactly the case for SHARK.

Since our design strategy can be applied to any SPN design, a possible interesting future problem would be to apply Hades to e.g. AES, in order to see if a certain number of rounds of AES can be replaced with rounds that contain partial non-linear layers without decreasing its security.

[7] To be as general as possible, $\hat{M}$ can be equal or different from M.

[8] If this is not possible, one must minimize the number of zero coefficients.

Choosing the S-Box. Before going on, we mention that we also considered possible variants of HADESMiMC instantiated by S-Boxes defined by e.g. a different power exponent. In order to motivate our choice, we remember that, since our final goal is to use HADESMiMC for MPC applications over a LAN, the performance in such application is mainly influenced by the total number of non-linear operations (the AND depth/multiplication depth has a small impact on the cost of an MPC application over a LAN, while it could play a crucial role in the case of a WAN). Since linear operations are basically free, the choice to consider a cube S-Box among many other non-linear permutations is motivated by the following considerations:

- First of all, since there are no quadratic permutation polynomials (namely, $x \mapsto x^2 + a \cdot x + b$ for $a, b \in \mathbb{F}_p$) over the finite field $\mathbb{F}_p$ (see e.g. [38, Theorem 6–7] and [21, Sect. 2] for details), the cube S-Box requires the smallest number of non-linear operations (namely, two) and at the same time it offers high security against statistical attacks (e.g. its maximum differential probability satisfies $DP_{max} \leq 2/|\mathbb{F}|$ where $|\mathbb{F}|$ is the size of the field $\mathbb{F}$);
- Secondly, let us focus on algebraic attacks when using an S-Box of the form S-Box$(x) = x^d$. An S-Box with a higher degree than the cube one allows to reach the maximum degree faster, hence a smaller number of rounds is potentially sufficient to provide security. However, an S-Box with a higher degree requires more operations to be computed. As a result, even if the number of rounds can *potentially* be decreased[9], in general the total number of non-linear operations does not change significantly (see e.g. [4, Sect. 5] for a detailed analysis[10]). Thus, from this point of view, *the choice of the S-Box is in continuity with the choice of the cube S-Box made e.g. for MiMC and for Rescue* [6] *for similar applications.*

4 Security Analysis

It is paramount for a new design to present a concrete security analysis. In the following, we provide an in-depth analysis of the security of the HADESMiMC family of block ciphers. Since we cannot ensure that a cipher is secure against all possible attacks, the best option of determining its security is to ensure that it is secure against all known attacks. We follow this strategy for our proposals and the number of rounds of HADESMiMC is then chosen accordingly.

The crucial points of our security analysis are the following:

[9] *We emphasize that this is not always the case.* For a concrete example, we analyze the security of HADESMiMC instantiated by the inverse S-Box S-Box$(x) = 1/x$ in [30, App. F]. In there, we show that, even though this S-Box has the highest possible degree, the number of rounds needed for security is of the same order as the number of rounds required for the cubic case (see also [33, Sect. 3.4] for more details).

[10] In there, authors showed e.g. that the total number of non-linear operations over $\mathbb{F}_p$ (hence, including the square operations) is constant for each permutation function of the form $x \mapsto x^d$ for $d = 2^{d'} - 1$.

- Security against statistical attacks is obtained exploiting the wide trail strategy by using $R_F^{\text{stat}} = 2 \cdot R_f^{\text{stat}}$ rounds with full S-Box layers.
- The combination of both rounds $R_F = R_F^{\text{stat}} + R'$ with full S-Box layers *and/or* rounds $R_P \geq 0$ with partial S-Box layers provide security against all other possible attacks. Indeed, even if rounds with partial S-Box layers are sufficient to increase the degree of the encryption/decryption function, other factors can also have a crucial impact on the cost of an algebraic attack.

In the following, we present our security analysis for the case $\kappa = N$ (and full data case). Then, we adapt it for the case $\kappa = n$ (together with the restriction $p^{t/2} \approx 2^{N/2}$) used for the MPC applications we have in mind.

4.1 Main Points of Our Cryptanalysis Results

Here we limit ourselves to highlight the main points of our cryptanalysis results – a detailed description of the attacks can be found in the following.

Number of Rounds. In the following, given the number of rounds of a distinguisher which is independent of the key, we add at least 2 rounds *with full S-Box layers* to prevent key-guessing attacks. This choice is motivated by the fact that it is not possible to skip more than a single round with a full S-Box layer without guessing the entire key. Indeed, one round of HadesMiMC already provides full diffusion at word level, while the S-Box provides full diffusion at bit level.

Statistical Attacks. As we are going to show, at least 6 rounds with full S-Box layers are needed to protect HadesMiMC against all statistical attacks in the literature (that is, differential, linear, truncated/impossible differential, boomerang, ...). Depending on p and t, in some cases 10 rounds are necessary in order to guarantee security against these attacks.

Algebraic Attacks. Algebraic attacks exploit mainly the low degree of the encryption/decryption function in order to break the cipher. However, as already mentioned, other factors can influence the cost of such attacks.

Interpolation Attack. The goal of an interpolation attack is to construct the polynomial that describes the function: If the number of monomials is too large, then such a polynomial cannot be constructed faster than via a brute force attack. A (lower/upper) bound of the number of different monomials can be estimated given the degree of the function. We show that – when the polynomial is dense – the attack complexity is approximately $\mathcal{O}(d^t)$, where d is the degree of the polynomial after r rounds. Since $d = 3^r$ for the cubic case, $\log_3(p) + \log_3(t)$ rounds with partial S-Box layers are necessary to guarantee security, where $\log_3(t)$ more rounds guarantee that the polynomial is dense. The cost of the attack does not change when working with rounds with full S-Box layers.

We finally remark that the degree of a function can also depend on its "representation". To give a concrete example, the function x^{-1} can be written as a function of degree $p-2$ (namely, $x^{-1} \equiv x^{p-2}$ for $x \neq 0$) or using the "fraction representation" $1/x$ as introduced in [33], where both the numerator and the denominator are functions of degree at most 1 (see [30, App. F] for more details on the influence of such representation on the interpolation attack).

Gröbner Basis Attack. In a Gröbner basis attack, one tries to solve a system of non-linear equations that describe the cipher. The cost of such an attack depends on the degree of the equations, but also on the number of equations and on the number of variables. We show that – when working with rounds with full S-Box layers – the attack complexity is approximately $\mathcal{O}((d/t)^t)$. If a partial S-Box layer is used in order to guarantee security against this attack, it could become more efficient to consider degree-3 equations for single S-Boxes. In this case, a higher number of rounds may be necessary to provide security.

To summarize, a round with a partial S-Box layer can be described by just 1 non-linear equation of degree d and $t-1$ linear equations, while a round with a full S-Box layer can be described by t non-linear equations of degree d. If the cost of the attack depends on other properties than just the degree (as in the case of a Gröbner basis attack), this fact can influence its final cost.

Higher-Order Differential Attack. The higher-order differential attack exploits the property that given a function $f(\cdot)$ of algebraic degree δ, then $\bigoplus_{x \in V \oplus \phi} f(x) = 0$ if the dimension of the subspace V satisfies $\dim(V) \geq \delta + 1$ (where the algebraic degree δ of a function $f(x) = x^d$ is given by the hamming weight of d, which we denote by hw(d)). If the algebraic degree is sufficiently high, then the attack does not work. In the case in which HadesMiMC is instantiated over $\mathbb{F}_p$, we conjecture that security against the interpolation attack implies security against this attack.

Other Attacks. *Related-Key Attacks.* The related-key attack model is a class of cryptanalytic attacks in which the attacker knows or chooses a relation between several keys and is given access to encryption/decryption functions with all these keys. We explicitly state that we do *not* make claims in the related-key model as we do not consider it to be relevant for the intended use case.

Hades*MiMc Permutation: Security.* Since we do not require the indistinguishability of the permutation obtained by HadesMiMC with a fixed key from a "randomly drawn" permutation[11] in the practical applications considered in the following, we explicitly state that we do *not* make claims about the indistinguishability of the HadesMiMC Permutation.

[11] This basically corresponds to the known-key or chosen-key models, where the attacker can have access or even choose the key(s) used, and where the goal is to find some (plaintext, ciphertext) pairs having a certain property with a complexity lower than what is expected for randomly chosen permutations.

4.2 Statistical Attacks – Security Level: $\kappa = N$

Differential Cryptanalysis. Differential cryptanalysis [11] and its variations are the most widely used techniques to analyze symmetric-key primitives. The differential probability of any function over the finite field $(\mathbb{F}, +, \times)$ is defined as

$$\text{Prob}[\alpha \to \beta] := |\{x : f(x+\alpha) - f(x) = \beta\}|/|\mathbb{F}|$$

where $|\mathbb{F}|$ is the size of the field and where "$-$" denotes the subtraction operation ($x - y = z$ iff $x = z + y$). The probability for the cube function $f(x) = x^3$ is bounded above by $2/|\mathbb{F}_p| = 2/p$, i.e., it has an optimal differential probability over a prime field [42].

As largely done in the literature, we first compute the number of rounds necessary to guarantee that each characteristic has probability at most $p^{-t} \approx 2^{-N}$. Since more characteristics can be used simultaneously in order to set up a differential attack, the previous number of rounds is in general not sufficient to guarantee security. For this reason, we claim that HadesMiMC is secure against differential cryptanalysis if each characteristic has probability smaller than $p^{-2\cdot t} \approx 2^{-2\cdot N}$. We emphasize that *(1st)* this basically corresponds to double the number of rounds necessary to guarantee that each characteristic has probability at most 2^{-N} and *(2nd)* that a similar strategy is largely used in the literature (including e.g. AES).

As we are going to show, the idea is to compute the *minimum number of rounds with full S-Box layers* that guarantee this. In other words, we consider a "weaker" version of the cipher defined as

$$R^{R_f} \circ L \circ R^{R_f}(\cdot), \text{ where} \tag{1}$$

- L is an *invertible linear layer* (which is the "weakest" possible assumption),
- $R(\cdot) = M \circ \text{S-Box} \circ ARK(\cdot)$ where S-Box$(\cdot)$ is a full S-Box layer (remember that M is an MDS matrix).

We show that this "weaker" cipher is secure against differential cryptanalysis for

$$R_F^{\text{stat}} = \begin{cases} 6 & \text{if } p \geq 2^{t+1}, \\ 10 & \text{otherwise.} \end{cases} \tag{2}$$

As a result, it follows that also HadesMiMC (instantiated with R_F rounds with full S-Box layers) is secure against such an attack. Indeed, if the linear layer L (which we only assume to be invertible) is replaced by R_P rounds of HadesMiMC, its security cannot decrease. *The same strategy is exploited in the following in order to prove security against all attacks in this subsection.*

In order to prove the result just given, we need a lower bound on the (minimum) number of active S-Boxes. Observe that the minimum number of active S-Boxes of a cipher of the form

$$R^s \circ L \circ R^r(\cdot) \equiv SB \circ \underbrace{M \circ SB}_{s-1 \text{ times}} \circ \underbrace{L'}_{\equiv L \circ M(\cdot)} \circ SB \circ \underbrace{M \circ SB}_{r-1 \text{ times}}(\cdot),$$

where $s, r \geq 1$, $R(\cdot)$ is a round with a full S-Box layer and where L' is an invertible linear layer, is at least[12]

$$\text{number } \textit{active} \text{ S-Boxes} \geq \left(\lfloor s/2 \rfloor + \lfloor r/2 \rfloor\right) \times (t+1) + \big(s \bmod 2\big) + \big(r \bmod 2\big).$$

We emphasize that the middle linear layer $L'(\cdot) \equiv L \circ M(\cdot)$ plays *no* role in the computation of the previous number (it has branch number equal to 2). By choosing $s = r = 2$, it follows that – since at least $2 \cdot (t+1)$ S-Boxes are active in the weaker cipher $R^2 \circ L \circ R^2(\cdot)$ and since the maximum differential probability of the cube S-Box is $DP_{max} = 2/p$ – each characteristic has probability at most

$$\left(\frac{2}{p}\right)^{2\cdot(t+1)} = \begin{cases} p^{-2t} \cdot \frac{4^{t+1}}{p^2} \leq p^{-2\cdot t} \approx 2^{-2\cdot N} & \textit{if } p \geq 2^{t+1} \\ p^{-1.25\cdot t} \cdot \frac{4^{t+1}}{p^{0.75\cdot t+2}} < p^{-1.25\cdot t} \approx 2^{-1.25\cdot N} & \text{since } p^{0.75} > 6 \end{cases}$$

where remember that $p \geq 11$. By doubling this number of rounds (i.e., by choosing $s = r = 4$), we get that each characteristic has probability at most $p^{-2.5\cdot t} \approx 2^{-2.5\cdot N}$. Finally, 2 more rounds with full S-Box layers guarantee that no differential attack can be set up by key guessing. Indeed, note that *(1st)* given a partial round key, one has no information about the other round keys (due to the key schedule), and *(2nd)* 1 round with a full S-Box layer is sufficient to provide full diffusion. Hence, no more than a single round can be skipped by exploiting a partial guessed key.

Other Attacks. In [30, App. D], we present a (detailed) security analysis against other statistical attacks, including the linear one [40], truncated [36] and impossible differential attacks [10], Meet-in-the-Middle statistical attacks, the integral attack [18], the boomerang attack [45], the multiple-of-8 distinguisher [31], the mixture differential attack [28], and the invariant subspace attack [37]. *In there, we argue that (the "basic" variants of) all these attacks do not outperform the differential attack discussed here.* Finally, a discussion about biclique cryptanalysis [12] is provided.

4.3 Algebraic Attacks – Security Level: $\kappa = N$

Interpolation Attack. One of the most powerful attacks against HadesMiMC is the interpolation attack, introduced by Jakobsen and Knudsen [33] in 1997.

The strategy of the attack is to construct a polynomial corresponding to the encryption function without knowledge of the secret key. Let $E_k : \mathbb{F} \to \mathbb{F}$ be an encryption function. For a randomly fixed key k, the interpolation polynomial $P(\cdot)$ representing $E_k(\cdot)$ can be constructed using e.g. the Vandermonde matrix (cost of $\approx \mathcal{O}(t^2)$) or Lagrange's theorem (cost of $\approx \mathcal{O}(t \cdot \log t)$). If an adversary can construct such an interpolation polynomial without using the full codebook, then she can potentially use it to set up a forgery attack or a key-recovery attack.

[12] If $s = 2 \cdot s'$ is even, then the minimum number of active S-Boxes over $R^s(\cdot)$ rounds with full S-Box layers is $\lfloor s/2 \rfloor \cdot (t+1)$. Instead, if $s = 2 \cdot s' + 1$ is odd, then the minimum number of active S-Boxes over $R^s(\cdot)$ rounds with full S-Box layers is $\lfloor s/2 \rfloor \cdot (t+1) + 1$.

The attack proceeds by simply guessing the key of the final round, decrypting the ciphertexts and constructing the polynomial for $r-1$ rounds[13]. With one extra (plaintext, ciphertext) pair, the attacker checks whether the polynomial is correct. The data cost of the attack is well approximated by the number of texts necessary to construct the interpolation polynomial.

Considering HadesMiMC, since the S-Box is the cube function, the degree of each word after r rounds is roughly approximated by 3^r. In particular, since in each round at least one S-Box is applied and since the affine layer does not change the degree, the degree of one round is three as well. It follows that, if the degree of each word after $r \geq 1$ rounds is 3^r, then the degree of each word after $r+1$ rounds is well approximated by 3^{r+1} even if only one S-Box per round (together with a linear layer that provides "sufficiently good" diffusion at word level, in our case the multiplication with an MDS matrix) is applied. For this reason, in the following we consider a *weaker cipher* in which each round contains only a single S-Box. If such a cipher is secure against the interpolation attack, then our design is also secure (more S-Boxes per round do not decrease the security). Finally, we recall that since at least 3 rounds with a full S-Box layer are applied at the beginning and at the end, our design prevents the possibility to skip a certain number of rounds by a proper choice of the input texts (e.g., by having no active S-Box), as happens for the case of partial SPN ciphers. For this reason, we do not take care of this last event.

Note that not all terms of (total) degree 3^r appear *before* the $(r+1)$-th round[14]. Thus, assuming the interpolation polynomial of degree 3^{r-1} is *not sparse* in the r-th round, a (rough) estimation for the number of monomials of the interpolation polynomial (and so of the attack complexity) is given by

$$(3^{r-1}+1)^t \geq 3^{(r-1)\cdot t},$$

since after r rounds there are t words each of degree *at least* 3^{r-1}. By requiring that the number of monomials is equal to the full codebook ($3^{(r-1)\cdot t} \simeq p^t$, that is, $3^{r-1} \simeq p$), the number of rounds must be at least $r \simeq 1 + \log_3(p)$. However, this estimation for the number of rounds does not guarantee that the interpolation polynomial is dense. For this reason, since the cipher works over a finite field with characteristic p and due to the specific algebraic structure of the cube function, we add $\lceil \log_3(t) \rceil$ more rounds in order to guarantee that the interpolation polynomial is not sparse – see [30, App. E] for details.

A MitM variant of the interpolation attack can also be performed. To thwart this variant and due to the high degree of $\text{S-Box}^{-1}(x) = x^{1/3} = x^{(2p-1)/3}$, it is sufficient to add 2 rounds. Finally, 2 more rounds are added to prevent key-

[13] The "hidden" assumption is that the cost to construct such a polynomial is smaller than the cost of an encryption. If this assumption does not hold, then the cost of the attack is bigger than the cost of a brute-force attack.

[14] E.g., after the first round not all words of degree 3 appear. Indeed, the input of each S-Box in the first round is composed of a single word, which means that after the first round there is no *non-linear* mixing of different words. Similarly, not all terms of (total) degree 3^r appear *before* the $(r+1)$-th round.

guessing attacks. As a result, the total number of rounds R must satisfy[15]

$$R = R_P + R_F \geq R^{\text{inter}}(N, t) \equiv 5 + \lceil \log_3(p) \rceil + \lceil \log_3(t) \rceil \tag{3}$$

to thwart the interpolation attack.

Gröbner Basis and GCD Attacks. In the Greatest Common Divisors (GCD) attack [4], given more than one known (plaintext, ciphertext) pair or working on the output of each S-Box of a single (known) pair, one constructs their polynomial representations and computes their polynomial GCD to recover a multiple of the key. We refer to [30, App. E] for all details about the GCD attack.

The natural generalization of GCDs is the notion of Gröbner bases [17]. The attack proceeds like the GCD attack with the final GCD computation replaced by a Gröbner basis computation. As our design exhibits a strong algebraic structure, it is paramount to carefully analyze its resistance against Gröbner basis attacks. For example, it has been shown recently that this attack vector has been able to break two proposed primitives which do not seem to be vulnerable to other types of classical algebraic attacks [2].

A Gröbner basis attack consists of the following steps:

1. computing the Gröbner basis in *degrevlex* order;
2. converting the Gröbner basis into *lex* order;
3. factorizing the univariate polynomial, and back-substituting its roots.

As largely done in the literature, we assume that *the security of ciphers against Gröbner basis attacks follows from the infeasible complexity of computing the Gröbner basis in degrevlex order.* For generic systems, the complexity of this step (hence, a lower bound for the complexity of computing a Gröbner basis) for a system of n_e polynomials f_i in n_v variables is $\mathcal{O}\left(\binom{n_v+D_{\text{reg}}}{D_{\text{reg}}}^{\omega}\right)$ operations over the base field $\mathbb{F}$ [17], where D_{reg} is the *degree of regularity* and $2 \leq \omega < 3$ is the linear algebra constant (the memory requirement of these algorithms is of the same order as the running time). The degree of regularity depends on the degrees of the polynomials d and the number of polynomials n_e.

In the following, we provide three different strategies to attack our design using Gröbner bases. We give a brief overview here, while we provide more details in [30, App. E].

First Strategy. The first strategy consists in using t variables $k_0, ..., k_{t-1}$ and t equations for each (plaintext, ciphertext) pair. When being provided at most $p^t - 1$ (plaintext, ciphertext) pairs, the system of equations that describes the cipher is composed of at most $n_e = t \cdot (p^t - 1)$ equations of the form $\hat{c}_i = f_i(\hat{p}_0, ..., \hat{p}_{t-1}, k_0, ..., k_{t-1})$ in $n_v = t$ variables $k_0, ..., k_{t-1}$ (remember that the key schedule is linear). In this over-determined case ($n_e > n_v$), there is no closed-form expression to compute D_{reg}, which is defined as the index of the first non-positive coefficient in

$$H(z) = \frac{\prod_{i=1}^{n_e}(1 - z^{d_i})}{(1 - z)^{n_v}} = \frac{(1 - z^{3^r})^{n_e}}{(1 - z)^{n_v}} = (1 - z^{3^r})^{n_e - n_v} \cdot (1 + z + z^2)^{n_v},$$

[15] We emphasize that *in this analysis we do not take into account the cost to construct the interpolation polynomial, which is (in general) non-negligible.*

where $d_i = 3^r$ is the degree of the i-th equation. By simple observation, the index of the first non-positive coefficient cannot be smaller than $d = 3^r$, since $(1+z+z^2)^{n_v}$ contains only positive terms.

Depending on parameter choices, the hybrid approach [9], which combines exhaustive search with Gröbner basis computations, may lead to a reduced cost. Following [9], guessing $\kappa < t$ parts of the key leads to a complexity of

$$\mathcal{O}\left(p^{\kappa} \cdot \binom{t-\kappa+D'_{\text{reg}}}{D'_{\text{reg}}}^{\omega}\right), \tag{4}$$

where $D'_{\text{reg}} \leq D_{\text{reg}}$ is the degree of regularity for the system of equations after substituting κ variables with their guesses. It follows that to prevent Gröbner basis attacks, the minimum number of rounds r must satisfy $p^{\kappa} \cdot \binom{t-\kappa+D'_{\text{reg}}}{D'_{\text{reg}}}^{\omega} \geq p^t$ for all $0 \leq \kappa \leq t-1$, and where the degree of regularity $D'_{\text{reg}} = \mathcal{O}(d) \approx 3^r$. In our cases, the expression (4) is minimized by $\kappa = 0$, which implies that

$$\binom{t+d}{d} = \frac{1}{t!} \cdot \prod_{i=1}^{t}(d+i) \geq \frac{d^t}{t!} \geq \left(\frac{d}{t}\right)^t = 2^{t\log_2(d/t)},$$

where $x! \leq x^x$ for $x \geq 1$. Setting $\omega = 2$, we obtain $2t\log_2(d/t) \approx \log_2(p) \cdot t$ and

$$r \geq 2 + \log_3(p)/2 + \log_3(t), \tag{5}$$

where 2 rounds are added to thwart the MitM version of the attack (note that the degree of the S-Box in the decryption direction is $(2p-1)/3$). As a result, $R \geq \lceil \log_3(p)/2 + \log_3(t) \rceil + 2$ rounds are sufficient to protect the cipher from this attack. Note that the analysis just proposed is independent of the fact whether the rounds contain a full or a partial S-Box layer.

Second Strategy. While we use only t variables in the first strategy, the second strategy is to add intermediate variables in each round. Specifically for the rounds with a partial S-Box layer, it is sufficient to add only one intermediate variable. In total, we get a system with more variables and equations compared to the first strategy, but with much lower degrees. We describe this strategy in detail in [30, App. E], where we conclude that R_F and R_P have to fulfill

$$R_F \cdot t + R_P \geq \left\lceil \frac{N}{2 \cdot (\log_2(27) - 2)} \right\rceil + \left\lceil \frac{N}{2 \cdot (\log_2(2p-1) - \log_2(3))} \right\rceil$$

in order for our design to be secure against this type of attack.

Third Strategy. The third strategy is merely a combination of the previous two strategies. We use $2t$ variables for the R_F rounds with full S-box layers (i.e., we do not add intermediate variables in these rounds), but we apply the idea from the second strategy during the R_P rounds with partial S-box layers (i.e., we add intermediate variables in these rounds). This approach gives us a system of $2t$ equations of degree 3^{R_f} and R_P equations of degree 3 in $2t + R_P$ variables (t variables for the key and $t + R_P$ intermediate variables). Since the number of variables is the same as the number of equations, we can estimate D_{reg} and conclude that our design is secure if[16]

$$R_F \geq 2 + \log_3(2) \cdot \left(\frac{N}{2t + R_P} + 2 \cdot \log_2(t + R_P) - 2 \cdot \log_2(t) \right),$$

is fulfilled (see [30, App. E] for more details).

Conclusion. We claim that if R_F and R_P satisfy

$$\begin{cases} R_P + R_F \geq R^{\text{1st-Grob}}(N,t) \equiv 2 + \left\lceil \log_3(p)/2 + \log_3(t) \right\rceil \\ R_F \cdot t + R_P \geq R^{\text{2nd-Grob}}(N,t) \equiv \left\lceil N/[2 \cdot \log_2(27/4)] \right\rceil + \left\lceil N/[2 \cdot \log_2((2p-1)/3)] \right\rceil \\ R_F \geq R^{\text{3rd-Grob}}(N,t,R_P) \equiv 2 + \log_3(2) \cdot \left(\frac{N}{2t+R_P} + 2 \cdot \log_2(t + R_P) - 2 \cdot \log_2(t) \right) \end{cases} \tag{6}$$

for $N \approx t \cdot \log_2(p)$, then HadesMiMC can be considered secure against the Gröbner basis attacks proposed here. We mention that if R_F satisfies $R_F \geq R^{\text{1st-Grob}}(N,t) \equiv 2 + \left\lceil \log_3(p)/2 + \log_3(t) \right\rceil$ (namely, rounds with full S-Box layers are sufficient to provide security w.r.t. the first strategy), then the second and the third condition are also satisfied.

Higher-Order Differential Attack. A well-known result from the theory of Boolean functions is that if the algebraic degree of a vectorial Boolean function $f(\cdot)$ (like a permutation) is d, then the sum over the outputs of the function applied to all elements of an affine vector space $\mathcal{V} \oplus c$ of dimension $\geq d + 1$ for an arbitrary constant c is zero, that is, $\sum_{v \in \mathcal{V} \oplus c} v = \sum_{v \in \mathcal{V} \oplus c} f(v) = 0$.

This property is exploited by higher-order differential attacks [36]. However, it only holds if $\mathcal{V}$ is a subspace, and not just a generic set of elements. While $\mathbb{F}_{2^m}$ is always a subspace of $\mathbb{F}_{2^n}$ for each $m \leq n$, the only subspaces of $\mathbb{F}_p$ are $\{0\}$ and $\mathbb{F}_p$. It follows that the biggest subspace of $(\mathbb{F}_p)^t$ has dimension t, in contrast to the biggest subspace of $(\mathbb{F}_{2^n})^t$, which has dimension $n \cdot t = N$. As a result, in the case in which a cipher is instantiated over $\mathbb{F}_p$, a lower degree (and hence a smaller number of rounds) is sufficient to protect it against the higher-order differential attack w.r.t. the number of rounds needed for the $\mathbb{F}_{2^n}$ case.

Security Analysis: Hades*MiMc Instantiated Over* $\mathbb{F}_p$. Due to the discussion just given (namely, the fact that the biggest (non-trivial) subspace of $(\mathbb{F}_p)^t$ has dimension at most $t - 1$), we conjecture that the number of rounds necessary to achieve maximum degree guarantees security against higher-order differential attacks over $\mathbb{F}_p$. In other words, we conjecture that if HadesMiMC over $\mathbb{F}_p$ is secure against the interpolation attack, then it is also secure against the higher-order differential attack[17].

[16] A "more precise" condition can be found in [30, App. E].

[17] We emphasize that this does not hold in general. In particular, working over $\mathbb{F}_2^N$, note that a scheme is secure against the interpolation attack if the corresponding polynomial is full/dense. However, for security against higher-order differential attacks, we want a maximum algebraic degree. These two things are in general not strictly related.

5 Security Analysis for MPC: $\kappa = n$ and Data $\leq p^{1/2}$

In this section, we will adjust our security arguments in order to provide a security level of only $\log_2(p) \approx n$ bits (instead of the previous $\log_2(p^t) \approx N$ bits). At the same time, we only allow an attacker to use $p^{1/2}$ data.

5.1 Statistical Attacks

Differential Attack. As before, we assume that the cipher is secure if every characteristic has probability smaller than p^{-2} (namely, smaller than the square of the data complexity equal to $\sqrt{p}$). Working with the weaker cipher $R^{R_f} \circ L \circ R^{R_f}(\cdot)$ defined as in (1), it follows that $R_f = 2$ rounds with full S-Box layers are sufficient, since each characteristic has a probability of at most

$$\left(\frac{2}{p}\right)^{2(t+1)} = \frac{1}{p^{1.25 \cdot t}} \cdot \frac{4^{t+1}}{(p^{0.75})^{t+1.25}} < p^{-2.5},$$

since $p^{1/2} \geq 11^{1/2} \approx 3.3$. However, since a total number of $R_F = 2$ full rounds would not lead to 2 consecutive full rounds in our design (recall that we use partial rounds in the middle), we add two other rounds to have at least 2 consecutive rounds both at the beginning and at the end. Finally, we add two more rounds to prevent differential attacks with key guessing and conclude that $R_F \geq R_F^{\text{stat}} = 6$ rounds are needed in this setting.

Other Attacks. The situation in this setting does not differ from the situation analyzed in Sect. 4.2 (namely, other statistical attacks do not outperform the differential attack just discussed). Therefore, we argue that $R_F = 6$ rounds also prevent (the "basic" variant of) all other statistical attacks in the literature.

5.2 Algebraic Attacks

Interpolation Attack. The approach in this setting follows the analysis given in Sect. 4.3. By choosing plaintexts with *just one active word*, the interpolation polynomial depends on a single variable (namely, the active word). Hence, the number of monomials after r rounds is approximated by $3^r + 1$. Since the data complexity is limited to $\sqrt{p}$, here we require that $3^r + 1 \geq \sqrt{p} \implies r \geq 0.5 \cdot \log_3(p)$. We finally add $\log_3(t) + 4$ rounds due to the reasons given in Sect. 4.3 and conclude that

$$R_F + R_P \geq R^{\text{inter}}(p,t) \equiv 4 + \left\lceil \frac{\log_3(p)}{2} \right\rceil + \lceil \log_3(t) \rceil \tag{7}$$

rounds are needed to prevent the interpolation attack.

GCD and Gröbner Basis Attack. As further explained in [30, App. E], the GCD attack for a key from $(\mathbb{F}_p)^t$ works by first guessing $t-1$ components of the key in order to have a univariate polynomial in the last component. Since we are using only one key component in this setting, we do not need to guess these components. With other words, the encryption path alone already yields a univariate polynomial. Since the cost of the GCD computation is approximated by $\mathcal{O}\left(d \log_2^2 d\right)$, we target a complexity of $d \log_2^2 d \approx p$, where d is well approximated by 3^{r-1} when using a cubic S-Box, and thus require that

$$R_F + R_P \geq R^{\text{GCD}}(p,t) \equiv 4 + \lceil \log_3(p) \rceil - \lfloor 2 \log_3(\log_2(p)) \rfloor . \tag{8}$$

Finally, since computing the Gröbner Basis of a univariate system of equations is equivalent to computing the greatest common divisor (GCD) [15], we expect that this attack does not outperform the GCD one just discussed (we refer to [30, App. E] for more details).

6 Number of Rounds: Security and Efficiency

The design goal of HadesMiMC is to offer a cipher optimized for schemes whose performance critically depends on the MULTdepth/ANDdepth, the number of MULTs/ANDs, or the number of MULTs/ANDs per bit. We thus try to be as close to the number of rounds needed for security as possible.

Security. HadesMiMC with a security level equal to $\kappa = N$ is secure iff

$$\begin{cases} R_F \geq \max\left\{R_F^{\text{stat}}; R^{\text{3rd-Grob}}(p,t,R_P)\right\}, \\ R_P + R_F \geq \Psi^{(1)}(p,t) \equiv \max\left\{R^{\text{inter}}(p,t); R^{\text{1st-Grob}}(p,t); R^{\text{GCD}}(p,t)\right\} = R^{\text{inter}}(p,t), \\ R_P + t \cdot R_F \geq \Psi^{(t)}(p,t) \equiv R^{\text{2nd-Grob}}(p,t), \end{cases}$$

where $R^{\text{inter}}(p,t)$ and $R^{\text{1st-Grob}}(p,t)$, $R^{\text{2nd-Grob}}(p,t)$, $R^{\text{3rd-Grob}}(p,t,R_P)$ are resp. defined in (3) and (6) for the case $\kappa = N$. The analogous case $\kappa = n$ (used for the MPC applications that we have in mind) is discussed in the following.

Several Combinations of $(\mathbf{R_F}, \mathbf{R_P})$ for the *Same* Security Level. Besides the possibility to choose the size of the S-Box, we emphasize that *one of the strengths of our design is the freedom to choose the ratio between the number of rounds R_F with full S-Box layers and the number of rounds R_P with partial S-Box layers without affecting the security level.* In other words, the crucial point here is that for each given p and t, the designer has in general the freedom to choose among several combinations of rounds (R_F, R_P) – that guarantee the same security – in order to minimize the analyzed cost metric.

In the following, we show how to choose the best combination of (R_F, R_P) in order to minimize a given cost metric (for the same security level). We provide *a script*[18] *that, given an input p, returns the best t and the best ratio between R_P and R_F for several cost metrics* – as the total number of non-linear operations, the depth, etc., *for both $\kappa = N$ and $\kappa = n$.*

[18] We mention that we propose also a variant of such script that takes p and t as input, and that returns the best choice of R_F and R_P that minimizes the given cost metric.

6.1 Efficiency in the Case of MPC Applications

Consider a generic scenario in which the main goal is to minimize the total number of non-linear operations (namely, the number of S-Boxes in our case) and/or the depth and/or the total number of linear operations proportional respectively to some parameters $0 \leq \varphi, \psi, \rho \leq 1$ s.t. $\varphi + \psi + \rho = 1$. Among all possible combinations of rounds (R_F, R_P) that provides the same security level, the goal is to find the one that minimizes the metric given by

$$\frac{\varphi}{\varphi+\psi+\rho} \times \#\ \textit{S-Boxes} + \frac{\psi}{\varphi+\psi+\rho} \times \textit{depth} + \frac{\rho}{\varphi+\psi+\rho} \times \#\ \textit{Linear Op.} =$$
$$= \frac{\varphi \times (t \cdot R_F + R_P) + \psi \times (R_F + R_P) + \rho \times (t^2 \cdot R_F + (3t-2) \cdot R_P)}{\varphi+\psi+\rho}$$

where the equality holds *only* for the HadesMiMC design (a precise estimation of the number of linear operations in the case of an efficient implementation of HadesMiMC is provided in [30, App. C]).

Cost Metric for MPC: "Number of S-Boxes" and Depth. Due to the MPC applications we have in mind, we limit ourselves to optimize HadesMiMC w.r.t. the metric that takes into account both the number of multiplications/S-Boxes and the depth. Motivated by real-life applications, the goal that we face is to reduce the total runtime (described in details in the following). Since the main bottleneck of a protocol run on top of the SPDZ framework is the triple generation mechanism, which is given by the number of non-linear operations, in such a case the goal would be to minimize the total number of S-Boxes, while the depth plays a minor role (and where the cost of a single linear operation is negligible compared to the cost of a single non-linear operation). Due to this consideration, here we focus only on the case $0 \leq \rho \ll \varphi$. For the simplified case $\rho = 0$, the previous metric can be simplified as follows:

$$\begin{aligned} &\alpha \times \textit{ number of S-Boxes } + (1-\alpha) \times \textit{depth } = \\ &= \alpha \times (t \cdot R_F + R_P) + (1-\alpha) \times (R_F + R_P) = R_F \times [1 + \alpha \cdot (t-1)] + R_P \end{aligned} \tag{9}$$

for different values of a parameter α, where $0 \leq \alpha \leq 1$. Note that $\alpha = 1$ and $\alpha = 0$ correspond to the cases in which one aims to minimize the total number of S-Boxes and the depth, respectively.

6.2 Best Ratio Between $\mathbf{R_F}$ and $\mathbf{R_P}$ – MPC Application

We focus on HadesMiMC with a security level of $\kappa = n$ (and the data complexity allowed for the attack is less than $p^{1/2}$), namely the case suitable for the MPC applications we have in mind.

Security. Due to the analysis provided in the previous section, HadesMiMC is secure if the following inequalities are satisfied:

$$\begin{cases} R_F \geq R_F^{\text{stat}} \qquad \text{and} \qquad R_P \geq 0; \\ R_P + R_F \geq \Psi(p,t) \equiv \max\{R^{\text{GCD}}(p,t); R^{\text{inter}}(p,t)\} \end{cases}$$

where $R^{\text{GCD}}(p, t)$ and $R^{\text{inter}}(p, t)$ are defined resp. in (8) and in (7).

Efficiency – Best Combination ($\mathbf{R_F}, \mathbf{R_P}$). The goal is to find the best combination of rounds $R_F = R_F^{\text{stat}} + R'_F \geq R_F^{\text{stat}}$ and R_P that minimizes the cost for different values of α, assuming $\Psi(p, t)$ is fixed (equivalently, both p and t are fixed). As we are going to show, in the case in which a single inequality of the form $R_P + R_F \geq \Psi(p, t)$ must be satisfied, for each α the cost metric (9) is always *minimized by choosing the smallest possible* R_F (namely, $R_F = R_F^{\text{stat}}$).

By combining the equation $R_P + R_F \geq \Psi(p, t)$ with the cost metric for generic α, we get that the cost is upper bounded by

$$R_F \times [1 + \alpha \cdot (t - 1)] + R_P \bigg|_{R_P + R_F \geq \Psi} \geq R_F \times \alpha \times (t - 1) + \Psi,$$

which is minimized by the following choice:

- if $\alpha \neq 0$, then the cost is minimized by taking the *minimum* value of R_F (where note that Ψ is fixed for t and N fixed), that is $R_F = R_F^{\text{stat}}$;
- if $\alpha = 0$, then the cost is equal for each choice of (R_F, R_P) s.t. $R_P + R_F = \Psi$.

Let us analyze the case in which $\alpha = 0$ in more details. Even if every choice of R_F and R_P lead to the same cost w.r.t. the metric $R_F + R_P$ (namely, the depth), one possibility would be to choose the combination that minimizes other metrics. By taking into account the number of non-linear and linear operations, it turns out that the best choice is to take the *minimum* value of R_F, since

$$\#\ \text{S-Boxes:} \quad t \times R_F + R_P \bigg|_{R_P + R_F \geq \Psi} \geq R_F \times (t - 1) + \Psi$$

$$\#\ \text{Linear Op.:} \quad t^2 \times R_F + (3t - 2) \times R_P \bigg|_{R_P + R_F \geq \Psi} \geq R_F \times (\underbrace{t^2 - 3t + 2}_{\geq 0 \text{ for each } t \geq 2}) + \Psi$$

are both minimized by taking the minimum $R_F \geq R_F^{\text{stat}}$.

6.3 Concrete Instantiations of HadesMiMC

Based on the security analysis just proposed, in Table 1 we present concrete instantiations of HadesMiMC for different security levels and/or applications. The corresponding test vectors of HadesMiMC are given in [30, App. A].

Reduced and Toy Versions. Many classes of cryptanalytic attacks become more difficult with an increased number of rounds. In order to facilitate third-party cryptanalysis and estimate the security margin, reduced-round variants need to be considered. Hence we encourage to study reduced-round variants of HadesMiMC where the symmetry around the middle is kept. For this reason, we highlight that it is also possible to specify toy versions of our cipher which aim at achieving, e.g., only 32 bits of security.

Table 1. *A range of different parameter sets for* HadesMiMC*offering different trade-offs.* The first set is for AES-like security (≈128 bits). The second set is for MPC applications (where the ratio between R_F and R_P is chosen in order to minimize the metric cost for given values of α). The last set includes an example of a toy version useful to facilitate third-party cryptanalysis.

Text size	**Security**	**S-Box size**	**# S-Box**	α	**Rounds $\mathbf{R_F}$**	**Rounds $\mathbf{R_P}$**
$\log_2 p \times t$	κ	$(\log_2 p)$	(t)		(Full S-Box)	(Partial S-Box)
128	128	8	16	–	10	4
128	128	16	8	–	8	10
256	128	128	2	$0, 0.25, 0.5, 0.75, 1$	6	71
256	256	128	2	$0, 0.25, 0.5, 0.75, 1$	12	76
512	128	128	4	$0, 0.25, 0.5, 0.75, 1$	6	71
512	512	128	4	$0, 0.25, 0.5, 0.75, 1$	12	76
1 024	128	128	8	$0, 0.25, 0.5, 0.75, 1$	6	71
1 024	1 024	128	8	$0, 0.25$	16	72
1 024	1 024	128	8	$0.5, 0.75, 1$	14	79
2 048	128	128	16	$0, 0.25, 0.5, 0.75, 1$	6	71
2 048	2 048	128	16	$0, 0.25, 0.5$	20	69
2 048	2 048	128	16	$0.75, 1$	18	93
4 096	128	128	32	$0, 0.25, 0.5, 0.75, 1$	6	71
4 096	4 096	128	32	0	24	66
4 096	4 096	128	32	$0.25, 0.5$	22	83
4 096	4 096	128	32	$0.75, 1$	20	121
8 192	128	128	64	$0, 0.25, 0.5, 0.75, 1$	6	71
8 192	8 192	128	64	0	32	58
8 192	8 192	128	64	$0.25, 0.5$	22	151
8 192	8 192	128	64	$0.75, 1$	20	240
32	32	8	4	–	6	7

About the case in which the security level κ is equal to the size of the S-Box (namely, $\kappa = \log_2 p$): the given number of rounds provided security only if the data used for the attack is smaller than $p^{1/2}$ – no restriction for the case $\kappa = \log_2 p \cdot t \approx N$.

Comparison with Ciphers in "Traditional Use Cases". We remark that our strategy is ***not*** primarily intended to be used for pure encryption/decryption purposes, and that it is specifically tailored towards new applications like the MPC use case explained previously.

However, if only encryption/decryption is needed, we still expect HadesMiMC to not be significantly worse than more suitable constructions when considering the number of S-Boxes. E.g, when choosing the first instance given in Table 1 (namely, $p \approx 2^8$ and $t = 16$) and comparing it to AES-128, we can observe that the total number of S-Boxes is $10 \cdot (16 + 4) = 200$ in AES-128 (including the key schedule), and only $10 \cdot 16 + 4 = 164$ in our design. At the same time, we point out that the linear layer of HadesMiMC compared to the one of AES is likely to be a bottleneck when trying to reduce the number of operations.

7 MPC Applications

For MPC applications, we evaluated the HadesMiMC cipher using the SPDZ framework [35] within a prime field $\mathbb{F}_p$ following the reasoning of [32].

Preliminaries. In the following, we denote by $[x]$ a sharing of x, where each party P_i holds a random $x_i \in \mathbb{F}_p$. The process of parties reconstructing x is called an opening, i.e., going from a shared value $[x]$ to a public value x known to all parties. As with modern MPC frameworks, a protocol is split into two steps: an input-independent preprocessing phase where parties generate random Beaver triples $[a] = [b] \cdot [c]$, and an input-dependent online phase where parties share their inputs and use the triples generated in the preprocessing phase. The cost of a multiplication between two secret values $[z] \leftarrow [x] \cdot [y]$ is twofold: one Beaver triple generated in the preprocessing phase as well as two openings and one round of communications in the online phase. Since secretly shared multiplications can be done in parallel, the number of communication rounds in the online phase is given by the multiplicative depth of the circuit (AND depth) to be evaluated. Linear operations such as additions and multiplications by public scalars are non-interactive and require only a small computational overhead.

To evaluate a blockcipher in our setting, both the key $[k]$ and the message $[m]$ are secretly shared between the parties. Since most of the computation is linear and is computed locally by the parties the last thing to show is how to compute the S-Box. The trivial way is to perform $[x^2] \leftarrow [x] \cdot [x]$ and then $[x^3] \leftarrow [x^2] \cdot [x]$ using two triples. This can be done with two communication rounds and it has an online cost of 3 openings and uses two triples. However, we use the Grassi *et al.* version [32] to reduce the online cost to one communication round with the same amount of openings and triples. Note that every multiplication translates into two field elements broadcasted by each party (256 bits for $p \approx 2^{128}$).

Standard Benchmarks. We implemented and benchmarked HadesMiMC with a security level of $\kappa = 128 \approx \log_2 p$ bits using the SPDZ protocol in the MP-SPDZ library[19] between two computers equipped with i7-7700K CPUs, 32GB RAM, and connected via a 10Gb/s LAN connection with an average round-trip time of 0.47 ms. The choice of MP-SPDZ was due to having the fastest triple generation mechanism for a dishonest majority [34] and because it integrates the preprocessing with the online phase to check the end-to-end runtime of a protocol.

In Table 2, we present a comparison between HadesMiMC and other existing PRFs/block-ciphers proposed in the literature for MPC applications – namely, MiMC and GMiMC$_{\mathsf{erf}}$ (both with a security level of $\kappa = 128$ bits) and *Rescue* (with a security level of $\kappa = t \cdot 128$ bits) – in terms of four metrics:

1. *latency* represents the best running time of a single cipher evaluation by running sequential single-threaded executions of it;

[19] https://github.com/data61/MP-SPDZ.

2. *throughput* represents 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;
3. *communication* done by each party per encrypted field element;
4. *round complexity* which is the multiplicative depth of the circuit when computed in MPC.

Moreover, we show the difference in throughput and communication between the online phase (columns denoted by 'Online') and when running the entire end-to-end protocols (Runtime).

Experiment Results: Table 2. Our design is better in all metrics for $t = 2$ compared to all other blockciphers (except round complexity when looking at MiMC in CTR mode), and also enjoys the smallest online latency for all t's.

In terms of online throughput it is surpassed by $\text{GMiMC}_{\text{erf}}$ from $t \geq 16$ due to the local computation involving MDS matrices. In more details, from $t \geq 16$ $\text{GMiMC}_{\text{erf}}$ has the best online throughput due to a low number of openings in the online phase and a low computational overhead as it is just swapping and adding states.

When looking at the Runtime column, we see that HADESMiMC outperforms all the existing work from $t = 2$ and the gap increases by a factor of four for $t = 64$ when comparing with $\text{GMiMC}_{\text{erf}}$. Note that for the runtime column one has to choose carefully the number of encryptions done in parallel. This is because for different t's MP-SPDZ produces triples in a batch of size 524288 and some of them might be unused. We tried to diminish this gap by tweaking the number of encryptions to be produced when benchmarking such that it utilizes a maximum number of triples from the last batch.

Remarks About $\text{GMiMC}_{\text{erf}}$ *and Rescue.* In order to understand the previous results, we emphasize two facts. First, all versions of $\text{GMiMC}_{\text{erf}}$ with $n \approx \log_2 p$ bits of security are vulnerable to an attack presented in [13]. Specifically, in [3] the authors propose a number of rounds for $n \approx \log_2 p$ bits of security, assuming the attacker has access to the full codebook (up to $p^t \approx 2^N$ different texts). Secondly, in order to have a more precise comparison, in [30, App. G] we adapt their analysis in the case in which the attacker has access to at most $p^{1/2}$ different chosen texts. This attack – which is reminiscent of a slide attack – makes *only* use of the weak key schedule and does not exploit any particular properties of the cipher. Hence, while the versions of $\text{GMiMC}_{\text{erf}}$ used here are broken in theory, we conjecture that a stronger key schedule can help to avoid this attack. Therefore, since in MPC applications round keys are precomputed (the cost of MPC applications is not influenced by the key schedule), we decided to keep the corresponding numbers in the table, noting that a secure variant of $\text{GMiMC}_{\text{erf}}$ using an appropriate key schedule would yield the same results.

We highlight that *Rescue* is specified with a security level of $p^t \approx 2^N$ bits only, besides a conservative security margin of 100%. Due to the particular design of *Rescue* (each round contains a non-linear layer and its inverse), this choice has been made due to the fact that "*[...] the field of algebraic attacks seems rather*

Table 2. Two-party costs for *Rescue*, MiMC$_t$ (namely, t parallel MiMC-128/128 in CTR mode), GMiMC$_{\mathsf{erf}}$ and HMiMC≡HadesMiMC over a 10Gb/s LAN. Communication is given in KiloBytes. Runtime column represents the entire protocol execution, including preprocessing.

Cipher	Text size	Online				Runtime (multi-thread)	
	$\log_2 p \times t$	(MPC) Rounds	Lat. (ms) (s-thr)	$\mathbb{F}_p$/s (m-thr)	Comm. per $\mathbb{F}_p$	$\mathbb{F}_p$/s	Comm. per $\mathbb{F}_p$
Rescue	256	98	5.54	23 464	6.10	70	971
MiMC$_2$	256	73	3.53	79 728	3.50	192	366
GMiMC$_{\mathsf{erf}}$	256	146	7.50	71 661	3.50	137	487
HMiMC	256	78	3.85	117 358	1.90	261	266
Rescue	512	50	1.25	46 890	3.08	136	485
MiMC$_4$	512	73	1.69	83 876	3.50	192	366
GMiMC$_{\mathsf{erf}}$	512	150	3.42	137 058	1.80	274	243
HMiMC	512	78	1.90	185 160	1.14	526	133.2
Rescue	1024	32	0.59	72 689	1.93	137	484
MiMC$_8$	1024	73	1.08	85 795	3.50	192	366
GMiMC$_{\mathsf{erf}}$	1024	158	1.98	252 102	0.94	271	241
HMiMC	1024	78	0.98	253 475	0.71	1045	66.8
Rescue	2048	32	0.45	66 830	1.93	273	243
MiMC$_{16}$	2048	73	0.63	87 318	3.50	192	366
GMiMC$_{\mathsf{erf}}$	2048	174	1.09	425 717	0.52	137	483
HMiMC	2048	78	0.5	283 678	0.50	1088	60.9
Rescue	4096	32	0.42	57 695	1.93	274	243
MiMC$_{32}$	4096	73	0.34	87 831	3.5	192	366
GMiMC$_{\mathsf{erf}}$	4096	206	0.68	637 747	0.3	276	241
HMiMC	4096	78	0.32	258 610	0.39	1098	60.8
Rescue	8192	32	0.31	44 697	1.93	283	243
MiMC$_{64}$	8192	73	0.20	87 773	3.50	192	366
GMiMC$_{\mathsf{erf}}$	8192	323	0.50	664 091	0.24	550	120
HMiMC	8192	78	0.11	189 772	0.32	2189	30.6

underexplored. As a result, it is difficult to make a compelling security argument valid for the entire family of attacks" (see [6, Sect. 3.5]). Hence, we mention that it is potentially possible that the gap (in term of performance) between *Rescue* and HadesMiMC can be actually reduced in the case in which the "*design choices* [of *Rescue* are] *indeed too conservative, and that the complexity and security margins can safely be reduced*" (see [6, Sect. 4.6]).

Related Work. At CCS'18, Agrawal *et al.* [1] applied a threshold PRF to compute an encryption between several parties where one party P_{ext} holds a plaintext m, does a 2-round protocol with multiple servers, and P_{ext} receives an encryption $E_k(m)$ where the key k is shared among the servers. This use case is covered by us as well by having the servers computing the blockcipher in MPC with P_{ext} as an external party providing the input m and getting the output $E_k(m)$. In the two-server case where one external party gets the ciphertext, Agrawal *et al.* obtain a latency of 0.05 ms and a throughput of around 2 million encrypted blocks. HadesMiMC with $t = 2$ blocks can achieve an online latency of 3.85 ms and an online throughput of more than 117 000 blocks per second.

Although this design performs orders of magnitude slower than Agrawal et al.'s, we provide more flexibility: *(1st)* P_{ext} does not have to be online with the other servers as in Agrawal *et al.* to compute the encryption; *(2nd)* it is more friendly towards working with encrypted databases: servers upload the ciphertext to a DB and anyone holding k can decrypt, whereas for Agrawal *et al.* each party (P_{ext} or else) needs to be online with the servers to decrypt.

Acknowledgements. The authors thank the anonymous reviewers for their valuable comments and suggestions. L. Grassi has been supported by IOV42. D. Rotaru has been supported in part by the Defense Advanced Research Projects Agency (DARPA) and Space and Naval Warfare Systems Center, Pacific (SSC Pacific) under contract No. N66001-15-C-4070, by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA) via Contract No. 2019-1902070006 and by the CyberSecurity Research Flanders with reference number VR20192203. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the ODNI, United States Air Force, IARPA, DARPA, the US Government or FWO. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

References

1. Agrawal, S., Mohassel, P., Mukherjee, P., Rindal, P.: DiSE: distributed symmetric-key encryption. In: CCS, pp. 1993–2010. ACM (2018)
2. Albrecht, M.R., et al.: Algebraic cryptanalysis of STARK-friendly designs: application to MARVELlous and MiMC. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11923, pp. 371–397. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34618-8_13
3. Albrecht, M.R., et al.: Feistel structures for MPC, and more. In: Sako, K., Schneider, S., Ryan, P.Y.A. (eds.) ESORICS 2019. LNCS, vol. 11736, pp. 151–171. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-29962-0_8
4. Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: efficient encryption and cryptographic hashing with minimal multiplicative complexity. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 191–219. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_7
5. Albrecht, M.R., Rechberger, C., Schneider, T., Tiessen, T., Zohner, M.: Ciphers for MPC and FHE. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 430–454. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_17
6. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. Cryptology ePrint Archive, Report 2019/426 (2019). https://eprint.iacr.org/2019/426

7. Ashur, T., Dhooghe, S.: MARVELlous: a STARK-Friendly Family of Cryptographic Primitives. Cryptology ePrint Archive, Report 2018/1098 (2018)
8. Bar-On, A., Dinur, I., Dunkelman, O., Lallemand, V., Keller, N., Tsaban, B.: Cryptanalysis of SP networks with partial non-linear layers. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 315–342. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_13
9. Bettale, L., Faugère, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. J. Math. Cryptol. **3**(3), 177–197 (2009)
10. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_2
11. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
12. Bogdanov, A., Khovratovich, D., Rechberger, C.: Biclique cryptanalysis of the full AES. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 344–371. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_19
13. Bonnetain, X.: Collisions on Feistel-MiMC and univariate GMiMC. Cryptology ePrint Archive, Report 2019/951 (2019). https://eprint.iacr.org/2019/951
14. Borghoff, J., et al.: PRINCE – a low-latency block cipher for pervasive computing applications. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_14
15. Buchberger, B.: Bruno Buchberger's PhD thesis 1965: an algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symb. Comput. **41**, 475–511 (2006)
16. Cogliati, B., et al.: Provable security of (tweakable) block ciphers based on substitution-permutation networks. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 722–753. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_24
17. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra. UTM. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16721-3
18. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher Square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052343
19. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45325-3_20
20. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer, Heidelberg (2002). https://doi.org/10.1007/978-3-662-04722-4
21. Diaz-Vargas, J., Rubio-Barrios, C.J., Sozaya-Chan, J.A., Tapia-Recillas, H.: Self-invertible permutation polynomials over $\mathbb{Z}_m$. Int. J. Algebra **5**(23), 1135–1153 (2011)
22. Dinur, I., Kales, D., Promitzer, A., Ramacher, S., Rechberger, C.: Linear equivalence of block ciphers with partial non-linear layers: application to LowMC. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019. LNCS, vol. 11476, pp. 343–372. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17653-2_12

23. Dinur, I., Liu, Y., Meier, W., Wang, Q.: Optimized interpolation attacks on LowMC. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 535–560. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48800-3_22
24. Dobraunig, C., et al.: Rasta: a cipher with low ANDdepth and Few ANDs per bit. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 662–692. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_22
25. Dobraunig, C., Eichlseder, M., Mendel, F.: Higher-order cryptanalysis of LowMC. In: Kwon, S., Yun, A. (eds.) ICISC 2015. LNCS, vol. 9558, pp. 87–101. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-30840-1_6
26. Dodis, Y., Stam, M., Steinberger, J.P., Liu, T.: Indifferentiability of confusion-diffusion networks. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 679–704. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_24
27. Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.-X.: Block ciphers that are easier to mask: how far can we go? In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 383–399. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40349-1_22
28. Grassi, L.: Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. IACR Trans. Symmetric Cryptol. **2018**(2), 133–160 (2018)
29. Grassi, L., Kales, D., Khovratovich, D., Roy, A., Rechberger, C., Schofnegger, M.: Starkad and Poseidon: New Hash Functions for Zero Knowledge Proof Systems. Cryptology ePrint Archive, Report 2019/458 (2019)
30. Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D., Schofnegger, M.: On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. Cryptology ePrint Archive, Report 2019/1107 (2019)
31. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 289–317. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_10
32. Grassi, L., Rechberger, C., Rotaru, D., Scholl, P., Smart, N.P.: MPC-friendly symmetric key primitives. In: CCS, pp. 430–443. ACM (2016)
33. Jakobsen, T., Knudsen, L.R.: The interpolation attack on block ciphers. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 28–40. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052332
34. Keller, M., Pastro, V., Rotaru, D.: Overdrive: making SPDZ great again. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10822, pp. 158–189. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78372-7_6
35. Keller, M., Scholl, P., Smart, N.P.: An architecture for practical actively secure MPC with dishonest majority. In: CCS, pp. 549–560. ACM (2013)
36. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-60590-8_16
37. Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E.: A cryptanalysis of PRINTcipher: the invariant subspace attack. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 206–221. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_12
38. Li, S.: Permutation Polynomials modulo m. arXiv Mathematics e-prints (2005)
39. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1978)

40. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_33
41. Miles, E., Viola, E.: Substitution-permutation networks, pseudorandom functions, and natural proofs. J. ACM **62**(6), 46:1–46:29 (2015)
42. Nyberg, K., Knudsen, L.R.: Provable security against differential cryptanalysis. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 566–574. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-48071-4_41
43. Rechberger, C., Soleimany, H., Tiessen, T.: Cryptanalysis of low-data instances of full LowMCv2. IACR Trans. Symmetric Cryptol. **2018**(3), 163–181 (2018)
44. Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., De Win, E.D.: The cipher SHARK. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 99–111. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_47
45. Wagner, D.: The Boomerang attack. In: Knudsen, L. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48519-8_12
46. Wang, Y., Wu, W., Guo, Z., Yu, X.: Differential cryptanalysis and linear distinguisher of full-round zorro. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) ACNS 2014. LNCS, vol. 8479, pp. 308–323. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07536-5_19