Towards Better Integral Distinguishers over $\mathbb{F}_p$ Based on Exact Coefficients of Monomials

Muzhou Li[1,2,3], Jiamin Cui[1,2,3], Longzheng Cui[1,2,3], Kai Hu[1,2,3], Chao Niu[4], and Meiqin Wang[1,2,✉]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, China
[2] State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao, China
[3] Quan Cheng Shandong Laboratory, Jinan, China
[4] Ant Group, Beijing, China
muzhouli@mail.sdu.edu.cn, cuijiamin@sdu.edu.cn, 202321179@mail.sdu.edu.cn, kai.hu@sdu.edu.cn, niuchao.niu@antgroup.com, mqwang@sdu.edu.cn

Abstract. Symmetric primitives used in multi-party computation, fully homomorphic encryption, and zero-knowledge proofs are often defined over Finite Field $\mathbb{F}_q$ with $q = 2^t$ or an odd prime p. Integral attack is one of the most effective methods against such primitives due to the common use of low-degree non-linear layers. This in turn highlights the importance of a deeper understanding of degree growth. For ciphers defined over $\mathbb{F}_{2^t}$, numerous works have explored the growth of the algebraic degree. However, these methods cannot be directly applied to $\mathbb{F}_p$. At CRYPTO 2020, Beyne *et al.* extended the integral cryptanalysis to $\mathbb{F}_p$ by comparing degree with $s(p-1)$ when using p^s data. However, given that the precise degree evaluation remains fundamentally challenging and often computationally infeasible, one may lose better integral distinguishers.

In this paper, we present the first automatic search model over $\mathbb{F}_p$ based on the exact coefficient $\mathcal{A}$ of the monomial $\prod_{w=1}^{s} x_w^{p-1}$ contained in the algebraic representation. This model is constructed following the Computation-Traceback-Determine framework, where $\mathcal{A}$ is represented by several sums of multinomial coefficients under specific conditions. The existence of integral properties is then transformed into a determination of whether these sums can consistently equal 0 mod p. This determination is facilitated by four newly developed propositions based on Lucas Theorem. To demonstrate the effectiveness of our framework, we apply it to all variants of GMiMC. As a result, we achieve the best integral distinguishers for GMiMC-erf/-crf using large primes when they are used as block ciphers. For GMiMC-nyb/-mrf using 32/64-bit primes, our integral distinguishers cover more rounds than all other attacks. Meanwhile, all distinguishers we identified are no worse than those trivial ones predicted only considering the maximal degree. This shows the necessity of considering exact coefficients when searching for integral distinguishers over $\mathbb{F}_p$. Our framework is further employed to assess the security of two HADES designs: HadesMiMC and Poseidon2$^\pi$. The results reveal that the full rounds at the beginning and end of HADES provide sufficient resistance against integral cryptanalysis.

Keywords: Prime Field · Integral Attacks · GMiMC · Lucas Theorem

1 Introduction

With increasing deployment of advanced protocols like multi-party computation (MPC), fully homomorphic encryption (FHE) and zero-knowledge proofs (ZKP), new symmetric primitives are required to enhance performance in this setting. Unlike traditional ones such as AES [13] and SHA-3 [29], these new symmetric primitives, referred to as *arithmetization-oriented* (AO) ciphers, are usually defined over Finite Field $\mathbb{F}_q$ where $q = 2^t$ or is a prime $p > 2$. Such ciphers can benefit from a natural algebraic description in these protocols. To further optimize performance, the main goal of AO ciphers is to minimize the number of multiplications. Examples include MiMC [3], GMiMC [2], HadesMiMC [19], Poseidon [16], Poseidon2 [17], *Vision/Rescue* [4], NEPTUNE [20], and Pluto [15].

Statistical attacks such as differential [6] and linear [27] cryptanalysis seem to not threaten the security level. However, algebraic attacks are usually the most powerful ones, which can even lead to the complete break of the cipher. At ASIACRYPT 2019, Albrecht *et al.* presented an algebraic attack on full-round Jarvis based on a simple algebraic representation [1]. Eichlseder *et al.* noticed that the algebraic degree grows linearly instead of exponentially with the number of rounds for MiMC-like schemes and proposed a full-round key-recovery attack on MiMC [14]. It seems to show that some of the designs are not mature enough and the algebraic property of AO ciphers still needs in-depth evaluation.

Related works. Integral attack [12, 24] is one of the most powerful cryptanalytic methods that exploit algebraic properties of symmetric primitives. Given a (keyed) function over $\mathbb{F}_2^n$, for each subspace $V \subseteq \mathbb{F}_2^n$, we have $\sum_{x \in V} F(x) = 0$ when $\deg(F) < \dim(\mathrm{V})$. After a productive line of research [22,23,31,32,34], the integral property is related to evaluating whether the polynomial representation contains some monomials of special form. For the binary extension field $\mathbb{F}_{2^t}$, [14] proposed a more refined degree evaluation method for MiMC-like schemes based on the link between $\mathbb{F}_{2^t}$ and $\mathbb{F}_2$. This underlying idea is the foundation of many follow-up works [8,11,25,26]. To better exploit the algebraic structure, novel dedicated methods have been recently proposed, including general monomial prediction technique [11], coefficient grouping [25, 26], and inner product masked integral [33]. The goal is to predict which monomials do not appear in the polynomial representation. Combined with automatic search tools, these methods can trace the evaluation of the exponents of monomials more accurately.

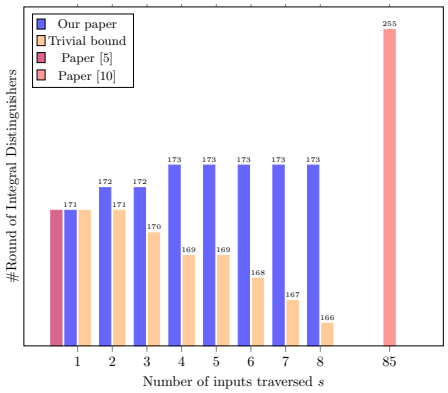
For $\mathbb{F}_p$, a major breakthrough was made at CRYPTO 2020 [5] where the integral attack was extended to Finite Fields of any characteristics. In [10], the authors established the links among impossible differential, zero-correlation linear and integral cryptanalysis over $\mathbb{F}_p$ and improved different types of distinguisher for GMiMC. To the best of knowledge, there are no other general methods for $\mathbb{F}_p$. However, current methods did not exploit the information of the algebraic representation, hence, one may lose better distinguishers in this case. Consider

a Hades-like construction defined over $\mathbb{F}_p$. The middle layer of such construction consists of partial S-Box rounds, *i.e.*, only a single S-Box is applied to the internal state, while the outer layer is a full S-Box layer. If only the maximal degree is considered, all of them will cover the same number of rounds once the data complexity is fixed, no matter how many middle rounds are included. That is counter-intuitive since the algebraic representation becomes simpler when the number of middle rounds increases.

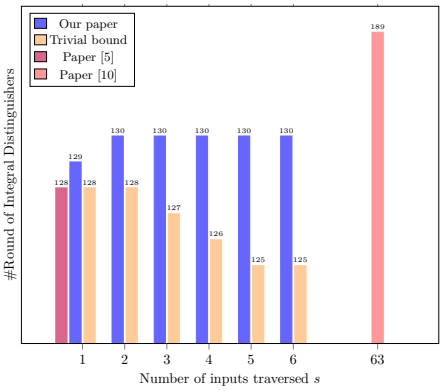
Contributions. Motivated by this fact, we aim to provide a more comprehensive analysis of the polynomial representation over $\mathbb{F}_p$. Notice that when analyzing ciphers over $\mathbb{F}_{2^t}$, previous works are not interested in the details of the coefficient of the monomial that appears due to the efficiency problem. However, things is different for $\mathbb{F}_p$. Considering a polynomial $(ax+b)^v$, all the x^u appears for $u \leq v$ if we do not take the effect of the coefficient into account. The resulting polynomial is thus dense and we can not get useful information from the algebraic representation. In this paper, we propose a novel framework to evaluate the integral property for $\mathbb{F}_p$ by considering the exact coefficient of monomials. Based on the framework, for the very first time, we construct the automatic search tool for the integral distinguisher over $\mathbb{F}_p$. The problem of searching for monomials then can be reduced to a satisfiability problem and solved with off-the-shelf solvers effectively. With the automatic search tool, our framework can take a step further on discovering integral property over $\mathbb{F}_p$ than [5]. Detailed contributions of this paper are summarized as follows:

New framework to find zero-sum integral properties over $\mathbb{F}_p$. Different with the criterion given in [5], we first show in Sect. 3.1 that existence of integral distinguishers over $\mathbb{F}_p$ is only determined by whether the monomial $\prod_{w=1}^{s} x_w^{p-1}$ is contained in its algebraic representation. Based on this, we introduce a three-step framework named as Computation-Traceback-Determine in Sect. 3.2. Following the first two steps, we can represent the exact coefficient $\mathcal{A}$ of $\prod_{w=1}^{s} x_w^{p-1}$ with several sums $\mathcal{S}$ of multinomial coefficients under specific conditions. In this way, existence of integral distinguishers is equivalent to whether these $\mathcal{S}$ can always be $0 \bmod p$. In the last step, we show how to construct a condition set BQ that ensure all $\mathcal{S} \equiv 0 \pmod{p}$ if there is no solution fulfilling all conditions in BQ. In Sect. 3.3, we give some propositions based on Lucas Theorem that are frequently utilized when building BQ. To verify the validity of automatic search model constructed following the new framework, we take GMiMC-erf with small primes as an example in Sect. 3.4. Experiment results show that our model can successfully detect all integral properties under these small primes.

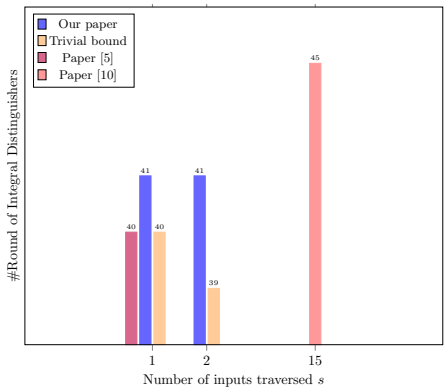
Applications on GMiMC. With the new framework, we have constructed the search model for GMiMC-erf in Sect. 3.2. As explained in Sect. 4.1, this model can also be used for GMiMC-crf after applying a linear transformation to its inputs. Our new found distinguishers for GMiMC-erf/-crf used as block ciphers are depicted in Figure 1, along with those found by [5, 10]. For variants



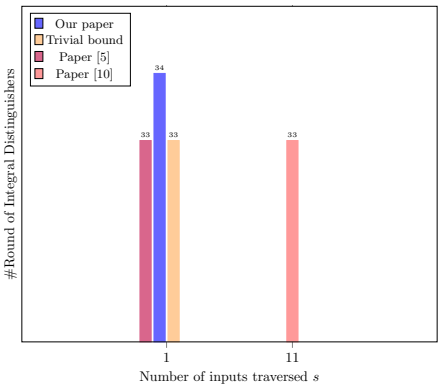
(a) $p = 7, n = 86$



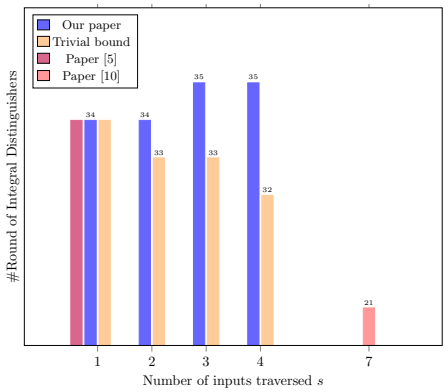
(b) $p = 17, n = 64$



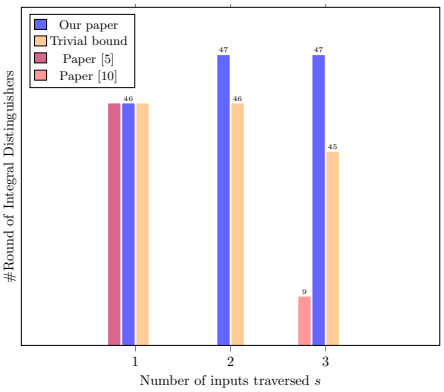
(c) $p = 65519, n = 16$



(d) $p = 531383, n = 12$



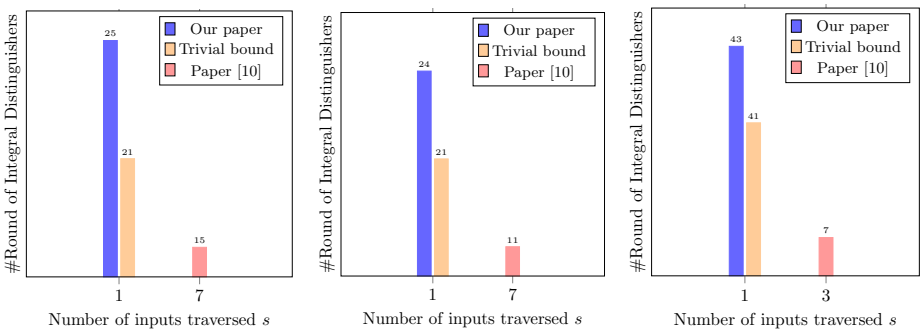
(e) $p = 2^{32} - 5, n = 8$



(f) $p = 2^{64} - 2^{32} + 1, n = 4$

Fig. 1: New found integral distinguishers for block cipher GMiMC-erf/-crf and comparison with previous works. Trivial bound is evaluated as $(n - s) + \lfloor \log_d(s(p-1) - 1) \rfloor + (n - 1)$.

defined over small primes, [10] achieves the best integral distinguishers, benefiting from a large number of branches, but at the cost of extremely high data and time complexities. But for variants over large prime fields, our method provides superior integral distinguishers compared to both prior works. In Sect. 4.2, we show how to construct the search model for GMiMC-nyb and GMiMC-mrf. Our new found distinguishers for these two variants with 32-/64-bit primes are shown in Figure 2, which are the best ones among all kinds of attacks. For all variants of GMiMC, we also compared our results with distinguishers predicted based on trivial bounds, which are significantly weaker than ours. This confirms that considering the exact coefficient of monomials indeed help to discover better distinguishers. Moreover, our model can detect distinguishers with different s, thereby narrows the gap between the methods proposed in [5] and [10]. All the source codes are available in `https://anonymous.4open.science/r/Integral_over_Fp-7300`.



(a) nyb, $p = 2^{32} - 5, n = 8$ (b) mrf, $p = 2^{32} - 5, n = 8$ (c) nyb/mrf, $p = 2^{64} - 2^{32} + 1, n = 4$

Fig. 2: New found integral distinguishers for GMiMC-nyb/-mrf and comparisons. Trivial bound here is $1 + \lfloor \log_d(p-2) \rfloor$.

Outline. In Section 2, we recall prior works on integral cryptanalysis over $\mathbb{F}_p$. Section 3 introduces the proposed framework, using GMiMC-erf as a case study. We then present newly detected integral distinguishers and extend the framework to three other GMiMC variants in Section 4. Additionally, Section 5 discusses the application of this framework to the HADES design. We conclude this paper in Section 6.

2 Previous Integral Cryptanalysis over Finite Field $\mathbb{F}_p$

Integral attack is one of the most powerful cryptanalytic methods on symmetric primitives [12,24]. It is a chosen-plaintext attack proposed for ciphers over binary

field. A structure of plaintexts is chosen and encrypted for a few rounds. If the corresponding state has *zero-sum* property, an integral distinguisher is obtained.

In [5], Beyne *et al.* extended the integral cryptanalysis to $\mathbb{F}_p$, where p can be any prime. Meanwhile, they show that, by checking the maximal degree of all possible monomials, one can determine whether an integral distinguisher with *zero-sum* property exists over $\mathbb{F}_p$. The basic conclusion behind this technique is shown in Proposition 1.

Proposition 1. *([5, Corollary 1]) Let F be the function defined over Finite Field $\mathbb{F}_p$ with n input variables $x_1, x_2, \cdots, x_n \in \mathbb{F}_p$. Let $\deg(F)$ denote the degree of F, defined the maximum degree among all monomials appearing in F. If $\deg(F) < s(p-1)$, and $V \subseteq \mathbb{F}_p^n$ is any affine subspace of dimension of at least s, we have*

$$\sum_{(x_1,x_2,\cdots,x_n)\in V} F(x_1, x_2, \cdots, x_n) \equiv 0 \pmod{p}.$$

To use this criterion, one must first obtain $\deg(F)$. However, the exact value is extremely hard to compute as deriving the complete polynomial representation of F is prohibitively complex. Meanwhile, unlike integral cryptanalysis over the binary field or binary extension field, methods to obtain a more precise value of $\deg(F)$ are still lacking.

Using Fermat's Little Theorem, we know that to check whether the upper bound of the algebraic degree is less than $s(p-1)$, it is sufficient to verify whether there exists a monomial of degree $s(p-1)$. When there is no monomial of degree $s(p-1)$, the existence of a zero-sum integral distinguisher is guaranteed. To the best of our knowledge, the only known approach over $\mathbb{F}_p$ is to simply iterate the highest degree for each round. However, when the degree is greater than $s(p-1)$, actually we do not know whether the monomial with degree $s(p-1)$ exists or not. Moreover, if the coefficients of the monomial with degree $s(p-1)$ is a multiple of p, in fact this monomial does not exist.

Example 1. Let F be the function with input $x \in \mathbb{F}_p$, and $F(x) = x^p + G(x)$, where $\deg(G) < p-1$ and $p \geq 3$. If we consider only the maximal degree of F, we would conclude that since it is greater than $1 \cdot (p-1)$, F does not have the zero-sum property. However, by Fermat's Little Theorem, $F(x) \equiv x + G(x) \bmod p$. Thus, according to Proposition 1, F does indeed have the zero-sum property.

Example 2. Let F be the function with input $x \in \mathbb{F}_p$, and $F(x) = c_1 x^{p-1} + G(x)$, where $\deg(G) < p-1$. If we do not know the concrete value of c_1, we would conclude that $\deg(F) = p-1$. Actually, it is common when analyzing block ciphers as the polynomial representation is usually too complicated to be computed or stored in practice. In this case, the sum under all possible x is not $0 \bmod p$ due to Proposition 1 since $\deg(F) \geq 1 \cdot (p-1)$. However, if we can obtain the exact value of c_1 and find that $c_1 \equiv 0 \bmod p$, we have

$$\sum_{x\in\mathbb{F}_p} F(x) \equiv \sum_{x\in\mathbb{F}_p} \left(c_1 x^{p-1} + G(x)\right) \bmod p \equiv \sum_{x\in\mathbb{F}_p} G(x) \bmod p \equiv 0.$$

This indicates that, in order to use Proposition 1 properly, it is significant to check whether the coefficients of monomials with degree $s(p-1)$ is 0 mod p.

In [10], Chen *et al.* introduced another way to find integral distinguishers over $\mathbb{F}_p$. Their method relies on the links among integral, zero-correlation linear and impossible differential distinguishers. With this link, one can indeed find better integral distinguishers in some cases. However, the effectiveness of this method depends highly on the structure of target cipher. For example, when they apply this method on GMiMC [2], only for variants with larger branches n and smaller p, better integral distinguishers can be found. Besides, in order to obtain distinguishers covering more rounds, zero-correlation linear distinguisher are often constructed by activating only one input and output masks. Thus, data complexity of the derived integral distinguisher will be p^{n-1}, which is relatively high.

3 New Method to Find Integral Distinguishers over $\mathbb{F}_p$

Currently, almost all works on detecting integral distinguishers defined over $\mathbb{F}_p$ are based on the criteria proposed by Beyne *et al.* [5]. In order to identify improved integral distinguishers, it is essential to obtain a more accurate upper bound on the degree of the target cipher. Otherwise, one may lose better distinguishers, as stated in Sect. 2. In Sect. 3.1, we prove that existence of integral distinguishers is only determined by that of a specific monomial. Based on this, we can construct an automatic search model to detect integral property in Sect. 3.2 by taking GMiMC-erf as an example with the help of STP[5].

3.1 Main Idea behind Our Method

Denote the input of the target cipher by $(x_1, x_2, \cdots, x_n)$, where $x_i \in \mathbb{F}_p$, $1 \leq i \leq n$. We take all possible values for s $(1 \leq s < n)$ inputs while keeping others fixed, and try to check whether the zero-sum integral property holds for one of these n outputs. Without loss of generality, we traverse $(x_1, x_2, \cdots, x_s)$. Let $\vec{u} = (u_1, u_2, \cdots, u_s)$. In this way, each output can be represented as

$$G(x_1, x_2, \cdots, x_s) = \sum_{\vec{u}} \mathcal{C}_{\vec{u}} \prod_{w=1}^{s} x_w^{u_w},$$

where $\mathcal{C}_{\vec{u}}$ are composed of multinomial coefficients and some unknown key variables. Denote $\mathcal{D}(u_w)$ as

$$\mathcal{D}(u_w) = \begin{cases} p-1, \text{ if } u_w \geq p-1 \text{ and } p-1 \mid u_w; \\ u_w \bmod (p-1), \text{ otherwise.} \end{cases}$$

Using Fermat's Little Theorem, we give the following proposition.

[5] https://stp.github.io/

Proposition 2. *If the monomial* $\prod_{w=1}^{s} x_w^{p-1}$ *does not appear in* $G \bmod p$*,* G *has the zero-sum integral property, and vice versa,* i.e.

$$\sum_{(x_1,x_2,\cdots,x_s)\in\mathbb{F}_p^s} G(x_1,x_2,\cdots,x_s) \equiv 0 \pmod{p}.$$

Proof. Depending on whether all $\mathcal{D}(u_w)$ equals to $p-1$, we can split G into two parts: $G = G_1 + G_2$, where

$$G_1 \equiv \mathcal{A} \cdot \prod_{w=1}^{s} x_w^{p-1} \pmod{p}, \text{ with } \mathcal{A} = \sum_{\forall 1\le w\le s, \mathcal{D}(u_w)=p-1} \mathcal{C}_{\vec{u}},$$

$$G_2 = \sum_{\exists 1\le w\le s, \mathcal{D}(u_w)\le p-2} \mathcal{C}_{\vec{u}} \prod_{w=1}^{s} x_w^{u_w}.$$

With Fermat's Little Theorem, for any $x_w \in \mathbb{F}_p$, we have $x_w^{p-1} \equiv 1 \pmod{p}$ when $x_w \neq 0$. Hence,

$$\sum_{x_w\in\mathbb{F}_p} x_w^{p-1} \equiv p-1 \pmod{p}.$$

Meanwhile, for any u_w where $\mathcal{D}(u_w) \le p-2$, we have

$$\sum_{x_w\in\mathbb{F}_p} x_w^{u_w} \equiv \sum_{x_w\in\mathbb{F}_p} x_w^{\mathcal{D}(u_w)} \equiv 0 \pmod{p}.$$

Therefore,

$$\begin{aligned}
\sum_{(x_1,x_2,\cdots,x_s)\in\mathbb{F}_p^s} G_2 &\equiv \sum_{\exists 1\le w\le s, \mathcal{D}(u_w)\le p-2} \mathcal{C}_{\vec{u}} \left(\sum_{(x_1,x_2,\cdots,x_s)\in\mathbb{F}_p^s} \prod_{w=1}^{s} x_w^{u_w} \right) \pmod{p} \\
&\equiv \sum_{\exists 1\le w\le s, \mathcal{D}(u_w)\le p-2} \mathcal{C}_{\vec{u}} \left(\prod_{w=1}^{s} \left(\sum_{x_w\in\mathbb{F}_p} x_w^{u_w} \right) \right) \pmod{p} \\
&\equiv 0 \bmod p.
\end{aligned}$$

Notice that for each monomial in G_2, there always exists a w s.t. $\mathcal{D}(u_w) \le p-2$. Hence, the last equation holds. In this case, we obtain that

$$\sum_{(x_1,x_2,\cdots,x_s)\in\mathbb{F}_p^s} G \equiv \sum_{(x_1,x_2,\cdots,x_s)\in\mathbb{F}_p^s} G_1 \equiv \mathcal{A} \cdot (p-1)^s \pmod{p}.$$

Thus, whether the above sum equals to 0 is fully determined by the value of $\mathcal{A}$, which is the coefficient of $\prod_{w=1}^{s} x_w^{p-1}$. If $\mathcal{A} \equiv 0 \bmod p$, then G has the zero-sum integral property; otherwise, it does not. □

Consequently, the key point here is to compute $\mathcal{A}$, which is the coefficient of $\prod_{w=1}^{s} x_w^{p-1}$, and then check whether $\mathcal{A} \equiv 0 \pmod{p}$ holds. In Sect. 3.2, we take GMiMC-erf as an example to show how to compute $\mathcal{A}$ and verify, and how it can subsequently be transformed into an automatic search model.

3.2 Automatic Search for Integral Distinguishers

In this subsection, we show how to construct the automatic search model with a three-step framework named as Computation-Traceback-Determine. To explain it more clearly, we take GMiMC-erf as an example.

GMiMC-erf is one of the variants of GMiMC, which is a family of symmetric-key primitives proposed by Albrecht *et al.* at ESORICS 2019 [2]. Its structure is shown in Figure 3. Other variants includes GMiMC-crf, -nyb and -mrf, whose structures are shown in Appendix A due to space limitations. In all variants of GMiMC, they adopt the power mapping $x^d \bmod p$ as S-Box. It can be used as block cipher and hash function, which can be instantiated over $\mathbb{F}_p$ and $\mathbb{F}_{2^t}$. For block cipher usage, it supports two key sizes, *i.e.* univariate case $\log_2 p$ and multivariate case $n \cdot \log_2 p$. Since Bonnetain [7] found that there exists special slide attacks on GMiMC in the univariate case, we only focus on the block cipher GMiMC instantiated over $\mathbb{F}_p$ with full key size (multivariate case).

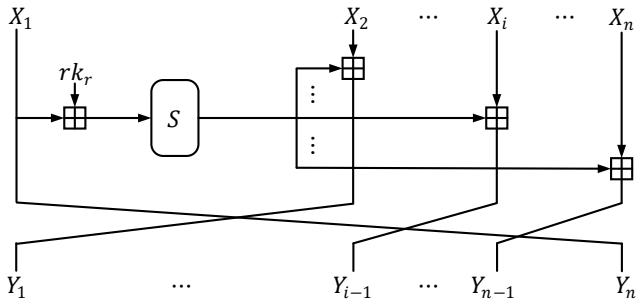


Fig. 3: Structure of GMiMC-erf

For GMiMC-erf with n blocks, one can add $(n-s)$ rounds without any costs when the leftmost s inputs are traversed. Thus, we only refer to this case when we say traversing s inputs. In this case, inputs of GMiMC-erf can be represented as $(x_1, x_2, \cdots, x_s, c_{s+1}, \cdots, c_n)$, where c_i are fixed values and x_w can take all possible values in $\mathbb{F}_p$.

Phase I Computation. Assume that our aim is to find an R-round integral distinguisher. Let rk_r denote the sum of round key and round constant in the r-th round, where $0 \le r \le R-1$, and Z_r is the output of S-Box in this round. Denote W_r as

$$W_r = \begin{cases} x_{(r \bmod n)+1} + rk_r, \text{ if } r \bmod n \le s-1; \\ c_{(r \bmod n)+1} + rk_r, \text{ otherwise.} \end{cases}$$

Then $Z_0 = W_0^d$. By symbolic computation with SageMath[6], one can derive the expression of each Z_r where $1 \leq r \leq R-1$. They follow the same form:

$$Z_r = (W_r + Z_{j_1} + Z_{j_2} + \cdots + Z_{j_r})^d,$$

where $\{Z_{j_1}, Z_{j_2}, \cdots, Z_{j_r}\}$ is a subset of $\{Z_0, Z_1, \cdots, Z_{r-1}\}$. To make it clear, we show a toy example in Figure 4 where $n = 4$, $s = 2$ and $R = 5$.

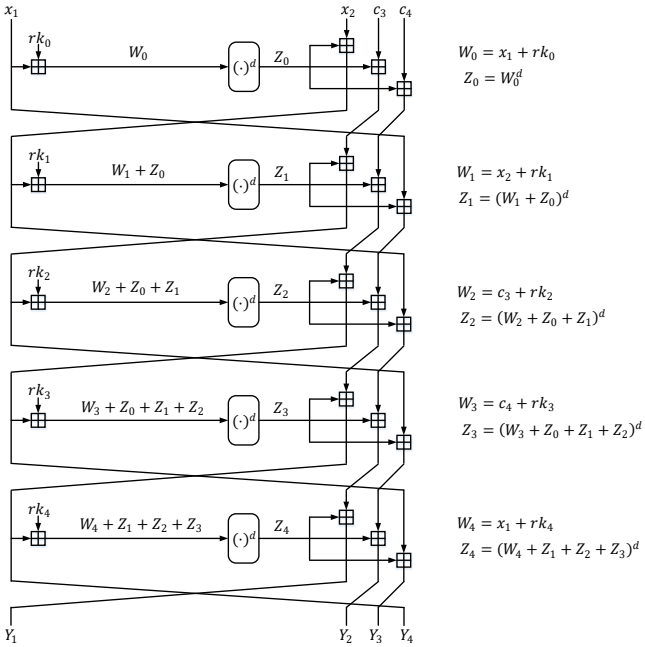


Fig. 4: A toy example of GMiMC-erf with $n = 4$, $s = 2$ and $R = 5$

Using these Z_r, one can finally obtain each output Y_i of GMiMC-erf after R rounds. Notice that in [5, Proposition 3], Beyne *et al.* revealed a linear relation between inputs and outputs of $(n-1)$ rounds of GMiMC-erf. With this relation, their distinguishers are extended by $(n-1)$ rounds. Hence, to find distinguishers covering more rounds, we also take this relation into consideration. In this way, what we care about is

$$T = \sum_{i=2}^{n} Y_i - (n-2) \cdot Y_1.$$

Through symbolic computation, one can find that

$$T = Z_{j_1} + Z_{j_2} + \cdots + Z_{j_t} + L(x_1, \cdots, x_s, c_{s+1}, \cdots, c_n),$$

[6] https://www.sagemath.org/

where $\{Z_{j_1}, Z_{j_2}, \cdots, Z_{j_t}\}$ is a subset of $\{Z_0, Z_1, \cdots, Z_{R-1}\}$ and L is linear.

For each involved Z_{j_*} variable, we will proceed the following two steps to detect whether all of them have the zero-sum integral property. If so, our target T will also fulfill this property, and thus we find an integral distinguisher covering R rounds where the leftmost s inputs are traversed. Notice that the total number of rounds covered by such distinguisher will be $(n-s+R)$, since $(n-s)$ rounds can be added in the head, as explained before.

Phase II Traceback. To check whether the coefficient $\mathcal{A}$ of the monomial $\prod_{w=1}^{s} x_w^{p-1}$ contained in each Z_{j_*} is 0 mod p or not, an intuitive way is to get its exact algebraic representation with the general form of Z_r iteratively. However, the number of possible monomials will be increased rapidly, making it infeasible to express Z_{j_*} with these x_w. Thus, one cannot get the detailed value of $\mathcal{A}$ in this way.

Different with above, we aim to express $\mathcal{A}$ through a set of equalities rather than try to get its exact value. After obtaining $\mathcal{A}$, we study under what condition $\mathcal{A} \neq 0 \pmod{p}$. To achieve this, we can also use the general form of Z_r iteratively, but in a different way.

Let's take the toy cipher shown in Figure 4 as an example. Assume that we're trying to obtain $\mathcal{A}$ for Z_4. The procedure is shown as follows.

$$
\begin{aligned}
Z_4 =& (W_4 + Z_1 + Z_2 + Z_3)^d \\
=& \sum_{v_4+u_{41}+u_{42}+u_{43}=d} \begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} W_4^{v_4} Z_1^{u_{41}} Z_2^{u_{42}} Z_3^{u_{43}} \\
=& \sum_{v_4+u_{41}+u_{42}+u_{43}=d} \begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} W_4^{v_4} Z_1^{u_{41}} Z_2^{u_{42}} (W_3 + Z_0 + Z_1 + Z_2)^{d \cdot u_{43}} \\
=& \sum_{\substack{v_4+u_{41}+u_{42}+u_{43}=d \\ v_3+u_{30}+u_{31}+u_{32}=d\cdot u_{43}}} \begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} \begin{bmatrix} d \cdot u_{43} \\ v_3, u_{30}, u_{31}, u_{32} \end{bmatrix} \\
& \qquad\qquad W_4^{v_4} W_3^{v_3} Z_0^{u_{30}} Z_1^{u_{31}+u_{41}} Z_2^{u_{32}+u_{42}} \\
=& \cdots \\
=& \sum_{EQ} \mathcal{C} \cdot \prod_{r=0}^{4} W_r^{v_r},
\end{aligned}
$$

where EQ represents the following equations

$$
\begin{cases}
v_4 + u_{41} + u_{42} + u_{43} = d \\
v_3 + u_{30} + u_{31} + u_{32} = d \cdot u_{43} \\
v_2 + u_{20} + u_{21} = d \cdot (u_{32} + u_{42}) \\
v_1 + u_{10} = d \cdot (u_{21} + u_{31} + u_{41}) \\
v_0 = d \cdot (u_{10} + u_{20} + u_{30})
\end{cases}
$$

and

$$\mathcal{C} = \begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} \begin{bmatrix} d \cdot u_{43} \\ v_3, u_{30}, u_{31}, u_{32} \end{bmatrix} \begin{bmatrix} d \cdot (u_{32} + u_{42}) \\ v_2, u_{20}, u_{21} \end{bmatrix} \begin{bmatrix} d \cdot (u_{21} + u_{31} + u_{41}) \\ v_1, u_{10} \end{bmatrix}.$$

Recall the definition of $\mathcal{D}(\cdot)$ and all W_i variables. We can obtain that

$$\prod_{r=0}^{4} W_r^{v_r} \equiv \prod_{r=0}^{4} W_r^{\mathcal{D}(v_r)} \pmod{p},$$

which then equals to

$$(x_1 + rk_0)^{\mathcal{D}(v_0)} (x_1 + rk_4)^{\mathcal{D}(v_4)} \cdot (x_2 + rk_1)^{\mathcal{D}(v_1)} \cdot W_2^{\mathcal{D}(v_2)} W_3^{\mathcal{D}(v_3)} \pmod{p}.$$

For $(x_2 + rk_1)^{\mathcal{D}(v_1)}$, to ensure that x_2^{p-1} appears, $\mathcal{D}(v_1)$ should equal to $p-1$. As for $(x_1 + rk_0)^{\mathcal{D}(v_0)}(x_1 + rk_4)^{\mathcal{D}(v_4)}$, we have to deal with two different cases.

- $rk_0 \neq rk_4$: One can expand $(x_1 + rk_0)^{\mathcal{D}(v_0)}(x_1 + rk_4)^{\mathcal{D}(v_4)}$, and obtain the coefficient $\mathcal{A}'$ of x_1^{p-1}:

$$\mathcal{A}' = \sum_{\substack{0 \leq i \leq \mathcal{D}(v_0) \\ 0 \leq j \leq \mathcal{D}(v_4) \\ i+j = p-1 \text{ or } 2(p-1)}} \binom{\mathcal{D}(v_0)}{i} \binom{\mathcal{D}(v_4)}{j} rk_0^{\mathcal{D}(v_0)-i} rk_4^{\mathcal{D}(v_4)-j} \bmod p.$$

  When $\mathcal{D}(v_0) + \mathcal{D}(v_4) < p-1$, $\mathcal{A}' = 0 \pmod{p}$ since there is no i and j fulfilling $i + j = p-1$ or $2(p-1)$.
  When $\mathcal{D}(v_0) + \mathcal{D}(v_4) \geq p-1$, let's take a closer look at $\mathcal{A}'$:
  - $rk_0 = 0$:

$$\mathcal{A}' \equiv \binom{\mathcal{D}(v_4)}{(p-1) - \mathcal{D}(v_0)} rk_4^{\mathcal{D}(v_0)+\mathcal{D}(v_4)-(p-1)} \pmod{p}.$$

    Since both $\mathcal{D}(v_4)$ and $(p-1)-\mathcal{D}(v_0)$ belong to $\mathbb{F}_p$, and $\mathcal{D}(v_4) \geq (p-1)-\mathcal{D}(v_0)$, one can conclude that $\mathcal{A}' \neq 0 \bmod p$ according to Lucas Theorem depicted in Lemma 2 of Appendix B.
  - $rk_4 = 0$:

$$\mathcal{A}' \equiv \binom{\mathcal{D}(v_0)}{(p-1) - \mathcal{D}(v_4)} rk_0^{\mathcal{D}(v_0)+\mathcal{D}(v_4)-(p-1)} \pmod{p},$$

    and also never be $0 \bmod p$ due to the same reason.
  - $rk_0 \neq 0$ and $rk_4 \neq 0$: Since $\mathcal{D}(v_0)$ and $\mathcal{D}(v_4)$ belong to $\mathbb{F}_p$, $\binom{\mathcal{D}(v_0)}{i}\binom{\mathcal{D}(v_4)}{j} \neq 0 \bmod p$. For each (i, j), the term $rk_0^{\mathcal{D}(v_0)-i} rk_4^{\mathcal{D}(v_4)-j}$ is unique and thus will not be merged with other terms. Hence, it cannot be $0 \bmod p$.

  In conclusion, one should require that $\mathcal{D}(v_0) + \mathcal{D}(v_4) \geq p-1$ to ensure the existence of x_1^{p-1} in this case.
- $rk_0 = rk_4$: It equals $(x_1 + rk_0)^{\mathcal{D}(v_0)+\mathcal{D}(v_4)}$. Thus, $\mathcal{D}(v_0) + \mathcal{D}(v_4) = p-1$ or $2(p-1)$ can ensure that x_1^{p-1} appears.

Combining above two cases together, we can use $\mathcal{D}(v_0)+\mathcal{D}(v_4) \geq p-1$ to ensure the existence of x_1^{p-1}. Finally, we can get the coefficient $\mathcal{A}$ of $x_1^{p-1}x_2^{p-1}$:

$$\mathcal{A} = \sum_{\substack{EQ \\ \mathcal{D}(v_0)+\mathcal{D}(v_4)\geq p-1 \\ \mathcal{D}(v_1)=p-1}} \left(W_2^{\mathcal{D}(v_2)} W_3^{\mathcal{D}(v_3)} \mathcal{A}' \cdot \mathcal{C}\right),$$

where $\mathcal{A}'$ only depends on $\mathcal{D}(v_0)$ and $\mathcal{D}(v_4)$. In other words, if $\mathcal{D}(v_0)$ and $\mathcal{D}(v_4)$ are fixed to be $\widetilde{v_0}$ and $\widetilde{v_4}$ respectively, $\mathcal{A}'$ will be fixed. Hence,

$$\mathcal{A} = \sum_{(\widetilde{v_0},\widetilde{v_1},\widetilde{v_2},\widetilde{v_3},\widetilde{v_4})\in MQ} \left(W_2^{\widetilde{v_2}} W_3^{\widetilde{v_3}} \mathcal{A}' \cdot \left(\sum_{\substack{EQ \\ \forall 0\leq r\leq 4,\ \mathcal{D}(v_r)=\widetilde{v_r}}} \mathcal{C} \right) \right),$$

where $MQ = \{\widetilde{v_0} + \widetilde{v_4} \geq p-1,\ \widetilde{v_1} = p-1\}$.

- If for every possible $(\widetilde{v_0}, \widetilde{v_1}, \widetilde{v_2}, \widetilde{v_3}, \widetilde{v_4}) \in MQ$, the sum

$$\sum_{\substack{EQ \\ \forall 1\leq w\leq s,\ \mathcal{D}(v_r)=\widetilde{v_r}}} \mathcal{C} \equiv 0 \pmod{p}.$$

  We can obtain that $\mathcal{A} \equiv 0 \bmod p$.
- If there are one or several $(\widetilde{v_0}, \widetilde{v_1}, \widetilde{v_2}, \widetilde{v_3}, \widetilde{v_4}) \in MQ$ s.t. the sum is not 0 mod p, the probability that $\mathcal{A} \equiv 0 \bmod p$ is extremely small.

In the second case, we'll assume that $\mathcal{A} \neq 0 \bmod p$ although it might be 0 mod p. This means that we may lose better distinguishers with little chance. However, we will never regard a non-integral distinguisher as integral one. Our automatic search model is based on this strategy.

Now, we show how to deal with the general case for Z_{R-1}, where $Z_0 = W_0^d$ and $Z_r = (W_r + Z_0 + Z_1 + \cdots + Z_{r-1})^d$ for any $1 \leq r \leq R-1$. The reason why such general forms of Z_r are adopted is that one can directly set $u_{r,j}$ as 0 in EQ and $\mathcal{C}$ if Z_j $(0 \leq j \leq R-1)$ is not contained in Z_r. This affects only the form of EQ while it does not affect the other two steps.

- **Recursively expand Z_{R-1} by iteratively substituting each Z_r.** This step can be performed using SageMath or executed manually.

  Proposition 3. *Under the general form of Z_r, we have*

$$Z_{R-1} = \sum_{EQ} \left(\mathcal{C} \cdot \prod_{r=0}^{R-1} W_r^{v_r} \right),$$

where EQ represents the following equations:

$$\begin{cases} v_{R-1} + u_{R-1,0} + \cdots + u_{R-1,R-2} = d \\ v_{R-2} + u_{R-2,0} + \cdots + u_{R-2,R-3} = d \cdot u_{R-1,R-2} \\ v_{R-3} + u_{R-3,0} + \cdots + u_{R-3,R-4} = d \cdot (u_{R-2,R-3} + u_{R-1,R-3}) \\ \cdots \\ v_r + u_{r,0} + \cdots + u_{r,r-1} = d \cdot \sum_{j=r+1}^{R-1} u_{j,r} \\ \cdots \\ v_1 + u_{1,0} = d \cdot \sum_{j=2}^{R-1} u_{j,1} \\ v_0 = d \cdot \sum_{j=1}^{R-1} u_{j,0} \end{cases}$$

and

$$\mathcal{C} = \begin{bmatrix} d \\ v_{R-1}, u_{R-1,0}, \cdots, u_{R-1,R-2} \end{bmatrix} \cdot \prod_{r=1}^{R-2} \begin{bmatrix} d \cdot \sum_{j=r+1}^{R-1} u_{j,r} \\ v_r, u_{r,0}, \cdots, u_{r,r-1} \end{bmatrix}.$$

– **Derive the coefficient $\mathcal{A}$ of monomial $\prod_{w=1}^{s} x_w^{p-1}$ contained in Z_{R-1}.** Similar with the toy example, $\mathcal{A}$ is in the form of

$$\mathcal{A} = \sum_{\substack{EQ \\ (\mathcal{D}(v_0), \mathcal{D}(v_1), \cdots, \mathcal{D}(v_{R-1})) \in MQ}} \left(\left(\prod_{r \bmod n \geq s} W_r^{\mathcal{D}(v_r)} \right) \cdot \mathcal{A}' \cdot \mathcal{C} \right),$$

where definitions of EQ and $\mathcal{C}$ can be found in Proposition 3, MQ and $\mathcal{A}'$ are shown in Proposition 4.

Proposition 4. *MQ contains all elements $(\mathcal{D}(v_0), \mathcal{D}(v_1), \cdots, \mathcal{D}(v_{R-1}))$ where*

$$\sum_{\delta=0}^{B_w} \mathcal{D}(v_{\delta n+w}) \geq p-1, \text{ for all } 1 \leq w \leq s.$$

And

$$\mathcal{A}' = \prod_{w=1}^{s} \left(\sum_{(i_0, i_1, \cdots, i_{B_w}) \in AQ_w} \prod_{\delta=0}^{B_w} \binom{\mathcal{D}(v_{\delta n+w})}{i_\delta} rk_{\delta n+w}^{\mathcal{D}(v_{\delta n+w}) - i_\delta} \right),$$

where AQ_w contains all $(i_0, i_1, \cdots, i_{B_w})$ that

$$\left\{ 0 \leq i_\delta \leq \mathcal{D}(v_{\delta n+w}) \text{ for } 0 \leq \delta \leq B_w, \sum_{\delta=0}^{B_w} i_\delta = m(p-1) \text{ where } m \geq 1 \right\}.$$

B_w in the above is defined as:

(1) when $R \bmod n \geq s$*, for all* $1 \leq w \leq s$*,*

$$B_w = \left\lfloor \frac{R+1}{n} \right\rfloor.$$

(2) when $R \bmod n \leq s-1$*,*

$$B_w = \begin{cases} \left\lfloor \frac{R+1}{n} \right\rfloor, \text{ when } 1 \leq w \leq (R \bmod n) \\ \left\lfloor \frac{R+1}{n} \right\rfloor - 1, \text{ when } (R \bmod n + 1) \leq w \leq s. \end{cases}$$

To prove Proposition 4, we have to use the following lemma.

Lemma 1 *Denote* x*,* a_i*,* e_i $(1 \leq i \leq t)$ *as elements in* $\mathbb{F}_p$*. For any* $q \in \mathbb{F}_p$*, the term* $\prod_{i=1}^{t}(x+a_i)^{e_i}$ *contains* x^q *if and only if* $\sum_{i=1}^{t} e_i \geq q$*.*

Proof. This can be proved with mathematical induction as follows.
(1) When $t = 1$, coefficient of x^q in $(x+a_1)^{e_1}$ is $\binom{e_1}{q} a_1^{e_1-q}$. If $a_1 \neq 0$, due to Lucas Theorem, $\binom{e_1}{q} \neq 0 \bmod p$ when $e_1 \geq q$. If $a_1 = 0$, $(x+a_1)^{e_1} = x^{e_1}$ leads to $e_1 = q$. Hence, $(x+a_1)^{e_1}$ contains x^q if and only if $e_1 \geq q$.
(2) Assume that this lemma holds when $t = h$. Let's check whether it holds when $t = h+1$. Notice that $\prod_{i=1}^{h+1}(x+a_i)^{e_i} = (\prod_{i=1}^{h}(x+a_i)^{e_i}) \cdot (x+a_{h+1})^{e_{h+1}}$. For each possible $e_{h+1} \leq q$, the existence of x^q in $\prod_{i=1}^{h+1}(x+a_i)^{e_i}$ is equivalent to the existence of $x^{q-e_{h+1}}$ in $\prod_{i=1}^{h}(x+a_i)^{e_i}$. The later is ensured by the condition that $\sum_{i=1}^{h} e_i \geq q - e_{h+1}$ since the lemma holds when $t = h$. Thus, $\sum_{i=1}^{h+1} e_i = e_{h+1} + \sum_{i=1}^{h} e_i \geq e_{h+1} + (q - e_{h+1}) = q$. □

Now we can prove Proposition 4 as follows:

Proof. Let's focus on the case when $R \bmod n \geq s$. The other case can be proved similarly. At the former step, we have obtained the form of Z_{R-1}. Here, we study whether $\prod_{w=1}^{s} x_w^{p-1}$ is contained in the monomial $\prod_{r=0}^{R-1} W_r^{v_r}$. Due to Fermat's Little Theorem, we have

$$\begin{aligned} \prod_{r=0}^{R-1} W_r^{v_r} &\equiv \prod_{r=0}^{R-1} W_r^{\mathcal{D}(v_r)} \pmod{p} \\ &\equiv \left(\prod_{r \bmod n \geq s} W_r^{\mathcal{D}(v_r)} \right) \cdot \left(\prod_{r \bmod n \leq s-1} W_r^{\mathcal{D}(v_r)} \right) \pmod{p} \\ &\equiv \left(\prod_{r \bmod n \geq s} W_r^{\mathcal{D}(v_r)} \right) \cdot \left(\prod_{w=1}^{s} \prod_{\delta=0}^{B_w} (x_w + r k_{\delta n+w})^{\mathcal{D}(v_{\delta n+w})} \right) \pmod{p}. \end{aligned}$$

Let's take a closer look at the second part. If $\sum_{\delta=0}^{B_w} \mathcal{D}(v_{\delta n+w}) \geq p-1$ holds for all $1 \leq w \leq s$, one can ensure the existence of $\prod_{w=1}^{s} x_w^{p-1}$ with Lemma 1.

Notice that this condition is MQ. Meanwhile,

$$(x_w + rk_{\delta n+w})^{\mathcal{D}(v_{\delta n+w})} = \sum_{i_\delta=0}^{\mathcal{D}(v_{\delta n+w})} \binom{\mathcal{D}(v_{\delta n+w})}{i_\delta} rk_{\delta n+w}^{\mathcal{D}(v_{\delta n+w})-i_\delta} x_w^{i_\delta}.$$

Hence, for all possible $(i_0, i_1, \cdots, i_{B_w})$ fulfilling that $\sum_{\delta=0}^{B_w} i_\delta = m(p-1)$ and $m \geq 1$, they all contribute to the coefficient of x_w^{p-1} contained in the term $\prod_{\delta=0}^{B_w}(x_w + rk_{\delta n+w})^{\mathcal{D}(v_{\delta n+w})}$. In this way, we can get $\mathcal{A}'$ by multiplying these coefficients together. □

– **Get the multinomial coefficient we care about.** From Proposition 4, $\mathcal{A}'$ is only related with $(\mathcal{D}(v_0), \mathcal{D}(v_1), \cdots, \mathcal{D}(v_{R-1}))$. Therefore, $\mathcal{A}$ equals

$$\sum_{(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v}_{R-1}) \in MQ} \left(\left(\prod_{r \bmod n \geq s} W_r^{\widetilde{v_r}} \right) \cdot \mathcal{A}' \cdot \left(\sum_{\substack{EQ \\ \forall 0 \leq r \leq R-1,\ \mathcal{D}(v_r) = \widetilde{v_r}}} \mathcal{C} \right) \right).$$

Now, we give the basic strategy behind our search model in Proposition 5.

Proposition 5. *Denote $\mathcal{S}$ as the sum*

$$\sum_{\substack{EQ \\ \forall 0 \leq r \leq R-1,\ \mathcal{D}(v_r) = \widetilde{v_r}}} \mathcal{C}.$$

If $\mathcal{S} \equiv 0 \pmod p$ holds for all $(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v}_{R-1}) \in MQ$, we get $\mathcal{A} \equiv 0 \bmod p$. EQ and $\mathcal{C}$ are defined in Proposition 3, MQ is shown in Proposition 4.

Main Idea of the Automatic Search Model. With Proposition 5, we only need to check whether there exists $(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v}_{R-1}) \in MQ$ s.t. $\mathcal{S} \neq 0 \pmod p$. To achieve this, we have to use the condition set BQ constructed in Phase III, which can be recognized by automatic search tools. In this case, the automatic search model can be constructed by finding a solution of $(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v}_{R-1}) \in MQ$ which should fulfill all equations defined in EQ under the relation that $\mathcal{D}(v_r) = \widetilde{v}_r$, and all conditions shown in BQ. If there is no solution, combining the principle of constructing BQ shown below, one can realize that $\mathcal{S} \equiv 0 \pmod p$ holds for any possible $(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v}_{R-1}) \in MQ$. Thus due to Proposition 5, we can obtain $\mathcal{A} \equiv 0 \pmod p$, which means the coefficient of monomial $\prod_{w=1}^{s} x_w^{p-1}$ is 0. Hence, according to Proposition 2, Z_{R-1} will have the zero-sum integral property, which then leads to an integral distinguisher covering $(n-s)+R$ rounds for GMiMC-erf.

Comparison with previous works. Currently, there is no automatic tool that can search for integral distinguishers over $\mathbb{F}_p$. Among all methods developed for ciphers over binary fields, monomial predication technique [23] proposed by Hu *et al.* is a powerful tool for degree evaluation. It allows us to precisely determine

whether or not a specific monomial appears in the ANF by counting the number of monomial trails. But it is typically more effective for stream ciphers than block ciphers. At Asiacrypt 2020 [11], it was generalized to $\mathbb{F}_{2^t}$ by Cui *et al.*, referred to as general monomial prediction. However, due to the heavy monomial transitions round by round, they adopted a compromised way. Instead of studying the details of the coefficient of the monomials that appear, they are interested only in predicting which monomials do not appear in the polynomial representation. The coefficient grouping technique [25,26] proposed recently also adopts the same way.

Phase III Determine. In order to construct the automatic search model following Proposition 5, one has to transform $\mathcal{S} \neq 0 \pmod p$ into its equivalent conditions that can be used by automated search tools. However, this is not an easy task. Here, we partially solve it by constructing a condition set BQ under the following principle.

Principle of Constructing BQ**.** Let $\mathcal{H}$ denote a condition that leads to $\mathcal{S} \equiv 0 \pmod p$, and $\overline{\mathcal{H}}$ denotes its opposite, where $\mathcal{S}$ is defined in Proposition 5. Then we add $\overline{\mathcal{H}}$ to BQ.

Notice that this condition set BQ is not equivalent with $\mathcal{S} \neq 0 \pmod p$. However, it can help to identify integral distinguishers by requiring that all $\overline{\mathcal{H}}$ in BQ should be fulfilled at the same time. Now, we explain why.

- Assume that we didn't find a solution under BQ. That is, there is no solution can satisfy all possible conditions in BQ. In other words, for all possible $(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v_{R-1}}) \in MQ$, there is one or several $\overline{\mathcal{H}} \in BQ$ that will never hold, which further indicates that their opposites $\mathcal{H}$ will hold with probability one. Hence, $\mathcal{S} \equiv 0 \pmod p$ holds for all possible $(\widetilde{v_0}, \widetilde{v_1}, \cdots, \widetilde{v_{R-1}}) \in MQ$. In this case, $\mathcal{A} \equiv 0 \pmod p$, and thus we find an integral distinguisher.
- Assume that we get a solution. This means that it can satisfy all possible conditions in BQ. In this case, we cannot decide whether $\mathcal{S} \neq 0 \pmod p$ hold or not, since these conditions are only necessary ones for $\mathcal{S} \neq 0 \pmod p$. So, if one can derive as many conditions $\mathcal{H}$ as possible, one will have more chance to find better integral distinguishers. This is what we do in the next part.

In the follows, we show how to derive the condition $\mathcal{H}$ that can lead to $\mathcal{S} \equiv 0 \pmod p$ as many as possible. Recall that

$$\mathcal{S} = \sum_{\substack{EQ \\ \forall 0 \le r \le R-1,\ \mathcal{D}(v_r) = \widetilde{v_r}}} \mathcal{C}$$

and $\mathcal{C}$ is the multiplication of several multinomial coefficients:

$$\mathcal{C} = \begin{bmatrix} d \\ v_{R-1}, u_{R-1,0}, \cdots, u_{R-1,R-2} \end{bmatrix} \cdot \prod_{r=1}^{R-2} \begin{bmatrix} d \cdot \sum_{j=r+1}^{R-1} u_{j,r} \\ v_r, u_{r,0}, \cdots, u_{r,r-1} \end{bmatrix}$$

under the general form of $Z_r = (W_r + Z_0 + Z_1 + \cdots + Z_{r-1})^d$. Notice that if Z_j doesn't consist of Z_r, we only need to set $u_{r,j}$ as 0 in $\mathcal{C}$ and EQ. This doesn't affect the following discussions.

We consider three types of conditions here. To have a better understanding of Type II/III conditions, we take the toy GMiMC previously used as an example, and give some details in Example 3 to 6, which are described in Appendix C.

– **Type I Condition.** If for every $\mathcal{C}$ contained in $\mathcal{S}$, there always exists one multinomial coefficient consisting of $\mathcal{C}$ that equals to 0 mod p, *i.e.*

$$\begin{bmatrix} d \\ v_{R-1}, u_{R-1,0}, \cdots, u_{R-1,R-2} \end{bmatrix} \equiv 0 \bmod p$$

or there exists $1 \leq r \leq R-2$ s.t.

$$\begin{bmatrix} d \cdot \sum_{j=r+1}^{R-1} u_{j,r} \\ v_r, u_{r,0}, \cdots, u_{r,r-1} \end{bmatrix} \equiv 0 \bmod p,$$

one can obtain that $\mathcal{C} \equiv 0 \pmod p$, and thus $\mathcal{S} \equiv 0 \pmod p$. Following the previous introduced principle, we consider its opposite, *i.e.*

$$\begin{bmatrix} d \\ v_{R-1}, u_{R-1,0}, \cdots, u_{R-1,R-2} \end{bmatrix} \neq 0 \bmod p$$

and for each $1 \leq r \leq R-2$,

$$\begin{bmatrix} d \cdot \sum_{j=r+1}^{R-1} u_{j,r} \\ v_r, u_{r,0}, \cdots, u_{r,r-1} \end{bmatrix} \neq 0 \bmod p.$$

With Lucas Theorem (Lemma 3), this condition can be represented by some equalities. One can then add them to the condition set BQ.

– **Type II Condition.** We consider $(R-1)$ different sums. The r-th one is

$$\widehat{\mathcal{C}}_{I,r} = \sum_{\widetilde{EQ}_r} \begin{bmatrix} \left(d \cdot \sum_{j=r+1}^{R-1} u_{j,r}\right) - (u_{r,1} + \cdots + u_{r,r-1}) \\ v_r, u_{r,0} \end{bmatrix},$$

where $1 \leq r \leq R-1$, and $\widetilde{EQ}_r$ is the following equalities:

$$\begin{cases} v_r + u_{r,0} = \left(d \cdot \sum_{j=r+1}^{R-1} u_{j,r}\right) - (u_{r,1} + \cdots + u_{r,r-1}) \\ v_0 = d \cdot u_{r,0} + d \cdot \sum_{\substack{1 \leq j \leq R-1 \\ j \neq r}} u_{j,0} \\ \mathcal{D}(v_i) = \widetilde{v_i},\ i \in \{0, r\}. \end{cases}$$

Following the principle introduced before, we can use their opposites to build BQ if they lead to $\mathcal{S} \equiv 0 \pmod p$. We show in Sect. 3.3 how to represent

these opposites with several equations. Now, we show why they lead to $\mathcal{S} \equiv 0 \pmod{p}$. To understand this more clearly, two examples are given in Example 3 and 4. Below is the formal explanation. Denote $\widehat{EQ}_r$ as

$$\begin{cases} v_{R-1} + u_{R-1,0} + \cdots + u_{R-1,R-2} = d \\ \cdots \\ v_{r+1} + u_{r+1,0} + \cdots + u_{r+1,r} = d \cdot \sum_{j=r+2}^{R-1} u_{j,r+1} \\ v_{r-1} + u_{r-1,0} + \cdots + u_{r-1,r-2} = d \cdot \sum_{j=r}^{R-1} u_{j,r-1} \\ \cdots \\ v_1 + u_{1,0} = d \cdot \sum_{j=2}^{R-1} u_{j,1} \\ \mathcal{D}(v_i) = \widetilde{v_i},\ i \notin \{0, r\}. \end{cases}$$

We can represent $\mathcal{S}$ as

$$\mathcal{S} = \sum_{u_{r,1}, u_{r,2}, \cdots, u_{r,r-1}} \left(\mathcal{C}' \cdot \sum_{\widehat{EQ}_r} \left(\widehat{U}_r \cdot \widehat{\mathcal{C}}_{I,r} \right) \right),$$

and this means that $\widehat{\mathcal{C}}_{I,r} \equiv 0 \pmod{p}$ leads to $\mathcal{S} \equiv 0 \pmod{p}$. In the above expression of $\mathcal{S}$, $\mathcal{C}'$ is the multiplication of several multinomial coefficients, *i.e.*

$$\binom{t_r}{u_{r,1}} \binom{t_r - u_{r,1}}{u_{r,2}} \binom{t_r - u_{r,1} - u_{r,2}}{u_{r,3}} \cdots \binom{t_r - (u_{r,1} + \cdots, u_{r,r-2})}{u_{r,r-1}}$$

with $t_r = d \cdot \sum_{j=r+1}^{R-1} u_{j,r}$, and

$$\widehat{U}_r = \begin{cases} \begin{bmatrix} d \\ v_{R-1}, \cdots, u_{R-1,R-2} \end{bmatrix} \cdot \prod_{\substack{1 \le r' \le R-1 \\ r' \ne r}} \begin{bmatrix} d \cdot \sum_{j=r'+1}^{R-1} u_{j,r'} \\ v_{r'}, \cdots, u_{r',r'-1} \end{bmatrix}, & \text{if } r \le R-2; \\ \prod_{1 \le r' \le R-1} \begin{bmatrix} d \cdot \sum_{j=r'+1}^{R-1} u_{j,r'} \\ v_{r'}, \cdots, u_{r',r'-1} \end{bmatrix}, & \text{if } r = R-1. \end{cases}$$

– **Type III Condition.** Similar with Type II, we consider the following two kinds of sums:
(1) when $r = 1$ and $q \ge 1$,

$$\widehat{\mathcal{C}}_{II,1,q} = \sum_{\widehat{EQ}_{1,q}} \begin{bmatrix} t_{1+q} - (u_{1+q,1} + \cdots + u_{1+q,q}) \\ v_{1+q}, u_{1+q,0} \end{bmatrix} \begin{bmatrix} \left(d \cdot \sum_{j=1+1}^{R-1} u_{j,1} \right) \\ v_1, u_{10} \end{bmatrix},$$

where $t_{1+q} = d \cdot \sum_{j=1+q+1}^{R-1} u_{j,1+q}$ and $\widetilde{EQ}_{1,q}$ is

$$\begin{cases} v_{1+q} + u_{1+q,0} = t_{1+q} - (u_{1+q,1} + \cdots + u_{1+q,q}) \\ v_1 + u_{10} = d \cdot \sum_{j=2}^{R-1} u_{j,1} \\ v_0 = d \cdot (u_{10} + u_{1+q,0}) + d \cdot \sum_{\substack{1 \le j \le R-1 \\ j \notin \{1, 1+q\}}} u_{j,0} \\ \mathcal{D}(v_i) = \widetilde{v_i},\ i \in \{0, 1, 1+q\} \end{cases}$$

The above sum $\widehat{\mathcal{C}}_{II,1,q} \equiv 0 \pmod{p}$ also lead to $\mathcal{S} \equiv 0 \pmod{p}$. An example is given in Example 5. In Sect. 3.3, we show how to represent their opposites into some equalities.

(2) when $r \ge 2$ and $q \ge 1$,

$$\widehat{\mathcal{C}}_{II,r,q} = \sum_{\widetilde{EQ}_{r,q}} \begin{bmatrix} t_{r+q} - (u_{r+q,r} + \cdots + u_{r+q,r+q-1}) \\ v_{r+q}, u_{r+q,0}, \cdots, u_{r+q,r-1} \end{bmatrix} \begin{bmatrix} \left(d \cdot \sum_{j=r+1}^{R-1} u_{j,r}\right) \\ v_r, u_{r,0}, \cdots, u_{r,r-1} \end{bmatrix},$$

where $t_{r+q} = d \cdot \sum_{j=r+q+1}^{R-1} u_{j,r+q}$ and $\widetilde{EQ}_{r,q}$ is

$$\begin{cases} v_{r+q} + u_{r+q,0} + \cdots + u_{r+q,r-1} = t_{r+q} - (u_{r+q,r} + \cdots + u_{r+q,r+q-1}) \\ v_r + u_{r,0} + \cdots + u_{r,r-1} = d \cdot \sum_{j=r+1}^{R-1} u_{j,r} \\ v_0 = d \cdot (u_{r,0} + u_{r+q,0}) + d \cdot \sum_{\substack{1 \le j \le R-1 \\ j \notin \{r, r+q\}}} u_{j,0} \\ \mathcal{D}(v_i) = \widetilde{v_i},\ i \in \{0, r, r+q\} \\ u_{r+q,j} + u_{r,j} = \hat{u}_{r+q,r,j},\ 1 \le j \le r-1. \end{cases}$$

When they equal 0 mod p, $\mathcal{S} \equiv 0 \pmod{p}$. An example for this case is shown in Example 6. One can use some equations through the way shown in Sect. 3.3 to represent their opposites.

3.3 Some Necessary Propositions for Phase III

To use Type II and III conditions depicted in Phase III, we have to convert them into some equalities which can be recognized by automatic search tools. In this subsection, we show how to do this by introducing several propositions.

From Sect. 3.2, we know that there are only three types of sums involved in Type II/III conditions, which are:

$$\widehat{\mathcal{C}}_{I,r} = \sum_{\substack{v_r + u_{r,0} = m_2 \\ v_0 = d \cdot u_{r,0} + m_3 \\ \mathcal{D}(v_i) = \widetilde{v_i},\ i \in \{0, r\}}} \begin{bmatrix} m_2 \\ v_r, u_{r,0} \end{bmatrix}$$

$$\widehat{\mathcal{C}}_{II,1,q} = \sum_{\substack{v_{1+q}+u_{1+q,0}=m_1 \\ v_1+u_{10}=m_2 \\ v_0=d\cdot(u_{10}+u_{1+q,0})+m_3 \\ \mathcal{D}(v_i)=\widetilde{v}_i,\ i\in\{0,1,1+q\}}} \begin{bmatrix} m_1 \\ v_{1+q}, u_{1+q,0} \end{bmatrix} \begin{bmatrix} m_2 \\ v_1, u_{10} \end{bmatrix}$$

$$\widehat{\mathcal{C}}_{II,r,q} = \sum_{\substack{v_{r+q}+u_{r+q,0}+\cdots+u_{r+q,r-1}=m_1 \\ v_r+u_{r,0}+\cdots+u_{r,r-1}=m_2 \\ v_0=d\cdot(u_{r,0}+u_{r+q,0})+m_3 \\ \mathcal{D}(v_i)=\widetilde{v}_i,\ i\in\{0,r,r+q\} \\ u_{r+q,j}+u_{r,j}=\hat{u}_{r+q,r,j},\ 1\le j\le r-1}} \begin{bmatrix} m_1 \\ v_{r+q}, u_{r+q,0}, \cdots, u_{r+q,r-1} \end{bmatrix} \begin{bmatrix} m_2 \\ v_r, u_{r,0}, \cdots, u_{r,r-1} \end{bmatrix}$$

m_1, m_2 and m_3 equal to different values in above three sums, which are not important in the following analysis, thus are omitted. Recall that these three sums are deduced under the general form of Z_r. In real applications, if Z_j doesn't consists of Z_r, the value $u_{r,j}$ will always be 0. Thus, we have to take this point into consideration in the following analyses.

Here, we take $\widehat{\mathcal{C}}_{I,r} \neq 0 \pmod p$ as an example. If Z_0 does not consist of Z_r, the value $u_{r,0}$ is always 0. Thus, $\widehat{\mathcal{C}}_{I,r} = 1 \neq 0$. Therefore, we don't need to derive any equations in this case. If Z_0 consists of Z_r, we have to deal with different $\widetilde{v}_0$ and $\widetilde{v}_r$, respectively. Recall the definition of $\mathcal{D}(v_r)$, which equals to $\widetilde{v}_r$ here. We can obtain that

$$v_r = \begin{cases} 0, \text{ when } \widetilde{v}_r = 0 \\ k_1(p-1),\ k_1 \ge 1, \text{ when } \widetilde{v}_r = p-1 \\ \widetilde{v}_r + k_1(p-1),\ k_1 \ge 0, \text{ when } 1 \le \widetilde{v}_r \le p-2. \end{cases}$$

According to $v_r + u_{r,0} = m_2$ and $v_0 = d \cdot u_{r,0} + m_3$, one can get $v_0 = dm_2 + m_3 - dv_r$. Since $\mathcal{D}(v_0) = \widetilde{v}_0$, we have:

(1) when $\widetilde{v}_0 = 0$, we get $v_0 = dm_2 + m_3 - dv_r = 0$, and thus $v_r = m_2 + \frac{m_3}{d}$.
(2) when $\widetilde{v}_0 = p-1$, we have $v_0 = k_0(p-1)$ where $k_0 \ge 1$. Thus, $dm_2+m_3-dv_r = k_0(p-1)$. In other words,

$$v_r \le m_2 + \frac{m_3-(p-1)}{d}, \text{ and } p-1 \mid dm_2 + m_3 - dv_r.$$

(3) when $1 \le \widetilde{v}_0 \le p-2$,

$$v_r = m_2 + \frac{m_3 - \widetilde{v}_0}{d}$$

or

$$v_r \le m_2 + \frac{(m_3-\widetilde{v}_0)-(p-1)}{d}, \text{ and } p-1 \mid dm_2 + m_3 - dv_r - \widetilde{v}_0.$$

With above analyses, one can derive equations for $\widehat{\mathcal{C}}_{I,r} \neq 0 \pmod p$ as follows, by considering different values of $\widetilde{v}_0$ and $\widetilde{v}_r$:

(1) when $\widetilde{v}_0 = 0$ or $\widetilde{v}_r = 0$, we can see that v_r is always a fixed value. In this case, $\widehat{\mathfrak{C}}_{I,r} = \begin{bmatrix} m_2 \\ v_r, u_{r,0} \end{bmatrix}$. Notice that this multinomial coefficient has been required not to be 0 mod p in Type I conditions.

(2) when $\widetilde{v}_0 = p-1$ and $\widetilde{v}_r = p-1$, we can obtain $v_r = k_1(p-1)$ with $k_1 \geq 1$, $0 \leq v_r \leq m_1$, $v_r \leq m_2 + \frac{m_3-(p-1)}{d}$, and $p-1 \mid dm_2 + m_3 - dv_r$. Thus, we have $p-1 \mid dm_2 + m_3$ since $p-1 \mid v_r$, and

$$1 \leq k_1 \leq \min\left\{ \left\lfloor \frac{m_2}{p-1} \right\rfloor, \left\lfloor \frac{m_2}{p-1} + \frac{m_3-(p-1)}{d(p-1)} \right\rfloor \right\}.$$

(2.1) if $m_3 \geq p-1$, we can obtain that

$$\widehat{\mathfrak{C}}_{I,r} = \sum_{k_1=1,\ v_r=k_1(p-1)}^{\lfloor \frac{m_2}{p-1} \rfloor} \begin{bmatrix} m_2 \\ v_r,\ u_{r,0} \end{bmatrix} = \sum_{k_1=1}^{\lfloor \frac{m_2}{p-1} \rfloor} \binom{m_2}{k_1(p-1)}.$$

Thus, $\widehat{\mathfrak{C}}_{I,r} \neq 0 \pmod p$ is equivalent with

$$\boxed{\sum_{k_1=1}^{\lfloor \frac{m_2}{p-1} \rfloor} \binom{m_2}{k_1(p-1)} \neq 0 \pmod p}.$$

(2.2) if $m_3 < p-1$,

$$\widehat{\mathfrak{C}}_{I,r} = \sum_{k_1=1}^{\lfloor \frac{m_2}{p-1} + \frac{m_3-(p-1)}{d(p-1)} \rfloor} \binom{m_2}{k_1(p-1)} = \sum_{k_1=1}^{\lfloor \frac{m_2}{p-1} \rfloor - 1} \binom{m_2}{k_1(p-1)}.$$

In this case, $\widehat{\mathfrak{C}}_{I,r} \neq 0 \pmod p$ is equivalent with

$$\boxed{\sum_{k_1=1}^{\lfloor \frac{m_2}{p-1} \rfloor - 1} \binom{m_2}{k_1(p-1)} \neq 0 \pmod p}.$$

(3) when $\widetilde{v}_0 = p-1$ and $1 \leq \widetilde{v}_r \leq p-2$, we get $v_r = \widetilde{v}_r + k_1(p-1)$ with $k_1 \geq 0$, $v_1 \leq m_2$, $v_r \leq m_2 + \frac{m_3-(p-1)}{d}$, and $p-1 \mid dm_2 + m_3 - dv_r$. Thus, we have $p-1 \mid dm_2 + m_3 - d\widetilde{v}_r$ since $dm_2 + m_3 - dv_r = dm_2 + m_3 - d\widetilde{v}_r - dk_1(p-1)$. Besides, we obtain that

$$0 \leq k_1 \leq \min\left\{ \left\lfloor \frac{m_2 - \widetilde{v}_r}{p-1} \right\rfloor, \left\lfloor \frac{m_2 - \widetilde{v}_r}{p-1} + \frac{m_3-(p-1)}{d(p-1)} \right\rfloor \right\}.$$

Therefore, $\widehat{\mathfrak{C}}_{I,r} \neq 0 \pmod p$ is equivalent with

$$\boxed{\sum_{k_1=0}^{\lfloor \frac{m_2-\widetilde{v}_r}{p-1} \rfloor} \binom{m_2}{\widetilde{v}_r + k_1(p-1)} \neq 0 \pmod p}, \text{ when } m_3 \geq p-1;$$

$$\boxed{\sum_{k_1=0}^{\left\lfloor \frac{m_2-\widetilde{v}_r}{p-1} \right\rfloor - 1} \binom{m_2}{\widetilde{v}_r + k_1(p-1)} \neq 0 \pmod{p}}, \text{ when } m_3 < p-1.$$

From the above analyses, one can find that $\widehat{\mathcal{C}}_{I,r} \neq 0 \pmod{p}$ is equivalent with four different sums, which are those boxed, under different conditions. We denote T_1, T_2, T_3 and T_4 respectively for these four sums, *i.e.*

$$T_1 = \sum_{k_1=1}^{\left\lfloor \frac{m_2}{p-1} \right\rfloor} \binom{m_2}{k_1(p-1)}, \qquad T_2 = \sum_{k_1=1}^{\left\lfloor \frac{m_2}{p-1} \right\rfloor - 1} \binom{m_2}{k_1(p-1)},$$

$$T_3 = \sum_{k_1=0}^{\left\lfloor \frac{m_2-\widetilde{v}_r}{p-1} \right\rfloor} \binom{m_2}{\widetilde{v}_r + k_1(p-1)}, \quad T_4 = \sum_{k_1=0}^{\left\lfloor \frac{m_2-\widetilde{v}_r}{p-1} \right\rfloor - 1} \binom{m_2}{\widetilde{v}_r + k_1(p-1)}.$$

Using Proposition 6, 7, 8 and 9 introduced in the end of this subsection, we can derive equations for $T_i \neq 0 \pmod{p}$ to construct the condition set BQ.

For the other two cases of $\widetilde{v}_0$ and $\widetilde{v}_r$, one also reach these four sums. We show these results without giving details since the deduction is almost the same.

(4) when $1 \leq \widetilde{v}_0 \leq p-2$ and $\widetilde{v}_r = p-1$, we have $p-1 \mid dm_2 + m_3 - \widetilde{v}_0$, and
- if $m_3 - \widetilde{v}_0 \geq p-1$, $\widehat{\mathcal{C}}_{I,r} \neq 0 \pmod{p}$ is equivalent to $T_1 \neq 0 \pmod{p}$.
- if $m_3 - \widetilde{v}_0 < p-1$, it is equivalent to $T_2 \neq 0 \pmod{p}$.

(5) when $1 \leq \widetilde{v}_0 \leq p-2$ and $1 \leq \widetilde{v}_r \leq p-2$, we get $p-1 \mid dm_2 + m_3 - d\widetilde{v}_r - \widetilde{v}_0$,
- if $m_3 - \widetilde{v}_0 \geq p-1$, it is equivalent to $T_3 \neq 0 \pmod{p}$.
- if $m_3 - \widetilde{v}_0 < p-1$, it is equivalent to $T_4 \neq 0 \pmod{p}$.

For $\widehat{\mathcal{C}}_{II,1,q}$ and $\widehat{\mathcal{C}}_{II,r,q}$, one can follow a similar way to derive their equations. As results, almost all cases lead to the sum of multinomial coefficients in the form of T_1, T_2, T_3 and T_4. The other cases lead to multinomial coefficients whose corresponding equations can be derived with Lucas Theorem. Due to space limitations, we discuss $\widehat{\mathcal{C}}_{II,1,q}$ and $\widehat{\mathcal{C}}_{II,r,q}$ in Appendix D.

Now, the key point here is to derive equations for $T_i \neq 0 \pmod{p}$, where $1 \leq i \leq 4$. To solve this, we introduce four different propositions here, and show their proofs in Appendix E.

Proposition 6. *For any $m \leq p^{L+1} - 1$ where $L \geq 1$ and $p \geq 3$, denote m in base p form: $m = \widehat{m}_L \cdot p^L + \widehat{m}_{L-1} \cdot p^{L-1} + \cdots + \widehat{m}_1 \cdot p + \widehat{m}_0$ and $t = \sum_{j=0}^{L} \widehat{m}_j$. If $m \geq p-1$ and $L \leq p-1$, one can obtain that*

$$\sum_{k=1}^{\left\lfloor \frac{m}{p-1} \right\rfloor} \binom{m}{k(p-1)} \neq 0 \pmod{p}$$

if and only if $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p) \right) \bmod p = p-1$.

Proposition 7. *For any $m \leq p^{L+1}-1$ where $L \geq 1$ and $p \geq 3$, if $m \geq p-1$ and $L \leq p-1$, one can obtain that*

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor - 1} \binom{m}{k(p-1)} \neq 0 \pmod{p}$$

if and only if one of following conditions holds:

(1) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p = p-1$, $\widehat{m}_0 < (t \bmod (p-1))$.

(2) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p = p-1$, $(t \bmod (p-1)) \notin \{\widehat{m}_0, 0\}$, *and* $\widehat{m}_0 \geq \max\{(t \bmod (p-1)), 2\}$.

(3) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \leq p-2$, $\widehat{m}_0 \geq (t \bmod (p-1))$.

Here, t follows the same definition as Proposition 6.

Proposition 8. *For any $1 \leq \widetilde{v} \leq p-2$ and $m \leq p^{L+1}-1$ where $L \geq 1$ and $p \geq 3$, if $m \geq p-1$ and $L \leq p-1$,*

$$\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor} \binom{m}{\widetilde{v}+k(p-1)} \neq 0 \pmod{p}$$

if and only if one of the following conditions holds:

(1) $L \leq \widetilde{v}$ *and* $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \geq \widetilde{v}$.

(2) $L \geq \widetilde{v}+1$, $\left\lfloor \frac{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{p} \right\rfloor = 0$, *and* $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \geq \widetilde{v}$.

(3) $L \geq \widetilde{v}+1$, $\left\lfloor \frac{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{p} \right\rfloor = 1$, *and* $\left(\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p\right) + 1 \geq \widetilde{v}$.

Here, t follows the same definition as Proposition 6.

Proposition 9. *For any $1 \leq \widetilde{v} \leq p-2$ and $m \leq p^{L+1}-1$ where $L \geq 1$ and $p \geq 3$, $m \geq p-1$ and $L \leq p-1$, to require*

$$\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor - 1} \binom{m}{\widetilde{v}+k(p-1)} \neq 0 \pmod{p},$$

we add following conditions to the condition set BQ:

(1) $(\mathcal{B}_3 \vee \mathcal{B}_4 \vee \mathcal{B}_5 \vee \mathcal{B}_6) \wedge \mathcal{B}_9$
(2) $(\mathcal{B}_1 \vee \mathcal{B}_2 \vee \mathcal{B}_7) \wedge \mathcal{B}_8$
(3) $(\mathcal{B}_1 \vee \mathcal{B}_2) \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{10} \vee \mathcal{B}_{11}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18})$
(4) $(\mathcal{B}_1 \vee \mathcal{B}_2) \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{12} \vee \mathcal{B}_{13}) \wedge (\mathcal{B}_{14} \vee \mathcal{B}_{15} \vee \mathcal{B}_{16})$
(5) $(\mathcal{B}_1 \vee \mathcal{B}_2) \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{12} \vee \mathcal{B}_{13}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18}) \wedge \{\widehat{m}_0 \neq (\widehat{t} \bmod p)\}$
(6) $\mathcal{B}_7 \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{19} \vee \mathcal{B}_{20}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18})$
(7) $\mathcal{B}_7 \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{21} \vee \mathcal{B}_{22}) \wedge (\mathcal{B}_{14} \vee \mathcal{B}_{15} \vee \mathcal{B}_{16})$
(8) $\mathcal{B}_7 \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{21} \vee \mathcal{B}_{22}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18}) \vee \{\widehat{m}_0 \neq ((\widehat{t} \bmod p)+1)\}$,

where conditions $\mathcal{B}_i$ are depicted in Table 3, $\widehat{t} = \left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)$, and t follows the same definition as Proposition 6.

3.4 Experiments on GMiMC-erf using Small Primes

To check whether the automatic search model constructed above is valid or not, we performed several experiments for GMiMC-erf with small primes.

In each experiment, the leftmost s inputs $x_1, x_2, \cdots, x_s$ are traversed, while the others are fixed to be random values. Denote Y_i as the i-th output after encrypting R rounds, where $1 \leq i \leq n$. Let $T = \sum_{i=2}^{n} Y_i - (n-2) \cdot Y_1$. We check whether $\sum_{x_1,x_2,\cdots,x_s} T \equiv 0 \pmod{p}$.

If the model find that there is no solution, it means we have found an integral distinguisher. Experimental results are shown in Table 1. From this table, one can see that this model can successfully detect the integral distinguisher. Meanwhile, it will not regard non-integral distinguishers as integral ones.

Table 1: Experimental Verification of Automatic Search Model for GMiMC-erf

degree d	prime p	blocks n	s	rounds R	model results	experiments
3	7	86	1	86	no solution (integral)	integral
			1	87/88	has solution	not integral
			2	88	no solution (integral)	integral
			2	89/90	has solution	not integral
			3	89	no solution (integral)	integral
			3	90/91	has solution	not integral
3	17	64	1	66	no solution (integral)	integral
			1	67/68	has solution	not integral
			2	68	no solution (integral)	integral
			2	69/70	has solution	not integral
3	65519	16	1	26	no solution (integral)	integral
			1	27/28	has solution	not integral

4 Applications on GMiMC

In Sect. 4.1, we show integral distinguishers for GMiMC-erf using the automatic search model constructed in Sect. 3. By applying a linear transformation to the inputs of GMiMC-crf, we can adopt the same model to search for distinguishers. We also apply the Computation-Traceback-Determine framework to construct models for GMiMC-nyb and -mrf in Sect. 4.2.

4.1 Integral Distinguishers for GMiMC-erf and -crf

Detailed results of GMiMC-erf and comparisons. Since we focus on the security of GMiMC used as a block cipher, we only involve integral distinguishers constructed for this setting here. We show the comparison between the number of

rounds covered by our new found integral distinguishers and those given by [5,10] in Figure 1. As results, for variants with large primes, one can use our method to obtain the best distinguishers that cover more rounds than previous works. For variants using small primes, although we cannot detect better distinguishers, our distinguishers need relatively small data and time complexities compared to [10].

Meanwhile, to stress the necessity of taking exact coefficients of monomials into consideration, we also give the number of rounds covered by distinguishers that are detected by only focusing on the maximal degree. To be more specific, these distinguishers are constructed following the way similar with that used in [5]. We take all possible values for the leftmost s branches, thus, one can add $(n-s)$ rounds before without any costs.. Since the maximal degree after R rounds is d^R which should be less than $s(p-1)$, we get $R = \lfloor \log_d(s(p-1)-1) \rfloor$. Then one can add $(n-1)$ rounds after using the linear relation [5, Proposition 3]. In total, these distinguishers cover $(n-s) + \lfloor \log_d(s(p-1)-1) \rfloor + (n-1)$ rounds. With the increase of s, the number of rounds covered by these distinguishers will be decreased, as shown in Figure 1. This confirmed that taking the exact coefficients of monomials into consideration indeed help to find better distinguishers.

Applying the same model to GMiMC-crf. For GMiMC-crf with n blocks, denote its whole input as $(X_1, X_2, \cdots, X_n)$. Let $\widehat{M}$ be a matrix. Denote $\widehat{M}_{i,j}$ as the element in its i-th row and j-th column, where $1 \leq i, j \leq n$. Then $\widehat{M}_{i,j} = 0$ if $i = j$; $\widehat{M}_{i,j} = 1$ if $i \neq j$. Let $(\widetilde{X}_1, \widetilde{X}_2, \cdots, \widetilde{X}_n)$ be n values, and

$$[\widetilde{X}_1 \ \widetilde{X}_2 \cdots \widetilde{X}_n] = [X_1 \ X_2 \cdots X_n] \cdot \widehat{M}.$$

Here, instead of traversing s blocks of $(X_1, X_2, \cdots, X_n)$, we consider traversing s blocks of $(\widetilde{X}_1, \widetilde{X}_2, \cdots, \widetilde{X}_n)$. To add $(n-s)$ rounds before, we traverse the leftmost s blocks, *i.e* $\widetilde{X}_i = x_i$ when $1 \leq i \leq s$, and $\widetilde{X}_j = c_j$ when $s+1 \leq j \leq n$. In this case, the output Z_r of S-Box in the r-th round will keep the same form as that in analyzing GMiMC-erf. One can take GMiMC-crf with $n = 4$, $s = 2$ and $R = 5$ as an example, which is depicted in Figure 8. Since all Z_r obey the same form, we can adopt the same model constructed for GMiMC-erf to find distinguishers of GMiMC-crf. As results, integral distinguishers we found for GMiMC-crf cover the same number of rounds with that of GMiMC-erf under the same parameters.

4.2 Search for Integral Distinguishers of GMiMC-nyb and -mrf

In this subsection, we follow the three-step framework to build the search model for GMiMC-nyb and -mrf. Assume that our aim is to find an R-round integral distinguisher for GMiMC-nyb/-mrf with $n = 2b$ blocks. Then there are b S-Boxes in each round. Denote these n inputs as $(X_1, X_2, X_3, X_4, \cdots, X_{2b-1}, X_{2b})$. For each $0 \leq i \leq b-1$ and $0 \leq r \leq R-1$, let rk_{rb+i} denote the sum of round key and round constants used before the i-th S-Box located in the r-th round. We use Z_{rb+i} to represent the state after the i-th S-Box in the r-th round.

In Phase I, according to whether X_j, $1 \le j \le 2b$, is traversed or not, W_{rb+i} is in the form of $x_{((2i+r) \bmod 2b)+1} + rk_{rb+i}$ or $c_{((2i+r) \bmod 2b)+1} + rk_{rb+i}$. Besides, when $r = 0$, we have $Z_i = W_i^d$ for all $0 \le i \le b-1$. When $r \ge 1$, with SageMath, one can derive the expression of each Z_{rb+i}, which follows the form:

$$Z_{rb+i} = \left(W_{rb+i} + Z_{j_1} + Z_{j_2} + \cdots + Z_{j_{rb+i}}\right)^d,$$

where $\{Z_{j_1}, Z_{j_2}, \cdots, Z_{j_{rb+i}}\}$ is a subset of $\{Z_{r'b+i} \mid 0 \le i \le b-1, r' \le r-1\}$. Each output after R rounds can be denoted as the sum of some Z_{rb+i} values. If all Z_{rb+i} values involved have the zero-sum integral property, we find an integral distinguisher covering R rounds. The remaining task here is to follow Phase II to derive the coefficient $\mathcal{A}$ of the monomial $\prod_{w=1}^{s} x_w^{p-1}$ for each Z_{rb+i}, and derive conditions to restrict $\mathcal{A} \neq 0 \pmod p$.

According to the form of Z_{rb+i} mentioned above, we find that each Z_{rb+i} also follows the same general form used in Sect. 3.2, which is

$$Z_{rb+i} = \left(W_{rb+i} + Z_0 + \cdots + Z_{rb+i-1}\right)^d.$$

Thus, one can get EQ, $\mathcal{C}$ and MQ according to Proposition 3 and 4. Automatic search model can then be built following Proposition 5. Meanwhile, one can use Type I/II/III conditions depicted in Phase III to require that $\mathcal{A} \neq 0 \pmod p$.

Notice that the difference between GMiMC-nyb and -mrf is the linear layer. This only affects the detailed expression of Z_{rb+i}, while does not affect the above mentioned general form. In other words, the same model can be adopted.

As results, we can gain much better distinguishers than [10] for both ciphers. We list these new found distinguishers in Figure 2, along with previous results. Our method gives the best integral distinguishers for both ciphers. To gain these distinguishers, we take all possible values of the leftmost branch, and use our model to detect the integral property. In this case, an extra round can be added before without any costs. To show the necessity of taking coefficients into consideration, we also give the trivial distinguisher that is built similarly, except that it only considers the maximal degree. The total round of such trivial distinguisher is $1 + \lfloor \log_d(p-2) \rfloor$.

5 Discussion on HADES Design

HADES [19] is a new design strategy proposed by Grassi *et al.* in EUROCRYPT 2020. Compared with SPN structure, it adopts two different round functions. A middle layer with PSPN rounds is surrounded by 2 outer layer of SPN rounds. Meanwhile, every round adopts a random MDS matrix applying on all blocks.

To demonstrate the generality of our proposed framework, we also apply it to two HADES designs: HadesMiMC and Poseidon2^π. Due to space limitations, detailed information is provided in Appendix F. As a result, we gain multiple distinguishers for HadesMiMC with $1 \le s \le n-1$. All of them are better than the trivial bounds obtained from the maximal degree estimation. However, they do not outperform the result in [5]. This stems from the exponential growth of

constraints caused by the MDS matrices used in full rounds, which makes the search model too large to be solved or even impossible to be built. We have to adopt a compromised way by limiting the number of full rounds on both sides. The usage of such full rounds at the beginning and end of HADES prevents the detection of integral properties covering more rounds. For Poseidon2$^\pi$, we also identify many new distinguishers that cover 1 more rounds than the trivial bound in most cases. Detailed results for these two ciphers are presented in Table 4 and 5, respectively. All these results serve as a supplementary evaluation of the security of the HADES designs.

6 Conclusion

To detect better integral properties for ciphers defined over $\mathbb{F}_p$, we introduce a new framework that takes exact coefficients of monomials into consideration. This framework consists of three phases. In the first two phases, the exact coefficient $\mathcal{A}$ of the target monomial $\prod_{w=1}^{s} x_w^{p-1}$ is represented as several sums $\mathcal{S}$ of multinomial coefficients under specific conditions MQ. If each $\mathcal{S} \equiv 0 \pmod{p}$ holds for all solutions of MQ, we have $\mathcal{A} \equiv 0 \pmod{p}$, and thus obtain the integral property. To achieve this, we construct a condition set BQ in the last phase. This set is constructed by adding all possible conditions whose opposite leads to $\mathcal{S} \equiv 0 \pmod{p}$. In this way, we can construct the automatic search model by searching a solution that satisfies both MQ and BQ. If no such solution exists, it means that for all possible solutions of MQ, there is at least one condition in BQ whose opposite will hold with probability one, thus $\mathcal{S} \equiv 0 \pmod{p}$ holds. Consequently, we obtain an integral distinguisher. The validity of our model is confirmed by performing experiments on GMiMC-erf with small primes. To further demonstrate the generality of the new framework, we also apply it to GMiMC-crf/-nyb/-mrf, as well as two HADES designs including HadesMiMC and Poseidon2$^\pi$. As a result, we achieve numerous new distinguishers for these two families of ciphers.

References

1. Albrecht, M.R., Cid, C., Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C., Schofnegger, M.: Algebraic cryptanalysis of stark-friendly designs: Application to marvellous and mimc. In: ASIACRYPT 2019. Lecture Notes in Computer Science, vol. 11923, pp. 371–397. Springer (2019). https://doi.org/10.1007/978-3-030-34618-8_13, https://doi.org/10.1007/978-3-030-34618-8_13
2. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for mpc, and more. In: ESORICS 2019. Lecture Notes in Computer Science, vol. 11736, pp. 151–171. Springer (2019). https://doi.org/10.1007/978-3-030-29962-0_8, https://doi.org/10.1007/978-3-030-29962-0_8
3. Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: Mimc: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In: ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031, pp. 191–219

(2016). https://doi.org/10.1007/978-3-662-53887-6_7, https://doi.org/10.1007/978-3-662-53887-6_7
4. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of symmetric-key primitives for advanced cryptographic protocols. IACR Trans. Symmetric Cryptol. **2020**(3), 1–45 (2020). https://doi.org/10.13154/tosc.v2020.i3.1-45, https://doi.org/10.13154/tosc.v2020.i3.1-45
5. Beyne, T., Canteaut, A., Dinur, I., Eichlseder, M., Leander, G., Leurent, G., Naya-Plasencia, M., Perrin, L., Sasaki, Y., Todo, Y., Wiemer, F.: Out of oddity - new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12172, pp. 299–328. Springer (2020). https://doi.org/10.1007/978-3-030-56877-1_11, https://doi.org/10.1007/978-3-030-56877-1_11
6. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: CRYPTO '90. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990). https://doi.org/10.1007/3-540-38424-3_1, https://doi.org/10.1007/3-540-38424-3_1
7. Bonnetain, X.: Collisions on feistel-MiMC and univariate GMiMC. Cryptology ePrint Archive, Paper 2019/951 (2019), https://eprint.iacr.org/2019/951
8. Bouvier, C., Canteaut, A., Perrin, L.: On the algebraic degree of iterated power functions. Des. Codes Cryptogr. **91**(3), 997–1033 (2023). https://doi.org/10.1007/S10623-022-01136-X, https://doi.org/10.1007/s10623-022-01136-x
9. Chao, C., Zhang, M.: On multinomial coefficients modulo a prime. Eur. J. Comb. **9**(1), 23–26 (1988). https://doi.org/10.1016/S0195-6698(88)80022-2, https://doi.org/10.1016/S0195-6698(88)80022-2
10. Chen, S., Guo, C., Guo, J., Liu, L., Wang, M., Wei, P., Xu, Z.: Towards the links of cryptanalytic methods on mpc/fhe/zk-friendly symmetric-key primitives. IACR Trans. Symmetric Cryptol. **2023**(2), 132–175 (2023). https://doi.org/10.46586/TOSC.V2023.I2.132-175, https://doi.org/10.46586/tosc.v2023.i2.132-175
11. Cui, J., Hu, K., Wang, M., Wei, P.: On the field-based division property: Applications to mimc, feistel mimc and gmimc. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13793, pp. 241–270. Springer (2022). https://doi.org/10.1007/978-3-031-22969-5_9, https://doi.org/10.1007/978-3-031-22969-5_9
12. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher square. In: Biham, E. (ed.) Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings. Lecture Notes in Computer Science, vol. 1267, pp. 149–165. Springer (1997). https://doi.org/10.1007/BFB0052343, https://doi.org/10.1007/BFb0052343
13. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer (2002)
14. Eichlseder, M., Grassi, L., Lüftenegger, R., Øygarden, M., Rechberger, C., Schofnegger, M., Wang, Q.: An algebraic attack on ciphers with low-degree round functions: Application to full mimc. In: ASIACRYPT 2020. Lecture Notes in Computer Science, vol. 12491, pp. 477–506. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_16, https://doi.org/10.1007/978-3-030-64837-4_16

15. Grassi, L.: Bounded surjective quadratic functions over fnp for mpc-/zk-/fhe-friendly symmetric primitives. IACR Trans. Symmetric Cryptol. **2023**(2), 94–131 (2023). https://doi.org/10.46586/TOSC.V2023.I2.94-131, https://doi.org/10.46586/tosc.v2023.i2.94-131
16. Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., Schofnegger, M.: Poseidon: A new hash function for zero-knowledge proof systems. In: Bailey, M.D., Greenstadt, R. (eds.) 30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021. pp. 519–535. USENIX Association (2021), https://www.usenix.org/conference/usenixsecurity21/presentation/grassi
17. Grassi, L., Khovratovich, D., Schofnegger, M.: Poseidon2: A faster version of the poseidon hash function. In: Mrabet, N.E., Feo, L.D., Duquesne, S. (eds.) Progress in Cryptology - AFRICACRYPT 2023 - 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21, 2023, Proceedings. Lecture Notes in Computer Science, vol. 14064, pp. 177–203. Springer (2023). https://doi.org/10.1007/978-3-031-37679-5_8, https://doi.org/10.1007/978-3-031-37679-5_8
18. Grassi, L., Khovratovich, D., Schofnegger, M.: Poseidon2: A faster version of the poseidon hash function. Cryptology ePrint Archive, Paper 2023/323 (2023), https://eprint.iacr.org/2023/323
19. Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D., Schofnegger, M.: On a generalization of substitution-permutation networks: The HADES design strategy. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 674–704. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_23, https://doi.org/10.1007/978-3-030-45724-2_23
20. Grassi, L., Onofri, S., Pedicini, M., Sozzi, L.: Invertible quadratic non-linear layers for mpc-/fhe-/zk-friendly schemes over fnp application to poseidon. IACR Trans. Symmetric Cryptol. **2022**(3), 20–72 (2022). https://doi.org/10.46586/TOSC.V2022.I3.20-72, https://doi.org/10.46586/tosc.v2022.i3.20-72
21. Grassi, L., Rechberger, C., Schofnegger, M.: Weak linear layers in word-oriented partial SPN and hades-like ciphers. IACR Cryptol. ePrint Arch. p. 500 (2020), https://eprint.iacr.org/2020/500
22. Hu, K., Sun, S., Todo, Y., Wang, M., Wang, Q.: Massive superpoly recovery with nested monomial predictions. In: ASIACRYPT 2021. Lecture Notes in Computer Science, vol. 13090, pp. 392–421. Springer (2021). https://doi.org/10.1007/978-3-030-92062-3_14, https://doi.org/10.1007/978-3-030-92062-3_14
23. Hu, K., Sun, S., Wang, M., Wang, Q.: An algebraic formulation of the division property: Revisiting degree evaluations, cube attacks, and key-independent sums. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 446–476. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_15, https://doi.org/10.1007/978-3-030-64837-4_15
24. Knudsen, L.R., Wagner, D.A.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers. Lecture Notes in Computer Science, vol. 2365, pp. 112–127. Springer (2002). https://doi.org/10.1007/3-540-45661-9_9, https://doi.org/10.1007/3-540-45661-9_9
25. Liu, F., Anand, R., Wang, L., Meier, W., Isobe, T.: Coefficient grouping: Breaking chaghri and more. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory

and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 287–317. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_10, https://doi.org/10.1007/978-3-031-30634-1_10
26. Liu, F., Grassi, L., Bouvier, C., Meier, W., Isobe, T.: Coefficient grouping for complex affine layers. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III. Lecture Notes in Computer Science, vol. 14083, pp. 540–572. Springer (2023). https://doi.org/10.1007/978-3-031-38548-3_18, https://doi.org/10.1007/978-3-031-38548-3_18
27. Matsui, M.: Linear cryptanalysis method for DES cipher. In: EUROCRYPT '93. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993). https://doi.org/10.1007/3-540-48285-7_33, https://doi.org/10.1007/3-540-48285-7_33
28. Meštrović, R.: Lucas' theorem: its generalizations, extensions and applications (1878–2014) (2014), https://arxiv.org/abs/1409.3820
29. NIST, Dworkin, M.J.: Sha-3 standard: Permutation-based hash and extendable-output functions (2015-08-04 00:08:00 2015). https://doi.org/https://doi.org/10.6028/NIST.FIPS.202, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919061
30. Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., Win, E.D.: The cipher SHARK. In: Gollmann, D. (ed.) Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings. Lecture Notes in Computer Science, vol. 1039, pp. 99–111. Springer (1996). https://doi.org/10.1007/3-540-60865-6_47, https://doi.org/10.1007/3-540-60865-6_47
31. Todo, Y.: Structural evaluation by generalized integral property. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 287–314. Springer (2015). https://doi.org/10.1007/978-3-662-46800-5_12, https://doi.org/10.1007/978-3-662-46800-5_12
32. Todo, Y., Morii, M.: Bit-based division property and application to simon family. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 357–377. Springer (2016). https://doi.org/10.1007/978-3-662-52993-5_18, https://doi.org/10.1007/978-3-662-52993-5_18
33. Wang, W., Tang, D., Wang, H.: Inner product masked integral distinguishers and integral sets over large finite fields. IACR Cryptol. ePrint Arch. p. 1872 (2023), https://eprint.iacr.org/2023/1872
34. Xiang, Z., Zhang, W., Bao, Z., Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 648–678 (2016). https://doi.org/10.1007/978-3-662-53887-6_24, https://doi.org/10.1007/978-3-662-53887-6_24

A Structure of GMiMC-crf, -nyb and -mrf

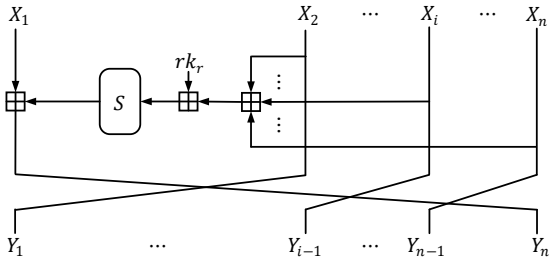


Fig. 5: Structure of GMiMC-crf

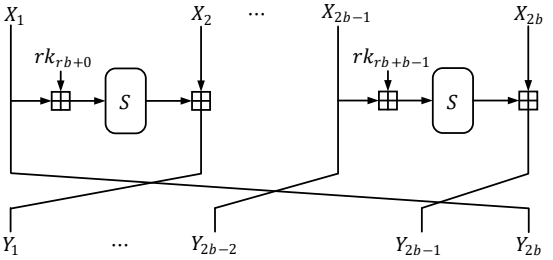


Fig. 6: Structure of GMiMC-nyb

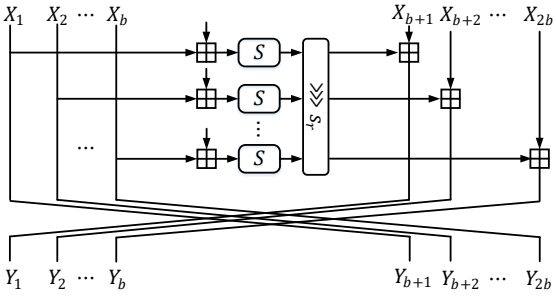


Fig. 7: Structure of GMiMC-mrf. Rotation number s_r is different in each round.

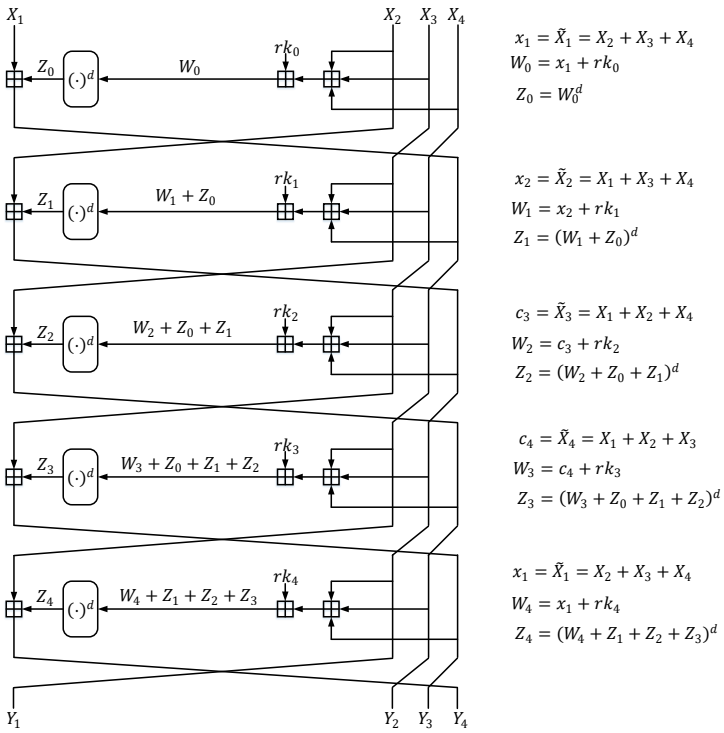


Fig. 8: A toy example of GMiMC-crf with $n = 4$, $s = 2$ and $R = 5$

B Lucas Theorem

Let $\binom{a}{b}$ denote the number of ways to select b elements from a set of a distinct elements without considering the order, and it equals $\frac{a!}{b!(a-b)!}$. Let $\begin{bmatrix} a \\ b_1, b_2, \cdots, b_h \end{bmatrix}$ be the following multinomial coefficient, where $a = \sum_{j=1}^{h} b_j$:

$$\begin{bmatrix} a \\ b_1, b_2, \cdots, b_h \end{bmatrix} = \frac{a!}{b_1! b_2! \cdots b_h!}.$$

In Combinations and Number Theory, one can use Lucas Theorem and its extensions [9,28] to compute $\binom{a}{b} \bmod p$ and $\begin{bmatrix} a \\ b_1, b_2, \cdots, b_h \end{bmatrix} \bmod p$, which are shown in Lemma 2 and 3, respectively.

Lemma 2 *For binomial coefficients $\binom{a}{b}$, denote a and b in base p form:*

$$\begin{aligned} a =& a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n \\ b =& b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n, \end{aligned}$$

where $0 \le a_i, b_i \le p-1$ *for* $0 \le i \le n$. *We have*

$$\binom{a}{b} \equiv \prod_{i=0}^{n} \binom{a_i}{b_i} \pmod{p},$$

where $\binom{a_i}{b_i}$ *is defined as 0 when* $b_i > a_i$.

Lemma 3 *For multinomial coefficients* $\left[\begin{smallmatrix} a \\ b_1, b_2, \cdots, b_h \end{smallmatrix}\right]$ *where* $a = \sum_{j=1}^{h} b_j$, *denote* a *and* b_j *in base* p *form as:*

$$\begin{aligned} a =& a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n \\ b_j =& b_{j0} + b_{j1} p + b_{j2} p^2 + \cdots + b_{jn} p^n, \ \forall 1 \le j \le h, \end{aligned}$$

where $0 \le a_i, b_{ji} \le p-1$. *If* $a_i = \sum_{j=1}^{h} b_{ji}$ *holds for any* $0 \le i \le n$, *we have* $\left[\begin{smallmatrix} a \\ b_1, b_2, \cdots, b_h \end{smallmatrix}\right] \neq 0 \pmod{p}$*; otherwise, it equals to* $0 \bmod p$.

C Examples of Type II/III Conditions used in Phase III

For the toy GMiMC depicted in Figure 4,

$$\begin{aligned} \mathcal{S} =& \sum_{\substack{EQ \\ \forall 0 \le r \le 4,\ \mathcal{D}(v_r) = \widetilde{v_r}}} \mathcal{C} \\ \equiv& \sum_{\substack{v_4 + u_{41} + u_{42} + u_{43} = d \\ v_3 + u_{30} + u_{31} + u_{32} = d \cdot u_{43} \\ v_2 + u_{20} + u_{21} = d \cdot (u_{32} + u_{42}) \\ v_1 + u_{10} = d \cdot (u_{21} + u_{31} + u_{41}) \\ v_0 = d \cdot (u_{10} + u_{20} + u_{30}) \\ \forall 0 \le r \le 4,\ \mathcal{D}(v_r) = \widetilde{v_r}}} \begin{bmatrix} d \\ v_4, \cdots, u_{43} \end{bmatrix} \begin{bmatrix} d \cdot u_{43} \\ v_3, \cdots, u_{32} \end{bmatrix} \begin{bmatrix} d \cdot (u_{32} + u_{42}) \\ v_2, u_{20}, u_{21} \end{bmatrix} \begin{bmatrix} d \cdot (u_{21} + u_{31} + u_{41}) \\ v_1, u_{10} \end{bmatrix}. \end{aligned}$$

Example 3. We focus on the sum:

$$\widehat{\mathcal{C}}_{I,1} = \sum_{\substack{v_1 + u_{10} = d \cdot (u_{21} + u_{31} + u_{41}) \\ v_0 = d \cdot u_{10} + d \cdot (u_{20} + u_{30}) \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r \in \{0,1\}}} \begin{bmatrix} d \cdot (u_{21} + u_{31} + u_{41}) \\ v_1, u_{10} \end{bmatrix}.$$

Notice that the relation between $\mathcal{S}$ and $\widehat{\mathcal{C}}_{I,1}$ is

$$\mathcal{S} = \sum_{\widehat{EQ}_1} \begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} \begin{bmatrix} d \cdot u_{43} \\ v_3, u_{30}, u_{31}, u_{32} \end{bmatrix} \begin{bmatrix} d \cdot (u_{32} + u_{42}) \\ v_2, u_{20}, u_{21} \end{bmatrix} \widehat{\mathcal{C}}_{I,1},$$

where $\widehat{EQ}_1$ is

$$\begin{cases} v_4 + u_{41} + u_{42} + u_{43} = d \\ v_3 + u_{30} + u_{31} + u_{32} = d \cdot u_{43} \\ v_2 + u_{20} + u_{21} = d \cdot (u_{32} + u_{42}) \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r \in \{2,3,4\}. \end{cases}$$

So if $\widehat{\mathcal{C}}_{I,1} \equiv 0 \pmod{p}$ holds for all solutions of $\widehat{EQ}_1$, we get $\mathcal{S} \equiv 0 \pmod{p}$.

Example 4. We study this sum:

$$\widehat{\mathcal{C}}_{I,2} = \sum_{\substack{v_2+u_{20}=(d\cdot(u_{32}+u_{42})-u_{21}) \\ v_0=d\cdot u_{20}+d\cdot(u_{10}+u_{30}) \\ \mathcal{D}(v_r)=\widetilde{v_r},\ r\in\{0,2\}}} \begin{bmatrix} d\cdot(u_{32}+u_{42})-u_{21} \\ v_2, u_{20} \end{bmatrix}.$$

In this case, $\mathcal{S}$ can be computed as

$$\mathcal{S} = \sum_{u_{21}} \left(\begin{pmatrix} d\cdot(u_{32}+u_{42}) \\ u_{21} \end{pmatrix} \cdot \sum_{\widehat{EQ}_2} \left(\widehat{U}_2 \cdot \widehat{\mathcal{C}}_{I,2} \right) \right),$$

where

$$\widehat{U}_2 = \begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} \begin{bmatrix} d\cdot u_{43} \\ v_3, u_{30}, u_{31}, u_{32} \end{bmatrix} \begin{bmatrix} d\cdot(u_{21}+u_{31}+u_{41}) \\ v_1, u_{10} \end{bmatrix}$$

and $\widehat{EQ}_2$ is

$$\begin{cases} v_4+u_{41}+u_{42}+u_{43} = d \\ v_3+u_{30}+u_{31}+u_{32} = d\cdot u_{43} \\ v_1+u_{10} = d\cdot(u_{21}+u_{31}+u_{41}) \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r\in\{1,3,4\}. \end{cases}$$

Thus, $\mathcal{S}\equiv 0 \pmod p$ if $\widehat{\mathcal{C}}_{I,2}\equiv 0 \pmod p$ holds for all u_{21} and $\widehat{EQ}_2$.

Example 5. Let's focus on the sum when $r=1$ and $q=2$.

$$\widehat{\mathcal{C}}_{II,1,2} = \sum_{\substack{v_3+u_{30}=d\cdot u_{43}-u_{31}-u_{32} \\ v_1+u_{10}=d\cdot(u_{21}+u_{31}+u_{41}) \\ v_0=d\cdot(u_{10}+u_{30})+d\cdot u_{20} \\ \mathcal{D}(v_r)=\widetilde{v_r},\ r\in\{0,1,3\}}} \begin{bmatrix} d\cdot u_{43}-u_{31}-u_{32} \\ v_3, u_{30} \end{bmatrix} \begin{bmatrix} d\cdot(u_{21}+u_{31}+u_{41}) \\ v_1, u_{10} \end{bmatrix}.$$

Denote $\widehat{EQ}$ as

$$\begin{cases} v_4+u_{41}+u_{42}+u_{43} = d \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r\in\{4\} \end{cases}$$

and

$$\widetilde{\mathcal{C}}_1 = \sum_{\substack{v_3+u_{30}+u_{31}+u_{32}=d\cdot u_{43} \\ v_2+u_{20}+u_{21}=d\cdot(u_{32}+u_{42}) \\ v_1+u_{10}=d\cdot(u_{21}+u_{31}+u_{41}) \\ v_0=d\cdot(u_{10}+u_{20}+u_{30}) \\ \forall 0\le r\le 3,\ \mathcal{D}(v_r)=\widetilde{v_r}}} \begin{bmatrix} d\cdot u_{43} \\ v_3, \cdots, u_{32} \end{bmatrix} \begin{bmatrix} d\cdot(u_{32}+u_{42}) \\ v_2, u_{20}, u_{21} \end{bmatrix} \begin{bmatrix} d\cdot(u_{21}+u_{31}+u_{41}) \\ v_1, u_{10} \end{bmatrix}.$$

One can represent $\mathcal{S}$ as

$$\mathcal{S} = \sum_{\widehat{EQ}} \left(\begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} \cdot \widetilde{\mathcal{C}}_1 \right).$$

Denote $\widehat{EQ}'$ as

$$\begin{cases} v_2 + u_{20} + u_{21} = d \cdot (u_{32} + u_{42}) \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r \in \{2\} \end{cases}.$$

Then we can represent $\widetilde{\mathcal{C}}_1$ as

$$\widetilde{\mathcal{C}}_1 = \sum_{u_{31}, u_{32}} \left(\binom{d \cdot u_{43}}{u_{32}} \binom{d \cdot u_{43} - u_{32}}{u_{31}} \cdot \sum_{\widehat{EQ}'} \left(\begin{bmatrix} d \cdot (u_{32} + u_{42}) \\ v_2, u_{20}, u_{21} \end{bmatrix} \cdot \widehat{\mathcal{C}}_{II,1,2} \right) \right).$$

Thus, if $\widehat{\mathcal{C}}_{II,1,2} \equiv 0 \pmod{p}$ holds for all u_{31}, u_{32} and $\widehat{EQ}'$, $\mathcal{S} \equiv 0 \pmod{p}$.

Example 6. Let's study the sum when $r = 2$ and $q = 1$.

$$\widehat{\mathcal{C}}_{II,2,1} = \sum_{\substack{v_3 + u_{30} + u_{31} = d \cdot u_{43} - u_{32} \\ v_2 + u_{20} + u_{21} = d \cdot (u_{32} + u_{42}) \\ v_0 = d \cdot (u_{20} + u_{30}) + d \cdot u_{10} \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r \in \{0,2,3\} \\ u_{31} + u_{21} = \hat{u}_{321}}} \begin{bmatrix} d \cdot u_{43} - u_{32} \\ v_3, u_{30}, u_{31} \end{bmatrix} \begin{bmatrix} d \cdot (u_{32} + u_{42}) \\ v_2, u_{20}, u_{21} \end{bmatrix}.$$

Under the same $\widehat{EQ}$ and $\widetilde{\mathcal{C}}_1$ as those in Example 5, we can represent $\mathcal{S}$ as

$$\mathcal{S} = \sum_{\widehat{EQ}} \left(\begin{bmatrix} d \\ v_4, u_{41}, u_{42}, u_{43} \end{bmatrix} \cdot \widetilde{\mathcal{C}}_1 \right).$$

Denote $\widehat{EQ}'$ as

$$\begin{cases} v_1 + u_{10} = d \cdot (\hat{u}_{321} + u_{41}) \\ \mathcal{D}(v_r) = \widetilde{v_r},\ r \in \{1\} \end{cases}.$$

Then we have

$$\widetilde{\mathcal{C}}_1 = \sum_{u_{32}, \hat{u}_{321}} \left(\binom{d \cdot u_{43}}{u_{32}} \cdot \sum_{\widehat{EQ}'} \left(\begin{bmatrix} d \cdot (\hat{u}_{321} + u_{41}) \\ v_1, u_{10} \end{bmatrix} \cdot \widehat{\mathcal{C}}_{II,2,1} \right) \right).$$

If $\widehat{\mathcal{C}}_{II,2,1} \equiv 0 \pmod{p}$ holds for all u_{32}, $\hat{u}_{321}$ and $\widehat{EQ}'$, $\mathcal{S} \equiv 0 \pmod{p}$.

D Deriving Equations for Type II/III Conditions

Derive equations for $\widehat{\mathcal{C}}_{II,1,q} \neq 0 \pmod{p}$. Recall that

$$\widehat{\mathcal{C}}_{II,1,q} = \sum_{\substack{v_{1+q} + u_{1+q,0} = m_1 \\ v_1 + u_{10} = m_2 \\ v_0 = d \cdot (u_{10} + u_{1+q,0}) + m_3 \\ \mathcal{D}(v_i) = \widetilde{v_i},\ i \in \{0,1,1+q\}}} \begin{bmatrix} m_1 \\ v_{1+q}, u_{1+q,0} \end{bmatrix} \begin{bmatrix} m_2 \\ v_1, u_{10} \end{bmatrix}.$$

If Z_0 doesn't consist of Z_{1+q}, the value $u_{1+q,0}$ is always 0. Thus, $\widehat{\mathcal{C}}_{II,1,q}$ becomes

$$\sum_{\substack{v_{1+q}=m_1\\ \mathcal{D}(v_{1+q})=\widetilde{v}_{1+q}}} \sum_{\substack{v_1+u_{10}=m_2\\ v_0=d\cdot u_{10}+m_3\\ \mathcal{D}(v_i)=\widetilde{v}_i,\, i\in\{0,1\}}} \begin{bmatrix} m_2 \\ v_1, u_{10} \end{bmatrix} = \sum_{\substack{v_1+u_{10}=m_2\\ v_0=d\cdot u_{10}+m_3\\ \mathcal{D}(v_i)=\widetilde{v}_i,\, i\in\{0,1\}}} \begin{bmatrix} m_2 \\ v_1, u_{10} \end{bmatrix}$$

when $\mathcal{D}(m_1) = \widetilde{v}_{1+q}$. Note that this sum is in the form of $\widehat{\mathcal{C}}_{I,1}$, thus can be converted to T_1, T_2, T_3 and T_4 under different conditions, as discussed in Sect. 3.3. Similarly, if Z_0 is not contained in Z_1, we can also convert it to these T_i sums.

Let's see what happens if the above cases don't occur. According to

$$\begin{cases} v_{1+q} + u_{1+q,0} = m_1 \\ v_1 + u_{10} = m_2 \\ v_0 = d\cdot(u_{10} + u_{1+q,0}) + m_3 \\ \mathcal{D}(v_i) = \widetilde{v}_i,\ i \in \{0, 1, 1+q\}, \end{cases}$$

we have $v_0 = d(m_1 + m_2) - d(v_1 + v_{1+q}) + m_3$. Since $\mathcal{D}(v_0) = \widetilde{v}_0$, we obtain that

(1) when $\widetilde{v}_0 = 0$, we get $v_1 + v_{1+q} = m_1 + m_2 + \frac{m_3}{d}$.
(2) when $\widetilde{v}_0 = p-1$,

$$v_1+v_{1+q} \le m_1+m_2+\frac{m_3-(p-1)}{d} \text{ and } p-1 \mid d(m_1+m_2)+m_3-d(v_1+v_{1+q}).$$

(3) when $1 \le \widetilde{v}_0 \le p-2$,

$$v_1 + v_{1+q} = m_1 + m_2 + \frac{m_3 - \widetilde{v}_0}{d}$$

or

$$v_1+v_{1+q} \le m_1+m_2+\frac{m_3-\widetilde{v}_0-(p-1)}{d},\ p-1 \mid d(m_1+m_2)+m_3-\widetilde{v}_0-d(v_1+v_{1+q}).$$

With a similar way as shown in Sect. 3.3, we can discuss each possible values of $\widetilde{v}_0$, $\widetilde{v}_1$ and $\widetilde{v}_{1+q}$, respectively. Detailed results are shown in Table 2. All cases should fulfill that $p-1 \mid d(m_1+m_2)+m_3-d(\widetilde{v}_1+\widetilde{v}_{1+q})-\widetilde{v}_0$. We denote T_5, T_6, T_7 and T_8 as follows, which are used in this table. Note that one can also use Proposition 6 to 9 to derive equations for $T_i \neq 0 \pmod p$ when $5 \le i \le 8$, since they obey a similar form as T_1 to T_4.

$$T_5 = \sum_{k_2=1}^{\lfloor \frac{m_1}{p-1} \rfloor} \binom{m_1}{k_2(p-1)}, \qquad T_6 = \sum_{k_2=1}^{\lfloor \frac{m_1}{p-1} \rfloor - 1} \binom{m_1}{k_2(p-1)},$$

$$T_7 = \sum_{k_2=0}^{\lfloor \frac{m_1-\widetilde{v}_{1+q}}{p-1} \rfloor} \binom{m_1}{\widetilde{v}_{1+q}+k_2(p-1)}, \quad T_8 = \sum_{k_2=0}^{\lfloor \frac{m_1-\widetilde{v}_r}{p-1} \rfloor - 1} \binom{m_1}{\widetilde{v}_{1+q}+k_2(p-1)}.$$

Table 2: Equivalence of $\widehat{\mathcal{C}}_{II,1,q} \neq 0 \pmod p$ used in Type III conditions

$\widetilde{v}_0$	$\widetilde{v}_1$	$\widetilde{v}_{1+q}$	Preconditions	Equivalence
0	any	any	Covered by Type I conditions	
≥ 1	0	0	Covered by Type I conditions	
≥ 1	0	$p-1$	$dm_2 + m_3 - \widetilde{v}_0 \geq p-1$ $dm_2 + m_3 - \widetilde{v}_0 \leq p-2$	$T_5 \neq 0$ $T_6 \neq 0$
≥ 1	0	$[1,\ p-2]$	$dm_2 + m_3 - \widetilde{v}_0 \geq p-1$ $dm_2 + m_3 - \widetilde{v}_0 \leq p-2$	$T_7 \neq 0$ $T_8 \neq 0$
≥ 1	$p-1$	0	$dm_1 + m_3 - \widetilde{v}_0 \geq p-1$ $dm_1 + m_3 - \widetilde{v}_0 \leq p-2$	$T_1 \neq 0$ $T_2 \neq 0$
≥ 1	$p-1$	$p-1$	$m_3 - \widetilde{v}_0 \geq p-1$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \leq p-2$ † $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \geq p-1$	$T_1 \neq 0$ and $T_5 \neq 0$ $T_2 \neq 0$ or $T_6 \neq 0$ $T_1 \neq 0$ and $T_5 \neq 0$
≥ 1	$p-1$	$[1,\ p-2]$	$m_3 - \widetilde{v}_0 \geq p-1$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \leq p-2$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \geq p-1$	$T_1 \neq 0$ and $T_7 \neq 0$ $T_2 \neq 0$ or $T_8 \neq 0$ $T_1 \neq 0$ and $T_7 \neq 0$
≥ 1	$[1,\ p-2]$	0	$dm_1 + m_3 - \widetilde{v}_0 \geq p-1$ $dm_1 + m_3 - \widetilde{v}_0 \leq p-2$	$T_3 \neq 0$ $T_4 \neq 0$
≥ 1	$[1,\ p-2]$	$p-1$	$m_3 - \widetilde{v}_0 \geq p-1$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \leq p-2$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \geq p-1$	$T_3 \neq 0$ and $T_5 \neq 0$ $T_4 \neq 0$ or $T_6 \neq 0$ $T_3 \neq 0$ and $T_5 \neq 0$
≥ 1	$[1,\ p-2]$	$[1,\ p-2]$	$m_3 - \widetilde{v}_0 \geq p-1$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \leq p-2$ $m_3 - \widetilde{v}_0 \leq p-2,\ f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) \geq p-1$	$T_3 \neq 0$ and $T_7 \neq 0$ $T_4 \neq 0$ or $T_8 \neq 0$ $T_3 \neq 0$ and $T_7 \neq 0$

† $f(m_1, m_2, \widetilde{v}_1, \widetilde{v}_{1+q}) = (m_1 - \widetilde{v}_{1+q}) \pmod{(p-1)} + (m_2 - \widetilde{v}_1) \pmod{(p-1)}$.

We show more details when $\widetilde{v}_0 = p-1$, $\widetilde{v}_1 = p-1$ and $\widetilde{v}_{1+q} = p-1$. From

$$\begin{cases} v_1 = k_1(p-1),\ k_1 \geq 1;\ v_1 \leq m_2; \\ v_{1+q} = k_2(p-1),\ k_2 \geq 1;\ v_{1+q} \leq m_1; \\ v_1 + v_{1+q} \leq m_1 + m_2 + \dfrac{m_3 - (p-1)}{d}; \\ p-1 \mid d(m_1+m_2) + m_3 - d(v_1 + v_{1+q}), \end{cases}$$

we obtain that

$$1 \leq k_1 \leq \left\lfloor \frac{m_2}{p-1} \right\rfloor,\ 1 \leq k_2 \leq \left\lfloor \frac{m_1}{p-1} \right\rfloor,\ k_1 + k_2 \leq \left\lfloor \frac{m_1+m_2}{p-1} + \frac{m_3-(p-1)}{d(p-1)} \right\rfloor.$$

(1) if $m_3 \geq p-1$, we get $k_1 + k_2 \leq \left\lfloor \frac{m_1+m_2}{p-1} \right\rfloor$. Since

$$\left\lfloor \frac{m_1+m_2}{p-1} \right\rfloor \geq \left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor,$$

we can obtain that $k_1 + k_2 \leq \left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor$. Therefore, $\widehat{\mathcal{C}}_{II,1,q}$ equals

$$\sum_{1 \leq k_1 \leq \lfloor \frac{m_2}{p-1} \rfloor} \binom{m_2}{k_1(p-1)} \cdot \sum_{1 \leq k_2 \leq \lfloor \frac{m_1}{p-1} \rfloor} \binom{m_1}{k_2(p-1)} = T_1 \cdot T_5.$$

To ensure $\widehat{\mathcal{C}}_{II,1,q} \neq 0 \pmod p$, we have $T_1 \neq 0 \pmod p$ and $T_5 \neq 0 \pmod p$.

(2) if $m_3 \leq p-2$, we get $k_1 + k_2 \leq \left\lfloor \frac{m_1+m_2}{p-1} \right\rfloor - 1$. Notice that

$$\left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor - 1 \leq \left\lfloor \frac{m_1+m_2}{p-1} \right\rfloor - 1 \leq \left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor.$$

(2.1) when $m_1 \pmod{(p-1)} + m_2 \pmod{(p-1)} \leq p-2$, we get

$$\left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor - 1 = \left\lfloor \frac{m_1+m_2}{p-1} \right\rfloor - 1.$$

Thus, $k_1 + k_2 \leq \left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor - 1$. In this case, $\widehat{\mathcal{C}}_{II,1,q}$ equals

$$\sum_{\substack{1 \leq k_1 \leq \lfloor \frac{m_2}{p-1} \rfloor \\ 1 \leq k_2 \leq \lfloor \frac{m_1}{p-1} \rfloor \\ k_1+k_2 \leq \lfloor \frac{m_1}{p-1} \rfloor + \lfloor \frac{m_2}{p-1} \rfloor - 1}} \binom{m_2}{k_1(p-1)} \binom{m_1}{k_2(p-1)}.$$

It can be represented as $(T_2 + \mathcal{C}_A)(T_6 + \mathcal{C}_B) - \mathcal{C}_A\mathcal{C}_B$, where

$$\mathcal{C}_A = \binom{m_2}{\left\lfloor \frac{m_2}{p-1} \right\rfloor (p-1)},\ \mathcal{C}_B = \binom{m_1}{\left\lfloor \frac{m_1}{p-1} \right\rfloor (p-1)}.$$

If $T_2 \equiv 0 \pmod{p}$ and $T_6 \equiv 0 \pmod{p}$, we get $\widehat{\mathcal{C}}_{II,1,q} \equiv 0 \pmod{p}$. Due to the principle of constructing the condition set BQ, we require that at least one of $T_2 \neq 0 \pmod{p}$ and $T_6 \neq 0 \pmod{p}$ hold.

(2.2) when $m_1 \pmod{(p-1)} + m_2 \pmod{(p-1)} \geq p-1$, we get

$$\left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor = \left\lfloor \frac{m_1+m_2}{p-1} \right\rfloor - 1.$$

Thus, $k_1 + k_2 \leq \left\lfloor \frac{m_1}{p-1} \right\rfloor + \left\lfloor \frac{m_2}{p-1} \right\rfloor$. Hence, it equals $T_1 \cdot T_5$. So we require that $T_1 \neq 0 \pmod{p}$ and $T_5 \neq 0 \pmod{p}$.

Derive equations for $\widehat{\mathcal{C}}_{II,r,q} \neq 0 \pmod{p}$. In real applications, expressions of Z_r and Z_{r+q} are various, which make the discussion here more complicated. Without loss of generality, we denote

$$Z_r = (W_r + \delta_r \cdot Z_0 + Z_{a_1} + Z_{a_2} + \cdots + Z_{a_{j_r}})^d$$

and

$$Z_{r+q} = (W_{r+q} + \delta_{r+q} \cdot Z_0 + Z_{b_1} + Z_{b_2} + \cdots + Z_{b_{j_{r+q}}})^d,$$

where δ_r and δ_{r+q} are defined as:

$$\delta_r = \begin{cases} 1, \text{ if } Z_0 \text{ is contained in } Z_r \\ 0, \text{ otherwise} \end{cases}, \ \delta_{r+q} = \begin{cases} 1, \text{ if } Z_0 \text{ is contained in } Z_{r+q} \\ 0, \text{ otherwise} \end{cases}.$$

Denote J as $\{a_1, a_2, \cdots, a_{j_r}\} \bigcap \{b_1, b_2, \cdots, b_{j_{r+q}}\}$, and denote its length as $|J|$.

(1) when $\delta_r = 1$ and $\delta_{r+q} = 1$:

(1.1) when $|J| = 0$, the sum $\widehat{\mathcal{C}}_{II,r,q}$ can be represented as

$$\sum_{\widetilde{EQ}} \begin{bmatrix} m_1 - (u_{r+q,b_1} + \cdots + u_{r+q,b_{j_{r+q}}}) \\ v_{r+q}, u_{r+q,0} \end{bmatrix} \begin{bmatrix} m_2 - (u_{r,a_1} + \cdots + u_{r,a_{j_r}}) \\ v_r, u_{r,0} \end{bmatrix},$$

where $\widetilde{EQ}$ is

$$\begin{cases} v_{r+q} + u_{r+q,0} = m_1 - (u_{r+q,b_1} + \cdots + u_{r+q,b_{j_{r+q}}}) \\ v_r + u_{r,0} = m_2 - (u_{r,a_1} + \cdots + u_{r,a_{j_r}}) \\ v_0 = d \cdot (u_{r+q,0} + u_{r,0}) + m_3 \\ \mathcal{D}(v_i) = \widetilde{v}_i, \ i \in \{0, r, r+q\}. \end{cases}$$

In this case, the sum is in a similar form as $\widehat{\mathcal{C}}_{II,1,q}$. Thus, we can follow Table 2 to get corresponding conditions.

(1.2) when $|J| = 1$, assume that $a_1 = b_1 = a$. Then we can represent $\widehat{\mathcal{C}}_{II,r,q}$ as

$$\sum_{\widetilde{EQ}} \begin{bmatrix} m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) \\ v_{r+q}, u_{r+q,0}, u_{r+q,a} \end{bmatrix} \begin{bmatrix} m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) \\ v_r, u_{r,0}, u_{r,a} \end{bmatrix},$$

where $\widetilde{EQ}$ is

$$\begin{cases} v_{r+q} + u_{r+q,0} + u_{r+q,a} = m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) \\ v_r + u_{r,0} + u_{r,a} = m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) \\ v_0 = d \cdot (u_{r+q,0} + u_{r,0}) + m_3 \\ \mathcal{D}(v_i) = \widetilde{v}_i, \ i \in \{0, r, r+q\} \\ u_{r+q,a} + u_{r,a} = \widehat{u}_{r+q,r,a}. \end{cases}$$

We consider two different cases here. The first one is checking each sum under every possible values of u_{r+q} and u_r, and the second one is checking that under every possible v_{r+q} and v_r. For the first case, under each u_{r+q} and u_r, we get

$$\sum_{\widetilde{EQ}'} \begin{bmatrix} m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) - u_{r+q,a} \\ v_{r+q}, u_{r+q,0} \end{bmatrix} \begin{bmatrix} m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) - u_{r,a} \\ v_r, u_{r,0} \end{bmatrix},$$

where $\widetilde{EQ}'$ is

$$\begin{cases} v_{r+q} + u_{r+q,0} = m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) - u_{r+q,a} \\ v_r + u_{r,0} = m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) - u_{r,a} \\ v_0 = d \cdot (u_{r+q,0} + u_{r,0}) + m_3 \\ \mathcal{D}(v_i) = \widetilde{v}_i, \ i \in \{0, r, r+q\}. \end{cases}$$

This is in a similar form with $\widehat{\mathcal{C}}_{II,1,q}$. For the second case, under each v_{r+q} and v_r, we have

$$\sum_{\widetilde{EQ}'} \begin{bmatrix} m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) - v_{r+q} \\ u_{r+q,0}, u_{r+q,a} \end{bmatrix} \begin{bmatrix} m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) - v_r \\ u_{r,0}, u_{r,a} \end{bmatrix},$$

where $\widetilde{EQ}'$ is

$$\begin{cases} u_{r+q,0} + u_{r+q,a} = m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) - v_{r+q} \\ u_{r,0} + u_{r,a} = m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) - v_r \\ v_0 = d \cdot (u_{r+q,0} + u_{r,0}) + m_3 \\ \mathcal{D}(v_i) = \widetilde{v}_i, \ i \in \{0\} \\ u_{r+q,a} + u_{r,a} = \widehat{u}_{r+q,r,a}. \end{cases}$$

Denote

$$m_1' = m_1 - (u_{r+q,b_2} + \cdots + u_{r+q,b_{j_{r+q}}}) - v_{r+q},\ m_2' = m_2 - (u_{r,a_2} + \cdots + u_{r,a_{j_r}}) - v_r.$$

We can represent above sum as

$$\sum_{\mathcal{D}\left(d(m_1'+m_2')+m_3-d\cdot\widehat{u}_{r+q,r,a}\right)=\widetilde{v}_0} \sum_{\substack{u_{r+q,0}+u_{r+q,a}=m_1' \\ u_{r,0}+u_{r,a}=m_2' \\ u_{r+q,a}+u_{r,a}=\widehat{u}_{r+q,r,a}}} \binom{m_1'}{u_{r+q,a}} \binom{m_2'}{u_{r,a}}.$$

With Vandermonde's Convolution Formula, it equals

$$\sum_{\mathcal{D}\left(d(m_1'+m_2')+m_3-d\cdot\widehat{u}_{r+q,r,a}\right)=\widetilde{v}_0} \binom{m_1'+m_2'}{\widehat{u}_{r+q,r,a}}.$$

One can then use Lucas Theorem to deduce its conditions.

(1.3) when $|J| \geq 2$, we consider every subset of J with size 1. For each subset, we can follow the way shown in (1.2) to derive conditions. Besides, we consider two other cases. The first one is checking each sum under every possible $u_{r+q,0}$ and $u_{r,0}$, which is discussed in (2) shown below. The second case is checking each sum under every possible v_{r+q} and v_r. In this case, we will finally reach a sum which has a similar form with the last case in (1.2), and conditions can be derived with Lucas Theorem.

(2) when $\delta_r = 0$ or $\delta_{r+q} = 0$, $u_{r+q,0}$ or $u_{r,0}$ will always be 0, thus be fixed values. In this case, we can finally reach a sum which can be determined by Lucas Theorem. We take $J = \{a, b\}$, $\delta_r = 0 = \delta_{r+q}$ as an example, and assume that $a_1 = b_1 = a$, $a_2 = b_2 = b$. In this case, the sum $\widehat{\mathcal{C}}_{II,r,q}$ can be represented as

$$\sum_{\widetilde{EQ}} \begin{bmatrix} m_1' \\ u_{r+q,a}, u_{r+q,b} \end{bmatrix} \begin{bmatrix} m_2' \\ u_{r,a}, u_{r,b} \end{bmatrix},$$

where $\widetilde{EQ}$ is

$$\begin{cases} u_{r+q,a} + u_{r+q,b} = m_1' \\ u_{r,a} + u_{r,b} = m_2' \\ u_{r+q,a} + u_{r,a} = \widehat{u}_{r+q,r,a} \\ u_{r+q,b} + u_{r,b} = \widehat{u}_{r+q,r,b}. \end{cases}$$

and

$$m_1' = m_1 - (u_{r+q,b_3} + \cdots + u_{r+q,b_{j_{r+q}}}) - v_{r+q},\ m_2' = m_2 - (u_{r,a_1} + \cdots + u_{r,a_{j_r}}) - v_r.$$

Under the conditions $\widehat{u}_{r+q,r,a} \geq m_1'$, $\widehat{u}_{r+q,r,a} \geq m_2'$, $\widehat{u}_{r+q,r,b} \geq m_1'$ and $\widehat{u}_{r+q,r,b} \geq m_2'$, the above sum equals

$$\begin{bmatrix} m_1' + m_2' \\ \widehat{u}_{r+q,r,a}, \widehat{u}_{r+q,r,a} \end{bmatrix}.$$

One can then use Lucas Theorem to derive conditions.

E Proofs of Propositions Claimed in Section 3.3

To show their proofs, we need to introduce the following two lemmas.

Lemma 4 *For any $m \leq p^{L+1}-1$ where $L \geq 1$ and $p \geq 3$, we have*

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor} \binom{m}{k(p-1)} \equiv \sum_{\delta=1}^{L+1} \binom{t}{\delta(p-1)} \pmod{p}.$$

Here,

$$m = \widehat{m}_L \cdot p^L + \widehat{m}_{L-1} \cdot p^{L-1} + \cdots + \widehat{m}_1 \cdot p + \widehat{m}_0$$

and $t = \sum_{j=0}^{L} \widehat{m}_j$, as defined in Proposition 6.

Proof. Since $m \leq p^{L+1}-1$, we can get

$$\left\lfloor \frac{m}{p-1} \right\rfloor \leq p^L + p^{L-1} + \cdots + p + 1.$$

Therefore, the left part can be represented as

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor} \binom{m}{k(p-1)} = \sum_{k=1}^{p^L+\cdots+p+1} \binom{m}{k(p-1)} - \sum_{k=\lfloor \frac{m}{p-1} \rfloor+1}^{p^L+\cdots+p+1} \binom{m}{k(p-1)}.$$

When $k \geq \left\lfloor \frac{m}{p-1} \right\rfloor + 1$, we have $k(p-1) \geq \left\lfloor \frac{m}{p-1} \right\rfloor (p-1) + (p-1) > m$. Hence,

$$\sum_{k=\lfloor \frac{m}{p-1} \rfloor+1}^{p^L+\cdots+p+1} \binom{m}{k(p-1)} = 0.$$

When $1 \leq k \leq p^L + p^{L-1} + \cdots + p + 1$, we can obtain that

$$p-1 \leq k(p-1) \leq (p-1) \cdot p^L + (p-1) \cdot p^{L-1} + \cdots + (p-1).$$

Therefore, $k(p-1)$ can be represented as $\widehat{k}_L \cdot p^L + \widehat{k}_{L-1} \cdot p^{L-1} + \cdots + \widehat{k}_1 \cdot p + \widehat{k}_0$, where each $\widehat{k}_j \in \mathbb{F}_p$ for $1 \leq j \leq L$, and

$$\begin{cases} \widehat{k}_0 = p-1, \text{ if } \widehat{k}_L = \widehat{k}_{L-1} = \cdots = \widehat{k}_1 = 0; \\ \widehat{k}_0 \in \mathbb{F}_p, \text{ otherwise.} \end{cases}$$

Meanwhile, since $p-1 \mid k(p-1)$ and

$$\begin{aligned} &\widehat{k}_L \cdot p^L + \widehat{k}_{L-1} \cdot p^{L-1} + \cdots + \widehat{k}_1 \cdot p + \widehat{k}_0 \\ &\qquad = \left(\widehat{k}_L \cdot (p^L - 1) + \cdots + \widehat{k}_1 \cdot (p-1)\right) + \widehat{k}_L + \widehat{k}_{L-1} + \cdots + \widehat{k}_0, \end{aligned}$$

we can get $p-1 \mid \widehat{k}_L+\widehat{k}_{L-1}+\cdots+\widehat{k}_0$. In other words, $\widehat{k}_L+\widehat{k}_{L-1}+\cdots+\widehat{k}_0 = \delta(p-1)$ with $1 \le \delta \le L+1$ considering the range of each $\widehat{k}_j$.

Hence, we can divide $1 \le k \le p^L+\cdots+p+1$ into $(L+1)$ sets according to different values of the sum $\widehat{k}_L + \widehat{k}_{L-1} + \cdots + \widehat{k}_0$. Therefore,

$$
\begin{aligned}
&\sum_{k=1}^{p^L+\cdots+p+1} \binom{m}{k(p-1)} \\
\equiv &\sum_{\delta=1}^{L+1} \sum_{\widehat{k}_L+\widehat{k}_{L-1}+\cdots+\widehat{k}_0=\delta(p-1)} \binom{\widehat{m}_L \cdot p^L + \widehat{m}_{L-1} \cdot p^{L-1} + \cdots + \widehat{m}_1 \cdot p + \widehat{m}_0}{\widehat{k}_L \cdot p^L + \widehat{k}_{L-1} \cdot p^{L-1} + \cdots + \widehat{k}_1 \cdot p + \widehat{k}_0} \\
\equiv &\sum_{\delta=1}^{L+1} \sum_{\widehat{k}_L+\widehat{k}_{L-1}+\cdots+\widehat{k}_0=\delta(p-1)} \prod_{j=0}^{L} \binom{\widehat{m}_j}{\widehat{k}_j} \qquad \text{due to Lucas Theorem} \\
\equiv &\sum_{\delta=1}^{L+1} \binom{\widehat{m}_L + \widehat{m}_{L-1} + \cdots + \widehat{m}_1 + \widehat{m}_0}{\delta(p-1)},
\end{aligned}
$$

which then equals $\sum_{\delta=1}^{L+1} \binom{t}{\delta(p-1)}$. The last equality comes from Vandermonde's Convolution Formula. □

Lemma 5 *For any $1 \le \widetilde{v} \le p-2$ and $m \le p^{L+1}-1$ where $L \ge 1$ and $p \ge 3$, we have*

$$
\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor} \binom{m}{\widetilde{v}+k(p-1)} \equiv \sum_{\delta=0}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} \pmod{p}.
$$

Here, t follows the same definition as Proposition 6.

Proof. The left part can be represented as

$$
\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor} \binom{m}{\widetilde{v}+k(p-1)} = \sum_{k=0}^{p^L+\cdots+p+1} \binom{m}{\widetilde{v}+k(p-1)} - \sum_{k=\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor+1}^{p^L+\cdots+p+1} \binom{m}{\widetilde{v}+k(p-1)}.
$$

Let $m-\widetilde{v} = \alpha(p-1)+\beta$, where $\beta \le p-2$. Then $m = (p-1)\alpha + \widetilde{v} + \beta$. When $k \ge \left\lfloor \frac{m-\widetilde{v}}{p-1} \right\rfloor + 1$, we have

$$
k(p-1)+\widetilde{v} \ge \alpha(p-1)+(p-1)+\widetilde{v} > \alpha(p-1)+\beta+\widetilde{v} = m.
$$

Hence, the second term is always 0. When $0 \le k \le p^L+\cdots+p+1$, we get $k(p-1)+\widetilde{v} \ge \widetilde{v}$ and

$$
k(p-1)+\widetilde{v} \le m \le p^{L+1}-1 = (p-1)p^L + \cdots + (p-1)p + (p-1).
$$

In other words, we can represent $k(p-1)+\widetilde{v}$ as

$$
k(p-1)+\widetilde{v} = \widehat{k}_L \cdot p^L + \widehat{k}_{L-1} \cdot p^{L-1} + \cdots + \widehat{k}_1 \cdot p + \widehat{k}_0,
$$

where $\widehat{k}_j \in \mathbb{F}_p$ for $1 \le j \le L$ and

$$\begin{cases} \widehat{k}_0 = \widetilde{v}, \text{ if } \widehat{k}_L = \widehat{k}_{L-1} = \cdots = \widehat{k}_1 = 0; \\ \widehat{k}_0 \in \mathbb{F}_p, \text{ otherwise.} \end{cases}$$

Thus, $k(p-1) = \widehat{k}_L \cdot p^L + \widehat{k}_{L-1} \cdot p^{L-1} + \cdots + \widehat{k}_1 \cdot p + (\widehat{k}_0 - \widetilde{v})$. Since $p-1 \mid k(p-1)$, we can obtain that $p-1 \mid \widehat{k}_L + \widehat{k}_{L-1} + \cdots + \widehat{k}_1 + (\widehat{k}_0 - \widetilde{v})$. In other words, $\widehat{k}_L + \widehat{k}_{L-1} + \cdots + \widehat{k}_1 + (\widehat{k}_0 - \widetilde{v}) = \delta(p-1)$ with $0 \le \delta \le L$. Hence,

$$\begin{aligned} &\sum_{k=0}^{p^L+\cdots+p+1} \binom{m}{\widetilde{v} + k(p-1)} \\ \equiv &\sum_{\delta=0}^{L} \sum_{\widehat{k}_L + \widehat{k}_{L-1} + \cdots + \widehat{k}_1 + (\widehat{k}_0 - \widetilde{v}) = \delta(p-1)} \binom{\widehat{m}_L \cdot p^L + \widehat{m}_{L-1} \cdot p^{L-1} + \cdots + \widehat{m}_1 \cdot p + \widehat{m}_0}{\widehat{k}_L \cdot p^L + \widehat{k}_{L-1} \cdot p^{L-1} + \cdots + \widehat{k}_1 \cdot p + \widehat{k}_0} \\ \equiv &\sum_{\delta=0}^{L} \sum_{\widehat{k}_L + \widehat{k}_{L-1} + \cdots + \widehat{k}_1 + (\widehat{k}_0 - \widetilde{v}) = \delta(p-1)} \prod_{j=0}^{L} \binom{\widehat{m}_j}{\widehat{k}_j} \\ \equiv &\sum_{\delta=0}^{L} \binom{\widehat{m}_L + \widehat{m}_{L-1} + \cdots + \widehat{m}_1 + \widehat{m}_0}{\delta(p-1) + \widetilde{v}}, \end{aligned}$$

which equals $\sum_{\delta=0}^{L} \binom{t}{\delta(p-1)+\widetilde{v}}$ since $t = \widehat{m}_L + \widehat{m}_{L-1} + \cdots + \widehat{m}_1 + \widehat{m}_0$. □

Proposition 10. *(Rephrase of Proposition 6) For any $m \le p^{L+1} - 1$ where $L \ge 1$ and $p \ge 3$, if $m \ge p-1$ and $L \le p-1$, one can obtain that*

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor} \binom{m}{k(p-1)} \neq 0 \pmod{p}$$

if and only if

$$\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p) \right) \bmod p = p-1,$$

Here, t follows the same definition as Proposition 6.

Proof. Due to Lemma 4,

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor} \binom{m}{k(p-1)} \neq 0 \pmod{p}$$

is equivalent to

$$\sum_{\delta=1}^{L+1} \binom{t}{\delta(p-1)} \neq 0 \pmod{p}.$$

Since $L \le p-1$, we know that $\delta \le L+1 \le p$. Then $\delta(p-1)$ can be represented in base p form: $(\delta-1)p+(p-\delta)$, where $0 \le \delta-1 \le L$ and $p-L \le p-\delta \le p-1$. According to Lucas Theorem depicted in Lemma 2, the left part equals

$$\sum_{\delta=1}^{L+1} \binom{\left\lfloor \frac{t}{p} \right\rfloor}{\delta-1} \binom{t \bmod p}{p-\delta} = \sum_{\delta=1}^{p} \binom{\left\lfloor \frac{t}{p} \right\rfloor}{\delta-1} \binom{t \bmod p}{p-\delta} - \sum_{\delta=L+2}^{p} \binom{\left\lfloor \frac{t}{p} \right\rfloor}{\delta-1} \binom{t \bmod p}{p-\delta}.$$

When $\delta \ge L+2$, we have $\delta-1 \ge L+1$. Meanwhile, since $t \le (L+1)(p-1) = Lp+(p-1)-L$ where $L \le p-1$, the maximal value of $\left\lfloor \frac{t}{p} \right\rfloor$ is L. Thus, the binomial coefficient $\binom{\left\lfloor \frac{t}{p} \right\rfloor}{\delta-1}$ is always 0 when $\delta \ge L+2$. This leads to

$$\sum_{\delta=1}^{L+1} \binom{\left\lfloor \frac{t}{p} \right\rfloor}{\delta-1} \binom{t \bmod p}{p-\delta} = \sum_{\delta=1}^{p} \binom{\left\lfloor \frac{t}{p} \right\rfloor}{\delta-1} \binom{t \bmod p}{p-\delta} - 0 = \binom{\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)}{p-1}.$$

Due to Lucas Theorem, only when

$$\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p) \right) \bmod p = p-1,$$

the above binomial coefficient is not 0 mod p. □

Proposition 11. *(Rephrase of Proposition 7) For any $m \le p^{L+1}-1$ where $L \ge 1$ and $p \ge 3$, if $m \ge p-1$ and $L \le p-1$, one can obtain that*

$$\sum_{k=1}^{\left\lfloor \frac{m}{p-1} \right\rfloor - 1} \binom{m}{k(p-1)} \neq 0 \pmod p$$

if and only if one of following conditions holds:

(1) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p) \right) \bmod p = p-1$, $\widehat{m}_0 < (t \bmod (p-1))$.

(2) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p) \right) \bmod p = p-1$, $(t \bmod (p-1)) \notin \{\widehat{m}_0, 0\}$, and $\widehat{m}_0 \ge \max\{(t \bmod (p-1)), 2\}$.

(3) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p) \right) \bmod p \le p-2$, $\widehat{m}_0 \ge (t \bmod (p-1))$.

Here, t follows the same definition as Proposition 6.

Proof. According to the proof of Proposition 10, we can obtain that

$$\sum_{k=1}^{\left\lfloor \frac{m}{p-1} \right\rfloor} \binom{m}{k(p-1)} \equiv \binom{\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)}{p-1} \pmod p.$$

Hence,

$$\begin{aligned} \sum_{k=1}^{\left\lfloor \frac{m}{p-1} \right\rfloor - 1} \binom{m}{k(p-1)} &\equiv \sum_{k=1}^{\left\lfloor \frac{m}{p-1} \right\rfloor} \binom{m}{k(p-1)} - \binom{m}{\left\lfloor \frac{m}{p-1} \right\rfloor (p-1)} \pmod p \\ &\equiv \binom{\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)}{p-1} - \binom{m}{\left\lfloor \frac{m}{p-1} \right\rfloor (p-1)} \pmod p. \end{aligned}$$

Therefore,

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor - 1} \binom{m}{k(p-1)} \neq 0 \pmod{p}$$

is equivalent with

$$\binom{\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)}{p-1} \neq \binom{m}{\left\lfloor \frac{m}{p-1} \right\rfloor (p-1)} \pmod{p}.$$

The left binomial coefficient is 1 when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p = p-1$, and it equals 0 if $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \leq p-2$. While for the right binomial coefficient, let's first check the term $\left\lfloor \frac{m}{p-1} \right\rfloor (p-1)$. Recall that

$$m = \widehat{m}_L \cdot p^L + \widehat{m}_{L-1} \cdot p^{L-1} + \cdots + \widehat{m}_1 \cdot p + \widehat{m}_0$$

and

$$\left\lfloor \frac{m}{p-1} \right\rfloor = \widehat{m}_L \cdot (p^{L-1} + \cdots + p + 1) + \widehat{m}_{L-1} \cdot (p^{L-2} + \cdots + p + 1) + \cdots + \widehat{m}_1 + \left\lfloor \frac{\widehat{m}_L + \widehat{m}_{L-1} + \cdots + \widehat{m}_0}{p-1} \right\rfloor.$$

Thus,

$$\begin{aligned}
\left\lfloor \frac{m}{p-1} \right\rfloor (p-1) =& \widehat{m}_L(p^L - 1) + \widehat{m}_{L-1}(p^{L-1} - 1) + \cdots + \widehat{m}_1(p-1) + \left\lfloor \frac{t}{p-1} \right\rfloor (p-1) \\
=& \widehat{m}_L \cdot p^L + \cdots + \widehat{m}_1 \cdot p + \left(\widehat{m}_0 - t + \left\lfloor \frac{t}{p-1} \right\rfloor (p-1) \right) \\
=& \widehat{m}_L \cdot p^L + \cdots + \widehat{m}_1 \cdot p + \left(\widehat{m}_0 - (t \bmod (p-1)) \right).
\end{aligned}$$

If $\widehat{m}_0 \geq (t \bmod (p-1))$, we obtain that

$$\binom{m}{\left\lfloor \frac{m}{p-1} \right\rfloor (p-1)} \equiv \binom{\widehat{m}_0}{\widehat{m}_0 - (t \bmod (p-1))}.$$

If $\widehat{m}_0 < (t \bmod (p-1))$, there is at least one $\widehat{m}_j \geq 1$ where $1 \leq j \leq L$, since in this case $\widehat{m}_0 \neq p-1$. Without loss of generality, we assume that there is only one $\widehat{m}_j \geq 1$. In this case,

$$\binom{m}{\left\lfloor \frac{m}{p-1} \right\rfloor (p-1)} \equiv \binom{\widehat{m}_j}{\widehat{m}_j - 1} \binom{\widehat{m}_0}{p + \widehat{m}_0 - (t \bmod (p-1))}.$$

Notice that $2 + \widehat{m}_0 \leq p + \widehat{m}_0 - (t \bmod (p-1)) \leq p-1$. Thus,

$$\binom{\widehat{m}_0}{p + \widehat{m}_0 - (t \bmod (p-1))} = 0$$

will always hold.

Now, we can discuss each case one-by-one.

(1) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p = p-1$ and $\widehat{m}_0 < (t \bmod (p-1))$, the left binomial coefficient equals 1 while the right one is 0, thus the target sum

$$\sum_{k=1}^{\lfloor \frac{m}{p-1} \rfloor - 1} \binom{m}{k(p-1)} \neq 0 \pmod p.$$

(2) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p = p-1$ and $\widehat{m}_0 \geq (t \bmod (p-1))$, the target sum equals

$$1 - \binom{\widehat{m}_0}{\widehat{m}_0 - (t \bmod (p-1))}.$$

When $\widehat{m}_0 \leq 1$, it equals 0. When $\widehat{m}_0 \geq 2$, if $(t \bmod (p-1)) \in \{0, \widehat{m}_0\}$, it is 0; otherwise, it is not. In other words, only when $\widehat{m}_0 \geq 2$ and $(t \bmod (p-1)) \notin \{0, \widehat{m}_0\}$, the target sum is not 0.

(3) when $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \leq p-2$, the left binomial coefficient is 0. So only if $\widehat{m}_0 \geq (t \bmod (p-1))$, the target sum is not 0. □

Proposition 12. *(Rephrase of Proposition 8) For any $1 \leq \widetilde{v} \leq p-2$ and $m \leq p^{L+1} - 1$ where $L \geq 1$ and $p \geq 3$, if $m \geq p-1$ and $L \leq p-1$,*

$$\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor} \binom{m}{\widetilde{v} + k(p-1)} \neq 0 \pmod p$$

if and only if one of the following conditions holds:

(1) when $L \leq \widetilde{v}$, $\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \geq \widetilde{v}$.

(2) when $L \geq \widetilde{v}+1$ and $\left\lfloor \frac{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{p} \right\rfloor = 0$,

$$\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \geq \widetilde{v}.$$

(3) when $L \geq \widetilde{v}+1$ and $\left\lfloor \frac{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{p} \right\rfloor = 1$,

$$\left(\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p\right) + 1 \geq \widetilde{v}.$$

Here, t follows the same definition as Proposition 6.

Proof. Due to Lemma 5,

$$\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor} \binom{m}{\widetilde{v}+k(p-1)} \neq 0 \pmod{p}$$

is equivalent to

$$\sum_{\delta=0}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} \neq 0 \pmod{p}.$$

(1) Let's first focus on the case when $L \leq \widetilde{v}$.
Since $\widetilde{v}-\delta \geq \widetilde{v}-L \geq 0$ and $\widetilde{v}-\delta \leq \widetilde{v} \leq p-2$,

$$\sum_{\delta=0}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} = \sum_{\delta=0}^{L} \binom{t}{\delta p+(\widetilde{v}-\delta)} = \sum_{\delta=0}^{L} \binom{\lfloor \frac{t}{p} \rfloor}{\delta} \binom{t \bmod p}{\widetilde{v}-\delta}$$

according to Lucas Theorem. Thus,

$$\begin{aligned}\sum_{\delta=0}^{L} \binom{\lfloor \frac{t}{p} \rfloor}{\delta} \binom{t \bmod p}{\widetilde{v}-\delta} &= \sum_{\delta=0}^{\widetilde{v}} \binom{\lfloor \frac{t}{p} \rfloor}{\delta} \binom{t \bmod p}{\widetilde{v}-\delta} - \sum_{\delta=L+1}^{\widetilde{v}} \binom{\lfloor \frac{t}{p} \rfloor}{\delta} \binom{t \bmod p}{\widetilde{v}-\delta} \\ &= \binom{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{\widetilde{v}} - \sum_{\delta=L+1}^{\widetilde{v}} \binom{\lfloor \frac{t}{p} \rfloor}{\delta} \binom{t \bmod p}{\widetilde{v}-\delta}.\end{aligned}$$

When $\delta \geq L+1$, to ensure that the second term in above not be 0, we have to require that $\lfloor \frac{t}{p} \rfloor \geq L+1$. However, the maximal value of t is $(L+1)(p-1)$, which leads to $\lfloor \frac{t}{p} \rfloor \leq L$. Hence, the second term in the above is always 0. In this case, the target sum equals

$$\binom{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{\widetilde{v}},$$

which is not 0 mod p if and only if $\left(\lfloor \frac{t}{p} \rfloor + (t \bmod p)\right) \bmod p \geq \widetilde{v}$.

(2) Now, we check the case when $L \geq \widetilde{v}+1$.

$$\begin{aligned}\sum_{\delta=0}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} &= \sum_{\delta=0}^{\widetilde{v}} \binom{t}{\widetilde{v}+\delta(p-1)} + \sum_{\delta=\widetilde{v}+1}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} \\ &= \sum_{\delta=0}^{\widetilde{v}} \binom{t}{\delta p+(\widetilde{v}-\delta)} + \sum_{\delta=\widetilde{v}+1}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} \\ &= \sum_{\delta=0}^{\widetilde{v}} \binom{\lfloor \frac{t}{p} \rfloor}{\delta} \binom{t \bmod p}{\widetilde{v}-\delta} + \sum_{\delta=\widetilde{v}+1}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} \\ &= \binom{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{\widetilde{v}} + \sum_{\delta=\widetilde{v}+1}^{L} \binom{t}{\widetilde{v}+\delta(p-1)}.\end{aligned}$$

For the second term in the above sum, we can represent it as

$$\sum_{\delta=\widetilde{v}+1}^{L}\binom{t}{\widetilde{v}+\delta(p-1)}=\sum_{\delta=\widetilde{v}+1}^{L}\binom{t}{(\delta-1)p+(p+\widetilde{v}-\delta)},$$

where $\widetilde{v}\le\delta-1\le L-1\le p-2$ and

$$\begin{aligned}p+\widetilde{v}-\delta\le&p+\widetilde{v}-(\widetilde{v}+1)=p-1,\\ p+\widetilde{v}-\delta\ge&p+\widetilde{v}-L\ge p+1-L\ge p+1-(p-1)=2.\end{aligned}$$

Thus, one can use Lucas Theorem and get

$$\sum_{\delta=\widetilde{v}+1}^{L}\binom{t}{\widetilde{v}+\delta(p-1)}=\sum_{\delta=\widetilde{v}+1}^{L}\binom{\lfloor\frac{t}{p}\rfloor}{\delta-1}\binom{t\bmod p}{p+\widetilde{v}-\delta},$$

which then equals

$$\sum_{\delta=1}^{p+\widetilde{v}}\binom{\lfloor\frac{t}{p}\rfloor}{\delta-1}\binom{t\bmod p}{p+\widetilde{v}-\delta}-\sum_{\delta=1}^{\widetilde{v}}\binom{\lfloor\frac{t}{p}\rfloor}{\delta-1}\binom{t\bmod p}{p+\widetilde{v}-\delta}-\sum_{\delta=L+1}^{p+\widetilde{v}}\binom{\lfloor\frac{t}{p}\rfloor}{\delta-1}\binom{t\bmod p}{p+\widetilde{v}-\delta}.$$

The first term in the above expression is

$$\binom{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{p-1+\widetilde{v}}.$$

When $\delta\le\widetilde{v}$, we get $p+\widetilde{v}-\delta\ge p$, thus the second term is always 0.
When $\delta\ge L+1$, to ensure $\binom{\lfloor\frac{t}{p}\rfloor}{\delta-1}\neq 0$, we have $\lfloor\frac{t}{p}\rfloor\ge\delta-1\ge L$. Recall that the maximal value of t is $(L+1)(p-1)$, which equals $Lp+(p-1-L)$. Thus, we only need to consider the case when $\lfloor\frac{t}{p}\rfloor=L$. In this case, $t\bmod p\le p-1-L$. Since $p+\widetilde{v}-\delta=p+\widetilde{v}-L\ge p+1-L$, we get $\binom{t\bmod p}{p+\widetilde{v}-\delta}=0$, which indicates that the third term is always 0. Therefore, when $L\ge\widetilde{v}+1$,

$$\begin{aligned}&\sum_{\delta=0}^{L}\binom{t}{\widetilde{v}+\delta(p-1)}=\binom{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{\widetilde{v}}+\binom{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{p-1+\widetilde{v}}\\ =&\binom{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{\widetilde{v}}+\binom{\lfloor\frac{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{p}\rfloor}{1}\binom{\left(\lfloor\frac{t}{p}\rfloor+(t\bmod p)\right)\bmod p}{\widetilde{v}-1}.\end{aligned}$$

(2.1) when $\left\lfloor\frac{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{p}\right\rfloor=0$, we have

$$\sum_{\delta=0}^{L}\binom{t}{\widetilde{v}+\delta(p-1)}=\binom{\lfloor\frac{t}{p}\rfloor+(t\bmod p)}{\widetilde{v}}.$$

Hence, if and only if

$$\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p \geq \widetilde{v},$$

one can see the target sum is not 0.

(2.2) when $\left\lfloor \frac{\lfloor \frac{t}{p} \rfloor + (t \bmod p)}{p} \right\rfloor = 1$, we have

$$\sum_{\delta=0}^{L} \binom{t}{\widetilde{v} + \delta(p-1)} = \binom{\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p + 1}{\widetilde{v}}.$$

Thus, under the condition

$$\left(\left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)\right) \bmod p + 1 \geq \widetilde{v},$$

the target sum is not 0. □

Proposition 13. *(Rephrase of Proposition 9) For any $1 \leq \widetilde{v} \leq p-2$ and $m \leq p^{L+1} - 1$ where $L \geq 1$ and $p \geq 3$, $m \geq p-1$ and $L \leq p-1$, to require*

$$\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor - 1} \binom{m}{\widetilde{v} + k(p-1)} \neq 0 \pmod{p},$$

we add following conditions to the condition set BQ:

(1) $(\mathcal{B}_3 \vee \mathcal{B}_4 \vee \mathcal{B}_5 \vee \mathcal{B}_6) \wedge \mathcal{B}_9$
(2) $(\mathcal{B}_1 \vee \mathcal{B}_2 \vee \mathcal{B}_7) \wedge \mathcal{B}_8$
(3) $(\mathcal{B}_1 \vee \mathcal{B}_2) \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{10} \vee \mathcal{B}_{11}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18})$
(4) $(\mathcal{B}_1 \vee \mathcal{B}_2) \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{12} \vee \mathcal{B}_{13}) \wedge (\mathcal{B}_{14} \vee \mathcal{B}_{15} \vee \mathcal{B}_{16})$
(5) $(\mathcal{B}_1 \vee \mathcal{B}_2) \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{12} \vee \mathcal{B}_{13}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18}) \wedge \{\widehat{m}_0 \neq (\widehat{t} \bmod p)\}$
(6) $\mathcal{B}_7 \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{19} \vee \mathcal{B}_{20}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18})$
(7) $\mathcal{B}_7 \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{21} \vee \mathcal{B}_{22}) \wedge (\mathcal{B}_{14} \vee \mathcal{B}_{15} \vee \mathcal{B}_{16})$
(8) $\mathcal{B}_7 \wedge \mathcal{B}_9 \wedge (\mathcal{B}_{21} \vee \mathcal{B}_{22}) \wedge (\mathcal{B}_{17} \vee \mathcal{B}_{18}) \vee \{\widehat{m}_0 \neq (\widehat{t} \bmod p+1)\}$,

where conditions $\mathcal{B}_i$ are depicted in Table 3, $\widehat{t} = \left\lfloor \frac{t}{p} \right\rfloor + (t \bmod p)$, and t follows the same definition as Proposition 6.

Proof. We only need to show what we claimed in Table 3 is correct.

Due to Lemma 5, we have

$$\begin{aligned}\sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor - 1} \binom{m}{\widetilde{v} + k(p-1)} &= \sum_{k=0}^{\lfloor \frac{m-\widetilde{v}}{p-1} \rfloor} \binom{m}{\widetilde{v} + k(p-1)} - \binom{m}{\widetilde{v} + \left\lfloor \frac{m-\widetilde{v}}{p-1} \right\rfloor (p-1)} \\ &= \sum_{\delta=0}^{L} \binom{t}{\widetilde{v} + \delta(p-1)} - \binom{m}{\widetilde{v} + \left\lfloor \frac{m-\widetilde{v}}{p-1} \right\rfloor (p-1)}.\end{aligned}$$

Table 3: Condition $\mathcal{B}_i$ used in Proposition 9 (13)

	Detailed Conditions	Under $\mathcal{B}_i$, we obtain
$\mathcal{B}_1$	$L \leq \widetilde{v}$, $\widehat{t} \bmod p \geq \widetilde{v}$	$\mathcal{C}_{Left} = \binom{\widehat{t} \bmod p}{\widetilde{v}}$
$\mathcal{B}_2$	$L \geq \widetilde{v}+1$, $\left\lfloor \frac{\widehat{t}}{p} \right\rfloor = 0$, $\widehat{t} \bmod p \geq \widetilde{v}$	
$\mathcal{B}_3$	$L \leq \widetilde{v}$, $\widehat{t} \bmod p \leq \widetilde{v}-1$	$\mathcal{C}_{Left} = 0$
$\mathcal{B}_4$	$L \geq \widetilde{v}+1$, $\left\lfloor \frac{\widehat{t}}{p} \right\rfloor = 0$, $\widehat{t} \bmod p \leq \widetilde{v}-1$	
$\mathcal{B}_5$	$L \geq \widetilde{v}+1$, $\left\lfloor \frac{\widehat{t}}{p} \right\rfloor = 1$, $\widehat{t} \bmod p \leq \widetilde{v}-2$	
$\mathcal{B}_6$	$L \geq \widetilde{v}+1$, $\left\lfloor \frac{\widehat{t}}{p} \right\rfloor = 1$, $\widehat{t} \bmod p = p-1$	
$\mathcal{B}_7$	$L \geq \widetilde{v}+1$, $\left\lfloor \frac{\widehat{t}}{p} \right\rfloor = 1$, $\widetilde{v}-1 \leq \widehat{t} \bmod p \leq p-2$	$\mathcal{C}_{Left} = \binom{\widehat{t} \bmod p+1}{\widetilde{v}}$
$\mathcal{B}_8$	$\widehat{m}_0 < ((t-\widetilde{v}) \bmod (p-1))$	$\mathcal{C}_{Right} = 0$
$\mathcal{B}_9$	$\widehat{m}_0 \geq ((t-\widetilde{v}) \bmod (p-1))$	$\mathcal{C}_{Right} = \binom{\widehat{m}_0}{(t-\widetilde{v}) \bmod (p-1)}$
$\mathcal{B}_{10}$	$\widehat{t} \bmod p = 1$, $\widehat{t} \bmod p \geq \widetilde{v}$	$\binom{\widehat{t} \bmod p}{\widetilde{v}} = 1$
$\mathcal{B}_{11}$	$\widehat{t} \bmod p \geq 2$, $\widehat{t} \bmod p = \widetilde{v}$	
$\mathcal{B}_{12}$	$\widehat{t} \bmod p \geq 2$, $\widetilde{v} = 1$	$\binom{\widehat{t} \bmod p}{\widetilde{v}} = \widehat{t} \bmod p$
$\mathcal{B}_{13}$	$\widehat{t} \bmod p \geq 2$, $\widetilde{v} = \widehat{t} \bmod p - 1$	
$\mathcal{B}_{14}$	$\widehat{m}_0 \geq ((t-\widetilde{v}) \bmod (p-1))$, $\widehat{m}_0 \leq 1$	$\binom{\widehat{m}_0}{(t-\widetilde{v}) \bmod (p-1)} = 1$
$\mathcal{B}_{15}$	$\widehat{m}_0 \geq 2$, $(t-\widetilde{v}) \bmod (p-1) = 0$	
$\mathcal{B}_{16}$	$\widehat{m}_0 \geq 2$, $(t-\widetilde{v}) \bmod (p-1) = \widehat{m}_0$	
$\mathcal{B}_{17}$	$\widehat{m}_0 \geq 2$, $(t-\widetilde{v}) \bmod (p-1) = 1$	$\binom{\widehat{m}_0}{(t-\widetilde{v}) \bmod (p-1)} = \widehat{m}_0$
$\mathcal{B}_{18}$	$\widehat{m}_0 \geq 2$, $(t-\widetilde{v}) \bmod (p-1) = \widehat{m}_0 - 1$	
$\mathcal{B}_{19}$	$\widehat{t} \bmod p = 0$, $\widehat{t} \bmod p + 1 \geq \widehat{v}$	$\binom{\widehat{t} \bmod p+1}{\widetilde{v}} = 1$
$\mathcal{B}_{20}$	$\widehat{t} \bmod p \geq 1$, $\widehat{t} \bmod p + 1 = \widetilde{v}$	
$\mathcal{B}_{21}$	$\widehat{t} \bmod p \geq 1$, $\widetilde{v} = 1$	$\binom{\widehat{t} \bmod p+1}{\widetilde{v}} = \widehat{t} \bmod p + 1$
$\mathcal{B}_{22}$	$\widehat{t} \bmod p \geq 1$, $\widehat{t} \bmod p = \widetilde{v}$	

Hence, it's equivalent to check under what condition

$$\sum_{\delta=0}^{L} \binom{t}{\widetilde{v}+\delta(p-1)} \neq \binom{m}{\widetilde{v}+\left\lfloor \frac{m-\widetilde{v}}{p-1} \right\rfloor (p-1)} \pmod{p}.$$

From the proof of Proposition 12, we can derive following results:

- if $\mathcal{B}_1$ or $\mathcal{B}_2$ holds, the left term will be $\binom{\widehat{t} \bmod p}{\widetilde{v}}$;
- if $\mathcal{B}_3$ or $\mathcal{B}_4$ or $\mathcal{B}_5$ or $\mathcal{B}_6$ holds, the left term is 0;
- if $\mathcal{B}_7$ holds, the left term equals $\binom{\widehat{t} \bmod p+1}{\widetilde{v}}$.

For the right term, we denote $m-\widetilde{v} = \alpha_1(p-1)+\alpha_2$ with $\alpha_2 \leq p-2$. Thus,

$$\left\lfloor \frac{m-\widetilde{v}}{p-1} \right\rfloor (p-1) + \widetilde{v} = \alpha_1(p-1) + \widetilde{v} = m - \alpha_2.$$

In this case, we obtain that

$$\binom{m}{\widetilde{v}+\left\lfloor \frac{m-\widetilde{v}}{p-1} \right\rfloor (p-1)} = \binom{m}{m-\alpha_2} = \binom{m}{\alpha_2}$$

Notice that $\alpha_2 = (m-\widetilde{v}) \bmod (p-1)$, and $(t-\widetilde{v}) \equiv (m-\widetilde{v}) \bmod (p-1)$. Hence, $\alpha_2 \equiv (t-\widetilde{v}) \bmod (p-1)$. Since $m \bmod p = \widehat{m}_0$, we obtain that the right term is

$$\binom{\widehat{m}_0}{(t-\widetilde{v}) \bmod (p-1)}.$$

In other words, if $\mathcal{B}_8$ holds, it equals 0; if $\mathcal{B}_9$ holds, it's a non-zero value.

It's easy to check that if only the left term or the right term equals 0, we can reach the conclusion that the target sum is not 0 mod p. When both terms are non-zero values, we cannot derive equivalent conditions, but we still can give some special cases here, which are $\mathcal{B}_{10}$ to $\mathcal{B}_{22}$ in Table 3. All these cases can be verified easily. □

F Find Integral Distinguishers for HADES Design

In this subsection, we show that the Computation-Traceback-Determine framework proposed in Sect. 3.2 can also apply to HADES structure.

HADES [19] is a new strategy in designing symmetric primitives proposed by Grassi *et al.* in EUROCRYPT 2020. Its full structure is shown in Figure 9. Each round function consists of three parts: Add Round Key $ARK(\cdot)$, SubWords $S(\cdot)$ and MixLayer $M(\cdot)$. The last $M(\cdot)$ can be omitted and there is one extra $ARK(\cdot)$ in the end. Compared with SPN structure, crucial property of HADES is that each round adopts different number of S-Boxes. Specifically, the first R_1 and last R_3 rounds use full S-Box layers, while the middle R_2 rounds only use one S-Box.

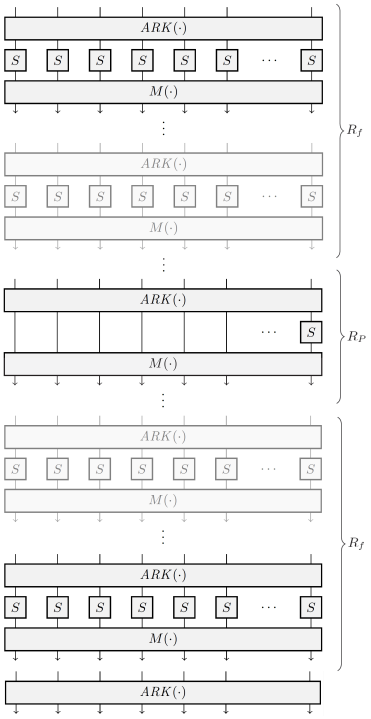


Fig. 9: Structure of HADES [19] (the final matrix multiplication can be omitted).

HadesMiMC is a keyed permutation obtained by applying HADES to the cipher SHARK [30]. It has n inputs with each lies in $\mathbb{F}_p$, where p is a prime larger than 8. Non-linear S-Box adopts the power mapping $S(x) = x^d \bmod p$. The power $d \geq 3$ is required to be the smallest integer s.t. $\gcd(p-1, d) = 1$. The Mixlayer is defined by a multiplication with fixed $n \times n$ MDS matrix satisfying some conditions [19,21]. Since our method can deal with any $n \times n$ matrix whose elements are all non-zeros and lies in $\mathbb{F}_p$, details of these conditions and the way to construct such matrix are omitted.

Assume that we aim to find distinguishers covering $(R_1 + R_2 + R_3)$ rounds for HADES with n blocks. Let $(x_1, x_2, \cdots, x_s)$ denote the s inputs traversed, while the others are random constants $I_{s+1}, I_{s+2}, \cdots, I_n$. Denote the master key as $(rk_{01}, rk_{02}, \cdots, rk_{0n})$. For $1 \leq w \leq s$, we introduce $W_w = x_w + rk_{0w}$.

Phase I Computation. Let $V_{R_1 j}$ be the j-th output after the first R_1 full rounds. Denote S as the set $\{\vec{H} = (b, e_1, e_2, \cdots, e_s) \mid b + \sum_{w=1}^{s} e_w = d^{R_1 - 1}\}$, and its size is L. We use $\vec{H}_i = (b_i, e_{i1}, e_{i2}, \cdots, e_{is})$ to denote the i-th value in S.

In Appendix F.1, we proved that algebraic form of each $V_{R_1 j}$ is equivalent to

$$F_{1j} = \sum_{i=1}^{L} X_{1ji} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}}$$

if $d^{R_1 - 1} \leq p - 1$, where X_{1ji} are random constants. In other words, they are composed of same set of monomials. One can refer to Definition 1 for a clear understanding. In practice, one can adopt SageMath to obtain the exact algebraic representation of F_{1j}.

Denote Z_{rj} as the j-th output after r partial rounds, where $1 \leq r \leq R_2$. In Appendix F.2, we can obtain that

$$Z_{rj} = \begin{cases} Y_{rj0} F_{11}^d + F_{(r+1)j}, \text{ when } r = 1; \\ Y_{rj(r-1)} Z_{(r-1)1}^d + \cdots + Y_{rj1} Z_{11}^d + Y_{rj0} F_{11}^d + F_{(r+1)j}, \text{ when } 2 \leq r \leq R_2. \end{cases}$$

Here, X_{rji}, Y_{rj*} involved are unknown constants. All F_{rj} obey the same form:

$$F_{rj} = \sum_{i=1}^{L} X_{rji} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}}.$$

For next R_3 full rounds, when $d^{R_3} \leq p - 1$, the algebraic form of the j-th output $U_{R_3 j}$ after $(R_1 + R_2 + R_3)$ rounds is equivalent to the union of all $Z_{R_2 1}^{m'}$ where $m' \leq d^{R_3}$. In other words, only when the monomial $\prod_{w=1}^{s} x_w^{p-1}$ doesn't contained in any of $Z_{R_2 1}^{m'}$, one can ensure that it is not composed of $U_{R_3 j}$. That is, we found an integral distinguisher covering $(R_1 + R_2 + R_3)$ rounds. We proved this in Appendix F.3.

Phase II Traceback and Phase III Determine. In these two phases, we first expand each $Z_{R_2 1}^{m'}$ to get the coefficient $\mathcal{A}$ of the monomial $\prod_{w=1}^{s} x_w^{p-1}$, then derive conditions to restrict $\mathcal{A} \neq 0 \pmod{p}$. In Appendix F.4, we show these two phases in more details.

New Found Integral Distinguishers for HadesMiMC. With the search model, we can obtain a lot of integral distinguishers varying from $s = 1$ to $n - 1$. In [5], integral distinguishers with data complexity p are constructed by making perfect use of the property of partial rounds. These distinguishers cover more rounds than ours. This arises from the exponential growth of constraints induced by MDS matrices used in full rounds, which make the search model too large to solve or even impossible to construct. To avoid this, we adopt a compromise approach by restricting the number of full rounds at both ends. The use of these full rounds at the beginning and end of HADES effectively prevents the detection of integral properties covering more rounds. To serve as a complementary component to integral cryptanalysis for HadesMiMC, we show all found distinguishers when $s \geq 2$ for $p = 251$ and $p = 65519$ in Table 4.

Compared with those predicted using the maximal degree, our distinguishers can cover at least 1 more round, which shows the necessity of considering exact coefficients of monomials when finding integral distinguishers over $\mathbb{F}_p$. We also applied this model for other prime numbers. Results are depicted in Appendix G.

New Found Integral Distinguishers for Poseidon2$^\pi$. Poseidon2$^\pi$ is the inner permutation of Poseidon2 hash function [17] proposed by Grassi *et al.* in AFRICACRYPT 2023. It follows the HADES structure, but has some differences. In the $ARK(\cdot)$ operation, Poseidon2$^\pi$ adds round constants rather than round keys. There is only one round constant added before the single $S(\cdot)$ operation in these partial rounds. Besides, matrices used in the full round and partial round are different here. An extra linear layer is applied at its input, however, it can be omitted when analyzing the security of Poseidon2$^\pi$. These differences will not affect the deduction of equivalent algebraic forms we used. Hence, one can directly use the model built for HadesMiMC here. In the specification of Poseidon2$^\pi$ [17], some instances focusing on 2-to-1 compressions are given. We searched integral distinguishers for all parameter sets depicted in its ePrint version [18, Table 1]. Here, we only show some of these distinguishers in Table 5, compared with the trivial bound.

F.1 Equivalent Algebraic Form in First R_1 Full Rounds

Let A_{ij} be the element lying in the i-th row and j-th column ($1 \leq i, j \leq n$) of the matrix used in MixLayer. After the first full round and the next $ARK(\cdot)$ operation, the j-th output is

$$V_{1j} = A_{j1}W_1^d + A_{j2}W_2^d + \cdots + A_{js}W_s^d + \left(\sum_{i=s+1}^{n} A_{ji}(I_i + rk_{0i})^d + rk_{1j}\right).$$

Denote the last constant part as B_j. Similarly, after the r-th full round ($r \geq 2$) and the next $ARK(\cdot)$, its j-th output is

$$V_{rj} = A_{j1}V_{(r-1)1}^d + A_{j2}V_{(r-1)2}^d + \cdots + A_{jn}V_{(r-1)n}^d + rk_{rj},$$

where rk_{rj} is the j-th block of round key rk_r. To make the following deduction more clear, we introduce Definition 1.

Definition 1 *Assume that function G has s inputs $y_1, y_2, \cdots, y_s$. Denote $\vec{u}$ as $(u_1, u_2, \cdots, u_s)$. Its algebraic form can be denoted as*

$$\sum_{\vec{u}} \left(\mathcal{C}_{\vec{u}} \cdot \mathcal{H}_{\vec{u}} \cdot \prod_{w=1}^{s} W_w^{u_w}\right),$$

where $\mathcal{C}_{\vec{u}}$ is only related with multinomial coefficients.

Denote $\mathcal{M}[G]$ as the set of monomials $\prod_{w=1}^{s} W_w^{u_w}$ where $\mathcal{C}_{\vec{u}} \neq 0 \pmod p$. Given two functions G_1 and G_2 sharing same s inputs, if $\mathcal{M}[G_1] = \mathcal{M}[G_2]$, we say their algebraic forms are equivalent.

Table 4: New Found Integral distinguishers for HadesMiMC.

p	blocks	$s^{\dagger}$	Trivial Bound‡	Ours
251	16	2	5	$7 = 1 + 4 + 2$ $6 = 2 + 3 + 1$
		3	6	$9 = 1 + 4 + 4$ $7 = 2 + 4 + 1$
		4	6	$10 = 1 + 4 + 5$ $7 = 2 + 4 + 1$
		5, 6	6	$10 = 1 + 4 + 5$ $8 = 2 + 4 + 2$
		7, 8	6	$10 = 1 + 4 + 5$ $9 = 2 + 4 + 3$
		$9, 10, \cdots, 15$	7	$10 = 1 + 4 + 5$ $9 = 2 + 4 + 3$
65519	8	1	10	$11 = 1 + 9 + 1$ $11 = 2 + 8 + 1$
		2	10	$12 = 1 + 10 + 1$ $11 = 2 + 8 + 1$
		3, 4	11	$14 = 1 + 10 + 3$ $12 = 2 + 9 + 1$
		5, 6, 7	11	$14 = 1 + 10 + 3$ $13 = 2 + 10 + 1$

† Number of blocks traversed. Data complexity is then p^s.
‡ Trivial bound is evaluated as $\lfloor \log_d(s(p-1)-1) \rfloor$.

With Definition 1, we introduce the following two lemmas, which can lead to our final conclusion (Theorem 1) for the first R_1 full rounds by mathematical induction.

Lemma 6 *$\mathcal{M}[V_{rj_1}^m] = \mathcal{M}[V_{rj_2}^m]$ holds for any $1 \le j_1, j_2 \le n$, $1 \le r \le R_1$ and $m \ge 0$.*

Proof. When $r = 1$, for each V_{1j}^m, it's algebraic representation form is

$$\begin{aligned} V_{1j}^m =& (A_{j1}W_1^d + A_{j2}W_2^d + \cdots + A_{js}W_s^d + B_j)^m \\ =& \sum_{l+\sum_{w=1}^{s} h_w = m} \frac{m!}{l! \cdot \prod_{w=1}^{s}(h_w!)} \cdot \left(B_j^l \prod_{w=1}^{s} A_{jw}^{h_w} \right) \cdot \prod_{w=1}^{s} W_w^{d \cdot h_w}. \end{aligned}$$

Table 5: New Found Integral distinguishers for Poseidon2$^\pi$.

p	d	blocks	$s^\dagger$	Trivial Bound‡	Ours
$0x78000001$	5	16 / 24	$2, 3$	13	$13 = 1 + 11 + 1$
			$4, 5, 6, 7$	14	$14 = 1 + 12 + 1$
			$8, 9, \cdots, 15$	14	$15 = 1 + 13 + 1$
		24	$16, 17, \cdots, 23$	15	$16 = 1 + 14 + 1$
$p_{Goldilocks}$	7	8	2	26	$25 = 1 + 22 + 2$
			$3, 4, 5, 6, 7$	24	$26 = 1 + 22 + 3$
		12	2	24	$25 = 1 + 22 + 2$
			$3, 4, \cdots, 10$	24	$26 = 1 + 22 + 3$
			11	25	$26 = 1 + 22 + 3$

– $p_{Goldilocks} =$ `0xffffffff00000001`
† Number of blocks traversed. Data complexity is then p^s.
‡ Trivial bound is evaluated as $\lfloor \log_d(s(p-1)-1) \rfloor$.

Since for each j, $\widehat{\mathcal{C}}_{\vec{u}}$ are the same one, $\mathcal{M}[V_{1j}^m]$ is the same for all j. When $r \geq 2$, for each V_{rj}^m, we have

$$\begin{aligned} V_{rj}^m =& (A_{j1}V_{(r-1)1}^d + A_{j2}V_{(r-1)2}^d + \cdots + A_{jn}V_{(r-1)n}^d + rk_{rj})^m \\ =& \sum_{l+\sum_{i=1}^n h_i = m} \frac{m!}{l! \cdot \prod_{i=1}^n (h_i!)} \cdot \left(rk_{rj}^l \prod_{i=1}^n A_{ji}^{h_i} \right) \cdot \prod_{i=1}^n V_{(r-1)i}^{d \cdot h_i}. \end{aligned}$$

Similarly, we can obtain that $\mathcal{M}[V_{rj}^m]$ is same for all j and r. □

Lemma 7 *When $d \cdot m \leq p-1$, $\mathcal{M}[V_{rj}^m] = \mathcal{M}[V_{(r-1)a}^{d \cdot m}]$ holds for any $1 \leq j, a \leq n$ and $2 \leq r \leq R_1$.*

Proof. Since $\mathcal{M}[V_{(r-1)a}^{d \cdot m}] = \mathcal{M}[V_{(r-1)1}^{d \cdot m}]$ holds for any a due to Lemma 6, we only have to consider the case $a = 1$ here. Recall that

$$\begin{aligned} V_{rj}^m =& (A_{j1}V_{(r-1)1}^d + A_{j2}V_{(r-1)2}^d + \cdots + A_{jn}V_{(r-1)n}^d + rk_{rj})^m \\ =& \sum_{l_2+\sum_{i=1}^n h_{2i} = m} \frac{m!}{l_2! \cdot \prod_{i=1}^n (h_{2i}!)} \cdot \left(rk_{rj}^{l_2} \prod_{i=1}^n A_{ji}^{h_{2i}} \right) \cdot \prod_{i=1}^n V_{(r-1)i}^{d \cdot h_{2i}}. \end{aligned}$$

– When $r = 2$, $V_{(r-1)i}^{d \cdot h_{2i}}$ equals

$$\sum_{l_{1i}+\sum_{w=1}^s h_{1iw} = d \cdot h_{2i}} \frac{(d \cdot h_{2i})!}{l_{1i}! \cdot \prod_{w=1}^s (h_{1iw}!)} \cdot \left(B_i^{l_{1i}} \prod_{w=1}^s A_{iw}^{h_{1iw}} \right) \cdot \prod_{w=1}^s W_w^{d \cdot h_{1iw}}.$$

Hence, $\prod_{i=1}^{n} V_{(r-1)i}^{d\cdot h_{2i}}$ is

$$\sum_{\substack{l_{11}+\sum_{w=1}^{s} h_{11w}=d\cdot h_{21}\\ l_{12}+\sum_{w=1}^{s} h_{12w}=d\cdot h_{22}\\ \cdots\\ l_{1n}+\sum_{w=1}^{s} h_{1nw}=d\cdot h_{2n}}} \prod_{i=1}^{n} \frac{(d\cdot h_{2i})!}{l_{1i}!\cdot\prod_{w=1}^{s}(h_{1iw}!)}\cdot\prod_{i=1}^{n}\left(B_i^{l_{1i}}\prod_{w=1}^{s}A_{iw}^{h_{1iw}}\right)\cdot\prod_{w=1}^{s}W_w^{d\cdot\sum_{i=1}^{n}h_{1iw}}.$$

Since $d\cdot h_{2i}\le d\cdot m\le p-1$ hold, all multinomial coefficients are not 0 mod p. Hence, V_{rj}^{m} contains monomials $\prod_{w=1}^{s}W_w^{d\cdot u_w}$ where

$$\sum_{w=1}^{s}u_w=\sum_{i=1}^{n}\sum_{w=1}^{s}h_{1iw}\le d\sum_{i=1}^{n}h_{2i}\le d\cdot m.$$

Note that $V_{(r-1)1}^{d\cdot m}$ equals to

$$\sum_{l_{11}+\sum_{w=1}^{s}h_{11w}=d\cdot m}\frac{(d\cdot m)!}{l_{11}!\cdot\prod_{w=1}^{s}(h_{11w}!)}\cdot\left(B_1^{l_{11}}\prod_{w=1}^{s}A_{1w}^{h_{11w}}\right)\cdot\prod_{w=1}^{s}W_w^{d\cdot h_{11w}}.$$

In other words, it is composed of monomials $\prod_{w=1}^{s}W_w^{d\cdot h_{11w}}$ where $\sum_{w=1}^{s}h_{11w}\le d\cdot m$ due to $d\cdot m\le p-1$, which are the same as those in V_{rj}^{m}.

– When $r\ge 3$, $V_{(r-1)i}^{d\cdot h_{2i}}$ equals to

$$\sum_{l_{1i}+\sum_{a=1}^{n}h_{1ia}=d\cdot h_{2i}}\frac{(d\cdot h_{2i})!}{l_{1i}!\cdot\prod_{a=1}^{n}(h_{1ia}!)}\cdot\left(rk_{(r-1)i}^{l_{1i}}\prod_{a=1}^{n}A_{ia}^{h_{1ia}}\right)\cdot\prod_{a=1}^{n}V_{(r-2)a}^{d\cdot h_{1ia}}.$$

Thus, $\prod_{i=1}^{n} V_{(r-1)i}^{d\cdot h_{2i}}$ is

$$\sum_{\substack{l_{11}+\sum_{a=1}^{n} h_{11a}=d\cdot h_{21}\\ l_{12}+\sum_{a=1}^{n} h_{12a}=d\cdot h_{22}\\ \cdots\\ l_{1n}+\sum_{a=1}^{n} h_{1na}=d\cdot h_{2n}}} \prod_{i=1}^{n} \frac{(d\cdot h_{2i})!}{l_{1i}!\cdot\prod_{a=1}^{n}(h_{1ia}!)}\cdot\prod_{i=1}^{n}\left(rk_{(r-1)i}^{l_{1i}}\prod_{a=1}^{n}A_{ia}^{h_{1ia}}\right)\cdot\prod_{a=1}^{n}V_{(r-2)a}^{d\cdot\sum_{i=1}^{n}h_{1ia}}.$$

Since $d\cdot h_{2i}\le d\cdot m\le p-1$, V_{rj}^{m} is composed of monomials $\prod_{a=1}^{n}V_{(r-2)a}^{d\cdot u_a}$ where $\sum_{a=1}^{n}u_a\le d\cdot m$. Similarly, we can obtain that $V_{(r-1)1}^{d\cdot m}$ equals to

$$\sum_{l_{11}+\sum_{a=1}^{n}h_{11a}=d\cdot m}\frac{(d\cdot m)!}{l_{11}!\cdot\prod_{a=1}^{n}(h_{11a}!)}\cdot\left(rk_{(r-1)1}^{l_{11}}\prod_{a=1}^{n}A_{1a}^{h_{11a}}\right)\cdot\prod_{a=1}^{n}V_{(r-2)a}^{d\cdot h_{11a}}.$$

Hence, it contains monomials $\prod_{a=1}^{n}V_{(r-2)a}^{d\cdot h_{11a}}$ with $\sum_{a=1}^{n}h_{11a}\le d\cdot m$, which are the same as those in V_{rj}^{m}. □

Theorem 1. *When* $d^{R_1-1} \leq p-1$, $\mathcal{M}[V_{R_1 j}] = \mathcal{M}[V_{1a}^{d^{R_1-1}}]$ *holds for* $1 \leq j, a \leq n$.

Proof. Due to Lemma 6, we only need to consider $a = 1$. According to Lemma 7,

$$\mathcal{M}[V_{R_1 j}] = \mathcal{M}[V_{(R_1-1)1}^{d}] = \mathcal{M}[V_{(R_1-2)1}^{d^2}] = \cdots = \mathcal{M}[V_{11}^{d^{R_1-1}}]$$

since $d^r \leq p-1$ for any $1 \leq r \leq R_1 - 1$. □

According to Theorem 1, $V_{R_1 j}$ is composed of monomials contained in

$$\begin{aligned} V_{1a}^{d^{R_1-1}} =& (A_{a1}W_1^d + A_{a2}W_2^d + \cdots + A_{as}W_s^d + B_a)^{d^{R_1-1}} \\ =& \sum_{b+\sum_{w=1}^{s} e_w = d^{R_1-1}} \frac{(d^{R_1-1})!}{b! \cdot \prod_{w=1}^{s}(e_w!)} \cdot \left(B_a^b \prod_{w=1}^{s} A_{aw}^{e_w} \right) \cdot \prod_{w=1}^{s} W_w^{d \cdot e_w}. \end{aligned}$$

In other words, it contains monomials $\prod_{w=1}^{s} W_w^{d \cdot e_w}$ where $\sum_{w=1}^{s} e_w + b = d^{R_1-1}$. With these notations, one can obtain the equivalent algebraic form of $V_{R_1 j}$:

$$F_{1j} = \sum_{i=1}^{L} X_{1ji} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}}.$$

F.2 Equivalent Algebraic Form in Next R_2 Partial Rounds

Now, let's see how to construct the equivalent algebraic form after going through the next R_2 partial rounds based on F_{1j}. After the 1-st partial round and the next $ARK(\cdot)$, the j-th output

$$\begin{aligned} Z_{1j} =& A_{j1}F_{11}^d + A_{j2}F_{12} + A_{j3}F_{13} + \cdots A_{jn}F_{1n} + rk_{(R_1+1)j} \\ =& A_{j1}F_{11}^d + A_{j2}\sum_{i=1}^{L} X_{12i} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + \cdots + A_{jn}\sum_{i=1}^{L} X_{1ni} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + rk_{(R_1+1)j} \\ =& A_{j1}F_{11}^d + \sum_{i=1}^{L} \left(\sum_{a=2}^{n} A_{ja}X_{1ai} \right) \cdot \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + rk_{(R_1+1)j}. \end{aligned}$$

Let F_{2j} be the sum of last two items, which is

$$\sum_{i=1}^{L} \left(\sum_{a=2}^{n} A_{ja}X_{1ai} \right) \cdot \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + rk_{(R_1+1)j}.$$

Note that among these L values $\vec{H}_i$, there is one equals to $(d^{R_1-1}, 0, \cdots, 0)$, which is a constant. Hence, we can add $rk_{(R_1+1)j}$ to this term. Now one can see that $\mathcal{M}[F_{2j}] = \mathcal{M}[F_{1j}]$, and hence Z_{1j} can be represented as $Z_{1j} = A_{j1}F_{11}^d + F_{2j}$.

After the 2-nd partial round and the next $ARK(\cdot)$, the j-th output Z_{2j} is

$$\begin{aligned}
Z_{2j} &= A_{j1}Z_{11}^d + A_{j2}Z_{12} + A_{j3}Z_{13} + \cdots + A_{jn}Z_{1n} + rk_{(R_1+2)j} \\
&= A_{j1}Z_{11}^d + A_{j2}(A_{21}F_{11}^d + F_{22}) + A_{j3}(A_{31}F_{11}^d + F_{23}) \\
&\qquad + \cdots + A_{jn}(A_{n1}F_{11}^d + F_{2n}) + rk_{(R_1+2)j} \\
&= A_{j1}Z_{11}^d + \left(\sum_{a=2}^{n} A_{ja}A_{a1}\right) F_{11}^d \\
&\qquad + A_{j2}F_{22} + A_{j3}F_{23} + \cdots + A_{jn}F_{2n} + rk_{(R_1+2)j}.
\end{aligned}$$

Denote F_{3j} as $A_{j2}F_{22}+A_{j3}F_{23}+\cdots+A_{jn}F_{2n}+rk_{(R_1+2)j}$. Since $\mathcal{M}[F_{2j}] = \mathcal{M}[F_{1j}]$, we can also represent each F_{2j} as

$$F_{2j} = \sum_{i=1}^{L} X_{2ji} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}}.$$

Thus,

$$\begin{aligned}
F_{3j} =& A_{j2}F_{22} + A_{j3}F_{23} + \cdots + A_{jn}F_{2n} + rk_{(R_1+2)j} \\
=& A_{j2}\sum_{i=1}^{L} X_{22i} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + \cdots + A_{jn}\sum_{i=1}^{L} X_{2ni} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + rk_{(R_1+2)j} \\
=& \sum_{i=1}^{L} \left(\sum_{a=2}^{n} A_{ja}X_{2ai}\right) \prod_{w=1}^{s} W_w^{d \cdot e_{iw}} + rk_{(R_1+2)j}.
\end{aligned}$$

Similar with before, one can see that $\mathcal{M}[F_{3j}] = \mathcal{M}[F_{2j}] = \mathcal{M}[F_{1j}]$. Meanwhile, we have $Z_{2j} = A_{j1}Z_{11}^d + (\sum_{a=2}^{n} A_{ja}A_{a1})\, F_{11}^d + F_{3j}$.

For any $r \geq 3$, one can do the same as what we did in deriving the form of Z_{2j}. Finally, using mathematical induction, one can achieve the following theorem, which leads to the equivalent algebraic form $Z_{R_2 j}$ of the j-th output after $(R_1 + R_2)$ rounds based on that of $V_{R_1 j}$.

Theorem 2. *The j-th output after r partial rounds is in the form:*

- $r = 1$*:*

$$Z_{rj} = Y_{rj0}F_{11}^d + F_{(r+1)j}$$

- $2 \leq r \leq R_2$*:*

$$Z_{rj} = Y_{rj(r-1)}Z_{(r-1)1}^d + \cdots + Y_{rj2}Z_{21}^d + Y_{rj1}Z_{11}^d + Y_{rj0}F_{11}^d + F_{(r+1)j}$$

where $F_{rj} = \sum_{i=1}^{L} X_{rji} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}}$. Here, all X_{rji}, Y_{rj*} are unknown constants related with A_{ij}, rk_{rj} and $I_{s+1}, I_{s+2}, \cdots, I_n$.

F.3 Equivalent Algebraic Form in Last R_3 Full Rounds

For next R_3 full rounds, we adopt a similar analysis with above. After the 1-st full round (only counting the full round in the end) and the next $ARK(\cdot)$, the j-th output can be represented with $Z_{R_2 j}$ as

$$U_{1j} = A_{j1} Z_{R_2 1}^d + A_{j2} Z_{R_2 2}^d + \cdots + A_{jn} Z_{R_2 n}^d + rk_{(R_1+R_2+1)j}.$$

Similarly, after r-th round ($2 \le r \le R_3$) and the next $ARK(\cdot)$, we have

$$U_{rj} = A_{j1} U_{(r-1)1}^d + A_{j2} U_{(r-1)2}^d + \cdots + A_{jn} U_{(r-1)n}^d + rk_{(R_1+R_2+r)j}.$$

Now, we show which monomials are contained in the equivalent algebraic form $U_{R_3 j}$ of the j-th output after $(R_1 + R_2 + R_3)$ rounds, with the help of following two lemmas.

Lemma 8 *When $d \cdot m \le p - 1$, $\mathcal{M}[U_{1a}^m] = \bigcup_{m' \le d \cdot m} \mathcal{M}[Z_{R_2 1}^{m'}]$ holds for any $1 \le a \le n$, where $Z_{R_2 1}$ is given in Theorem 2.*

Proof. Let's firstly check which monomial lies in U_{1a}^m. Without loss of generality, we assume that $rk_{(R_1+R_2+1)a} \bmod p \neq 0$.

$$\begin{aligned} U_{1a}^m &= \left(A_{a1} Z_{R_2 1}^d + A_{a2} Z_{R_2 2}^d + \cdots + A_{an} Z_{R_2 n}^d + rk_{(R_1+R_2+1)a}\right)^m \\ &= \sum_{v_{1a} + \sum_{j=1}^n u_{1aj} = m} \left[\frac{m!}{v_{1a}! \cdot \prod_{j=1}^n (u_{1aj}!)} rk_{(R_1+R_2+1)a}^{v_{1a}} \prod_{j=1}^n A_{aj}^{u_{1aj}} \right] \cdot \prod_{j=1}^n Z_{R_2 j}^{d \cdot u_{1aj}}. \end{aligned}$$

It's obvious that $\mathcal{M}[U_{1a}^m] = \mathcal{M}[U_{1b}^m]$ for any $1 \le a, b \le n$, since they only different at these random non-zero coefficients $rk_{(R_1+R_2+1)a}$ and A_{aj}. Hence, we can take $a = 1$ as an example in the following.

With Theorem 2, for any j, $Z_{R_2 j}^{d \cdot u_{11j}}$ equals to

$$\sum_{l_j + \sum_{t=0}^{R_2-1} h_{jt} = d \cdot u_{11j}} \left[\frac{(d \cdot u_{11j})!}{l_j! \cdot \prod_{t=0}^{R_2-1} (h_{jt}!)} \prod_{t=0}^{R_2-1} Y_{R_2 jt}^{h_{jt}} \right] \cdot F_{(R_2+1)j}^{l_j} \cdot \prod_{t=1}^{R_2-1} Z_{t1}^{d \cdot h_{jt}} \cdot F_{11}^{d \cdot h_{j0}}.$$

Hence,

$$\begin{aligned} U_{11}^m = \sum_{\substack{v_{11} + \sum_{j=1}^n u_{11j} = m \\ l_1 + \sum_{t=0}^{R_2-1} h_{1t} = d \cdot u_{111} \\ l_2 + \sum_{t=0}^{R_2-1} h_{2t} = d \cdot u_{112} \\ \cdots \\ l_n + \sum_{t=0}^{R_2-1} h_{nt} = d \cdot u_{11n}}} & \frac{m!}{v_{11}! \cdot \prod_{j=1}^n (u_{11j}!)} \cdot \prod_{j=1}^n \frac{(d \cdot u_{11j})!}{l_j! \cdot \prod_{t=0}^{R_2-1} (h_{jt}!)} \\ & \cdot rk_{(R_1+R_2+1)1}^{v_{11}} \cdot \prod_{j=1}^n A_{1j}^{u_{11j}} \cdot \prod_{j=1}^n \prod_{t=0}^{R_2-1} Y_{R_2 jt}^{h_{jt}} \\ & \cdot \prod_{j=1}^n F_{(R_2+1)j}^{l_j} \cdot \prod_{t=1}^{R_2-1} Z_{t1}^{d \cdot \sum_{j=1}^n h_{jt}} \cdot F_{11}^{d \cdot \sum_{j=1}^n h_{j0}}. \end{aligned}$$

Next, we show $\mathcal{M}\left[\prod_{j=1}^{n} F_{(R_2+1)j}^{l_j}\right] = \mathcal{M}\left[F_{(R_2+1)1}^{\sum_{j=1}^{n} l_j}\right]$. According to Theorem 2,

$$\begin{aligned} F_{(R_2+1)j}^{l_j} &= \left(\sum_{i=1}^{L} X_{(R_2+1)ji} \prod_{w=1}^{s} W_w^{d \cdot e_{iw}}\right)^{l_j} \\ &= \sum_{\sum_{i=1}^{L} c_{ij} = l_j} \frac{l_j!}{\prod_{i=1}^{L}(c_{ij}!)} \cdot \prod_{i=1}^{L} X_{(R_2+1)ji}^{c_{ij}} \cdot \prod_{w=1}^{s} W_w^{d \cdot \sum_{i=1}^{L} e_{iw} \cdot c_{ij}}. \end{aligned}$$

Hence, $\prod_{j=1}^{n} F_{(R_2+1)j}^{l_j}$ equals to

$$\sum_{\substack{\sum_{i=1}^{L} c_{i1} = l_1 \\ \sum_{i=1}^{L} c_{i2} = l_2 \\ \cdots \\ \sum_{i=1}^{L} c_{in} = l_n}} \prod_{j=1}^{n} \frac{l_j!}{\prod_{i=1}^{L}(c_{ij}!)} \cdot \prod_{j=1}^{n} \prod_{i=1}^{L} X_{(R_2+1)ji}^{c_{ij}} \cdot \prod_{w=1}^{s} W_w^{d \cdot \sum_{i=1}^{L} \sum_{j=1}^{n} (e_{iw} c_{ij})}.$$

Since all $l_j \leq \sum_{j=1}^{n} l_j \leq d \cdot \sum_{j=1}^{n} u_{11j} \leq d \cdot m \leq p-1$, it contains monomials $\prod_{w=1}^{s} W_w^{d \cdot u_w}$ where

$$u_w = \sum_{i=1}^{L} \sum_{j=1}^{n} (e_{iw} c_{ij}) = \sum_{i=1}^{L} e_{iw} \cdot \left(\sum_{j=1}^{n} c_{ij}\right)$$

and $\sum_{j=1}^{n} c_{ij}$ fulfills that $\sum_{i=1}^{L} \sum_{j=1}^{n} c_{ij} = \sum_{j=1}^{n} l_j$. Similarly, since

$$F_{(R_2+1)1}^{\sum_{j=1}^{n} l_j} = \sum_{\sum_{i=1}^{L} c'_{i1} = \sum_{j=1}^{n} l_j} \frac{(\sum_{j=1}^{n} l_j)!}{\prod_{i=1}^{L}(c'_{i1}!)} \cdot \prod_{i=1}^{L} X_{(R_2+1)1i}^{c'_{i1}} \cdot \prod_{w=1}^{s} W_w^{d \cdot \sum_{i=1}^{L} e_{iw} \cdot c'_{i1}},$$

one can see that it is composed of $\prod_{w=1}^{s} W_w^{d \cdot u_w}$ where $u_w = \sum_{i=1}^{L} e_{iw} \cdot c'_{i1}$ and c'_{i1} fulfills that $\sum_{i=1}^{L} c'_{i1} = \sum_{j=1}^{n} l_j$. Hence, $\mathcal{M}\left[\prod_{j=1}^{n} F_{(R_2+1)j}^{l_j}\right] = \mathcal{M}\left[F_{(R_2+1)1}^{\sum_{j=1}^{n} l_j}\right]$. In this case, U_{11}^{m} contains monomials

$$F_{(R_2+1)1}^{\sum_{j=1}^{n} l_j} \cdot \prod_{t=1}^{R_2-1} Z_{t1}^{d \cdot \sum_{j=1}^{n} h_{jt}} \cdot F_{11}^{d \cdot \sum_{j=1}^{n} h_{j0}},$$

where

$$\sum_{j=1}^{n} l_j + \sum_{t=0}^{R_2-1} (\sum_{j=1}^{n} h_{jt}) = d \cdot \sum_{j=1}^{n} u_{11j} \leq d \cdot m$$

since $m \leq p-1$ and $d \cdot u_{11j} \leq d \cdot m \leq p-1$.

Now, let's check which monomials are contained in $Z_{R_21}^{m'}$, where $m' \leq d \cdot m$. With the definition of Z_{R_21} depicted in Theorem 2, we have

$$Z_{R_21}^{m'} = \sum_{l + \sum_{t=0}^{R_2-1} h_t = m'} \left[\frac{(m')!}{l! \cdot \prod_{t=0}^{R_2-1}(h_t!)} \prod_{t=0}^{R_2-1} Y_{R_21t}^{h_t}\right] \cdot F_{(R_2+1)1}^{l} \cdot \prod_{t=1}^{R_2-1} Z_{t1}^{d \cdot h_t} \cdot F_{11}^{d \cdot h_0}.$$

Since $m' \leq p-1$, it contains $F^{l}_{(R_2+1)1} \cdot \prod_{t=1}^{R_2-1} Z^{d\cdot h_t}_{t1} \cdot F^{d\cdot h_0}_{11}$ where $l + \sum_{t=0}^{R_2-1} h_t = m'$. Thus, the union of $\mathcal{M}[Z^{m'}_{R_2 1}]$ for $m' \leq d \cdot m$ equals to $\mathcal{M}[U^m_{11}]$ as claimed. $\square$

Lemma 9 *When $d \cdot m \leq p-1$, $\mathcal{M}[U^m_{ra_1}] = \bigcup_{m' \leq d\cdot m} \mathcal{M}[U^{m'}_{(r-1)a_2}]$ holds for any $1 \leq a_1, a_2 \leq n$ and $r \geq 2$.*

Proof. Let's take U^m_{r1} as an example since $\mathcal{M}[U^m_{r1}] = \mathcal{M}[U^m_{ra_1}]$ holds for any a_1.

$$
\begin{aligned}
U^m_{r1} &= \Big(A_{11} U^d_{(r-1)1} + A_{12} U^d_{(r-1)2} + \cdots + A_{1n} U^d_{(r-1)n} + rk_{(R_1+R_2+r)1} \Big)^m \\
&= \sum_{v_{r1} + \sum_{a=1}^n u_{r1a} = m} \left[\frac{m!}{v_{r1}! \cdot \prod_{a=1}^n (u_{r1a}!)} rk^{v_{r1}}_{(R_1+R_2+r)1} \prod_{a=1}^n A^{u_{r1a}}_{1a} \right] \cdot \prod_{a=1}^n U^{d\cdot u_{r1a}}_{(r-1)a}
\end{aligned}
$$

Now we show that when $d \cdot m \leq p-1$, $\mathcal{M}\left[\prod_{a=1}^n U^{d\cdot u_{r1a}}_{(r-1)a}\right] = \mathcal{M}\left[U^{d\cdot \sum_{a=1}^n u_{r1a}}_{(r-1)a_2}\right]$ holds for any $1 \leq a_2 \leq n$.

(1) For $r = 2$,

$$
\begin{aligned}
\prod_{a=1}^n U^{d\cdot u_{21a}}_{1a} = \sum_{\substack{v_{11} + \sum_{j=1}^n u_{11j} = d\cdot u_{211} \\ v_{12} + \sum_{j=1}^n u_{12j} = d\cdot u_{212} \\ \cdots \\ v_{1n} + \sum_{j=1}^n u_{1nj} = d\cdot u_{21n}}} & \prod_{a=1}^n \frac{(d\cdot u_{21a})!}{v_{1a}! \cdot \prod_{j=1}^n (u_{1aj}!)} \cdot \prod_{a=1}^n rk^{v_{1a}}_{(R_1+R_2+1)a} \\
& \cdot \prod_{a=1}^n \prod_{j=1}^n A^{u_{1aj}}_{aj} \cdot \prod_{j=1}^n Z^{d\cdot \sum_{a=1}^n u_{1aj}}_{R_2 j}.
\end{aligned}
$$

Since $d \cdot u_{21a} \leq d \cdot \sum_{a=1}^n u_{21a} \leq d \cdot m \leq p-1$, $\prod_{a=1}^n U^{d\cdot u_{21a}}_{1a}$ contains monomials $\prod_{j=1}^n Z^{d\cdot \sum_{a=1}^n u_{1aj}}_{R_2 j}$ where $\sum_{j=1}^n \sum_{a=1}^n u_{1aj} \leq d \cdot \sum_{a=1}^n u_{21a}$.

Similarly, $U^{d\cdot \sum_{a=1}^n u_{21a}}_{1a_2}$ can be represented as

$$
\sum_{v + \sum_{j=1}^n u_j = d\cdot \sum_{a=1}^n u_{21a}} \left[\frac{(d\cdot \sum_{a=1}^n u_{21a})!}{v! \cdot \prod_{j=1}^n (u_j!)} rk^{v}_{(R_1+R_2+1)a_2} \prod_{j=1}^n A^{u_j}_{a_2 j} \right] \cdot \prod_{j=1}^n Z^{d\cdot u_j}_{R_2 j}.
$$

Due that $d \cdot \sum_{a=1}^n u_{21a} \leq d \cdot m \leq p-1$, it is composed of monomials $\prod_{j=1}^n Z^{d\cdot u_j}_{R_2 j}$ where $\sum_{j=1}^n u_j \leq d \cdot \sum_{a=1}^n u_{21a}$, which are the same as $\prod_{a=1}^n U^{d\cdot u_{21a}}_{1a}$.

(2) When $r \geq 3$,

$$
\begin{aligned}
\prod_{a=1}^n U^{d\cdot u_{r1a}}_{(r-1)a} = \sum_{\substack{v_{(r-1)1} + \sum_{j=1}^n u_{(r-1)1j} = d\cdot u_{r11} \\ v_{(r-1)2} + \sum_{j=1}^n u_{(r-1)2j} = d\cdot u_{r12} \\ \cdots \\ v_{(r-1)n} + \sum_{j=1}^n u_{(r-1)nj} = d\cdot u_{r1n}}} & \prod_{a=1}^n \frac{(d\cdot u_{r1a})!}{(v_{(r-1)a}! \cdot \prod_{j=1}^n (u_{(r-1)aj}!))} \\
& \cdot \prod_{a=1}^n rk^{v_{(r-1)a}}_{(R_1+R_2+r-1)a} \cdot \prod_{a=1}^n \prod_{j=1}^n A^{u_{(r-1)aj}}_{aj} \cdot \prod_{j=1}^n U^{d\cdot \sum_{a=1}^n u_{(r-1)aj}}_{(r-2)j}.
\end{aligned}
$$

Let $u'_j = \sum_{a=1}^{n} u_{(r-1)aj}$. Then it is composed of monomials $\prod_{j=1}^{n} U_{(r-2)j}^{d \cdot u'_j}$ where $\sum_{j=1}^{n} u'_j = \sum_{j=1}^{n} \sum_{a=1}^{n} u_{(r-1)aj} \leq d \cdot \sum_{a=1}^{n} u_{r1a}$, since each $d \cdot u_{r1a} \leq d \cdot m \leq p-1$.

Similarly, $U_{(r-1)a_2}^{d \cdot \sum_{a=1}^{n} u_{r1a}}$ equals to

$$\sum_{v+\sum_{j=1}^{n} u_j = d \cdot \sum_{a=1}^{n} u_{r1a}} \left[\frac{(d \cdot \sum_{a=1}^{n} u_{r1a})!}{v! \cdot \prod_{j=1}^{n} (u_j!)} \cdot rk^{v}_{(R_1+R_2+r-1)a_2} \cdot \prod_{j=1}^{n} A_{a_2 j}^{u_j} \right] \cdot \prod_{j=1}^{n} U_{(r-2)j}^{d \cdot u_j}.$$

Hence, it contains monomials $\prod_{j=1}^{n} U_{(r-2)j}^{d \cdot u_j}$ where $\sum_{j=1}^{n} u_j \leq d \cdot \sum_{a=1}^{n} u_{r1a}$ due to $d \cdot \sum_{a=1}^{n} u_{r1a} \leq d \cdot m \leq p-1$. Therefore, they are composed of the same set of monomials.

Given $\mathcal{M}\left[\prod_{a=1}^{n} U_{(r-1)a}^{d \cdot u_{r1a}}\right] = \mathcal{M}\left[U_{(r-1)a_2}^{d \cdot \sum_{a=1}^{n} u_{r1a}}\right]$, one can see that U_{r1}^{m} contains all $U_{(r-1)a_2}^{d \cdot \sum_{a=1}^{n} u_{r1a}}$ that $\sum_{a=1}^{n} u_{r1a} \leq m$. That is, $\mathcal{M}[U_{r1}^{m}] = \bigcup_{m' \leq d \cdot m} \mathcal{M}[U_{(r-1)a_2}^{m'}]$ as claimed. □

Given Lemma 8 and 9, one can deduce the following theorem through mathematical induction, which shows the set of monomials consists of the equivalent algebraic form $U_{R_3 j}$ of the j-th output after $(R_1 + R_2 + R_3)$ rounds.

Theorem 3. *When* $d^{R_3} \leq p-1$, $\mathcal{M}[U_{R_3 j}] = \bigcup_{m' \leq d^{R_3}} \mathcal{M}[Z_{R_2 1}^{m'}]$ *holds for any* $1 \leq j \leq n$.

Proof. By definition of $U_{R_3 j}$, $\mathcal{M}[U_{R_3 j}] = \bigcup_{a=1}^{n} \mathcal{M}[U_{(R_3-1)a}^{d}]$. Expanding $U_{(R_3-1)a}^{d}$, we can see that $\mathcal{M}[U_{(R_3-1)1}^{d}] = \mathcal{M}[U_{(R_3-1)a}^{d}]$ holds for any a. Therefore, we have $\mathcal{M}[U_{R_3 j}] = \mathcal{M}\left[U_{(R_3-1)1}^{d}\right]$. With Lemma 8 and 9, we have

$$\begin{aligned}
\mathcal{M}\left[U_{(R_3-1)1}^{d}\right] &= \bigcup_{m' \leq d^2} \mathcal{M}\left[U_{(R_3-2)1}^{m'}\right] \\
&= \bigcup_{m' \leq d^3} \mathcal{M}\left[U_{(R_3-3)1}^{m'}\right] \\
&= \cdots \\
&= \bigcup_{m' \leq d^{R_3-1}} \mathcal{M}\left[U_{11}^{m'}\right] \\
&= \bigcup_{m' \leq d^{R_3}} \mathcal{M}\left[Z_{R_2 1}^{m'}\right].
\end{aligned}$$

Hence, $\mathcal{M}[U_{R_3 j}] = \bigcup_{m' \leq d^{R_3}} \mathcal{M}[Z_{R_2 1}^{m'}]$ holds as claimed. □

F.4 Detailed Phase II/III for HADES

Let's firstly see which $\prod_{w=1}^{s} W_w^{u_w}$ consists of $U_{R_3 j}$. Due to Theorem 3, it's equivalent to check $Z_{R_2 1}^{m'}$ for each $m' \leq d^{R_3}$. By Theorem 2, $Z_{R_2 1}^{m'}$ equals to

$$\begin{aligned}
&\left(Y_{R_2 1(R_2-1)} Z_{(R_2-1)1}^{d} + \cdots + Y_{R_2 12} Z_{21}^{d} + Y_{R_2 11} Z_{11}^{d} + Y_{R_2 10} F_{11}^{d} + F_{(R_2+1)1}\right)^{m'} \\
= &\sum_{v_0+h_0+\sum_{r=1}^{R_2-1} u_{0r}=m'} \left[\frac{m'!}{v_0! h_0! \prod_{r=1}^{R_2-1}(u_{0r}!)} Y_{R_2 10}^{v_0} \cdot \prod_{r=1}^{R_2-1} Y_{R_2 1r}^{u_{0r}}\right] \\
&\qquad \cdot F_{11}^{d\cdot v_0} \cdot F_{(R_2+1)1}^{h_0} \cdot \prod_{r=1}^{R_2-2} Z_{r1}^{d\cdot u_{0r}} \cdot Z_{(R_2-1)1}^{d\cdot u_{0(R_2-1)}}.
\end{aligned}$$

Expanding $Z_{(R_2-1)1}$ using Theorem 2, we get

$$\begin{aligned}
Z_{R_2 1}^{m'} = &\sum_{\substack{v_0+h_0+\sum_{r=1}^{R_2-1} u_{0r}=m' \\ v_1+h_1+\sum_{r=1}^{R_2-2} u_{1r}=d\cdot u_{0(R_2-1)}}} \frac{m'!}{v_0! h_0! \prod_{r=1}^{R_2-1}(u_{0r}!)} \frac{(d\cdot u_{0(R_2-1)})!}{v_1! h_1! \prod_{r=1}^{R_2-2}(u_{1r}!)} \\
&\cdot Y_{R_2 10}^{v_0} \cdot \prod_{r=1}^{R_2-1} Y_{R_2 1r}^{u_{0r}} \cdot Y_{(R_2-1)10}^{v_1} \cdot \prod_{r=1}^{R_2-2} Y_{(R_2-1)1r}^{u_{1r}} \\
&\cdot F_{11}^{d\cdot(v_0+v_1)} \cdot F_{(R_2+1)1}^{h_0} \cdot F_{R_2 1}^{h_1} \prod_{r=1}^{R_2-3} Z_{r1}^{d\cdot(u_{0r}+u_{1r})} \cdot Z_{(R_2-2)1}^{d\cdot(u_{0(R_2-2)}+u_{1(R_2-2)})}.
\end{aligned}$$

After expanding $Z_{(R_2-2)1}$, $Z_{(R_2-3)1}$, $\cdots$, and Z_{11} step-by-step, we can obtain

$$\begin{aligned}
Z_{R_2 1}^{m'} = &\sum_{\substack{v_0+h_0+\sum_{r=1}^{R_2-1} u_{0r}=m' \\ v_1+h_1+\sum_{r=1}^{R_2-2} u_{1r}=d\cdot u_{0(R_2-1)} \\ v_2+h_2+\sum_{r=1}^{R_2-3} u_{2r}=d\cdot(u_{0(R_2-2)}+u_{1(R_2-2)}) \\ \cdots \\ v_{R_2-1}+h_{R_2-1}=d\cdot\sum_{t=0}^{R_2-2} u_{t1}}} \mathcal{C}_1\mathcal{C}_2\mathcal{C}_3 \cdot F_{11}^{d\cdot\sum_{t=0}^{R_2-1} v_t} \cdot \prod_{t=0}^{R_2-1} F_{(t+2)1}^{h_{R_2-1-t}},
\end{aligned}$$

where

$$\mathcal{C}_1 = \frac{m'!}{v_0! h_0! \prod_{r=1}^{R_2-1}(u_{0r}!)},\ \mathcal{C}_2 = \prod_{b=1}^{R_2-1} \frac{(d\cdot\sum_{t=0}^{b-1} u_{t(R_2-b)})!}{v_b! h_b! \prod_{r=1}^{R_2-1-b}(u_{br}!)}$$

and

$$\mathcal{C}_3 = \prod_{t=0}^{R_2-1} \left(Y_{(R_2-t)10}^{v_t} \cdot \prod_{r=1}^{R_2-1-t} Y_{(R_2-t)1r}^{u_{tr}}\right).$$

Since we aim to find integral distinguishers hold for all keys and constants, it's reasonable to assume that all Y_{***} are non-zero mod p, which leads to $\mathcal{C}_3 \neq 0 \pmod p$. Due to $m' \leq d^{R_3} \leq p-1$, $\mathcal{C}_1 \neq 0 \pmod p$. Hence, in this step, only $\mathcal{C}_2$ needs to be considered.

Now, let's take a step further by express these F_{**} with $W_1, W_2, \cdots, W_s$. For each $d \cdot \sum_{t=0}^{R_2-1} v_t$ and h_{R_2-1-t} $(0 \le t \le R_2 - 1)$, we have

$$
\begin{aligned}
& F_{11}^{d\cdot\sum_{t=0}^{R_2-1} v_t} \cdot \prod_{t=0}^{R_2-1} F_{(t+2)1}^{h_{R_2-1-t}} \\
&= \left(\sum_{i=1}^{L} X_{11i} \prod_{w=1}^{s} W_w^{d\cdot e_{iw}} \right)^{d\cdot\sum_{t=0}^{R_2-1} v_t} \cdot \prod_{t=0}^{R_2-1} \left(\sum_{i=1}^{L} X_{(t+2)1i} \prod_{w=1}^{s} W_w^{d\cdot e_{iw}} \right)^{h_{R_2-1-t}} \\
&= \sum_{\substack{\sum_{i=1}^{L} g_{1i} = d\cdot\sum_{t=0}^{R_2-1} v_t \\ \sum_{i=1}^{L} g_{2i} = h_{R_2-1} \\ \sum_{i=1}^{L} g_{3i} = h_{R_2-2} \\ \cdots \\ \sum_{i=1}^{L} g_{(R_2+1)i} = h_0}} \mathcal{C}_4 \mathcal{C}_5 \cdot \prod_{w=1}^{s} W_w^{d\cdot\sum_{i=1}^{L}\left(e_{iw}\cdot\sum_{r=1}^{R_2+1} g_{ri}\right)},
\end{aligned}
$$

where

$$
\mathcal{C}_4 = \frac{(d \cdot \sum_{t=0}^{R_2-1} v_t)!}{\prod_{i=1}^{L}(g_{1i}!)} \prod_{r=2}^{R_2+1} \frac{h_{R_2-1+2-r}!}{\prod_{i=1}^{L}(g_{ri}!)}
$$

and

$$
\mathcal{C}_5 = \left(\prod_{i=1}^{L} X_{11i}^{g_{1i}} \right) \cdot \left(\prod_{r=2}^{R_2+1} \prod_{i=1}^{L} X_{r1i}^{g_{ri}} \right) = \prod_{r=1}^{R_2+1} \prod_{i=1}^{L} X_{r1i}^{g_{ri}}.
$$

Due to the similar reason, all X_{***} are assumed to be not 0 mod p, $\mathcal{C}_5$ mod p is not zero. Hence, we only need to check whether $\mathcal{C}_4 \neq 0 \pmod{p}$ or not.

From above analysis, for each $m' \le d^{R_3}$, one can represent $Z_{R_2 1}^{m'}$ as:

$$
Z_{R_2 1}^{m'} = \sum_{EQ_1} \left(\mathcal{C}_1 \mathcal{C}_2 \mathcal{C}_3 \cdot \sum_{EQ_2} \left(\mathcal{C}_4 \mathcal{C}_5 \cdot \prod_{w=1}^{s} W_w^{m_w} \right) \right),
$$

where

$$
m_w = d \cdot \sum_{i=1}^{L} \left(e_{iw} \cdot \sum_{r=1}^{R_2+1} g_{ri} \right)
$$

$$
EQ_1 : \begin{cases}
v_0 + h_0 + \sum_{r=1}^{R_2-1} u_{0r} = m' \\
v_1 + h_1 + \sum_{r=1}^{R_2-2} u_{1r} = d \cdot u_{0(R_2-1)} \\
v_2 + h_2 + \sum_{r=1}^{R_2-3} u_{2r} = d \cdot (u_{0(R_2-2)} + u_{1(R_2-2)}) \\
\qquad \cdots \\
v_{R_2-1} + h_{R_2-1} = d \cdot \sum_{t=0}^{R_2-2} u_{t1}
\end{cases}
$$

$$EQ_2: \sum_{i=1}^{L} g_{1i} = d \cdot \sum_{t=0}^{R_2-1} v_t \text{ and } \sum_{i=1}^{L} g_{ri} = h_{R_2+1-r},\ 2 \le r \le R_2+1.$$

In this case, if for all $m' \le d^{R_3}$, monomial $\prod_{w=1}^{s} x_w^{p-1}$ doesn't consists of $Z_{R_2 1}^{m'}$, one can find an integral distinguisher covering $(R_1+R_2+R_3)$ rounds. To achieve this, we consider the following conditions.

- $\mathcal{C}_2 \neq 0 \pmod p$ and $\mathcal{C}_4 \neq 0 \pmod p$.
- $m_w \ge p-1$ for any $1 \le w \le s$.
- To ensure that x_w^{p-1} is contained in $W_w^{m_w} = (x_w + rk_{0w})^{m_w}$, we have

$$\sum_{k=1}^{\lfloor \frac{m_w}{p-1} \rfloor} \binom{m_w}{k(p-1)} \neq 0 \pmod p.$$

  This can be converted to equations that can be recognized by automatic search tools using Proposition 6. That's the condition set BQ here.

G Integral Distinguishers of HadesMiMC under Other Prime Numbers

According to the specification of HadesMiMC [19], all primes such that $\lceil \log_2 p \rceil = t$ and $\log_2 p \approx t$ where $t \in \{8, 16\}$ can be used. Here, degree of S-Box is fixed as $d = 3$. So only those fulfill that $\gcd(3, p-1) = 1$ is kept.

When $t = 8$, there are 5 other primes $\{239, 233, 227, 197, 191\}$. Table 6 lists $TR_1 - TR_2$. Here, TR_1 is the number of rounds covered by the integral distinguisher found by our model, while TR_2 is that predicted only considering the maximal degree. For $t = 16$, there are 872 other primes. We list some of their distinguishers in Table 7 by means of $TR_1 - TR_2$.

Table 6: Integral distinguishers for HadesMiMC where $\log_2 p \approx 8$ and $n = 16$.

p	R_1	$s=1$	2	3	4	5	6	7	8	9	10	11	12	13	14	15
239	1	+1	+2	+4	+3	+3	+3	+3	+3	+3	+2	+2	+2	+2	+2	+2
	2	+1	+1	+1	+1	+1	+2	+2	+2	+2	+1	+1	+1	+1	+1	+1
233, 237	1	+1	+2	+3	+3	+3	+3	+3	+3	+3	+2	+2	+2	+2	+2	+2
	2	+1	+1	+1	+1	+1	+2	+2	+2	+2	+1	+1	+1	+1	+1	+1
197, 191	1	+1	+2	+3	+3	+3	+3	+3	+3	+3	+3	+3	+2	+2	+2	+2
	2	+1	+1	+1	+1	+1	+2	+2	+2	+2	+2	+2	+1	+1	+1	+1

Table 7: Integral distinguishers for HadesMiMC where $\log_2 p \approx 16$ and $n = 8$.

p	R_1	$s = 1$	2	3	4	5	6	7
65447, 65423, 65393, 65381, 65357, 65327, 65309	1	+1	+2	+3	+3	+3	+3	+3
	2	+1	+1	+1	+1	+2	+2	+2
59051	1	+2	+2	+3	+3	+3	+3	+3
	2	+2	+1	+1	+1	+2	+2	+2
59021, 59009, 58997, 58991, 58979, 58967, 58943	1	+1	+2	+3	+2	+2	+2	+2
	2	+1	+1	+1	+1	+1	+1	+1