IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, 62 pages.

Finer-Grained Fixed-Key Differential Probability Distributions via Quasidifferential Decoupling

Kai Hu[2], Thomas Peyrin[1], Quan Quan Tan[3], Hongyi Zhang[a,1] and Chunning Zhou[1]

[1] Nanyang Technological University, Singapore, Singapore
[2] Shandong University, Qingdao, China
[3] Inria, Paris, France

Abstract

The recent study of fixed-key differential probabilities mainly follows two complementary approaches. The first derives key-dependent constraints from the internal structure of the primitive. This approach is intuitive, but a complete theory is difficult to build. The second approach is based on quasidifferentials. It is complete in theory when all quasidifferentials are considered, but exhaustive enumeration is usually infeasible in practice.

In this paper, we relate quasidifferentials to concrete key-dependent constraints. This gives new insights into quasidifferentials. Each quasidifferential with a nonzero mask carries one relation, equating a linear parity of the involved key bits to a generally nonlinear Boolean function of the intermediate-state bits, and the relations that share these bits together constrain the key. Under the common threshold-based treatment, where only quasidifferential trails with sufficiently large absolute correlation are kept, some constraints on intermediate-state bits may be lost. This can produce an *incomplete* quasidifferential trail set with respect to the induced intermediate-state constraints. This, for example, can result in the fixed-key differential probabilities computed by quasidifferential aggregation to become negative on some key subspaces.

To obtain a more precise distribution of fixed-key differential probabilities over the key space, we decouple quasidifferential trails according to their induced constraints. After decoupling, each resulting quasidifferential trail set is *locally complete*, so the derived probability distribution for the particular subspace is always valid. The decoupling also reduces the number of trails in each set, improving the efficiency of the quasidifferential method. As a result, our method yields a finer-grained key-space partition that could allow us to better approximate the true distribution under the quasidifferential framework.

We instantiate this decoupling strategy in the threshold-based setting and apply it to differential trails of `GIFT-64`, `GIFT-128`, `SKINNY-64`, `SKINNY-128`, and `RECTANGLE`. The resulting locally complete trail sets always give valid fixed-key differential probability distributions and are no coarser than direct threshold-based quasidifferential aggregation. They coincide with direct aggregation when the retained trails are already locally complete. In our experiments, using our decoupling method is actually better for many evaluated trails and refines the key-space restrictions reported by prior constraint-detection frameworks. As each quasidifferential is a constraint, the same insight also lets us write the induced linear and nonlinear key constraints explicitly for the bit-wise ciphers `GIFT-64`, `GIFT-128` and `RECTANGLE`, addressing a limitation of the Trail-Estimator constraint detector described in [PTZZ25].

Emails: kai.hu@sdu.edu.cn (Kai Hu), thomas.peyrin@ntu.edu.sg (Thomas Peyrin), quanquan.tan@inria.fr (Quan Quan Tan), hongyi003@e.ntu.edu.sg (Hongyi Zhang), chunning.zhou@ntu.edu.sg (Chunning Zhou)
[a]Corresponding Author

Keywords: Quasidifferential, Differential cryptanalysis, Constraint detection, Probability estimation

1 Introduction

Differential cryptanalysis, introduced by Biham and Shamir [BS90], studies how an input difference propagates through a symmetric-key primitive. The probability of a differential characteristic (DC) is usually estimated by multiplying the local transition probabilities along it. The Markov cipher assumption justifies this for the key-averaged probability, and stochastic equivalence assumes that the fixed-key probability stays close to this average [LMM91]. These assumptions make DC search tractable. They also replace the fixed key by an average over keys, although the key is fixed throughout an attack and the fixed-key probability can lie far from the average. Peyrin and Tan found that 21 of 43 published `SKINNY` DCs and 1 of 15 `GIFT-64` DCs are impossible, and that most of the rest hold only on a small part of the key space [PT22]. Plateau DCs are the classical case, constant on a set of weak keys and zero elsewhere [DR07], and such behaviour is common in lightweight ciphers, whose simple round functions and key schedules tie state and key bits together [CF25, PT22]. This has a direct impact on attacks. When the DCs of a differential are valid on different weak-key sets, adding their probabilities overestimates the differential because no clustering takes place [CF25], and an average can hide weak keys whose probability is far above the mean [BR22]. The fixed-key probability decides which keys support a DC and how the attack complexity is spread over the key space.

One line of work exposes this key dependence by tracing value restrictions through the cipher [PT22, Sun26, PTZZ25, NGJE25]. Peyrin and Tan follow the input and output values that allow each S-box transition and derive the conditions on the round keys that a DC requires [PT22]. Read directly from the internal equations, these conditions are interpretable, and they let the method invalidate published DCs or restrict them to a key subspace. Sun observed that in the case of `GIFT-64`, the mapping of right values through active S-boxes is affine, leading to what is known as the linearized constraints. This allows them to detect additional constraints [Sun26], and the `Trail-Estimator` automates the detection of such conditions [PTZZ25]. The approach is intuitive, but it has not been shown to capture every condition. `Trail-Estimator` and [BDG25] note that the earlier detector does not consider all relations among the variables and misses some of them [PTZZ25]. The analysis is also organized around cells, which limits its reach on ciphers whose linear layer and key schedule act on single bits, such as `GIFT-64` and `RECTANGLE`.

The geometric approach of Beyne gives a unified algebraic account of linear cryptanalysis, in which each cryptanalytic property of a primitive is evaluated through a single linear map, the transition matrix, on the space of functions over its state, and the usual variants of linear cryptanalysis appear as instances of one construction [Bey21]. Carrying this viewpoint to differential cryptanalysis in the fixed-key model yields the quasidifferential framework of Beyne and Rijmen, which describes the same key dependence in a single language [BR22]. A quasidifferential characteristic (QDC) attaches a mask to the values that satisfy each transition of a DC, so it records a probabilistic linear relation among those values, and its correlation carries the involved key bits through the key additions. The quasidifferential transition matrices are the differential counterpart of the correlation matrices of linear cryptanalysis, which puts the two theories on the same footing. Summing the correlations of all QDCs of a DC gives its exact fixed-key probability, with no further hypothesis [BR22, BDG25]. In this sense the framework is complete and partitions the key space precisely [BDG25]. It also covers the constraint viewpoint. Sun also observes that the conditions her method found can equivalently be obtained from QDCs [Sun26]. However, this completeness comes at high computational cost. In practice, for the search of QDCs without a fixed DC, we will have to use the full quasidifferential transition matrix,

which is much larger than the difference distribution table. To the best of our knowledge, no one has attempted such a search. If a DC is fixed during the search process, the required parts of a quasidifferential transition matrix reduces to a size similar to that of a difference distribution table and the search is reduced to a level comparable to that of searching for (all) DCs. However, this is by no means an easy task. A practical search done by [BDG25] further only keeps the QDCs whose absolute correlation exceeds a certain bound.

This bound sacrifices the exactness that the full family of QDCs guarantees. The exact probability is a signed sum over the complete family of QDCs, and a thresholded search replaces it by a partial sum. Boura, Derbez and Germon report that on `SKINNY-128` DCs this partial sum takes negative values for some key bits, so it cannot be a fixed-key probability [BDG25]. They show that the effect is intrinsic to QDCs rather than an artifact of their model, and that the assumption that low-correlation QDCs are negligible can fail. Boura, Derbez and Germon explicitly leave this as an open problem, namely identifying "a criterion for quasidifferential trails that ensures a reliable formula" [BDG25].

Contributions. We resolve this open problem by connecting the two lines of work above. In Section 3 we show that each QDC carries one relation on the round-key bits, so the QDCs that share a set of masked state bits all constrain those bits. This correspondence explains the negative probabilities of Boura, Derbez and Germon. Such a set of bits is evaluated correctly only when every QDC that constrains it is kept; we call such a set of QDCs complete on those bits. A correlation threshold keeps some of these QDCs and drops others, so the constraints on those bits are left incomplete, and the resulting partial sum is no longer a probability. The negative values are the visible symptom of this incompleteness.

In Section 4, we turn this diagnosis into a method, namely Decoupling QuasiDifferential (`Decoupling-QD`). Muting some intermediate-state bits isolates the masks of different QDCs from one another, so the constraints they support become independent and the QDCs decouple into separate groups. Within each group the QDCs are enumerated exhaustively, so each group is locally complete by construction, and the distribution it induces is a genuine probability distribution. This removes the negative values on every DC we test, and it is the criterion left open by Boura, Derbez and Germon. The remaining cost is resolution, since the fineness of the distribution depends on the search budget. Decoupling helps as the groups are independent, each local QDC in one group combines with a local QDC in every other group into a distinct global QDC, so the per-group QDC counts multiply. At a fixed budget the decoupled search therefore covers far more QDCs than a direct enumeration, and on many DCs it yields a strictly finer key-space distribution than prior work, as shown in Table 1 and Figure 2 (Section 5).

In Section 5, we apply the method to DCs of `GIFT-64`, `GIFT-128`, `SKINNY-64`, `SKINNY-128` and `RECTANGLE`, and collect the results in Table 1 and 2. It returns a valid distribution on every DC, including the `SKINNY` DCs on which a direct thresholded quasidifferential computation gives negative probabilities. It recovers the key-space restrictions reported by prior constraint-detection work [PT22, Sun26, PTZZ25, NGJE25], and on 9 DCs it refines them into a finer key-space distribution than any previous framework. Reading each QDC as a constraint also makes the induced key constraints explicit, linear and nonlinear, at the bit level. This answers a second open problem: the constraint detector in [PTZZ25] is built for word-oriented ciphers and its applicability declines for bit-wise ciphers, whereas our reading gives the bit-wise constraints directly for `GIFT-64`, `GIFT-128` and `RECTANGLE`.

Outline. The remainder of the paper is organized as follows. Section 2 provides an overview of the background and related works. Section 3 establishes the correspondence between QDCs and key constraints. Section 4 presents the decoupling method. Section 5 reports the experimental results on `GIFT-64`, `GIFT-128`, `SKINNY-64`, `SKINNY-128`,

Table 1: Results comparison between `Decoupling-QD` and threshold-based QD. Values highlighted in blue indicate cases where `Decoupling-QD` achieves a strictly more precise probability estimation than all previous work. The `Decoupling-QD` and threshold-based QD always use the same correlation bound in experiments. With an appropriate choice of correlation-weight threshold (Definition 8), `Decoupling-QD` covers at least as many trails as the threshold-based quasidifferential method.

Cipher	R	Stated Prob.	# Covered QDCs		Cor. Bound	CW_{thres} ($\times P_{avg}$)	Distribution by `Decoupling-QD`	Distribution by `Thresholded QD`	Trail Source
			`Decoupling-QD`	`QD`					
GIFT-64	9	2^{-42}	11312	11312	2^{-58}	1	$2^{-38.1} - 2^{-37.9}$	$2^{-38.1} - 2^{-37.9}$	Table 2 [LWZZ19]
	10	2^{-57}	8448	5088	2^{-64}	0.5	$2^{-53.5} - 2^{-50.94}$	$2^{-53.3} - 2^{-51.3}$	Table 5 [JYSYZ+18]
	12	2^{-60}	17440	1088	2^{-70}	1	$2^{-56.2} - 2^{-55.8}$	$2^{-56.1} - 2^{-55.9}$	Table 3 [CZD20]
	12	2^{-58}	4000	416	2^{-65}	1	$2^{-53.3} - 2^{-52.7}$	$2^{-53.1} - 2^{-52.9}$	Table 7 [LWZZ19]
	12	2^{-59}	3048	1160	2^{-68}	0.5	$2^{-56.9} - 2^{-55.3}$	$2^{-56.4} - 2^{-55.7}$	Table 4 [ZDY19]
	12	2^{-60}	1	1	2^{-68}	1	2^{-60}	2^{-60}	Table 6 [ZDY19]
	13	2^{-62}	8000	832	2^{-68}	1	$2^{-56.3} - 2^{-55.9}[E]$	$2^{-56.2} - 2^{-55.8}$	Table 8 [LWZZ19]
	13	2^{-64}	2	2	2^{-70}	1	2^{-63}	2^{-63}	Table 8-1 [SWW21b]
	13	2^{-64}	64	64	2^{-70}	1	2^{-59}	2^{-59}	Table 8-2 [SWW21b]
	13	2^{-64}	552	552	2^{-70}	1	$2^{-61.2} - 2^{-60.8}$	$2^{-61.2} - 2^{-60.8}$	Table 8-3 [SWW21b]
	18	2^{-58}	11520	11520	2^{-64}	1	$2^{-52} - 2^{-48.9}$	$2^{-51} - 2^{-49.42}$	Figure 8 [SWW21a]
GIFT-128	12	$2^{-62.4}$	4	4	2^{-70}	0.01	$2^{-61.41} - 2^{-61.39}$	$2^{-61.41} - 2^{-61.39}$	Table 13 [ZDY19]
	18	2^{-109}	Invalid	Invalid	2^{-112}	1	–	–	Table 10 [ZDY19]
	20	$2^{-121.4}$	64	64	$2^{-127.4}$	1	$2^{-115.4}$	$2^{-115.4}$	Trail 1 [JZZD21, Tab. 12]
	20	$2^{-122.4}$	1280	1280	$2^{-132.4}$	1	$2^{-114.41} - 2^{-114.4}[E]$	$2^{-114.41} - 2^{-114.4}$	Trail 2 [JZZD21, Tab. 12]
	20	$2^{-122.4}$	1280	1280	$2^{-132.4}$	1	$2^{-114.41} - 2^{-114.4}[E]$	$2^{-114.41} - 2^{-114.4}$	Trail 3 [JZZD21, Tab. 12]
	20	$2^{-123.4}$	2560	2560	$2^{-133.4}$	1	$2^{-114.412} - 2^{-114.388}[E]$	$2^{-114.41} - 2^{-114.4}$	Trail 4 [JZZD21, Tab. 12]
SKINNY-64	5	2^{-44}	4608	4608	2^{-50}	1	$2^{-39.3} - 2^{-35.8}$	$2^{-39} - 2^{-35.4}$	Table 4 [PT22]
	7	2^{-52}	4.3×10^6	83840	2^{-58}	1	$2^{-47.4} - 2^{-42.7}[E]$	✘	Table 6 [DDH+21]
	10	2^{-46}	Invalid	Invalid	2^{-48}	1	–	–	Table 7 [DDH+21]
	13	2^{-55}	16	16	2^{-60}	1	2^{-51}	2^{-51}	Table 8 [DDH+21]
	15	2^{-54}	224	224	2^{-58}	1	$2^{-48} - 2^{-47}$	$2^{-48} - 2^{-47}$	Table 9 [DDH+21]
SKINNY-128	13	2^{-123}	Invalid	Invalid	2^{-125}	1	–	–	Table 11 [AST+17]
	14	2^{-120}	1.3×10^7	7168	2^{-122}	1	$2^{-120.7} - 2^{-107.8}[E]$	✘	Table 10 [DDH+21]
	16	$2^{-127.66}$	1.4×10^9	88624	2^{-131}	0.25	$2^{-134.2} - 2^{-111.1}[E]$	✘	Table 11 [DDH+21]
RECTANGLE	14	2^{-63}	24576	444	2^{-68}	1	$2^{-68.7} - 2^{-58.1}$	✘	[ZBL+14, Appendix E]
	14	2^{-66}	1×10^6	516	2^{-70}	1	$2^{-69.9} - 2^{-60.2}$[E]	✘	[ZBL+14, Appendix E]

R: the round number of the differential trail; Stated Prob.: the probability reported by the original authors; **# Covered QDCs**: the number of covered QDCs of both methods under same correlation bound; The **Distribution** columns detail the range of conditional probabilities across the valid key space, contrasting `Decoupling-QD` against the threshold-based QD framework; CW_{thres}: the threshold of correlation weight to filter bits, for example, the value 0.5 means $CW_{thres} = 0.5 \times P_{avg}$; $[E]$: results are estimated based on sampled master keys; ✘: there is negative probability within estimated distribution.

and `RECTANGLE`. Section 6 compares the `Decoupling-QD` with previous work. Section 7 concludes the paper.

2 Preliminaries

2.1 Differential Characteristics and the Markov Assumption

Differential cryptanalysis [BS90] studies the propagation of input differences through a block cipher to the corresponding output differences. The central object of this analysis is the *differential characteristic*, which we define below.

Definition 1 (One-round differential characteristic [BS90])**.** Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. A *one-round differential characteristic* of F is a pair $(\Delta_{\text{in}}, \Delta_{\text{out}}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ of input and output differences. Its probability, taken over a uniformly random $x \in \mathbb{F}_2^n$, is

$$P(\Delta_{in} \to \Delta_{out}) = \frac{\#\{x \in \mathbb{F}_2^n : F(x) \oplus F(x \oplus \Delta_{in}) = \Delta_{out}\}}{2^n}.$$

Definition 2 (r-round differential characteristic [BS90])**.** Let $F = F_r \circ F_{r-1} \circ \cdots \circ F_1$ be the composition of r vectorial Boolean functions $F_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$. An *$r$-round differential characteristic (DC)* of F is a tuple $\mathcal{T} = (\Delta_{in} = \Delta_0, \Delta_1, \ldots, \Delta_r = \Delta_{out})$, where Δ_i is the n-bit output difference of $F_i \circ \cdots \circ F_1$ $(0 < i \leq r)$.

Computing the exact probability of an r-round DC is usually intractable, so cryptographers rely on the Markov cipher assumption.

Table 2: Results comparison between `Decoupling-QD` and previous constraint-detection work for `GIFT`, `SKINNY` and `RECTANGLE`. Notably, `Decoupling-QD` is the first to identify bit-wise probabilistic constraints, which introduce non-uniformity into probability distribution. Meanwhile, `Decoupling-QD` recovers all linear constraints on keys.

Cipher	R	Stated Prob.	Reduction on Key Space ($\log_2$)					# New Cons.	Trail Source
			[PTZZ25]	[Sun26]	[PT22]	[NGJE25]	`Decoupling-QD`		
GIFT-64	9	2^{-42}	–	–	4	4	**4**	1	Table 2 [LWZZ19]
	10	2^{-57}	–	5	–	–	**5.02**$^{[E]}$	2	Table 5 [JYSYZ+18]
	12	2^{-60}	–	3 (4°)	–	–	**3.03**$^{[E]}$	1	Table 3 [CZD20]
	12	2^{-58}	–	–	4	4	**4**	1	Table 7 [LWZZ19]
	12	2^{-59}	–	–	3	3	**3**	2	Table 4 [ZDY19]
	12	2^{-60}	–	–	0	0	**0**	0	Table 6 [ZDY19]
	13	2^{-62}	–	–	4	4	**4**	1	Table 8 [LWZZ19]
	13	2^{-64}	–	–	1	1	**1**	0	Table 8-1 [SWW21b]
	13	2^{-64}	–	–	5	5	**5**	0	Table 8-2 [SWW21b]
	13	2^{-64}	–	–	3	3	**3**	0	Table 8-3 [SWW21b]
	18	2^{-58}	–	8	–	–	**8**	2	Figure 8 [SWW21a]
GIFT-128	12	$2^{-62.4}$	–	1	1	1	**1**	1	Table 13 [ZDY19]
	18	2^{-109}	–	Invalid	Invalid	Invalid	**Invalid**	1	Table 10 [ZDY19]
	20	$2^{-121.4}$	–	–	–	–	**5**	0	Trail 1 [JZZD21, Tab. 12]
	20	$2^{-122.4}$	–	7	–	–	**7.05**$^{[E]}$	2	Trail 2 [JZZD21, Tab. 12]
	20	$2^{-122.4}$	–	7	–	–	**7**$^{[E]}$	2	Trail 3 [JZZD21, Tab. 12]
	20	$2^{-123.4}$	–	9	–	–	**9.01**$^{[E]}$	2	Trail 4 [JZZD21, Tab. 12]
SKINNY-64	5	2^{-44}	–	–	–	–	**6.9**	2	Table 4 [PT22]
	7	2^{-52}	7.3	6	6	–	**7.1**$^{[E]}$	2	Table 6 [DDH+21]
	10	2^{-46}	Invalid	Invalid	Invalid	–	Invalid	1	Table 7 [DDH+21]
	13	2^{-55}	4	4	4	–	**4**	0	Table 8 [DDH+21]
	15	2^{-54}	6.2	6.2	6.2	[6.11, 6.48]	**6.2**	1	Table 9 [DDH+21]
SKINNY-128	13	2^{-123}	Invalid	–	Invalid	Invalid	Invalid	0	Table 11 [AST+17]
	14	2^{-120}	8.1	–	7.66	–	**7.65**$^{[E]}$	4	Table 10 [DDH+21]
	16	$2^{-127.66}$	7.1(11.1†)	–	6.1	–	**6.4**$^{[E]}$	3	Table 11 [DDH+21]
RECTANGLE	14	2^{-63}	–	–	–	1	**1**	12	[ZBL+14, Appendix E]
	14	2^{-66}	–	–	–	2	**2**$^{[E]}$	11	[ZBL+14, Appendix E]

R: the round number of the differential trail; Stated Prob.: the probability reported by the original authors; **Reduction on Key Space**: the $\log_2$ reduction factor of the valid key space; **#New Cons.**: the number of newly identified bit-wise probabilistic nonlinear constraints; $[E]$: results are estimated via sampling method; Dash ("–"): indicates the method was not applied to the given trail; $\diamond$ The value 4 reported in [Sun26] is a typo, and we verify the corrected value is 3; The value $11.1^{\dagger}$ reported in [PTZZ25] is a typo, and we verified the corrected value is 7.1 based on their codes.

Definition 3 (Markov cipher [LMM91])**.** An iterated cipher with one-round map $Y = \mathcal{C}(X, k)$, where $\mathcal{C}$ encrypts state X under subkey k, is said to be a Markov cipher if there exists a group operation $\otimes$ for defining differences such that, for any nonzero choices of Δ_{in} and Δ_{out}, the probability

$$P(\Delta_Y = \Delta_{\text{out}} \mid \Delta_X = \Delta_{\text{in}}, X = \gamma) = P(\Delta_Y = \Delta_{\text{out}} \mid \Delta_X = \Delta_{\text{in}})$$

holds when the subkey k is uniformly random.

Under the Markov assumption, the probability of a difference transition from Δ_{in} to Δ_{out} is independent of the value of X.

We also use the hypothesis of stochastic equivalence, which assumes the probability of a DC stays approximately the same across all key values.

Definition 4 (Hypothesis of stochastic equivalence [LMM91])**.** For an r-round DC ($\Delta_{in} = \Delta_0, \Delta_1, \ldots, \Delta_r = \Delta_{out}$),

$$P(\Delta_1 = \delta_1, \ldots, \Delta_r = \delta_r \mid \Delta_0 = \delta_0) \approx P(\Delta_1 = \delta_1, \ldots, \Delta_r = \delta_r \mid \Delta_0 = \delta_0, k_1 = \beta_1, \cdots, k_r = \beta_r)$$

for almost all subkey values $(k_1 = \beta_1, \cdots, k_r = \beta_r)$, where k_i is the subkey of round i, $1 \leq i \leq r$.

Under these assumptions, the probability of a DC $\mathcal{T} = (\Delta_0, \Delta_1, \ldots, \Delta_r)$ is estimated as the product of the per-round S-box transition probabilities,

$$\Pr[\mathcal{T}] \;\approx\; \prod_s \Pr[a_s \xrightarrow{S} b_s],$$

where s ranges over the active S-boxes with prescribed input and output differences a_s, b_s. Note that this estimate is key-averaged, the fixed-key probability $\Pr[\mathcal{T} \mid k]$, however, can deviate substantially from it, as the prescribed differences fix value restrictions at the active S-boxes whose consistency with a given key is determined by the key schedule and the linear layer.

2.2 Quasidifferential Characteristics

The quasidifferential technique [BR22] applies the geometric approach [Bey21] to differential cryptanalysis. The geometric approach is a unified language for cryptanalytic techniques, and has been applied to linear [Bey21], differential [BR22], integral [BV23, BV24, BV25], differential-linear [HZC+25, HNW26], and boomerang [CHH+25] cryptanalysis.

In the language of the geometric approach, statements about a function $F\colon X \to Y$ between finite sets become statements about a linear map $T^F\colon \mathbb{K}[X] \to \mathbb{K}[Y]$ between vector spaces over a field $\mathbb{K}$. The free vector space $\mathbb{K}[X]$ on a finite set X consists of all linear combinations $\sum_{x\in X} u[x]\,\delta_x$, with coordinates $u[x] \in \mathbb{K}$ and formal basis vectors δ_x; an element of $\mathbb{K}[X]$ assigns a weight to each state. For $F\colon X \to Y$, the map $T^F\colon \mathbb{K}[X] \to \mathbb{K}[Y]$ is defined by $T^F\,\delta_x = \delta_{F(x)}$. The dual space $\mathbb{K}^X$ consists of the $\mathbb{K}$-valued functions on X, which probe states. A cryptanalytic property of F is then a pair (u, v) with $u \in \mathbb{K}[X]$ and $v \in \mathbb{K}^Y$, evaluated as $v(T^F u)$.

For differential cryptanalysis, $X = G \times G$ for a finite Abelian group G, and F is extended to pairs by $(x, y) \mapsto (F(x), F(y))$. The associated basis is the quasidifferential basis [BR22]. We take $X = \mathbb{F}_2^n \times \mathbb{F}_2^n$ and $\mathbb{K} = \mathbb{R}$, for which the quasidifferential basis of the function space $\mathbb{K}^X$ on pairs has vectors

$$q^{(u,a)}(x, y) = (-1)^{u^\top x}\,\delta_a(x + y).$$

Definition 5 (Quasidifferential transition matrix (QDTM))**.** Under the quasidifferential basis, the matrix corresponding to $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the matrix representation of the pair map $T^F \otimes T^F$. This quasidifferential transition matrix has entries

$$D^F_{(v,b),(u,a)} = 2^{-n} \sum_{\substack{x\in\mathbb{F}_2^n \\ F(x+a)=F(x)+b}} (-1)^{u^\top x + v^\top F(x)}.$$

Setting $u = v = 0$ recovers the differential probability of F for input and output differences a and b,

$$D^F_{(0,b),(0,a)} = 2^{-n} \sum_{\substack{x\in\mathbb{F}_2^n \\ F(x+a)=F(x)+b}} 1 = \Pr[a \xrightarrow{F} b].$$

For a composite $F = F_r \circ F_{r-1} \circ \cdots \circ F_1$, the transition matrix factorises as $D^F = D^{F_r} D^{F_{r-1}} \cdots D^{F_1}$, so a single entry is a sum over intermediate indices,

$$D^F_{\omega_r,\omega_0} = \sum_{\omega_{r-1},\ldots,\omega_1} D^{F_r}_{\omega_r,\omega_{r-1}} D^{F_{r-1}}_{\omega_{r-1},\omega_{r-2}} \cdots D^{F_1}_{\omega_1,\omega_0},$$

where $\omega_i = (u_i, a_i)$ pairs a *mask* u_i with a *difference* a_i. The sequence $(\omega_0, \omega_1, \ldots, \omega_r)$ is a *quasidifferential characteristic (QDC)*, and the corresponding product of entries is its *correlation*.

When all the masks are zero, the QDC reduces to the sequence of differences $(a_0, a_1, \ldots, a_r)$, which is the underlying DC. The probability of a DC is the sum of the correlations of all QDCs with that difference sequence:

$$\Pr[(a_0, a_1, \ldots, a_r)] = \sum_{u_1, u_2, \ldots, u_{r-1}} D^{F_r}_{(0,a_r),(u_{r-1},a_{r-1})} D^{F_{r-1}}_{(u_{r-1},a_{r-1}),(u_{r-2},a_{r-2})} \cdots D^{F_1}_{(u_1,a_1),(0,a_0)}.$$

The two end masks are zero, hence, such a QDC is written as $(0, u_1, u_2, \ldots, u_{r-1}, 0)$. These intermediate masks are found by an automated trail search, using an SMT model [BR22] or a MILP model [BDG25].

2.3 Constraints on the Key Bits

A fixed DC pins value restrictions on the intermediate states, and through the round-key additions these restrictions become relations on the key. We write such a relation in a single form. A *constraint* of a DC is an equation

$$v^\top k \oplus \lambda(x) = c,$$

where k collects the round-key bits, v selects an $\mathbb{F}_2$-linear combination of them, λ is a Boolean function of the intermediate-state values x along the DC, and $c \in \mathbb{F}_2$ is a constant. Such constraints are what the constraint-detection line extracts from the cipher equations [PT22, Sun26, PTZZ25]; Section 3 shows that they are exactly the relations carried by quasidifferential characteristics.

3 From Quasidifferential Characteristics to Key Constraints

Section 2 wrote a key constraint as $v^\top k \oplus \lambda(x) = c$. We show that each QDC of a DC carries one such relation: its key masks give the key side $v^\top k$, and its S-box masks give the non-key side λ. The QDCs that act on a common set of bits each constrain those bits, and the fixed-key probability is recovered correctly only when the whole set of them is kept. In Section 3.1 we read this off a toy cipher. We also point out the problem of the so-called *incompleteness* in current methods in generating quasidifferential trails that is the cause of an open problem mentioned by Boura, Derbez and Germon [BDG25]. In Section 3.2, we show how we can derive the key constraints, which puts it on the same level (in terms of intuitiveness) with the various value restriction methods. In Section 3.3, we define *completeness* which can be used to decide if a set of QDCs gives a reliable probability. This will be the criterion to solve the open problem aforementioned.

3.1 A Toy Example

The cipher of Figure 1 has two 4-bit nibbles and three rounds; each round applies the `GIFT-64` S-box to both nibbles, a bit permutation, and a round-key XOR on every wire. We study the DC [4]

$$\mathcal{T}: \quad (2,0) \to (5,0) \to (0,5) \to (0,15) \to (13,8) \to (4,*),$$

which activates S_A, S_C, S_D with transitions $2 \to 5$, $5 \to 15$, $13 \to 4$ of probability $\frac{1}{4}$, so its average probability is 2^{-6}; the S-box S_B on the bridge carries no difference and stays inactive.

By the expansion of Section 2, a QDC q contributes $(-1)^{\mu_q^\top k} \operatorname{cor}(q)$, where μ_q collects the masks q places on the keyed wires; a key XOR $x \mapsto x \oplus k$ has QDTM entries

[4] This is actually a truncated DC, but the truncation does not influence our analysis.

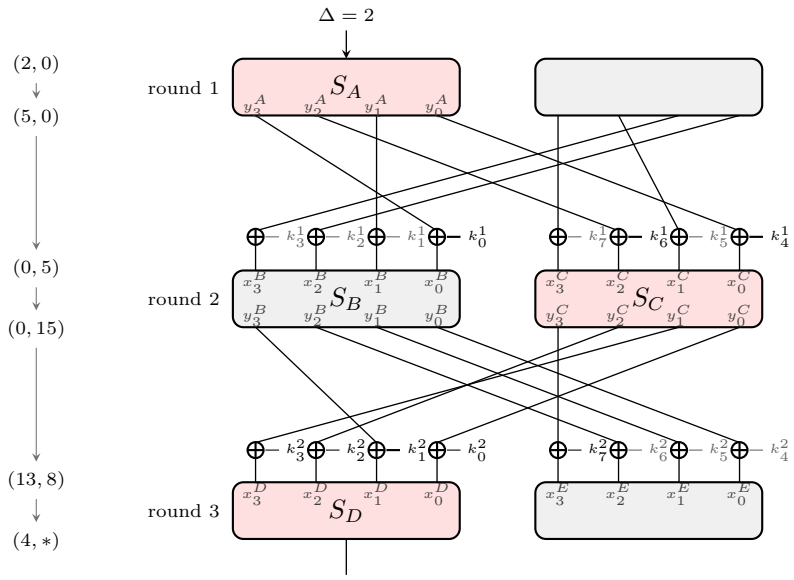


Figure 1: The three-round toy cipher. The red (resp. gray) boxes are the active (resp. inactive) S-boxes. Each $\oplus$ adds the round-key bit drawn to its right.

$(-1)^{u^\top k}\delta_{u,v}\delta_{a,b}$, so a mask crossing a key addition only picks up the sign $(-1)^{u^\top k}$. Exactly four QDCs of $\mathcal{T}$ are non-zero, written by their nibble masks (Γ^0, Γ^1) at the inputs of rounds $1, 2, 3$:

	quasidifferential characteristic	$\mathrm{cor}(q)$	key sign
q_0	$(0,0) \to (0,0) \to (0,0)$	2^{-6}	$+1$
q_1	$(0,0) \to (0,5) \to (0,0)$	2^{-6}	$(-1)^{k_4^1 \oplus k_6^1}$
q_2	$(0,0) \to (1,0) \to (2,0)$	-2^{-7}	$(-1)^{k_0^1 \oplus k_1^2}$
q_3	$(0,0) \to (1,5) \to (2,0)$	-2^{-7}	$(-1)^{k_4^1 \oplus k_6^1 \oplus k_0^1 \oplus k_1^2}$

We read each QDC as a relation on the key. Its key masks give a key parity, and the S-box masks it carries give a parity of intermediate bits; the bits it acts on are where its masks are non-zero, not where the difference is, so q_2 reaches the inactive S_B. The four read off as

- q_0 carries no mask, so it adds no relation; it is the average-probability term 2^{-6}.
- q_1 carries the parity $y_0^A \oplus y_2^A$ of S_A and the key mask $k_4^1 \oplus k_6^1$, the relation $k_4^1 \oplus k_6^1 \oplus (y_0^A \oplus y_2^A) \oplus 1 = 0$.
- q_2 carries the parity $x_0^B \oplus y_3^B$ of the inactive S_B and the key mask $k_0^1 \oplus k_1^2$, the relation $k_0^1 \oplus k_1^2 \oplus (x_0^B \oplus y_3^B) \oplus 1 = 0$.
- q_3 carries both parities and both key masks, the relation $k_4^1 \oplus k_6^1 \oplus k_0^1 \oplus k_1^2 \oplus (y_0^A \oplus y_2^A) \oplus (x_0^B \oplus y_3^B) = 0$.

These relations are of two kinds. A relation is of the first kind when the parity is constant on the right pairs of the DC, so the carrying QDC has $|\mathrm{cor}(q)| = P_{avg}$ (the probability of the studied DC, i.e., 2^{-6} for this example). It is a hard key condition that removes part of the key space, and we call it a *deterministic constraint*. The S_A parity $y_0^A \oplus y_2^A$ is constant, equal to 1, on the pairs that take $2 \to 5$, so q_1 pins the hard key

condition $k_4^1 \oplus k_6^1 = 0$. A relation is of the second kind when the parity is not constant, so the QDC has $0 < |\mathrm{cor}(q)| < P_{avg}$. It holds only for a fraction of the values, which makes the fixed-key probability non-uniform over the surviving keys rather than removing them; we call it a *probabilistic constraint*. The S_B parity $x_0^B \oplus y_3^B$ is not constant: it has correlation $\frac{1}{2}$ over the bridge, so q_2 holds only with probability $\frac{3}{4}$ when $k_0^1 \oplus k_1^2 = 1$ and contributes a biased term, not a fixed condition. Which kind a parity gives is set by its correlation, not by whether its S-box is active.

No QDC is a fixed-key probability on its own; the probability is their signed sum. With $a = k_4^1 \oplus k_6^1$ and $b = k_0^1 \oplus k_1^2$,

$$\Pr[\mathcal{T} \mid k] = \sum_i (-1)^{\mu_{q_i}^\top k} \mathrm{cor}(q_i) = \big(1 + (-1)^a\big)\big(2^{-6} - 2^{-7}(-1)^b\big),$$

which is 0 when $a = 1$, and 2^{-6} or $3 \cdot 2^{-6}$ when $a = 0$, according to b. The hard condition $a = 0$ from q_1 halves the key space; the biased pair q_2, q_3 splits the surviving half. The four must be summed together: dropping q_3, the set $\{q_0, q_1, q_2\}$ sums to $2^{-6}(1 + (-1)^a) - 2^{-7}(-1)^b$, which on the keys with $a = 1, b = 0$ reads -2^{-7}, no longer a probability. This is a toy example illustrating the reason behind negative probabilities reported on `SKINNY-128` by [BDG25].

3.2 The Correspondence

The toy shows the general pattern. Every QDC of a DC carries one relation on the key, and the fixed-key probability is the signed sum of their contributions $(-1)^{\mu_q^\top k} \mathrm{cor}(q)$ over a set of QDCs.

Definition 6 (Masked bits of a QDC)**.** The *masked bits* $\mathrm{mb}(q)$ of a QDC q are the intermediate-state bits on which q places a non-zero mask.

At each S-box in $\mathrm{mb}(q)$ the QDC selects a parity $u^\top x \oplus v^\top S(x)$ of the input and output bits. The bits it acts on are where its masks are non-zero, not where the difference is, which is why q_2 reaches the inactive S_B.

Proposition 1 (Each QDC carries a relation)**.** *Every QDC q of a DC $\mathcal{T}$ carries one relation*

$$\mu_q^\top k = \lambda_q(x) \oplus c_q,$$

an equation of the form of Section 2, where $\mu_q^\top k$ is the parity of the round-key bits that q masks, λ_q is the XOR of the masked S-box parities $u^\top x \oplus v^\top S(x)$ that q selects, and $c_q \in \mathbb{F}_2$ is a constant. Its contribution to $\Pr[\mathcal{T} \mid k]$ is the signed term $(-1)^{\mu_q^\top k} \mathrm{cor}(q)$.

Proof. A QDC is a linear characteristic on the right values (one value of the right pairs) that are restricted by the DC, thus its behavior is the same as a normal linear characteristic. The masks of q are propagated by the transpose of each linear layer, so across a linear map L the incoming and outgoing masks satisfy $u_{\mathrm{in}} = L^\top u_{\mathrm{out}}$. Each masked internal bit then appears in exactly two of the affine relations that q selects, on the output side of one map and the input side of the next, and cancels when these relations are added. What remains is the round-key parity $\mu_q^\top k$ on one side, and the XOR of the masked S-box parities $u^\top x \oplus v^\top S(x)$ with the affine constants on the other (assume we do not cancel variables), that is $\lambda_q(x) \oplus c_q$. □

A single QDC gives one relation and one signed term, not a probability. The relation is a deterministic constraint when $|\mathrm{cor}(q)| = P_{avg}$, fixing a condition that removes part of the key space, and a probabilistic constraint when $0 < |\mathrm{cor}(q)| < P_{avg}$, biasing the fixed-key probability over the surviving keys. The masked S-box parity $u^\top x \oplus v^\top S(x)$ is affine in

the wire variables, but eliminating the internal wires writes λ_q as a Boolean function of the free variables that is in general nonlinear; the parity $x_0^B \oplus y_3^B$ of q_2 is such a case. The fixed-key probability is recovered only by summing the terms of all QDCs that act on the same bits, as the toy showed. We therefore pass from a single QDC to the set of QDCs acting on a given set of bits.

Remark 1. Proposition 1 says that the relationship between a QDC with its corresponding DC (which can be seen as a function for which the right pairs are the only solutions) is equivalent to the relationship between linear cryptanalysis with its corresponding function. A hint of this is reported by [Sun26] where they observed that the linear constraints are specific cases of deterministic linear relations which are the same as the strong QDCs. Thus, if we can find the full linear hull of a subspace, then, we can guarantee that the sum of the correlations will be the exact probability. This motivates Definition 7 in Section 3.3.

Remark 2. When tracing the same toy example by hand (similar to value-restriction methods), we can clearly derive the same constraints as the quasidifferential framework (we show this derivation in Appendix A). However, a major challenge is when a (nonlinear) S-box is included among the constraints. At this point, in the case of value-restriction, one has two choices: treat certain bits as independent and exclude them from the computation, at the cost of ignoring potentially useful dependencies. Conversely, explicitly modeling these bits increases the number of involved variables substantially, often making the resulting system way too expensive to evaluate. The quasidifferential trail framework circumvents this difficulty by decomposing the constraint set into multiple QDC (splitting precisely at each nonlinear parts), each representing a particular linear correlation. As a result, the nonlinear behavior can be analyzed while keeping the complexity of each individual computation manageable.

3.3 Completeness

By Section 2, $\Pr[\mathcal{T} \mid k]$ is the sum of the signed terms of all QDCs of $\mathcal{T}$, exact only when every QDC is included. Enumerating all of them is usually intractable, so a search keeps a set Q of QDCs, for instance those above an absolute correlation threshold [BDG25], and sums over Q. Whether this partial sum is still a probability is a property of Q. The toy already shows that an arbitrary Q can fail: the set $\{q_0, q_1, q_2\}$ omits q_3 and sums to -2^{-7} on the keys with $k_4^1 \oplus k_6^1 = 1$ and $k_0^1 \oplus k_1^2 = 0$.

Definition 7 ((Locally) complete QDC set)**.** Let M be a set of intermediate-state bits and Q a set of QDCs of $\mathcal{T}$. Then Q is *complete on* M if it contains every QDC q of $\mathcal{T}$ with $\mathrm{mb}(q) \subseteq M$. When M is all internal bits, Q is the full set of QDCs of $\mathcal{T}$ and its sum is the exact $\Pr[\mathcal{T} \mid k]$; we then call Q *complete*. When M is only a part of the internal bits, we call Q *locally complete*.

A QDC with $\mathrm{mb}(q) \subseteq M$ depends only on the bits in M, because the transposed mask maps keep every mask of such a q inside M, so the QDCs over M are exactly the quasidifferential terms of the marginal distribution of the bits in M. If Q is complete on M, summing the signed terms of the QDCs over M gives that marginal, hence for each key a value in $[0, 1]$. If Q is incomplete, some terms are missing, so the partial sum need not be a probability and can turn negative, as with $\{q_0, q_1, q_2\}$ above. Completeness on M is the condition under which the QDCs over M give a valid distribution.

This is the criterion that Boura, Derbez and Germon ask for, "a criterion for quasidifferential trails that ensures a reliable formula" [BDG25]. A correlation threshold does not meet it. It ranks QDCs by absolute correlation, so it can drop a small-correlation QDC q even though $\mathrm{mb}(q) \subseteq M$; by Definition 7 the kept set is then incomplete on M, and its partial signed sum is what turns negative, the behaviour they report on `SKINNY-128` DCs.

Completeness is a criterion, not yet a method: a threshold-based search keeps a single, generally incomplete set. Section 4 turns the criterion into a construction.

Algorithm 1: Quasidifferential Decoupling (`Decoupling-QD`)

Input : DC $\mathcal{T}$; correlation bound θ; weight threshold CW_{thres}
Output : fixed-key probability $\Pr[\mathcal{T} \mid k]$

`// Stage 1: collect QDCs (Trail-Collector)`
$Q \leftarrow$ QDCs q of $\mathcal{T}$ with $|\text{cor}(q)| \geq \theta$; `// baseline search`
$M \leftarrow \bigcup_{q \in Q} \text{mb}(q)$;

`// Stage 2: mute weak bits and decouple (Bit-Extractor)`
foreach $b \in M$ **do**
  $CW(b) \leftarrow \sum_{q \in Q:\, b \in \text{mb}(q)} |\text{cor}(q)|$;
end
$M_{\text{s}} \leftarrow \{\, b \in M : CW(b) \geq CW_{\text{thres}} \,\}$; `// mute weak bits`
$\{M_1, \ldots, M_{N_d}\} \leftarrow$ `Decouple`(M_{s}, Q) ; `// Union-Find on the QDC relations, more details can be found in Alg. 2`

`// Stage 3: solve each block and combine (Cons-Solver)`
foreach $j = 1, \ldots, N_d$ **do**
  $Q_j \leftarrow$ *all* QDCs q of $\mathcal{T}$ with $\text{mb}(q) \subseteq M_j$, no correlation bound ; `// locally complete`
  $\Pr_j[\mathcal{T} \mid k_j] \leftarrow \sum_{q \in Q_j} (-1)^{\mu_q^\top k_j} \text{cor}(q)$;
end
$\Pr[\mathcal{T} \mid k] \leftarrow \prod_{j=1}^{N_d} \Pr_j[\mathcal{T} \mid k_j]$; `// map each` k_j `to the master key`
return $\Pr[\mathcal{T} \mid k]$

4 Quasidifferential Decoupling

We introduce `Decoupling-QD`, a method that builds a locally complete QDC set and so turns the criterion of Section 3.3 into a fixed-key probability. The method mutes the mask bits that carry little correlation, which then allows us to form independent groups, each acting on its own block of state bits under this assumption. Each block is small enough to enumerate in full, so its QDC set is locally complete by construction (Definition 7) and the local distribution it induces is a genuine probability. The blocks combine into a valid distribution over the whole key space. This is the step that removes the negative values yielded by the sum of quasidifferential trails with a correlation higher than an arbitrary value and it is the constructive answer to the open problem of Boura, Derbez and Germon.

`Decoupling-QD` runs in three stages. The `Trail-Collector` runs a threshold-based QDC search similar to what has been done in [BDG25] and records the masked bits $\text{mb}(q)$ of every QDC it finds. The `Bit-Extractor` then scores each masked bit by its correlation weight (Definition 8), mutes the weak ones, and groups the rest into independent blocks $M_1, \ldots, M_{N_d}$. The `Cons-Solver` enumerates the QDCs of each block in full, a locally complete set, turns it into a local distribution, and combines the blocks into the global key space and distribution. Algorithm 1 states the procedure; we detail the `Bit-Extractor` and the `Cons-Solver` in turn.

4.1 Decoupling by Muting Weak Bits

Let $\text{mb}(q_i)$ be the masked bits of QDC q_i (Section 3.2); the global bit set is $M = \bigcup_i \text{mb}(q_i)$. Completeness on all of M would need every QDC over M, which is intractable in most cases that we have observed in literature. We instead mute the bits that contribute little and keep the rest complete block by block. Thus, we would have to define the contribution (correlation weight) of a bit found in QDCs.

Definition 8 (Correlation weight)**.** Given a set of QDCs in which each q has correlation $\mathrm{cor}(q) \in [-1, 1]$ and masked bits $\mathrm{mb}(q)$, the *correlation weight* of a bit b is the sum of absolute correlations over the QDCs that mask it,

$$CW(b) = \sum_{q\,:\,b \in \mathrm{mb}(q)} |\mathrm{cor}(q)|.$$

A bit with small $CW(b)$ lies only on a few QDCs, or only on low-correlation ones, so the QDCs through it barely move the distribution. Muting these weak bits, those with $CW(b) < CW_{\mathrm{thres}}$, is the decoupling. A QDC survives only when all of its masked bits survive, so muting cuts every QDC that bridged two parts of M, and the surviving QDCs fall into groups that share no masked bit. We form the groups with a Union-Find pass (Algorithm 2): two surviving bits join the same block when a QDC's relation links them. The result is a partition of the surviving bits into disjoint blocks $M_1, \ldots, M_{N_d}$, with no QDC masking bits of two different blocks.

This decoupling differs from a correlation threshold in the one way that matters. A correlation threshold drops QDCs whose masked bits lie inside a region, leaving it incomplete, and as Section 3.3 shows its signed sum can turn negative. Muting bits drops only the cross-block QDCs, and within each block we enumerate and keep *every* QDC, without any restrictions on the correlation. Each block is therefore locally complete, so by Section 3.3 its local distribution is a genuine probability. Decoupling trades coverage for validity: it discards the cross-block QDCs, so the result approximates the true fixed-key probability, but the approximation is always a valid distribution.

The threshold CW_{thres} sets this trade-off. A lower threshold mutes fewer bits, keeps more QDCs, and gives a tighter approximation, at the cost of larger blocks that are harder to enumerate. It is tuned to keep the blocks enumerable while retaining the dominant QDCs. One natural choice CW_{thres} is P_{avg}, the average key probability of a DC. Setting the threshold at this value guarantees that the strong QDCs [5] are retained.

4.2 Solving and Combining the Blocks

As the decoupled blocks share no masked bit, the QDCs in a block are independent of another block. A QDC over $M = M_1 \sqcup \cdots \sqcup M_{N_d}$ is one local QDC per block, its correlation is the product of the local correlations and its key sign is the sum of their key signs. The signed sum of Section 2 therefore factorises, and the fixed-key probability is a product of local factors,

$$\Pr[\mathcal{T} \mid k] \;=\; \prod_{j=1}^{N_d} \Pr_j[\mathcal{T} \mid k_j],$$

where $\Pr_j$ is the local contribution of block M_j and k_j the round-key bits it involves. Each block carries the active S-boxes that fall in it, so the block averages multiply to the global one, $P_{avg} = \prod_j P_{avg,j}$; a block with no active S-box has $P_{avg,j} = 1$ and still contributes a non-negative factor. Each factor comes from a locally complete QDC set and is therefore non-negative, and a product of non-negative factors is non-negative. The decoupled distribution is valid, with none of the negative values a thresholded sum produces. The `Cons-Solver` computes the factors and multiplies them. For each block it stays within the quasidifferential framework: it restricts the QDC search to the bits of M_j, enumerates that block without a correlation bound, which is feasible because the block is small, and aggregates the correlations into $\Pr_j$. Since the block's QDC set is locally complete, the result is valid by Section 3.3, and it handles blocks whose surviving subkey space is far too large to enumerate directly. The blocks are independent, so one local QDC per block combines into a distinct global QDC and the per-block counts multiply; at a fixed budget

[5] Strong QDCs are QDCs that have a correlation that is the maximal among all QDCs [BR22].

a decoupled search therefore reaches QDCs of much lower correlation than a single global search, as Section 5 quantifies.

To state the result on the master key, `Cons-Solver` replaces each subkey bit by its key-schedule expression and folds it into the block, exactly for a linear key schedule and approximately for a nonlinear one such as `RECTANGLE`, where the subkey bits are treated as independent. The surviving master-key space is the product of the per-block survivals.

5 Applications

In this section, we apply `Decoupling-QD` to 27 published differential characteristics from `GIFT-64`, `GIFT-128`, `SKINNY-64`, `SKINNY-128`, and `RECTANGLE`. For the evaluated characteristics, `Decoupling-QD` recovers the key-space restrictions reported by previous constraint-detection frameworks while also identifying additional probabilistic constraints that refine the fixed-key probability distribution. For characteristics where the direct threshold-based quasidifferential method produces negative probabilities, the decoupled computation returns non-negative, more detailed distributions by solving locally complete constraint subsets. We stress that the non-negative probability is guaranteed by the completeness of the constraint subset.

When the threshold-based quasidifferential method already gives a valid distribution, our experiments show that `Decoupling-QD` is at least as fine as that distribution and finer for several characteristics under the same correlation bound. For each target characteristic, we report the stated Markov probability, the valid-key fraction, the number of newly identified bit-wise probabilistic constraints, the probability distribution over the valid key space, and the solver mode used to obtain the distribution. Results marked by [E] are obtained by estimation and should be interpreted with the corresponding sampling or local-search setting. Unless otherwise stated, comparisons with the baseline quasidifferential framework use the same correlation bound. For ciphers with nonlinear key schedules, such as `RECTANGLE`, key-space reductions are reported at the subkey level unless a separate master-key validation is explicitly given. Table 2 reports the $\log_2$ key-space reduction ratios for all target characteristics, together with the probability distributions returned by `Decoupling-QD` in Table 1.

5.1 Application to `GIFT`

`GIFT` is a lightweight block cipher introduced by Banik et al. [BPP+17], adopting a bit-sliced SPN structure. Its 64-bit and 128-bit variants are denoted `GIFT-64` and `GIFT-128`, respectively. We apply `Decoupling-QD` to 11 `GIFT-64` and 6 `GIFT-128` differential characteristics, and compare the extracted key-space restrictions with those reported by prior constraint-detection frameworks [Sun26, PT22], AutoDiVer [NGJE25], and the threshold-based quasidifferential method [BDG25]. The fixed-key probability distributions obtained by `Decoupling-QD` are summarized in Table 3.

For all evaluated `GIFT` characteristics, `Decoupling-QD` recovers the tightest key-space restrictions reported by previous work. In addition, `Decoupling-QD` identifies probabilistic constraints that were not reported by prior work on 12 of the 17 evaluated characteristics. These probabilistic constraints do not merely remove invalid keys, they further split the surviving key space into different fixed-key probability classes. Under the same correlation bound, `Decoupling-QD` also yields a more accurate probability estimate than the threshold-based quasidifferential framework [BDG25] on 4 `GIFT` characteristics.

Results of `GIFT-64`. We now describe the constraints found by `Decoupling-QD` on each evaluated `GIFT-64` characteristic. For the 9-round characteristic [LWZZ19], `Decoupling-QD` extracts three new nonlinear constraints, including two deterministic constraints and one

probabilistic constraint $\mathbb{E}_0^1$ (Table B.3). The deterministic constraints recover the key-space reduction, while the newly identified probabilistic constraint makes the distribution over the surviving keys non-uniform, giving a finer distribution. For the 10-round characteristic from [JYSYZ+18], `Decoupling-QD` identifies two probabilistic constraints that were not reported in previous work, as detailed in Table B.3. The resulting overall probability distribution across the valid key space is illustrated in Figure 2a. In particular, the nonlinear constraint $\mathbb{E}_0^2$ encapsulates five deterministic linear constraints. In addition to reducing the valid key space by a factor of 2^5, it makes the probability distribution non-uniform. For the three 12-round characteristics, `Decoupling-QD` identifies a new probabilistic constraint spanning 11 rounds for the characteristic of [CZD20], a new probabilistic constraint spanning 10 rounds for the characteristic of [LWZZ19], and two probabilistic constraints together with three deterministic constraints for the characteristic presented in Table 4 of [ZDY19]. For the 13-round characteristic from [LWZZ19], `Decoupling-QD` finds one new probabilistic constraint spanning over 12 rounds, which contains 8,000 quasidifferential trails, and provides a more precise distribution than the threshold-based quasidifferential framework. Furthermore, for the 18-round characteristic from [SWW21a], `Decoupling-QD` finds two new probabilistic constraints ($\mathbb{E}_2^7$ and $\mathbb{E}_3^7$ in Table B.8) and produces a better distribution than the threshold-based quasidifferential framework, as illustrated in Figure 2f. For the remaining 4 `GIFT-64` characteristics, `Decoupling-QD` finds no new probabilistic constraint, so the results match previous work.

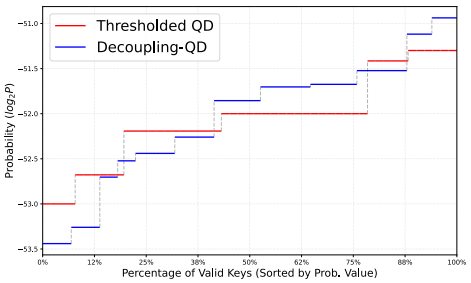
Results of `GIFT-128`. For `GIFT-128`, we evaluate `Decoupling-QD` on one 12-round characteristic, one 18-round characteristic, and four 20-round characteristics. For the 12-round characteristic from [ZDY19], at an initial correlation bound of 2^{-64}, `Decoupling-QD` detects a deterministic constraint that halves the valid key space. Lowering the correlation bound to 2^{-70} and reducing the correlation-weight threshold for weak-bit filtering, `Decoupling-QD` then captures a previously undiscovered probabilistic constraint. For the 18-round characteristic from [ZDY19], `Decoupling-QD` finds a contradictory deterministic constraint, which means the entire characteristic is invalid. For the four 20-round characteristics from [JZZD21, Table 12], `Decoupling-QD` recovers all previously known constraints. In particular, for each of Trail 2, Trail 3, and Trail 4, `Decoupling-QD` identifies two additional probabilistic constraints, as summarized in Table B.9, B.10, and B.11.

5.2 Application to `SKINNY`

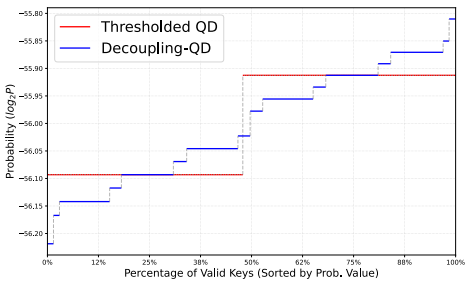
`SKINNY` is a lightweight tweakable block cipher family proposed by Beierle et al. [BJK+16], adopting a tweakable SPN-based structure. We apply `Decoupling-QD` to 8 `SKINNY` differential characteristics, and compare our results with previous frameworks.

Results of `SKINNY-64`. We apply `Decoupling-QD` to five `SKINNY-64` differential characteristics, and summarize the results in Table 1 and Table 2. For these characteristics, `Decoupling-QD` recovers all constraints reported by AutoDiVer [NGJE25] and by Peyrin and Tan [PT22]. For the 7-round characteristic from [DDH+21], `Decoupling-QD` identifies one probabilistic constraint missed by previous work [PT22], also reported by `Trail-Estimator` [PTZZ25]. The key-space estimate of `Decoupling-QD` for this characteristic matches that of `Trail-Estimator`.

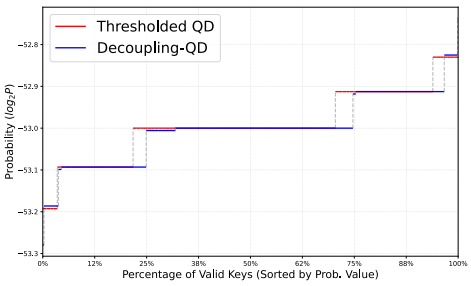
Applying the threshold-based quasidifferential framework to the 7-round characteristic of [DDH+21] yields a distribution with negative probabilities, so the estimate is incorrect. In contrast, `Decoupling-QD` produces more precise distributions than the threshold-based method on all five `SKINNY-64` characteristics, each matching the best previously reported result. Figure 3 shows `Decoupling-QD`'s distribution estimates for the 5-round and 7-round



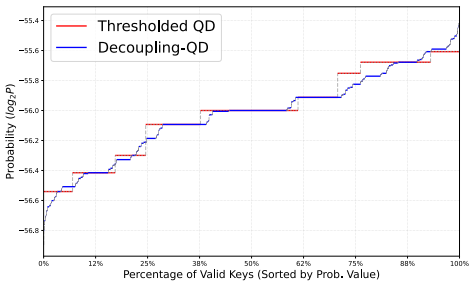
(a) 10-round `GIFT-64` DC [JYSYZ+18]



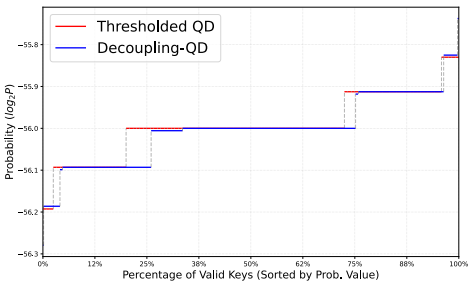
(b) 12-round `GIFT-64` DC [CZD20]



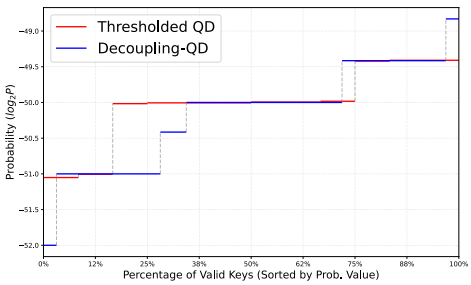
(c) 12-round `GIFT-64` DC [LWZZ19]



(d) 12-round `GIFT-64` DC [ZDY19, Table 4]



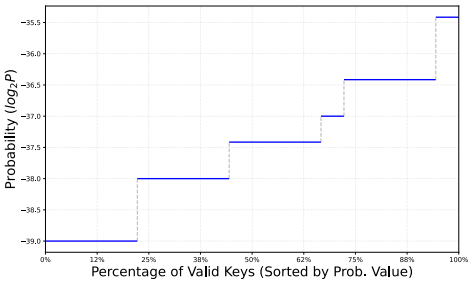
(e) 13-round `GIFT-64` DC [LWZZ19]



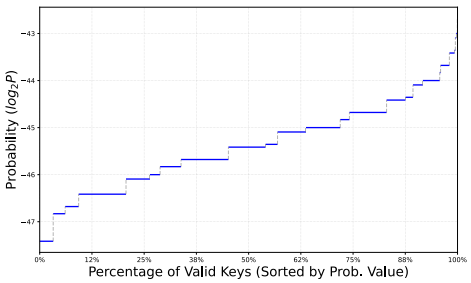
(f) 18-round `GIFT-64` DC [SWW21a]

Figure 2: Distributions comparison of `GIFT-64` differential characteristics between `Decoupling-QD` and the baseline quasidifferential framework

`SKINNY-64` characteristics; both closely match the distributions reported in [PT22, Fig. 7] and [PTZZ25, Fig. 11].



(a) Distribution of the 5-round characteristic from [PT22]



(b) Distribution of the 7-round characteristic from [DDH+21]

Figure 3: Distributions of `SKINNY-64` characteristics

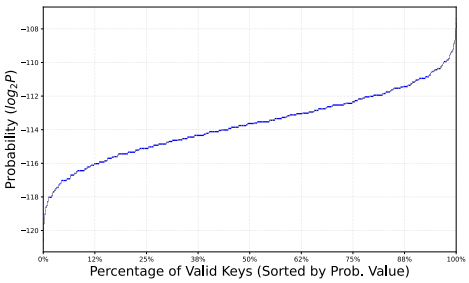
Table 3: Experimental results for GIFT by Decoupling-QD

Version	Rds	Reduced key space	Stated prob.	Probability Distribution Percentage of prob.					Source
GIFT-64	9	2^{-4}	2^{-42}			38.1 50%		37.9 50%	Table 2 [LWZZ19]
	10	$2^{-5.02}[E]$	2^{-57}	53.5-53.2 14%	53.1-52.26 27%	52.25-51.6 35%	51.59-51.2 12%	51.1-50.9 12%	Table 5 [JYSYZ+18]
	12	$2^{-3.03}[E]$	2^{-60}	56.22-56.15 12%	56.14-56.09 19%	56.08-55.92 38%	55.91-55.86 19%	55.85-55.81 12%	Table 3 [CZD20]
	12	2^{-4}	2^{-58}	53.3-53.2 4%	53.19-53.1 21%	53.09-53 50%	53.01-52.91 21%	52.9-52.7 4%	Table 7 [LWZZ19]
	12	2^{-3}	2^{-59}	56.9-56.41 15%	56.4-56.1 17%	56.09-55.9 36%	55.8-55.7 17%	55.69-55.3 15%	Table 4 [ZDY19]
	12	1	2^{-60}			60 100%			Table 6 [ZDY19]
	13	2^{-4}	2^{-62}		56.3-56.2 25%	56.1-55.9 50%	55.8-55.9 25%		Table 8 [LWZZ19]
	13	2^{-1}	2^{-64}			63 100%			Table 8-1 [SWW21b]
	13	2^{-5}	2^{-64}			59 100%			Table 8-2 [SWW21b]
	13	2^{-3}	2^{-64}			61 100%			Table 8-3 [SWW21b]
	18	2^{-8}	2^{-58}	52 4%	51 25%	50.9-50 42%	49.4 25%	48.8 4%	Figure 8 [SWW21a]
GIFT-128	12	2^{-1}	$2^{-62.4}$			61.41 50%		61.39 50%	Table 13 [ZDY19]
	18	0	2^{-109}			—			Table 10 [ZDY19]
	20	2^{-5}	$2^{-121.4}$			115.4 100%			Trail 1 [JZZD21, Tab. 12]
	20	$2^{-7.05}[E]$	$2^{-122.4}$		114.407 25%	114.4 50%	114.396 25%		Trail 2 [JZZD21, Tab. 12]
	20	$2^{-7}[E]$	$2^{-122.4}$		114.407 25%	114.4 50%	114.396 25%		Trail 3 [JZZD21, Tab. 12]
	20	$2^{-9.01}[E]$	$2^{-123.4}$	114.412 10%	114.406 30%	114.4 34%	114.395 20%	114.388 6%	Trail 4 [JZZD21, Tab. 12]

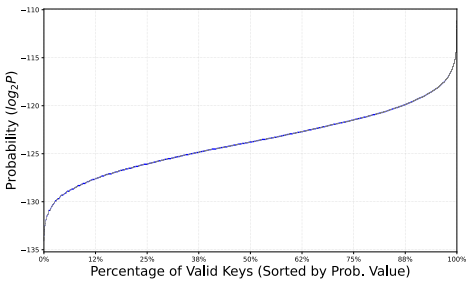
Stated Prob.: the probability reported in the original papers; Reduced key Space: refers to the proportion of the estimated valid key space for the differential characteristic. Probability Distribution: the $-log_2$ probabilities distribution range.

Results of SKINNY-128. For SKINNY-128, we evaluate three differential characteristics: one single-key characteristic and two related-key characteristics, which have been previously studied under the threshold-based quasidifferential framework of [BDG25]. For the 13-round single-key SKINNY-128 characteristic, Decoupling-QD extracts 10 independent linear constraint subsets. Among these constraints, the Cons-Solver identifies one linear condition on k_{123} as internally contradictory, which makes the characteristic invalid (as shown in Appendix C.1). For the 14-round related-key characteristic of SKINNY-128, at a correlation bound of 2^{-122}, Decoupling-QD decouples the global constraint into 9 independent subsets, including 4 linear and 5 probabilistic constraints. The Cons-Solver computes a key-space reduction factor of $2^{-7.65}$, matching the bound established in [PT22]. Decoupling-QD additionally identifies a nonlinear constraint $\mathbb{E}_4^{S1}$ (see Table C.2) that was missed by [PT22] but later recovered by [PTZZ25], which doubles the average probability. For the 16-round SKINNY-128-256 characteristic, Decoupling-QD extracts 9 constraint subsets. One large nonlinear subset unifies four constraints from [PT22] into a single cluster. By sampling, we obtain a key-space reduction of $2^{-6.4}$, stricter than that of [PT22]. The threshold-based quasidifferential method of [BDG25] assigns negative probabilities to 50% of the key space, whereas Decoupling-QD assigns positive probability only to the valid key space. The bound reported by [PTZZ25] is slightly stricter on this SKINNY-128 characteristic. In Section 6, we analyze this cell-level versus bit-level difference. The

distributions estimated by `Decoupling-QD` for the 14-round and 16-round `SKINNY-128` trails are shown in Figure 4.



(a) Distribution of the 14-round `SKINNY-128` characteristic from [DDH+21]



(b) Distribution of the 16-round `SKINNY-128` characteristic from [DDH+21]

Figure 4: Distributions of `SKINNY-128` characteristics

5.3 Application to `RECTANGLE`

We apply `Decoupling-QD` to two 14-round `RECTANGLE` differential characteristics from [ZBL+14, Appendix E], with stated probabilities 2^{-63} and 2^{-66} respectively. The overall results are summarized in Table 1 and 2.

For the first characteristic T_{REC1} in Table 5, `Decoupling-QD` extracts 12 constraint subsets, as detailed in Table C.4.1. Among them, the new probabilistic constraint $\mathbb{E}_1^{REC}$ makes exactly 50% of the key space invalid. In addition, `Decoupling-QD` recovers all key conditions recently reported by AutoDiVer [NGJE25]: the conditions on $\{k_{10}^{10},\ k_{15}^{10},\ k_{12}^{11},\ k_{13}^{11}\}$. For the second characteristic T_{REC2} in Table 6, `Decoupling-QD` extracts 11 constraint subsets, as detailed in Table C.4.2, and recovers all linear key conditions recently reported by AutoDiVer [NGJE25] on the key bits: $\{k_{10}^{10}, k_{15}^{10},\ k_{12}^{11},\ k_{13}^{11},\ k_{3}^{11},\ k_{0}^{12},\ k_{3}^{12}\}$, which are included in the newly identified probabilistic constraint $\mathbb{E}_0^{REC2}$, making 75% of the key space invalid.

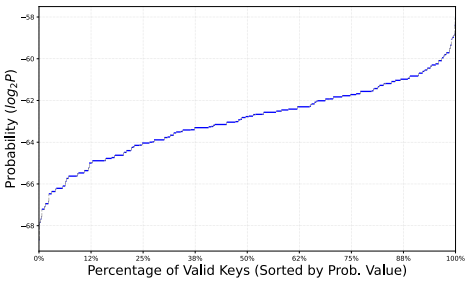
For both characteristics, beyond the recovered deterministic key conditions, `Decoupling-QD` extracts larger nonlinear constraint subsets that encapsulate the known conditions as deterministic linear constraints and further explain the non-uniform fixed-key distributions over the surviving key space. To compute the overall distributions, we solve the large constraints E_1^{REC} and E_0^{REC2} by sampling values on master key. In the solving phase, the master key is expanded into subkey variables following the `RECTANGLE-80` key schedule. The final estimated distributions for both characteristics are shown in Figure 5. By contrast, the threshold-based framework of [BDG25] produces distributions with negative probabilities for both characteristics, which makes them inaccurate.

6 Comparison with Previous Work

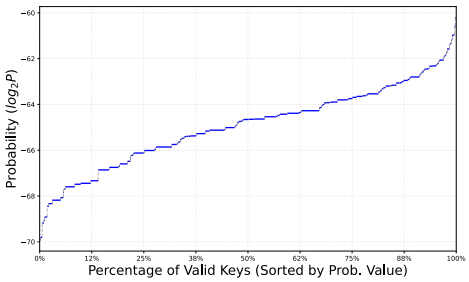
In this section, we compare `Decoupling-QD` with the threshold-based quasidifferential (QD) method, and then with previous algebraic constraint search frameworks: those of [PT22], [Sun26], AutoDiVer [NGJE25], and `Trail-Estimator` [PTZZ25].

6.1 Advantages over Threshold-Based QD Methods

`Decoupling-QD` improves on the threshold-based approach in two ways. For any given correlation threshold, with a proper choice of CW_{thres} ($0 \le CW_{thres} \le P_{avg}$, where P_{avg} is the average Markov probability of the characteristic), it covers a strictly larger set of



(a) Distribution of the 14-round differential characteristic from [ZBL+14] with 2^{-63}



(b) Distribution of the 14-round differential characteristic from [ZBL+14] with 2^{-66}

Figure 5: Distributions of two `RECTANGLE` characteristics

high-correlation quasidifferential trails. It also always yields a valid distribution, with no negative probabilities.

Coverage advantage At the same correlation bound, `Decoupling-QD` enumerates more quasidifferential trails than the global search used by the threshold-based QD method. The reason is the decoupling step. Instead of enumerating the entire trail population in a single MILP over the full cipher, `Decoupling-QD` uses the `Bit-Extractor` to partition the cipher into k independent constraint subsets and solves each locally. Since the global trail space factors as the combinatorial product of the trail subspaces, enumerating N_j trails in subset j yields an aggregate coverage of $\prod_{j=1}^{k} N_j$ trails.

This coverage matters for the precision of the distribution estimate. Quasidifferential aggregation enumerates trails up to a correlation bound; trails missed by the search leave the corresponding algebraic structure incomplete, which produces either imprecise key-space estimates or negative probabilities. The per-subset enumeration of `Decoupling-QD` is bounded only by a much smaller per-subset search budget: within a subset, trail correlations are weaker than those of the global trails, which carry large-scale bit masks. Complete enumeration within each subset therefore remains tractable.

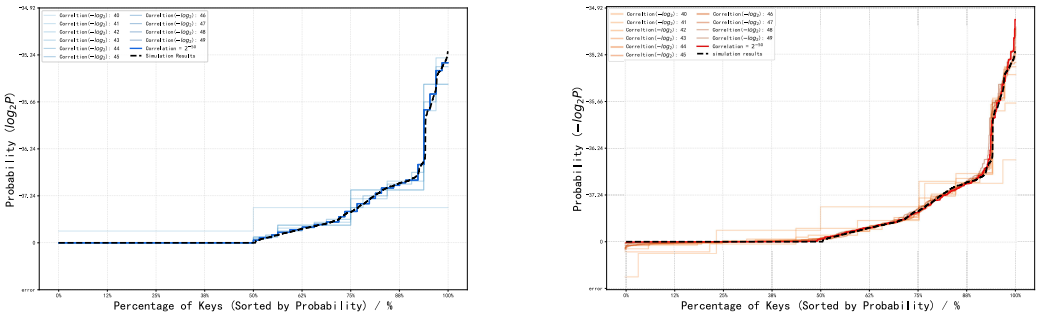
As an example, consider the 4-round toy `GIFT-64` trail of Table 4. Under global correlation bound 2^{-50}, the baseline framework [BDG25] returns 8,188 trails. Taking these as input, `Decoupling-QD` applies the `Bit-Extractor` with correlation-weight threshold $\mathrm{CW}_{\mathrm{thres}} = 2^{-38.24}$ and decouples the system into five independent subsets. A non-thresholded MILP enumeration on each subset returns 46, 3, 1, 81, and 2 trails respectively, with combinatorial product:

$$46 \times 3 \times 1 \times 81 \times 2 = 22{,}356,$$

a factor of 2.7 over the global count at the same correlation threshold. The local searches run faster than the global one because each subset contains far fewer trail combinations. The combinatorial product also identifies global trails with correlation as low as $2^{-62.24}$, a depth at which the correlation-bounded global search does not terminate within our time budget. The gap widens on longer characteristics, where the global trail population exceeds standard MILP budgets. For the 13-round `GIFT-64` characteristic of [LWZZ19], the threshold-based QD method identifies 832 trails at correlation bound 2^{-68}. `Decoupling-QD` isolates a new probabilistic constraint subset on this characteristic; a local MILP search on this single subset, without any correlation bound, returns 8,000 trails within seconds. Through this larger trail coverage, `Decoupling-QD` recovers more distributional information than the correlation-bounded method at the same correlation bound. On 12 of the 27 target characteristics, `Decoupling-QD` yields a more precise probability distribution from the decoupled constraints than threshold-based QD.

6.2 Elimination of Negative Probabilities

The threshold-based method of [BDG25, BR22] often produces negative probabilities. For long-round differential characteristics, it truncates the search at a fixed correlation bound, leaving the constraint structure incomplete and so producing negative probabilities. In contrast, `Decoupling-QD` computes its distribution from explicit algebraic structures and avoids these negative values.



(a) Results by `Decoupling-QD` (b) Results by framework in [BDG25]

Figure 6: Distribution estimations of 4-round `GIFT-64` trail

To illustrate this advantage in practice, we evaluate `Decoupling-QD` on the 4-round toy differential characteristic of `GIFT-64` with average probability $2^{-38.24}$ (Table 4). Figure 6 compares the convergence behavior of `Decoupling-QD` against the threshold-based QD method of [BDG25] as the correlation bound is progressively tightened from 2^{-40} to 2^{-50}. Throughout this range, the threshold-based QD method assigns negative probabilities to 25% of the key space while classifying the remainder as valid; lowering the correlation bound reduces the magnitude of these negative values but does not eliminate them. `Decoupling-QD`, by contrast, isolates the full nonlinear constraint $\mathbb{E}_0$ already at correlation bound 2^{-41} and proves that 50% of the key space is invalid. The constraint $\mathbb{E}_0$ imposes a deterministic condition on the master key, enforcing $k_{120} = 1$. Because `Decoupling-QD` derives its estimate from complete algebraic substructures, the resulting distributions are valid by construction and never produce negative probabilities. The estimated distribution of `Decoupling-QD` is shown in Figure 6a, which agrees closely with the Monte Carlo reference simulation. The corresponding baseline estimate (Figure 6b) instead retains negative probabilities on 25% of key-space throughout, rendering its distribution incorrect.

6.3 Comparison with Constraint-Searching Frameworks

`Decoupling-QD` differs from prior constraint-searching frameworks in the class of constraints it recovers. It identifies new probabilistic constraints on `GIFT` and `RECTANGLE` characteristics which were not reported before. In this part, we compare against four prior frameworks.

The detection framework of [PT22] recovers half-constraints, which capture only part of the relationships between constrained and free variables. On every target characteristic, `Decoupling-QD` recovers more constraints and reports a tighter key-space estimate.

The framework of [Sun26] extracts deterministic linear relations between the input and output bits of active S-boxes in `GIFT` cipher, but does not consider the probabilistic relations that arise elsewhere in the characteristic. `Decoupling-QD` additionally accounts for the probabilistic relations induced via inactive S-boxes, which leads to new probabilistic constraints on `GIFT` and `RECTANGLE`.

AutoDiVer [NGJE25] derives the necessary linear key conditions of `GIFT` and `RECTANGLE` characteristics but does not identify bit-wise nonlinear constraints within these ciphers.

`Decoupling-QD` recovers all of AutoDiVer's linear conditions and additionally identifies nonlinear constraints, giving a more complete description of the key-space distribution.

`Trail-Estimator` [PTZZ25] recovers all constraints on cell-oriented characteristics by reducing the cipher to a cell-wise linear system and solving it via Gaussian elimination. Its effectiveness decreases on bit-oriented ciphers such as `GIFT` and `RECTANGLE`, where the cell-level abstraction does not apply. `Decoupling-QD` operates directly at bit granularity and is the first method to identify new probabilistic nonlinear constraints on these ciphers. On `SKINNY` characteristics, `Decoupling-QD` additionally reports bit-level key conditions that `Trail-Estimator` does not produce. The two methods are therefore complementary: `Trail-Estimator` is suited to cell-oriented ciphers, and `Decoupling-QD` to bit-oriented ones.

On `SKINNY-64` characteristics, `Decoupling-QD` obtains the same results as `Trail-Estimator`, with distribution estimates matching those of [PTZZ25]. On `SKINNY-128` characteristics, `Decoupling-QD` does not recover all nonlinear constraints, and its key-space estimate is slightly looser than that of `Trail-Estimator` (a reduction of $2^{-6.4}$ versus 2^{-7} on the 16-round characteristic). This gap stems from the structure of the 8-bit `SKINNY-128` S-box QDTM. For the 4-bit S-boxes of `GIFT`, `RECTANGLE`, and `SKINNY-64`, the mask pairs with nonzero correlation form an affine subspace in most cases, so the number of mask transitions per S-box is small and the quasidifferential trail count grows slowly as the correlation bound is lowered. The 8-bit `SKINNY-128` S-box does not exhibit this affine structure: its QDTM contains many more distinct correlation values, so the trail population grows much faster as the bound deepens, and the constraints whose contributing trails lie below our search budget remain out of reach. The cell-level abstraction of `Trail-Estimator` avoids this growth by treating each 8-bit cell as a single transition unit, reducing the cipher to a cell-wise linear system solvable by Gaussian elimination.

7 Discussion and Conclusion

In this paper, we take the correspondence between QDCs and constraint subsets, connecting the quasidifferential framework with constraint-detection research. This correspondence explains the negative probabilities of the threshold-based quasidifferential method of [BDG25]: a correlation threshold drops some of the QDCs constraining a set of bits, leaving the constraint incomplete, so the partial sum is no longer a probability.

Based on this, we introduced `Decoupling-QD`, which mutes the weak mask bits of QDCs to decouple the global constraints into independent groups. `Decoupling-QD` enumerates the complete set of QDCs within each group and computes a valid distribution from it. With an appropriate correlation-weight threshold, `Decoupling-QD` covers more QDCs than the threshold-based method at the same correlation bound, giving a finer-grained distribution estimate.

In our experiments, `Decoupling-QD` returns a valid distribution on all 27 target characteristics, recovers the key-space restrictions of [PT22, Sun26, PTZZ25, NGJE25], and refines the estimated distribution on 9 of them. It also recovers the bit-wise probabilistic key conditions for `GIFT-64`, `GIFT-128`, and `RECTANGLE` that the word-oriented detector of [PTZZ25] does not reach.

The main limitation appears when the active S-boxes are not affine maps under an arbitrary difference (one example being the 8-bit S-box of `SKINNY`). On `SKINNY-128`, the QDC population grows quickly as the correlation bound is lowered, so some constraints remain below the reachable bound; on the 16-round `SKINNY-128` characteristic, this leaves our estimate slightly looser than `Trail-Estimator` [PTZZ25]. Improving the efficiency of `Decoupling-QD` on these ciphers, and extracting constraints under a tighter search budget, are left for future work.

Acknowledgement

The 2nd, 4th and 5th authors are supported by the Singapore NRF Investigatorship grant NRF-NRFI08-2022-0013. This work has been partially funded by the European Union ERC-2023-COG, SoBaSyC, 101125450. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

[AST+17] Ahmed Abdelkhalek, Yu Sasaki, Yosuke Todo, Mohamed Tolba, and Amr M. Youssef. Milp modeling for (large) s-boxes to optimize probability of differential characteristics. *IACR Transactions on Symmetric Cryptology*, 2017(4):99–129, Dec. 2017. URL: https://tosc.iacr.org/index.php/ToSC/article/view/805, doi:10.13154/tosc.v2017.i4.99-129.

[BDG25] Christina Boura, Patrick Derbez, and Baptiste Germon. Extending the quasidifferential framework: From fixed-key to expected differential probability. *IACR Transactions on Symmetric Cryptology*, 2025(1):515–541, Mar. 2025. URL: https://tosc.iacr.org/index.php/ToSC/article/view/12086, doi:10.46586/tosc.v2025.i1.515-541.

[Bey21] Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 36–66. Springer, Cham, December 2021. doi:10.1007/978-3-030-92062-3_2.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016. doi:10.1007/978-3-662-53008-5_5.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer, 2017. doi:10.1007/978-3-319-66787-4_16.

[BR22] Tim Beyne and Vincent Rijmen. Differential Cryptanalysis in the Fixed-Key Model. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 687–716. Springer, 2022. doi:10.1007/978-3-031-15982-4_23.

[BS90] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances*

in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990. doi:10.1007/3-540-38424-3_1.

[BV23] Tim Beyne and Michiel Verbauwhede. Integral cryptanalysis using algebraic transition matrices. *IACR Trans. Symm. Cryptol.*, 2023(4):244–269, 2023. doi:10.46586/tosc.v2023.i4.244-269.

[BV24] Tim Beyne and Michiel Verbauwhede. Ultrametric integral cryptanalysis. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VII*, volume 15490 of *LNCS*, pages 392–423. Springer, Singapore, December 2024. doi:10.1007/978-981-96-0941-3_13.

[BV25] Tim Beyne and Michiel Verbauwhede. Integral cryptanalysis in characteristic p. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part I*, volume 16245 of *LNCS*, pages 66–96. Springer, Singapore, December 2025. doi:10.1007/978-981-95-5018-0_3.

[CF25] Anne Canteaut and Merlin Fruchon. Understanding unexpected fixed-key differential behaviours: How to avoid major weaknesses in lightweight designs. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part I*, volume 16245 of *LNCS*, pages 97–130. Springer, Singapore, December 2025. doi:10.1007/978-981-95-5018-0_4.

[CHH+25] Chengcheng Chang, Hosein Hadipour, Kai Hu, Muzhou Li, and Meiqin Wang. Mix-basis geometric approach to boomerang distinguishers. *IACR Trans. Symm. Cryptol.*, 2025(3):693–728, 2025. doi:10.46586/tosc.v2025.i3.693-728.

[CZD20] Huaifeng Chen, Rui Zong, and Xiaoyang Dong. Improved differential attacks on gift-64. In Jianying Zhou, Xiapu Luo, Qingni Shen, and Zhen Xu, editors, *Information and Communications Security*, pages 447–462, Cham, 2020. Springer International Publishing.

[DDH+21] Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard, and Charles Prud'homme. Efficient Methods to Search for Best Differential Characteristics on SKINNY. In *Applied Cryptography and Network Security - 19th International Conference, ACNS 2021, Kamakura, Japan, June 21-24, 2021, Proceedings, Part II*, volume 12727 of *Lecture Notes in Computer Science*, pages 184–207. Springer, 2021. doi:10.1007/978-3-030-78375-4_8.

[DR07] Joan Daemen and Vincent Rijmen. Plateau characteristics. *IET Information Security*, 1(1):11–18, 2007. doi:10.1049/iet-ifs:20060099.

[HNW26] Kai Hu, Zhongfeng Niu, and Meiqin Wang. Round-based approximation of (higher-order) differential-linear correlation - A geometric approach perspective. In Joan Daemen and Emmanuel Thomé, editors, *Advances in Cryptology - EUROCRYPT 2026 - 45th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Rome, Italy, May 10-14, 2026, Proceedings, Part VI*, Lecture Notes in Computer Science, pages 152–180. Springer, 2026. doi:10.1007/978-3-032-25333-0_6.

[HZC+25] Kai Hu, Chi Zhang, Chengcheng Chang, Jiashu Zhang, Meiqin Wang, and Thomas Peyrin. Unlocking mix-basis potential: Geometric approach for

combined attacks. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part V*, volume 16004 of *LNCS*, pages 293–334. Springer, Cham, August 2025. doi:10.1007/978-3-032-01901-1_10.

[JYSYZ+18] ZHAO Jing-Yuan, XU Song-Yan, Zi-Jian ZHANG, Zheng LI, et al. Differential analysis of lightweight block cipher gift. *Journal of Cryptologic Research*, 5(4):335, 2018.

[JZZD21] Fulei Ji, Wentao Zhang, Chunning Zhou, and Tianyou Ding. Improved (related-key) differential cryptanalysis on gift. In Orr Dunkelman, Michael J. Jacobson, Jr., and Colin O'Flynn, editors, *Selected Areas in Cryptography*, pages 198–228, Cham, 2021. Springer International Publishing.

[LMM91] Xuejia Lai, James L. Massey, and Sean Murphy. Markov Ciphers and Differential Cryptanalysis. In Donald W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer, 1991. doi:10.1007/3-540-46416-6_2.

[LWZZ19] Lingchen Li, Wenling Wu, Yafei Zheng, and Lei Zhang. The relationship between the construction and solution of the MILP models and applications. Cryptology ePrint Archive, Paper 2019/049, 2019. URL: https://eprint.iacr.org/2019/049.

[NGJE25] Marcel Nageler, Shibam Ghosh, Marlene Jüttler, and Maria Eichlseder. AutoDiVer: Automatically Verifying Differential Characteristics and Learning Key Conditions. Cryptology ePrint Archive, Paper 2025/185, 2025. URL: https://eprint.iacr.org/2025/185.

[PT22] Thomas Peyrin and Quan Quan Tan. Mind Your Path: On (Key) Dependencies in Differential Characteristics. *IACR Trans. Symmetric Cryptol.*, 2022(4):179–207, 2022. URL: https://doi.org/10.46586/tosc.v2022.i4.179-207, doi:10.46586/TOSC.V2022.I4.179-207.

[PTZZ25] Thomas Peyrin, Quan Quan Tan, Hongyi Zhang, and Chunning Zhou. Trail-estimator: An automated verifier for differential trails in block ciphers. *IACR Transactions on Symmetric Cryptology*, 2025(3):475–515, Sep. 2025. URL: https://tosc.iacr.org/index.php/ToSC/article/view/12478, doi:10.46586/tosc.v2025.i3.475-515.

[Sun26] Ling Sun. A Linearisation Method for Identifying Dependencies in Differential Characteristics: Examining the Intersection of Deterministic Linear Relations and Nonlinear Constraints, 2026. doi:10.1007/s10623-025-01765-y.

[SWW21a] Ling Sun, Wei Wang, and Meiqin Wang. Accelerating the search of differential and linear characteristics with the sat method. *IACR Transactions on Symmetric Cryptology*, 2021(1):269–315, Mar. 2021. URL: https://tosc.iacr.org/index.php/ToSC/article/view/8840, doi:10.46586/tosc.v2021.i1.269-315.

[SWW21b] Ling Sun, Wei Wang, and Meiqin Wang. Improved attacks on GIFT-64. Cryptology ePrint Archive, Paper 2021/1179, 2021. URL: https://eprint.iacr.org/2021/1179.

[ZBL+14] Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, and Ingrid Verbauwhede. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. Cryptology ePrint Archive, Paper 2014/084, 2014. URL: https://eprint.iacr.org/2014/084, doi:10.1007/s11432-015-5459-7.

[ZDY19] Baoyu Zhu, Xiaoyang Dong, and Hongbo Yu. Milp-based differential attack on round-reduced gift. In Mitsuru Matsui, editor, *Topics in Cryptology – CT-RSA 2019*, pages 372–390, Cham, 2019. Springer International Publishing.

Algorithm 2: Constraint Decoupling via Union-Find (`Bit-Extractor`)

Input : $\mathcal{B}_{strong}$: set of strong masked bits;
$\mathcal{C}$: set of algebraic constraints of bits (linear and nonlinear equations);
Output : $\mathcal{S}$: partition of $\mathcal{B}_{strong}$ into decoupled constraint subsets

`// Phase 1: each bit starts in its own singleton cluster`
foreach $b \in \mathcal{B}_{strong}$ **do**
  $\texttt{Parent}[b] \leftarrow b$;
end

`// Phase 2: merge bits sharing a constraint`
foreach $c \in \mathcal{C}$ **do**
  $\mathcal{V}_c \leftarrow \mathrm{Vars}(c) \cap \mathcal{B}_{strong}$; `// strong bits connected by` c
  if $|\mathcal{V}_c| > 1$ **then**
    $b_0 \leftarrow$ any element of $\mathcal{V}_c$;
    foreach $b \in \mathcal{V}_c \setminus \{b_0\}$ **do**
      $\texttt{Union}(b_0, b)$;
    end
  end
end

`// Phase 3: collect connected components`
$\mathcal{M} \leftarrow \emptyset$; `// maps each root to its cluster`
foreach $b \in \mathcal{B}_{strong}$ **do**
  $r \leftarrow \texttt{Find}(b)$;
  if $r \notin \mathcal{M}$ **then**
    $\mathcal{M}[r] \leftarrow \emptyset$;
  end
  $\mathcal{M}[r] \leftarrow \mathcal{M}[r] \cup \{b\}$;
end
$\mathcal{S} \leftarrow \{\, \mathcal{M}[r] : r \in \mathcal{M} \,\}$;
return $\mathcal{S}$

`// Union-Find with path compression and union by rank`
Function $\texttt{Find}(b)$**:**
  if $\mathit{Parent}[b] \neq b$ **then**
    $\texttt{Parent}[b] \leftarrow \texttt{Find}(\mathit{Parent}[b])$;
  end
  return $\texttt{Parent}[b]$;

Function $\texttt{Union}(b_1, b_2)$**:**
  $r_1 \leftarrow \texttt{Find}(b_1)$; $r_2 \leftarrow \texttt{Find}(b_2)$;
  if $r_1 \neq r_2$ **then**
    $\texttt{Parent}[r_2] \leftarrow r_1$;
  end

A Method of value-restriction applied to a toy example

We recall the toy cipher in Section 3.1 and we color coded the wires of Figure 1 and re-present it in Figure 7 to show the constraints in a clearer view. We will derive the constraints by tracing the constraints.

We derive the fixed-key probability of the characteristic $(2,0) \to (5,0) \to (0,5) \to (0,15) \to (13,8) \to (4,*)$ by reading off, S-box by S-box, the conditions that the trail

Table 4: 4-round GIFT-64 differential characteristic T_0

Round	ΔI_s	ΔO_s
0	0x9c000c0a00000005	0x8400040100000002
1	0x000000000002c500	0x0000000000054200
2	0x0006004000000010	0x0002007000000050
3	0x0101000024040200	0x0505000057070500

Table 5: The 14-round RECTANGLE differential Characteristic T_{REC1} with stated probability of 2^{-63}

Round	ΔI_s	ΔO_s
0	0x0020000600000000	0x0060000200000000
1	0x0200006000000000	0x0600002000000000
2	0x2000060000000000	0x6000020000000000
3	0x0000600000000002	0x0000200000000006
4	0x0006000000000020	0x0002000000000060
5	0x0060000000000200	0x0020000000000600
6	0x0600000000002000	0x0200000000006000
7	0x6000000000020000	0x2000000000060000
8	0x0000000000200006	0x0000000000600002
9	0x0000000002000060	0x000000000c000020
10	0x0000000000008600	0x0000000000001200
11	0x0000000000003000	0x0000000000008000
12	0x0000000000000008	0x0000000000000001
13	0x0000000000000001	0x0000000000000006

Table 6: The 14-round RECTANGLE differential characteristic T_{REC2} with stated probability of 2^{-66}

Round	ΔI_s	ΔO_s
0	0x0020000600000000	0x0060000200000000
1	0x0200006000000000	0x0600002000000000
2	0x2000060000000000	0x6000020000000000
3	0x0000600000000002	0x0000200000000006
4	0x0006000000000020	0x0002000000000060
5	0x0060000000000200	0x0020000000000600
6	0x0600000000002000	0x0200000000006000
7	0x6000000000020000	0x2000000000060000
8	0x0000000000200006	0x0000000000600002
9	0x0000000002000060	0x000000000c000020
10	0x0000000000008600	0x0000000000009200
11	0x0000000000003008	0x0000000000008001
12	0x0000000000000009	0x0000000000000001
13	0x0000000000000001	0x0000000000000006

places on the round-key bits of Figure 7. For a transition $a \to b$ we write $\mathsf{XDDT}_S(a,b) = \{x : S(x+a) = S(x) + b\}$ for its right input set and $\mathsf{YDDT}_S(a,b) = S(\mathsf{XDDT}_S(a,b))$ for its right output set.

First, we can derive all the constraints out based on the $\mathsf{XDDT}_S(a,b)$ and $\mathsf{YDDT}_S(a,b)$. From $\mathsf{YDDT}_{S_A}(2,5) = \{1,4,6,3\}$, we obtain

$$y_3^A = 0 \quad \text{and} \quad y_0^A \oplus y_2^A = 1 \tag{1}$$

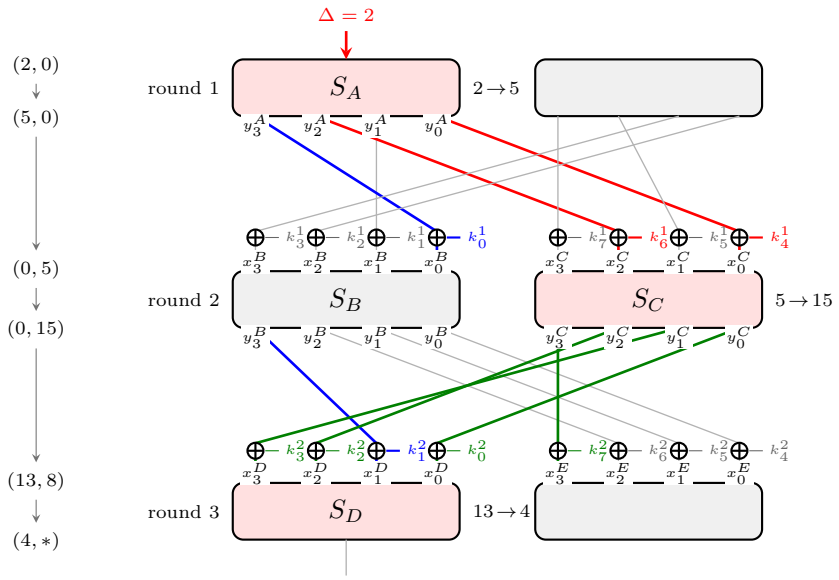


Figure 7: The same toy example presented in Section 3.1. The important wires are color-coded to show the different constraint sets. The red (resp. grey) boxes are the active (resp. inactive) `GIFT-64` S-boxes.

From $\mathsf{XDDT}_{S_C}(5, 15) = \{3, 6, 11, 14\}$, we obtain

$$x_2^C \oplus x_0^C = 1 \quad \text{and} \quad x_1^C = 1 \tag{2}$$

From $\mathsf{YDDT}_{S_C}(5, 15) = \{12, 3, 7, 8\}$, we obtain

$$y_3^C \oplus y_0^C = 1 \quad \text{and} \quad y_1^C \oplus y_0^C = 0 \tag{3}$$

From $\mathsf{XDDT}_{S_D}(13, 4) = \{3, 6, 11, 14\}$, we obtain

$$x_2^D \oplus x_0^D = 1 \quad \text{and} \quad x_1^D = 1 \tag{4}$$

Following the red wires with the red equations, we obtain the following system of equations

$$\begin{cases} y_0^A \oplus y_2^A = 1 \\ x_0^C \oplus x_2^C = 1 \\ x_0^C = y_0^A \oplus k_4^1 \\ x_2^C = y_2^A \oplus k_6^1 \end{cases}$$

All the non-key variables can be eliminated, leaving just the constraints on the keys. Solving the system gives $1 \oplus k_4^1 \oplus k_6^1 = 1$, so the red path forces the linear key condition

$$k_4^1 \oplus k_6^1 = 0. \tag{5}$$

Note that the set $\mathsf{XDDT}_{S_C}(5, 15)$ also fixes $x_1^C = 1$, but that bit is fed by an inactive S-box and is free over the keys, so it only scales the probability.

Following the green wires with the green equations, we have

$$\begin{cases} x_2^D \oplus k_2^2 = y_2^C \\ x_3^D \oplus k_3^2 = y_1^C \\ x_0^D \oplus k_0^2 = y_0^C \\ x_3^E \oplus k_7^2 = y_3^C \\ y_0^C \oplus y_3^C = 0 \\ y_0^C \oplus y_1^C = 0 \\ x_2^D \oplus x_0^D = 1 \end{cases}$$

If we simplify the system, we get the following:

$$y_2^C \oplus y_0^C \oplus x_3^D \oplus x_3^E = k_2^2 \oplus k_3^2 \oplus k_7^2 \oplus k_0^2$$

Given any fixed key values of $k^* = k_2^2 \oplus k_3^2 \oplus k_7^2 \oplus k_0^2$, we must have $y_2^C \oplus y_0^C \oplus x_3^D \oplus x_3^E = k^*$, which means the plaintexts are split into two groups, depending on the value of k^*. Since we do not have any other constraints that involve these variables, we can say that the probability is $\frac{1}{2}$ and it is independent of k^*.

Following the blue wires with the blue equations, we have

$$\begin{cases} y_3^A = 0 \\ x_1^D = 1 \\ x_0^B = k_0^1 \oplus y_3^A \\ x_1^D = k_1^2 \oplus y_3^B \\ y_3^B, y_2^B, y_1^B, y_0^B = S(x_3^B, x_2^B, x_1^B, x_0^B) \end{cases}$$

Given that $y_2^B, y_1^B, y_0^B, x_3^B, x_2^B$ and x_1^B are not involved in any other constraint sets, we can assume that they are uniformly random and derive that $x_0^B \oplus y_3^B = k_0^1 \oplus k_1^2 \oplus 1$ occurs with a probability of $\frac{3}{4}$, which holds with a probability of $\frac{3}{4}$ when $k_0^1 \oplus k_1^2 = 1$ and $\frac{1}{4}$ when $k_0^1 \oplus k_1^2 = 0$. Once again, unlike the linear condition in Equation 5, this constraint set removes no key; it splits the surviving keys into two probability classes. Collecting the three independent sets, the fixed-key probability is

$$\Pr[\mathcal{T} \mid k] = \begin{cases} 0, & k_4^1 \oplus k_6^1 = 1, \\ 2^{-6}, & k_4^1 \oplus k_6^1 = 0,\ k_0^1 \oplus k_1^2 = 0, \\ 3 \cdot 2^{-6}, & k_4^1 \oplus k_6^1 = 0,\ k_0^1 \oplus k_1^2 = 1. \end{cases} \tag{6}$$

Half of the keys give probability 0; among the rest the inactive S_B splits the probability in the ratio $3:1$, and the average over all keys is the Markov value 2^{-6}.

B Identified Constraints for GIFT Characteristics

B.1 Nonlinear Constraints from 4-round GIFT-64 Toy characteristic

Nonlinear Constraint $\mathbb{E}_0$:

$$\begin{aligned} [y_{60}^0] \oplus x_{28}^1 \oplus k_{120} &= 0 \\ [y_{59}^0] \oplus x_{31}^1 &= 0 \\ y_{31}^1 \oplus [x_7^2] &= 0 \\ S(x_{28}^1, \ldots, x_{31}^1) &= (y_{28}^1, \ldots, y_{31}^1) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_1$:

$$
\begin{aligned}
[y_{34}^0] \oplus x_{42}^1 &= 0 \\
y_{42}^1 \oplus x_{10}^2 &= 0 \\
y_{47}^1 \oplus x_{11}^2 &= 0 \\
y_9^2 \oplus [x_{49}^3] \oplus k_{35} &= 0 \\
S(x_{44}^1, \ldots, x_{47}^1) &= (y_{44}^1, \ldots, y_{47}^1) \\
S(x_{40}^1, \ldots, x_{43}^1) &= (y_{40}^1, \ldots, y_{43}^1) \\
S(x_8^2, \ldots, x_{11}^2) &= (y_8^2, \ldots, y_{11}^2)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2$:

$$
\begin{aligned}
[y_{43}^0] \oplus x_{27}^1 &= 0 \\
y_{26}^1 \oplus [x_6^2] &= 0 \\
y_{24}^1 \oplus [x_{36}^2] \oplus k_{86} &= 0 \\
S(x_{24}^1, \ldots, x_{27}^1) &= (y_{24}^1, \ldots, y_{27}^1)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_3$:

$$
\begin{aligned}
[y_0^0] \oplus x_0^1 \oplus k_{127} &= 0 \\
y_0^1 \oplus x_0^2 \oplus k_{95} &= 0 \\
[y_{10}^1] \oplus x_2^2 &= 0 \\
[y_{15}^1] \oplus x_3^2 &= 0 \\
[y_8^1] \oplus x_{32}^2 \oplus k_{87} &= 0 \\
y_2^1 \oplus x_{34}^2 &= 0 \\
y_3^1 \oplus [x_{51}^2] &= 0 \\
y_{32}^2 \oplus [x_8^3] \oplus k_{61} &= 0 \\
y_1^2 \oplus x_{17}^3 \oplus k_{43} &= 0 \\
y_{33}^2 \oplus x_{25}^3 \oplus k_{41} &= 0 \\
y_3^2 \oplus [x_{51}^3] &= 0 \\
y_{35}^2 \oplus [x_{59}^3] &= 0 \\
S(x_{16}^3, \ldots, x_{19}^3) &= (y_{16}^3, \ldots, y_{19}^3) \\
S(x_0^2, \ldots, x_3^2) &= (y_0^2, \ldots, y_3^2) \\
S(x_{24}^3, \ldots, x_{27}^3) &= (y_{24}^3, \ldots, y_{27}^3) \\
S(x_0^1, \ldots, x_3^1) &= (y_0^1, \ldots, y_3^1) \\
S(x_{32}^2, \ldots, x_{35}^2) &= (y_{32}^2, \ldots, y_{35}^2)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_4$:

$$
\begin{aligned}
[y_3^0] \oplus x_{51}^1 &= 0 \\
[y_{35}^0] \oplus x_{59}^1 &= 0 \\
[y_{62}^0] \oplus x_{62}^1 &= 0 \\
y_{48}^1 \oplus x_{12}^2 \oplus k_{92} &= 0 \\
y_{58}^1 \oplus x_{14}^2 &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{63}^1 \oplus x_{15}^2 &= 0 \\
y_{56}^1 \oplus x_{44}^2 \oplus k_{84} &= 0 \\
y_{61}^1 \oplus x_{45}^2 \oplus k_{68} &= 0 \\
y_{50}^1 \oplus x_{46}^2 &= 0 \\
y_{57}^1 \oplus x_{61}^2 \oplus k_{64} &= 0 \\
y_{62}^1 \oplus x_{62}^2 &= 0 \\
y_{51}^1 \oplus x_{63}^2 &= 0 \\
y_{47}^2 \oplus [x_{11}^3] &= 0 \\
y_{12}^2 \oplus [x_{16}^3] \oplus k_{59} &= 0 \\
y_{44}^2 \oplus [x_{24}^3] \oplus k_{57} &= 0 \\
y_{60}^2 \oplus [x_{28}^3] \oplus k_{56} &= 0 \\
y_{14}^2 \oplus [x_{50}^3] &= 0 \\
y_{46}^2 \oplus [x_{58}^3] &= 0 \\
S(x_{48}^1, \ldots, x_{51}^1) &= (y_{48}^1, \ldots, y_{51}^1) \\
S(x_{60}^2, \ldots, x_{63}^2) &= (y_{60}^2, \ldots, y_{63}^2) \\
S(x_{60}^1, \ldots, x_{63}^1) &= (y_{60}^1, \ldots, y_{63}^1) \\
S(x_{56}^1, \ldots, x_{59}^1) &= (y_{56}^1, \ldots, y_{59}^1) \\
S(x_{12}^2, \ldots, x_{15}^2) &= (y_{12}^2, \ldots, y_{15}^2) \\
S(x_{44}^2, \ldots, x_{47}^2) &= (y_{44}^2, \ldots, y_{47}^2)
\end{aligned}
$$

B.2 Constraints from 9-round GIFT-64 Characteristic

Nonlinear Constraint $\mathbb{E}_0^1$:

$$
\begin{aligned}
y_{16}^1 \oplus x_4^2 \oplus k_{94} &= 0 \\
y_{26}^1 \oplus x_6^2 &= 0 \\
y_{24}^1 \oplus x_{36}^2 \oplus k_{86} &= 0 \\
y_{18}^1 \oplus x_{38}^2 &= 0 \\
y_5^2 \oplus x_1^3 \oplus k_{47} &= 0 \\
y_{37}^2 \oplus x_9^3 \oplus k_{45} &= 0 \\
y_0^3 \oplus x_0^4 \oplus k_{31} &= 0 \\
y_{10}^3 \oplus x_2^4 &= 0 \\
y_1^3 \oplus x_{17}^4 \oplus k_{11} &= 0 \\
[y_{11}^3] \oplus x_{19}^4 &= 0 \\
y_8^3 \oplus x_{32}^4 \oplus k_{23} &= 0 \\
y_2^3 \oplus x_{34}^4 &= 0 \\
y_9^3 \oplus x_{49}^4 \oplus k_3 &= 0 \\
[y_3^3] \oplus x_{51}^4 &= 0 \\
y_{17}^4 \oplus x_{21}^5 \oplus k_{104} &= 0 \\
y_{49}^4 \oplus x_{29}^5 \oplus k_{102} &= 0 \\
y_{31}^5 \oplus [x_7^6] &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{23}^5 \oplus [x_{39}^6] &= 0 \\
S(x_0^4, \ldots, x_3^4) &= (y_0^4, \ldots, y_3^4) \\
S(x_{48}^4, \ldots, x_{51}^4) &= (y_{48}^4, \ldots, y_{51}^4) \\
S(x_{28}^5, \ldots, x_{31}^5) &= (y_{28}^5, \ldots, y_{31}^5) \\
S(x_{24}^1, \ldots, x_{27}^1) &= (y_{24}^1, \ldots, y_{27}^1) \\
S(x_0^3, \ldots, x_3^3) &= (y_0^3, \ldots, y_3^3) \\
S(x_{32}^4, \ldots, x_{35}^4) &= (y_{32}^4, \ldots, y_{35}^4) \\
S(x_4^2, \ldots, x_7^2) &= (y_4^2, \ldots, y_7^2) \\
S(x_8^3, \ldots, x_{11}^3) &= (y_8^3, \ldots, y_{11}^3) \\
S(x_{16}^4, \ldots, x_{19}^4) &= (y_{16}^4, \ldots, y_{19}^4) \\
S(x_{20}^5, \ldots, x_{23}^5) &= (y_{20}^5, \ldots, y_{23}^5) \\
S(x_{16}^1, \ldots, x_{19}^1) &= (y_{16}^1, \ldots, y_{19}^1) \\
S(x_{36}^2, \ldots, x_{39}^2) &= (y_{36}^2, \ldots, y_{39}^2)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_1^1$:

$$
\begin{aligned}
y_0^7 \oplus x_0^8 \oplus k_{19} &= 0 \\
y_{10}^7 \oplus x_2^8 &= 0 \\
y_8^7 \oplus x_{32}^8 \oplus k_{27} &= 0 \\
y_2^7 \oplus x_{34}^8 &= 0 \\
S(x_0^8, \ldots, x_3^8) &= (y_0^8, \ldots, y_3^8) \\
S(x_{32}^8, \ldots, x_{35}^8) &= (y_{32}^8, \ldots, y_{35}^8) \\
S(x_0^7, \ldots, x_3^7) &= (y_0^7, \ldots, y_3^7) \\
S(x_8^7, \ldots, x_{11}^7) &= (y_8^7, \ldots, y_{11}^7)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2^1$:

$$
\begin{aligned}
y_{16}^5 \oplus x_4^6 \oplus k_{82} &= 0 \\
y_{26}^5 \oplus x_6^6 &= 0 \\
y_{24}^5 \oplus x_{36}^6 \oplus k_{90} &= 0 \\
y_{18}^5 \oplus x_{38}^6 &= 0 \\
S(x_{16}^5, \ldots, x_{19}^5) &= (y_{16}^5, \ldots, y_{19}^5) \\
S(x_{24}^5, \ldots, x_{27}^5) &= (y_{24}^5, \ldots, y_{27}^5) \\
S(x_4^6, \ldots, x_7^6) &= (y_4^6, \ldots, y_7^6) \\
S(x_{36}^6, \ldots, x_{39}^6) &= (y_{36}^6, \ldots, y_{39}^6)
\end{aligned}
$$

B.3 New Nonlinear Constraints from 10-round GIFT-64 Characteristic in [JYSYZ+18]

Nonlinear Constraint $\mathbb{E}_0^2$:

$$
\begin{aligned}
y_{16}^1 \oplus x_4^2 \oplus k_{94} &= 0 \\
y_{18}^1 \oplus x_{38}^2 &= 0 \\
[y_{19}^1] \oplus x_{55}^2 &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{6}^{2} \oplus x_{18}^{3} &= 0 \\
y_{54}^{2} \oplus x_{30}^{3} &= 0 \\
y_{4}^{2} \oplus x_{48}^{3} \oplus k_{51} &= 0 \\
y_{36}^{2} \oplus x_{56}^{3} \oplus k_{49} &= 0 \\
y_{52}^{2} \oplus x_{60}^{3} \oplus k_{48} &= 0 \\
y_{16}^{3} \oplus x_{4}^{4} \oplus k_{30} &= 0 \\
y_{26}^{3} \oplus x_{6}^{4} &= 0 \\
y_{31}^{3} \oplus [x_{7}^{4}] &= 0 \\
y_{48}^{3} \oplus x_{12}^{4} \oplus k_{28} &= 0 \\
y_{58}^{3} \oplus x_{14}^{4} &= 0 \\
y_{63}^{3} \oplus [x_{15}^{4}] &= 0 \\
y_{17}^{3} \oplus x_{21}^{4} \oplus k_{10} &= 0 \\
[y_{27}^{3}] \oplus x_{23}^{4} &= 0 \\
y_{60}^{3} \oplus x_{28}^{4} \oplus k_{24} &= 0 \\
[y_{49}^{3}] \oplus x_{29}^{4} \oplus k_{8} &= 0 \\
[y_{59}^{3}] \oplus x_{31}^{4} &= 0 \\
y_{24}^{3} \oplus x_{36}^{4} \oplus k_{22} &= 0 \\
y_{29}^{3} \oplus [x_{37}^{4}] \oplus k_{6} &= 0 \\
y_{18}^{3} \oplus x_{38}^{4} &= 0 \\
y_{56}^{3} \oplus x_{44}^{4} \oplus k_{20} &= 0 \\
y_{61}^{3} \oplus [x_{45}^{4}] \oplus k_{4} &= 0 \\
y_{50}^{3} \oplus x_{46}^{4} &= 0 \\
y_{25}^{3} \oplus x_{53}^{4} \oplus k_{2} &= 0 \\
y_{30}^{3} \oplus x_{54}^{4} &= 0 \\
[y_{19}^{3}] \oplus x_{55}^{4} &= 0 \\
[y_{57}^{3}] \oplus x_{61}^{4} \oplus k_{0} &= 0 \\
[y_{51}^{3}] \oplus x_{63}^{4} &= 0 \\
y_{5}^{4} \oplus x_{1}^{5} \oplus k_{109} &= 0 \\
y_{15}^{4} \oplus x_{3}^{5} &= 0 \\
y_{21}^{4} \oplus x_{5}^{5} \oplus k_{108} &= 0 \\
y_{31}^{4} \oplus x_{7}^{5} &= 0 \\
y_{37}^{4} \oplus x_{9}^{5} \oplus k_{107} &= 0 \\
y_{47}^{4} \oplus x_{11}^{5} &= 0 \\
y_{53}^{4} \oplus x_{13}^{5} \oplus k_{106} &= 0 \\
y_{63}^{4} \oplus x_{15}^{5} &= 0 \\
[y_{13}^{4}] \oplus x_{33}^{5} \oplus k_{101} &= 0 \\
[y_{7}^{4}] \oplus x_{35}^{5} &= 0 \\
y_{29}^{4} \oplus x_{37}^{5} \oplus k_{100} &= 0 \\
[y_{45}^{4}] \oplus x_{41}^{5} \oplus k_{99} &= 0
\end{aligned}
$$

$$
\begin{aligned}
[y^4_{39}] \oplus x^5_{43} &= 0\\
y^4_{61} \oplus x^5_{45} \oplus k_{98} &= 0\\
[y^5_0] \oplus x^6_0 \oplus k_{83} &= 0\\
y^5_5 \oplus x^6_1 \oplus k_{77} &= 0\\
[y^5_{10}] \oplus x^6_2 &= 0\\
y^5_{15} \oplus x^6_3 &= 0\\
y^5_{12} \oplus [x^6_{16}] \oplus k_{95} &= 0\\
y^5_1 \oplus x^6_{17} \oplus k_{73} &= 0\\
y^5_6 \oplus x^6_{18} &= 0\\
y^5_{11} \oplus x^6_{19} &= 0\\
y^5_{44} \oplus x^6_{24} \oplus k_{93} &= 0\\
y^5_{33} \oplus x^6_{25} \oplus k_{71} &= 0\\
y^5_{38} \oplus x^6_{26} &= 0\\
[y^5_8] \oplus x^6_{32} \oplus k_{91} &= 0\\
y^5_{13} \oplus x^6_{33} \oplus k_{69} &= 0\\
[y^5_2] \oplus x^6_{34} &= 0\\
y^5_7 \oplus x^6_{35} &= 0\\
y^5_4 \oplus [x^6_{48}] \oplus k_{87} &= 0\\
y^5_9 \oplus x^6_{49} \oplus k_{65} &= 0\\
y^5_{14} \oplus x^6_{50} &= 0\\
y^5_3 \oplus x^6_{51} &= 0\\
y^5_{36} \oplus x^6_{56} \oplus k_{85} &= 0\\
y^5_{41} \oplus x^6_{57} \oplus k_{79} &= 0\\
y^5_{46} \oplus x^6_{58} &= 0\\
y^6_0 \oplus x^7_0 \oplus k_{51} &= 0\\
y^6_{16} \oplus x^7_4 \oplus k_{50} &= 0\\
y^6_{26} \oplus [x^7_6] &= 0\\
y^6_{32} \oplus x^7_8 \oplus k_{49} &= 0\\
y^6_{48} \oplus x^7_{12} \oplus k_{48} &= 0\\
y^6_{58} \oplus [x^7_{14}] &= 0\\
y^7_{12} \oplus x^8_{16} \oplus k_{31} &= 0\\
y^7_6 \oplus x^8_{18} &= 0\\
y^7_{11} \oplus [x^8_{19}] &= 0\\
y^7_4 \oplus x^8_{48} \oplus k_{23} &= 0\\
y^7_{14} \oplus x^8_{50} &= 0\\
y^7_3 \oplus [x^8_{51}] &= 0\\
S(x^6_{48}, \ldots, x^6_{51}) &= (y^6_{48}, \ldots, y^6_{51})\\
S(x^3_{16}, \ldots, x^3_{19}) &= (y^3_{16}, \ldots, y^3_{19})\\
S(x^4_{12}, \ldots, x^4_{15}) &= (y^4_{12}, \ldots, y^4_{15})
\end{aligned}
$$

$$
\begin{aligned}
S(x^4_{36},\ldots,x^4_{39}) &= (y^4_{36},\ldots,y^4_{39})\\
S(x^3_{28},\ldots,x^3_{31}) &= (y^3_{28},\ldots,y^3_{31})\\
S(x^5_{4},\ldots,x^5_{7}) &= (y^5_{4},\ldots,y^5_{7})\\
S(x^4_{60},\ldots,x^4_{63}) &= (y^4_{60},\ldots,y^4_{63})\\
S(x^5_{40},\ldots,x^5_{43}) &= (y^5_{40},\ldots,y^5_{43})\\
S(x^8_{48},\ldots,x^8_{51}) &= (y^8_{48},\ldots,y^8_{51})\\
S(x^7_{4},\ldots,x^7_{7}) &= (y^7_{4},\ldots,y^7_{7})\\
S(x^6_{32},\ldots,x^6_{35}) &= (y^6_{32},\ldots,y^6_{35})\\
S(x^6_{56},\ldots,x^6_{59}) &= (y^6_{56},\ldots,y^6_{59})\\
S(x^4_{20},\ldots,x^4_{23}) &= (y^4_{20},\ldots,y^4_{23})\\
S(x^5_{0},\ldots,x^5_{3}) &= (y^5_{0},\ldots,y^5_{3})\\
S(x^3_{24},\ldots,x^3_{27}) &= (y^3_{24},\ldots,y^3_{27})\\
S(x^5_{12},\ldots,x^5_{15}) &= (y^5_{12},\ldots,y^5_{15})\\
S(x^5_{36},\ldots,x^5_{39}) &= (y^5_{36},\ldots,y^5_{39})\\
S(x^4_{44},\ldots,x^4_{47}) &= (y^4_{44},\ldots,y^4_{47})\\
S(x^3_{48},\ldots,x^3_{51}) &= (y^3_{48},\ldots,y^3_{51})\\
S(x^3_{60},\ldots,x^3_{63}) &= (y^3_{60},\ldots,y^3_{63})\\
S(x^2_{4},\ldots,x^2_{7}) &= (y^2_{4},\ldots,y^2_{7})\\
S(x^7_{0},\ldots,x^7_{3}) &= (y^7_{0},\ldots,y^7_{3})\\
S(x^6_{16},\ldots,x^6_{19}) &= (y^6_{16},\ldots,y^6_{19})\\
S(x^2_{52},\ldots,x^2_{55}) &= (y^2_{52},\ldots,y^2_{55})\\
S(x^7_{12},\ldots,x^7_{15}) &= (y^7_{12},\ldots,y^7_{15})\\
S(x^4_{4},\ldots,x^4_{7}) &= (y^4_{4},\ldots,y^4_{7})\\
S(x^4_{28},\ldots,x^4_{31}) &= (y^4_{28},\ldots,y^4_{31})\\
S(x^5_{8},\ldots,x^5_{11}) &= (y^5_{8},\ldots,y^5_{11})\\
S(x^3_{56},\ldots,x^3_{59}) &= (y^3_{56},\ldots,y^3_{59})\\
S(x^8_{16},\ldots,x^8_{19}) &= (y^8_{16},\ldots,y^8_{19})\\
S(x^4_{52},\ldots,x^4_{55}) &= (y^4_{52},\ldots,y^4_{55})\\
S(x^5_{44},\ldots,x^5_{47}) &= (y^5_{44},\ldots,y^5_{47})\\
S(x^5_{32},\ldots,x^5_{35}) &= (y^5_{32},\ldots,y^5_{35})\\
S(x^1_{16},\ldots,x^1_{19}) &= (y^1_{16},\ldots,y^1_{19})\\
S(x^2_{36},\ldots,x^2_{39}) &= (y^2_{36},\ldots,y^2_{39})\\
S(x^7_{8},\ldots,x^7_{11}) &= (y^7_{8},\ldots,y^7_{11})\\
S(x^6_{0},\ldots,x^6_{3}) &= (y^6_{0},\ldots,y^6_{3})\\
S(x^6_{24},\ldots,x^6_{27}) &= (y^6_{24},\ldots,y^6_{27})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}^2_1$:

$$
\begin{aligned}
[y^4_{12}] \oplus x^5_{16} \oplus k_{127} &= 0\\
[y^4_{6}] \oplus x^5_{18} &= 0\\
[y^4_{44}] \oplus x^5_{24} \oplus k_{125} &= 0
\end{aligned}
$$

$$
\begin{aligned}
[y_{38}^4] \oplus x_{26}^5 &= 0 \\
y_{17}^5 \oplus x_{21}^6 \oplus k_{72} &= 0 \\
y_{27}^5 \oplus x_{23}^6 &= 0 \\
y_{25}^5 \oplus x_{53}^6 \oplus k_{64} &= 0 \\
y_{19}^5 \oplus x_{55}^6 &= 0 \\
y_{21}^6 \oplus [x_5^7] \oplus k_{44} &= 0 \\
y_{53}^6 \oplus [x_{13}^7] \oplus k_{42} &= 0 \\
S(x_{16}^5, \ldots, x_{19}^5) &= (y_{16}^5, \ldots, y_{19}^5) \\
S(x_{20}^6, \ldots, x_{23}^6) &= (y_{20}^6, \ldots, y_{23}^6) \\
S(x_{24}^5, \ldots, x_{27}^5) &= (y_{24}^5, \ldots, y_{27}^5) \\
S(x_{52}^6, \ldots, x_{55}^6) &= (y_{52}^6, \ldots, y_{55}^6)
\end{aligned}
$$

B.4 New Nonlinear Constraints from 12-round GIFT-64 Characteristic [CZD20]

Nonlinear Constraint $\mathbb{E}_0^3$:

$$
\begin{aligned}
y_{16}^1 \oplus x_4^2 \oplus k_{94} &= 0 \\
y_{26}^1 \oplus x_6^2 &= 0 \\
y_{24}^1 \oplus x_{36}^2 \oplus k_{86} &= 0 \\
y_{18}^1 \oplus x_{38}^2 &= 0 \\
y_5^2 \oplus x_1^3 \oplus k_{47} &= 0 \\
y_{37}^2 \oplus x_9^3 \oplus k_{45} &= 0 \\
y_0^3 \oplus x_0^4 \oplus k_{31} &= 0 \\
y_{10}^3 \oplus x_2^4 &= 0 \\
y_1^3 \oplus x_{17}^4 \oplus k_{11} &= 0 \\
[y_{11}^3] \oplus x_{19}^4 &= 0 \\
y_8^3 \oplus x_{32}^4 \oplus k_{23} &= 0 \\
y_2^3 \oplus x_{34}^4 &= 0 \\
y_9^3 \oplus x_{49}^4 \oplus k_3 &= 0 \\
[y_3^3] \oplus x_{51}^4 &= 0 \\
y_1^4 \oplus x_{17}^5 \oplus k_{105} &= 0 \\
y_{17}^4 \oplus x_{21}^5 \oplus k_{104} &= 0 \\
y_{33}^4 \oplus x_{25}^5 \oplus k_{103} &= 0 \\
y_{49}^4 \oplus x_{29}^5 \oplus k_{102} &= 0 \\
y_{28}^5 \oplus [x_{20}^6] \oplus k_{94} &= 0 \\
y_{17}^5 \oplus x_{21}^6 \oplus k_{72} &= 0 \\
y_{22}^5 \oplus x_{22}^6 &= 0 \\
y_{27}^5 \oplus x_{23}^6 &= 0 \\
y_{20}^5 \oplus [x_{52}^6] \oplus k_{86} &= 0 \\
y_{25}^5 \oplus x_{53}^6 \oplus k_{64} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{30}^{5} \oplus x_{54}^{6} &= 0 \\
y_{19}^{5} \oplus x_{55}^{6} &= 0 \\
y_{20}^{6} \oplus x_{52}^{7} \oplus k_{54} &= 0 \\
y_{52}^{6} \oplus x_{60}^{7} \oplus k_{52} &= 0 \\
y_{53}^{7} \oplus x_{13}^{8} \oplus k_{10} &= 0 \\
y_{61}^{7} \oplus x_{45}^{8} \oplus k_{2} &= 0 \\
y_{12}^{8} \oplus x_{16}^{9} \oplus k_{115} &= 0 \\
y_{44}^{8} \oplus x_{24}^{9} \oplus k_{113} &= 0 \\
y_{16}^{9} \oplus x_{4}^{10} \oplus k_{86} &= 0 \\
y_{26}^{9} \oplus x_{6}^{10} &= 0 \\
y_{24}^{9} \oplus x_{36}^{10} \oplus k_{94} &= 0 \\
y_{18}^{9} \oplus x_{38}^{10} &= 0 \\
S(x_{0}^{4}, \ldots, x_{3}^{4}) &= (y_{0}^{4}, \ldots, y_{3}^{4}) \\
S(x_{16}^{5}, \ldots, x_{19}^{5}) &= (y_{16}^{5}, \ldots, y_{19}^{5}) \\
S(x_{48}^{4}, \ldots, x_{51}^{4}) &= (y_{48}^{4}, \ldots, y_{51}^{4}) \\
S(x_{28}^{5}, \ldots, x_{31}^{5}) &= (y_{28}^{5}, \ldots, y_{31}^{5}) \\
S(x_{12}^{8}, \ldots, x_{15}^{8}) &= (y_{12}^{8}, \ldots, y_{15}^{8}) \\
S(x_{36}^{10}, \ldots, x_{39}^{10}) &= (y_{36}^{10}, \ldots, y_{39}^{10}) \\
S(x_{24}^{1}, \ldots, x_{27}^{1}) &= (y_{24}^{1}, \ldots, y_{27}^{1}) \\
S(x_{20}^{6}, \ldots, x_{23}^{6}) &= (y_{20}^{6}, \ldots, y_{23}^{6}) \\
S(x_{52}^{7}, \ldots, x_{55}^{7}) &= (y_{52}^{7}, \ldots, y_{55}^{7}) \\
S(x_{0}^{3}, \ldots, x_{3}^{3}) &= (y_{0}^{3}, \ldots, y_{3}^{3}) \\
S(x_{24}^{5}, \ldots, x_{27}^{5}) &= (y_{24}^{5}, \ldots, y_{27}^{5}) \\
S(x_{32}^{4}, \ldots, x_{35}^{4}) &= (y_{32}^{4}, \ldots, y_{35}^{4}) \\
S(x_{44}^{8}, \ldots, x_{47}^{8}) &= (y_{44}^{8}, \ldots, y_{47}^{8}) \\
S(x_{16}^{9}, \ldots, x_{19}^{9}) &= (y_{16}^{9}, \ldots, y_{19}^{9}) \\
S(x_{4}^{2}, \ldots, x_{7}^{2}) &= (y_{4}^{2}, \ldots, y_{7}^{2}) \\
S(x_{52}^{6}, \ldots, x_{55}^{6}) &= (y_{52}^{6}, \ldots, y_{55}^{6}) \\
S(x_{60}^{7}, \ldots, x_{63}^{7}) &= (y_{60}^{7}, \ldots, y_{63}^{7}) \\
S(x_{8}^{3}, \ldots, x_{11}^{3}) &= (y_{8}^{3}, \ldots, y_{11}^{3}) \\
S(x_{16}^{4}, \ldots, x_{19}^{4}) &= (y_{16}^{4}, \ldots, y_{19}^{4}) \\
S(x_{20}^{5}, \ldots, x_{23}^{5}) &= (y_{20}^{5}, \ldots, y_{23}^{5}) \\
S(x_{24}^{9}, \ldots, x_{27}^{9}) &= (y_{24}^{9}, \ldots, y_{27}^{9}) \\
S(x_{4}^{10}, \ldots, x_{7}^{10}) &= (y_{4}^{10}, \ldots, y_{7}^{10}) \\
S(x_{16}^{1}, \ldots, x_{19}^{1}) &= (y_{16}^{1}, \ldots, y_{19}^{1}) \\
S(x_{36}^{2}, \ldots, x_{39}^{2}) &= (y_{36}^{2}, \ldots, y_{39}^{2})
\end{aligned}
$$

B.5 New Nonlinear Constraints from 12-round GIFT-64 Characteristic [LWZZ19]

Nonlinear Constraint $\mathbb{E}_0^4$:

$$
\begin{aligned}
y_{16}^1 \oplus x_4^2 \oplus k_{94} &= 0\\
y_{26}^1 \oplus x_6^2 &= 0\\
y_{24}^1 \oplus x_{36}^2 \oplus k_{86} &= 0\\
y_{18}^1 \oplus x_{38}^2 &= 0\\
y_5^2 \oplus x_1^3 \oplus k_{47} &= 0\\
y_{37}^2 \oplus x_9^3 \oplus k_{45} &= 0\\
y_0^3 \oplus x_0^4 \oplus k_{31} &= 0\\
y_{10}^3 \oplus x_2^4 &= 0\\
y_1^3 \oplus x_{17}^4 \oplus k_{11} &= 0\\
[y_{11}^3] \oplus x_{19}^4 &= 0\\
y_8^3 \oplus x_{32}^4 \oplus k_{23} &= 0\\
y_2^3 \oplus x_{34}^4 &= 0\\
y_9^3 \oplus x_{49}^4 \oplus k_3 &= 0\\
[y_3^3] \oplus x_{51}^4 &= 0\\
y_1^4 \oplus x_{17}^5 \oplus k_{105} &= 0\\
y_{17}^4 \oplus x_{21}^5 \oplus k_{104} &= 0\\
y_{33}^4 \oplus x_{25}^5 \oplus k_{103} &= 0\\
y_{49}^4 \oplus x_{29}^5 \oplus k_{102} &= 0\\
y_{16}^5 \oplus x_4^6 \oplus k_{82} &= 0\\
y_{21}^5 \oplus [x_5^6] \oplus k_{76} &= 0\\
y_{26}^5 \oplus x_6^6 &= 0\\
y_{31}^5 \oplus [x_7^6] &= 0\\
y_{17}^5 \oplus x_{21}^6 \oplus k_{72} &= 0\\
[y_{27}^5] \oplus x_{23}^6 &= 0\\
y_{24}^5 \oplus x_{36}^6 \oplus k_{90} &= 0\\
y_{29}^5 \oplus [x_{37}^6] \oplus k_{68} &= 0\\
y_{18}^5 \oplus x_{38}^6 &= 0\\
y_{23}^5 \oplus [x_{39}^6] &= 0\\
y_{25}^5 \oplus x_{53}^6 \oplus k_{64} &= 0\\
[y_{19}^5] \oplus x_{55}^6 &= 0\\
y_5^6 \oplus x_1^7 \oplus k_{45} &= 0\\
y_{21}^6 \oplus x_5^7 \oplus k_{44} &= 0\\
y_{37}^6 \oplus x_9^7 \oplus k_{43} &= 0\\
y_{53}^6 \oplus x_{13}^7 \oplus k_{42} &= 0\\
y_0^7 \oplus x_0^8 \oplus k_{19} &= 0\\
y_5^7 \oplus [x_1^8] \oplus k_{13} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{10}^{7} \oplus x_{2}^{8} &= 0 \\
y_{15}^{7} \oplus [x_{3}^{8}] &= 0 \\
y_{1}^{7} \oplus x_{17}^{8} \oplus k_{9} &= 0 \\
[y_{11}^{7}] \oplus x_{19}^{8} &= 0 \\
y_{8}^{7} \oplus x_{32}^{8} \oplus k_{27} &= 0 \\
y_{13}^{7} \oplus [x_{33}^{8}] \oplus k_{5} &= 0 \\
y_{2}^{7} \oplus x_{34}^{8} &= 0 \\
y_{7}^{7} \oplus [x_{35}^{8}] &= 0 \\
y_{9}^{7} \oplus x_{49}^{8} \oplus k_{1} &= 0 \\
[y_{3}^{7}] \oplus x_{51}^{8} &= 0 \\
y_{17}^{8} \oplus x_{21}^{9} \oplus k_{102} &= 0 \\
y_{49}^{8} \oplus x_{29}^{9} \oplus k_{100} &= 0 \\
y_{16}^{9} \oplus x_{4}^{10} \oplus k_{86} &= 0 \\
y_{21}^{9} \oplus [x_{5}^{10}] \oplus k_{74} &= 0 \\
y_{26}^{9} \oplus x_{6}^{10} &= 0 \\
y_{31}^{9} \oplus [x_{7}^{10}] &= 0 \\
y_{24}^{9} \oplus x_{36}^{10} \oplus k_{94} &= 0 \\
y_{29}^{9} \oplus [x_{37}^{10}] \oplus k_{66} &= 0 \\
y_{18}^{9} \oplus x_{38}^{10} &= 0 \\
y_{23}^{9} \oplus [x_{39}^{10}] &= 0 \\
S(x_{0}^{4}, \ldots, x_{3}^{4}) &= (y_{0}^{4}, \ldots, y_{3}^{4}) \\
S(x_{16}^{5}, \ldots, x_{19}^{5}) &= (y_{16}^{5}, \ldots, y_{19}^{5}) \\
S(x_{48}^{4}, \ldots, x_{51}^{4}) &= (y_{48}^{4}, \ldots, y_{51}^{4}) \\
S(x_{0}^{8}, \ldots, x_{3}^{8}) &= (y_{0}^{8}, \ldots, y_{3}^{8}) \\
S(x_{28}^{5}, \ldots, x_{31}^{5}) &= (y_{28}^{5}, \ldots, y_{31}^{5}) \\
S(x_{20}^{9}, \ldots, x_{23}^{9}) &= (y_{20}^{9}, \ldots, y_{23}^{9}) \\
S(x_{48}^{8}, \ldots, x_{51}^{8}) &= (y_{48}^{8}, \ldots, y_{51}^{8}) \\
S(x_{36}^{10}, \ldots, x_{39}^{10}) &= (y_{36}^{10}, \ldots, y_{39}^{10}) \\
S(x_{24}^{1}, \ldots, x_{27}^{1}) &= (y_{24}^{1}, \ldots, y_{27}^{1}) \\
S(x_{4}^{7}, \ldots, x_{7}^{7}) &= (y_{4}^{7}, \ldots, y_{7}^{7}) \\
S(x_{20}^{6}, \ldots, x_{23}^{6}) &= (y_{20}^{6}, \ldots, y_{23}^{6}) \\
S(x_{0}^{3}, \ldots, x_{3}^{3}) &= (y_{0}^{3}, \ldots, y_{3}^{3}) \\
S(x_{24}^{5}, \ldots, x_{27}^{5}) &= (y_{24}^{5}, \ldots, y_{27}^{5}) \\
S(x_{32}^{4}, \ldots, x_{35}^{4}) &= (y_{32}^{4}, \ldots, y_{35}^{4}) \\
S(x_{28}^{9}, \ldots, x_{31}^{9}) &= (y_{28}^{9}, \ldots, y_{31}^{9}) \\
S(x_{16}^{9}, \ldots, x_{19}^{9}) &= (y_{16}^{9}, \ldots, y_{19}^{9}) \\
S(x_{32}^{8}, \ldots, x_{35}^{8}) &= (y_{32}^{8}, \ldots, y_{35}^{8}) \\
S(x_{4}^{2}, \ldots, x_{7}^{2}) &= (y_{4}^{2}, \ldots, y_{7}^{2}) \\
S(x_{4}^{6}, \ldots, x_{7}^{6}) &= (y_{4}^{6}, \ldots, y_{7}^{6})
\end{aligned}
$$

$$
\begin{aligned}
S(x_0^7, \ldots, x_3^7) &= (y_0^7, \ldots, y_3^7) \\
S(x_{12}^7, \ldots, x_{15}^7) &= (y_{12}^7, \ldots, y_{15}^7) \\
S(x_{52}^6, \ldots, x_{55}^6) &= (y_{52}^6, \ldots, y_{55}^6) \\
S(x_8^3, \ldots, x_{11}^3) &= (y_8^3, \ldots, y_{11}^3) \\
S(x_{16}^4, \ldots, x_{19}^4) &= (y_{16}^4, \ldots, y_{19}^4) \\
S(x_{20}^5, \ldots, x_{23}^5) &= (y_{20}^5, \ldots, y_{23}^5) \\
S(x_{16}^8, \ldots, x_{19}^8) &= (y_{16}^8, \ldots, y_{19}^8) \\
S(x_{24}^9, \ldots, x_{27}^9) &= (y_{24}^9, \ldots, y_{27}^9) \\
S(x_4^{10}, \ldots, x_7^{10}) &= (y_4^{10}, \ldots, y_7^{10}) \\
S(x_{16}^1, \ldots, x_{19}^1) &= (y_{16}^1, \ldots, y_{19}^1) \\
S(x_{36}^2, \ldots, x_{39}^2) &= (y_{36}^2, \ldots, y_{39}^2) \\
S(x_8^7, \ldots, x_{11}^7) &= (y_8^7, \ldots, y_{11}^7) \\
S(x_{36}^6, \ldots, x_{39}^6) &= (y_{36}^6, \ldots, y_{39}^6)
\end{aligned}
$$

B.6 Nonlinear Constraints from 12-round GIFT-64 Characteristic [ZDY19]

Nonlinear Constraint $\mathbb{E}_0^5$:

$$
\begin{aligned}
[y_{31}^3] \oplus x_7^4 &= 0 \\
y_5^4 \oplus x_1^5 \oplus k_{109} &= 0 \\
y_3^5 \oplus [x_{51}^6] &= 0 \\
S(x_0^5, \ldots, x_3^5) &= (y_0^5, \ldots, y_3^5) \\
S(x_4^4, \ldots, x_7^4) &= (y_4^4, \ldots, y_7^4)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_1^5$:

$$
\begin{aligned}
y_{12}^1 \oplus x_{16}^2 \oplus k_{91} &= 0 \\
y_6^1 \oplus x_{18}^2 &= 0 \\
y_{13}^1 \oplus x_{33}^2 \oplus k_{71} &= 0 \\
[y_7^1] \oplus x_{35}^2 &= 0 \\
y_4^1 \oplus x_{48}^2 \oplus k_{83} &= 0 \\
y_{14}^1 \oplus x_{50}^2 &= 0 \\
y_{33}^2 \oplus x_{25}^3 \oplus k_{41} &= 0 \\
y_{27}^3 \oplus [x_{23}^4] &= 0 \\
y_{25}^3 \oplus [x_{53}^4] \oplus k_2 &= 0 \\
S(x_{12}^1, \ldots, x_{15}^1) &= (y_{12}^1, \ldots, y_{15}^1) \\
S(x_{32}^2, \ldots, x_{35}^2) &= (y_{32}^2, \ldots, y_{35}^2) \\
S(x_{24}^3, \ldots, x_{27}^3) &= (y_{24}^3, \ldots, y_{27}^3) \\
S(x_{16}^2, \ldots, x_{19}^2) &= (y_{16}^2, \ldots, y_{19}^2) \\
S(x_4^1, \ldots, x_7^1) &= (y_4^1, \ldots, y_7^1) \\
S(x_{48}^2, \ldots, x_{51}^2) &= (y_{48}^2, \ldots, y_{51}^2)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2^5$:

$$
y_{12}^5 \oplus x_{16}^6 \oplus k_{95} = 0
$$

$$
\begin{aligned}
y_6^5 \oplus x_{18}^6 &= 0 \\
y_4^5 \oplus x_{48}^6 \oplus k_{87} &= 0 \\
y_{14}^5 \oplus x_{50}^6 &= 0 \\
S(x_{48}^6, \ldots, x_{51}^6) &= (y_{48}^6, \ldots, y_{51}^6) \\
S(x_4^5, \ldots, x_7^5) &= (y_4^5, \ldots, y_7^5) \\
S(x_{12}^5, \ldots, x_{15}^5) &= (y_{12}^5, \ldots, y_{15}^5) \\
S(x_{16}^6, \ldots, x_{19}^6) &= (y_{16}^6, \ldots, y_{19}^6)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_3^5$:

$$
\begin{aligned}
y_{28}^3 \oplus x_{20}^4 \oplus k_{26} &= 0 \\
y_{22}^3 \oplus x_{22}^4 &= 0 \\
y_{20}^3 \oplus x_{52}^4 \oplus k_{18} &= 0 \\
y_{30}^3 \oplus x_{54}^4 &= 0 \\
S(x_{28}^3, \ldots, x_{31}^3) &= (y_{28}^3, \ldots, y_{31}^3) \\
S(x_{20}^4, \ldots, x_{23}^4) &= (y_{20}^4, \ldots, y_{23}^4) \\
S(x_{20}^3, \ldots, x_{23}^3) &= (y_{20}^3, \ldots, y_{23}^3) \\
S(x_{52}^4, \ldots, x_{55}^4) &= (y_{52}^4, \ldots, y_{55}^4)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_4^5$:

$$
\begin{aligned}
y_{28}^7 \oplus x_{20}^8 \oplus k_{30} &= 0 \\
y_{22}^7 \oplus x_{22}^8 &= 0 \\
y_{20}^7 \oplus x_{52}^8 \oplus k_{22} &= 0 \\
y_{30}^7 \oplus x_{54}^8 &= 0 \\
S(x_{28}^7, \ldots, x_{31}^7) &= (y_{28}^7, \ldots, y_{31}^7) \\
S(x_{20}^8, \ldots, x_{23}^8) &= (y_{20}^8, \ldots, y_{23}^8) \\
S(x_{52}^8, \ldots, x_{55}^8) &= (y_{52}^8, \ldots, y_{55}^8) \\
S(x_{20}^7, \ldots, x_{23}^7) &= (y_{20}^7, \ldots, y_{23}^7)
\end{aligned}
$$

B.7 New Nonlinear Constraints from 13-round GIFT-64 Characteristic [LWZZ19]

Nonlinear Constraint $\mathbb{E}_0^6$:

$$
\begin{aligned}
y_{16}^1 \oplus x_4^2 \oplus k_{94} &= 0 \\
y_{26}^1 \oplus x_6^2 &= 0 \\
y_{24}^1 \oplus x_{36}^2 \oplus k_{86} &= 0 \\
y_{18}^1 \oplus x_{38}^2 &= 0 \\
y_5^2 \oplus x_1^3 \oplus k_{47} &= 0 \\
y_{37}^2 \oplus x_9^3 \oplus k_{45} &= 0 \\
y_0^3 \oplus x_0^4 \oplus k_{31} &= 0 \\
y_{10}^3 \oplus x_2^4 &= 0 \\
y_1^3 \oplus x_{17}^4 \oplus k_{11} &= 0
\end{aligned}
$$

$$
\begin{aligned}
[y_{11}^3] \oplus x_{19}^4 &= 0 \\
y_8^3 \oplus x_{32}^4 \oplus k_{23} &= 0 \\
y_2^3 \oplus x_{34}^4 &= 0 \\
y_9^3 \oplus x_{49}^4 \oplus k_3 &= 0 \\
[y_3^3] \oplus x_{51}^4 &= 0 \\
y_1^4 \oplus x_{17}^5 \oplus k_{105} &= 0 \\
y_{17}^4 \oplus x_{21}^5 \oplus k_{104} &= 0 \\
y_{33}^4 \oplus x_{25}^5 \oplus k_{103} &= 0 \\
y_{49}^4 \oplus x_{29}^5 \oplus k_{102} &= 0 \\
y_{16}^5 \oplus x_4^6 \oplus k_{82} &= 0 \\
y_{21}^5 \oplus [x_5^6] \oplus k_{76} &= 0 \\
y_{26}^5 \oplus x_6^6 &= 0 \\
y_{31}^5 \oplus [x_7^6] &= 0 \\
y_{17}^5 \oplus x_{21}^6 \oplus k_{72} &= 0 \\
[y_{27}^5] \oplus x_{23}^6 &= 0 \\
y_{24}^5 \oplus x_{36}^6 \oplus k_{90} &= 0 \\
y_{29}^5 \oplus [x_{37}^6] \oplus k_{68} &= 0 \\
y_{18}^5 \oplus x_{38}^6 &= 0 \\
y_{23}^5 \oplus [x_{39}^6] &= 0 \\
y_{25}^5 \oplus x_{53}^6 \oplus k_{64} &= 0 \\
[y_{19}^5] \oplus x_{55}^6 &= 0 \\
y_5^6 \oplus x_1^7 \oplus k_{45} &= 0 \\
y_{21}^6 \oplus x_5^7 \oplus k_{44} &= 0 \\
y_{37}^6 \oplus x_9^7 \oplus k_{43} &= 0 \\
y_{53}^6 \oplus x_{13}^7 \oplus k_{42} &= 0 \\
y_0^7 \oplus x_0^8 \oplus k_{19} &= 0 \\
y_5^7 \oplus [x_1^8] \oplus k_{13} &= 0 \\
y_{10}^7 \oplus x_2^8 &= 0 \\
y_{15}^7 \oplus [x_3^8] &= 0 \\
y_1^7 \oplus x_{17}^8 \oplus k_9 &= 0 \\
[y_{11}^7] \oplus x_{19}^8 &= 0 \\
y_8^7 \oplus x_{32}^8 \oplus k_{27} &= 0 \\
y_{13}^7 \oplus [x_{33}^8] \oplus k_5 &= 0 \\
y_2^7 \oplus x_{34}^8 &= 0 \\
y_7^7 \oplus [x_{35}^8] &= 0 \\
y_9^7 \oplus x_{49}^8 \oplus k_1 &= 0 \\
[y_3^7] \oplus x_{51}^8 &= 0 \\
y_{17}^8 \oplus x_{21}^9 \oplus k_{102} &= 0 \\
y_{49}^8 \oplus x_{29}^9 \oplus k_{100} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{16}^{9} \oplus x_{4}^{10} \oplus k_{86} &= 0 \\
y_{21}^{9} \oplus [x_{5}^{10}] \oplus k_{74} &= 0 \\
y_{26}^{9} \oplus x_{6}^{10} &= 0 \\
y_{31}^{9} \oplus [x_{7}^{10}] &= 0 \\
y_{24}^{9} \oplus x_{36}^{10} \oplus k_{94} &= 0 \\
y_{29}^{9} \oplus [x_{37}^{10}] \oplus k_{66} &= 0 \\
y_{18}^{9} \oplus x_{38}^{10} &= 0 \\
y_{23}^{9} \oplus [x_{39}^{10}] &= 0 \\
y_{0}^{11} \oplus x_{0}^{12} \oplus k_{23} &= 0 \\
y_{10}^{11} \oplus x_{2}^{12} &= 0 \\
y_{8}^{11} \oplus x_{32}^{12} \oplus k_{31} &= 0 \\
y_{2}^{11} \oplus x_{34}^{12} &= 0 \\
S(x_{0}^{4}, \ldots, x_{3}^{4}) &= (y_{0}^{4}, \ldots, y_{3}^{4}) \\
S(x_{16}^{5}, \ldots, x_{19}^{5}) &= (y_{16}^{5}, \ldots, y_{19}^{5}) \\
S(x_{48}^{4}, \ldots, x_{51}^{4}) &= (y_{48}^{4}, \ldots, y_{51}^{4}) \\
S(x_{0}^{8}, \ldots, x_{3}^{8}) &= (y_{0}^{8}, \ldots, y_{3}^{8}) \\
S(x_{28}^{5}, \ldots, x_{31}^{5}) &= (y_{28}^{5}, \ldots, y_{31}^{5}) \\
S(x_{20}^{9}, \ldots, x_{23}^{9}) &= (y_{20}^{9}, \ldots, y_{23}^{9}) \\
S(x_{8}^{11}, \ldots, x_{11}^{11}) &= (y_{8}^{11}, \ldots, y_{11}^{11}) \\
S(x_{48}^{8}, \ldots, x_{51}^{8}) &= (y_{48}^{8}, \ldots, y_{51}^{8}) \\
S(x_{36}^{10}, \ldots, x_{39}^{10}) &= (y_{36}^{10}, \ldots, y_{39}^{10}) \\
S(x_{24}^{1}, \ldots, x_{27}^{1}) &= (y_{24}^{1}, \ldots, y_{27}^{1}) \\
S(x_{4}^{7}, \ldots, x_{7}^{7}) &= (y_{4}^{7}, \ldots, y_{7}^{7}) \\
S(x_{20}^{6}, \ldots, x_{23}^{6}) &= (y_{20}^{6}, \ldots, y_{23}^{6}) \\
S(x_{0}^{12}, \ldots, x_{3}^{12}) &= (y_{0}^{12}, \ldots, y_{3}^{12}) \\
S(x_{0}^{3}, \ldots, x_{3}^{3}) &= (y_{0}^{3}, \ldots, y_{3}^{3}) \\
S(x_{24}^{5}, \ldots, x_{27}^{5}) &= (y_{24}^{5}, \ldots, y_{27}^{5}) \\
S(x_{32}^{4}, \ldots, x_{35}^{4}) &= (y_{32}^{4}, \ldots, y_{35}^{4}) \\
S(x_{28}^{9}, \ldots, x_{31}^{9}) &= (y_{28}^{9}, \ldots, y_{31}^{9}) \\
S(x_{16}^{9}, \ldots, x_{19}^{9}) &= (y_{16}^{9}, \ldots, y_{19}^{9}) \\
S(x_{32}^{8}, \ldots, x_{35}^{8}) &= (y_{32}^{8}, \ldots, y_{35}^{8}) \\
S(x_{4}^{2}, \ldots, x_{7}^{2}) &= (y_{4}^{2}, \ldots, y_{7}^{2}) \\
S(x_{4}^{6}, \ldots, x_{7}^{6}) &= (y_{4}^{6}, \ldots, y_{7}^{6}) \\
S(x_{0}^{7}, \ldots, x_{3}^{7}) &= (y_{0}^{7}, \ldots, y_{3}^{7}) \\
S(x_{12}^{7}, \ldots, x_{15}^{7}) &= (y_{12}^{7}, \ldots, y_{15}^{7}) \\
S(x_{52}^{6}, \ldots, x_{55}^{6}) &= (y_{52}^{6}, \ldots, y_{55}^{6}) \\
S(x_{8}^{3}, \ldots, x_{11}^{3}) &= (y_{8}^{3}, \ldots, y_{11}^{3}) \\
S(x_{32}^{12}, \ldots, x_{35}^{12}) &= (y_{32}^{12}, \ldots, y_{35}^{12}) \\
S(x_{16}^{4}, \ldots, x_{19}^{4}) &= (y_{16}^{4}, \ldots, y_{19}^{4})
\end{aligned}
$$

$$
\begin{aligned}
S(x_{20}^5, \ldots, x_{23}^5) &= (y_{20}^5, \ldots, y_{23}^5) \\
S(x_{16}^8, \ldots, x_{19}^8) &= (y_{16}^8, \ldots, y_{19}^8) \\
S(x_{0}^{11}, \ldots, x_{3}^{11}) &= (y_{0}^{11}, \ldots, y_{3}^{11}) \\
S(x_{24}^9, \ldots, x_{27}^9) &= (y_{24}^9, \ldots, y_{27}^9) \\
S(x_{4}^{10}, \ldots, x_{7}^{10}) &= (y_{4}^{10}, \ldots, y_{7}^{10}) \\
S(x_{16}^1, \ldots, x_{19}^1) &= (y_{16}^1, \ldots, y_{19}^1) \\
S(x_{36}^2, \ldots, x_{39}^2) &= (y_{36}^2, \ldots, y_{39}^2) \\
S(x_{8}^7, \ldots, x_{11}^7) &= (y_{8}^7, \ldots, y_{11}^7) \\
S(x_{36}^6, \ldots, x_{39}^6) &= (y_{36}^6, \ldots, y_{39}^6)
\end{aligned}
$$

B.8 Constraints from 18-round GIFT-64 Characteristic in [SWW21a]

Nonlinear Constraint $\mathbb{E}_0^7$:

$$
\begin{aligned}
y_{12}^5 \oplus x_{16}^6 \oplus k_{32} &= 0 \\
y_{6}^5 \oplus x_{18}^6 &= 0 \\
y_{4}^5 \oplus x_{48}^6 \oplus k_{40} &= 0 \\
y_{14}^5 \oplus x_{50}^6 &= 0 \\
y_{17}^6 \oplus x_{21}^7 \oplus k_{87} &= 0 \\
y_{49}^6 \oplus x_{29}^7 \oplus k_{89} &= 0 \\
y_{21}^7 \oplus x_{5}^8 \oplus k_{115} &= 0 \\
y_{22}^7 \oplus x_{22}^8 &= 0 \\
y_{29}^7 \oplus x_{37}^8 \oplus k_{123} &= 0 \\
y_{4}^8 \oplus x_{48}^9 \oplus k_{4} &= 0 \\
y_{20}^8 \oplus x_{52}^9 \oplus k_{5} &= 0 \\
y_{36}^8 \oplus x_{56}^9 \oplus k_{6} &= 0 \\
y_{60}^9 \oplus x_{28}^{10} \oplus k_{47} &= 0 \\
y_{54}^9 \oplus x_{30}^{10} &= 0 \\
y_{59}^9 \oplus x_{31}^{10} &= 0 \\
y_{52}^9 \oplus x_{60}^{10} \oplus k_{39} &= 0 \\
y_{62}^9 \oplus x_{62}^{10} &= 0 \\
y_{51}^9 \oplus x_{63}^{10} &= 0 \\
S(x_{48}^6, \ldots, x_{51}^6) &= (y_{48}^6, \ldots, y_{51}^6) \\
S(x_{4}^5, \ldots, x_{7}^5) &= (y_{4}^5, \ldots, y_{7}^5) \\
S(x_{36}^8, \ldots, x_{39}^8) &= (y_{36}^8, \ldots, y_{39}^8) \\
S(x_{56}^9, \ldots, x_{59}^9) &= (y_{56}^9, \ldots, y_{59}^9) \\
S(x_{60}^{10}, \ldots, x_{63}^{10}) &= (y_{60}^{10}, \ldots, y_{63}^{10}) \\
S(x_{28}^7, \ldots, x_{31}^7) &= (y_{28}^7, \ldots, y_{31}^7) \\
S(x_{12}^5, \ldots, x_{15}^5) &= (y_{12}^5, \ldots, y_{15}^5) \\
S(x_{20}^8, \ldots, x_{23}^8) &= (y_{20}^8, \ldots, y_{23}^8) \\
S(x_{52}^9, \ldots, x_{55}^9) &= (y_{52}^9, \ldots, y_{55}^9)
\end{aligned}
$$

$$
\begin{aligned}
S(x_{16}^{6},\ldots,x_{19}^{6}) &= (y_{16}^{6},\ldots,y_{19}^{6})\\
S(x_{4}^{8},\ldots,x_{7}^{8}) &= (y_{4}^{8},\ldots,y_{7}^{8})\\
S(x_{48}^{9},\ldots,x_{51}^{9}) &= (y_{48}^{9},\ldots,y_{51}^{9})\\
S(x_{28}^{10},\ldots,x_{31}^{10}) &= (y_{28}^{10},\ldots,y_{31}^{10})\\
S(x_{60}^{9},\ldots,x_{63}^{9}) &= (y_{60}^{9},\ldots,y_{63}^{9})\\
S(x_{20}^{7},\ldots,x_{23}^{7}) &= (y_{20}^{7},\ldots,y_{23}^{7})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_1^7$:

$$
\begin{aligned}
y_{44}^{11} \oplus x_{24}^{12} \oplus k_{110} &= 0\\
y_{38}^{11} \oplus x_{26}^{12} &= 0\\
y_{36}^{11} \oplus x_{56}^{12} \oplus k_{102} &= 0\\
y_{46}^{11} \oplus x_{58}^{12} &= 0\\
S(x_{44}^{11},\ldots,x_{47}^{11}) &= (y_{44}^{11},\ldots,y_{47}^{11})\\
S(x_{24}^{12},\ldots,x_{27}^{12}) &= (y_{24}^{12},\ldots,y_{27}^{12})\\
S(x_{56}^{12},\ldots,x_{59}^{12}) &= (y_{56}^{12},\ldots,y_{59}^{12})\\
S(x_{36}^{11},\ldots,x_{39}^{11}) &= (y_{36}^{11},\ldots,y_{39}^{11})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2^7$:

$$
\begin{aligned}
[y_{48}^{9}] \oplus x_{12}^{10} \oplus k_{43} &= 0\\
[y_{53}^{9}] \oplus x_{13}^{10} \oplus k_{55} &= 0\\
[y_{58}^{9}] \oplus x_{14}^{10} &= 0\\
[y_{63}^{9}] \oplus x_{15}^{10} &= 0\\
y_{13}^{10} \oplus x_{33}^{11} \oplus k_{92} &= 0\\
y_{33}^{11} \oplus [x_{25}^{12}] \oplus k_{122} &= 0\\
y_{35}^{11} \oplus [x_{59}^{12}] &= 0\\
S(x_{12}^{10},\ldots,x_{15}^{10}) &= (y_{12}^{10},\ldots,y_{15}^{10})\\
S(x_{32}^{11},\ldots,x_{35}^{11}) &= (y_{32}^{11},\ldots,y_{35}^{11})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_3^7$:

$$
\begin{aligned}
[y_{56}^{9}] \oplus x_{44}^{10} \oplus k_{35} &= 0\\
[y_{50}^{9}] \oplus x_{46}^{10} &= 0\\
[y_{55}^{9}] \oplus x_{47}^{10} &= 0\\
y_{45}^{10} \oplus x_{41}^{11} \oplus k_{94} &= 0\\
y_{43}^{11} \oplus [x_{27}^{12}] &= 0\\
y_{41}^{11} \oplus [x_{57}^{12}] \oplus k_{114} &= 0\\
S(x_{44}^{10},\ldots,x_{47}^{10}) &= (y_{44}^{10},\ldots,y_{47}^{10})\\
S(x_{40}^{11},\ldots,x_{43}^{11}) &= (y_{40}^{11},\ldots,y_{43}^{11})
\end{aligned}
$$

Linear Constraints:

$$
\begin{aligned}
[y_{28}^{7}] \oplus [x_{20}^{8}] \oplus k_{97} &= 0\\
[y_{49}^{9}] \oplus [x_{29}^{10}] \oplus k_{59} &= 0\\
[y_{57}^{9}] \oplus [x_{61}^{10}] \oplus k_{51} &= 0
\end{aligned}
$$

B.9 Nonlinear Constraints for Second 20-round GIFT-128 Characteristic from [JZZD21]

Nonlinear Constraint $\mathbb{E}_0^8$:

$$\begin{aligned}
y_{112}^9 \oplus x_{28}^{10} &= 0\\
y_{122}^9 \oplus x_{30}^{10} \oplus k_{16} &= 0\\
y_{120}^9 \oplus x_{92}^{10} &= 0\\
y_{114}^9 \oplus x_{94}^{10} \oplus k_4 &= 0\\
S(x_{92}^{10}, \ldots, x_{95}^{10}) &= (y_{92}^{10}, \ldots, y_{95}^{10})\\
S(x_{112}^{9}, \ldots, x_{115}^{9}) &= (y_{112}^{9}, \ldots, y_{115}^{9})\\
S(x_{28}^{10}, \ldots, x_{31}^{10}) &= (y_{28}^{10}, \ldots, y_{31}^{10})\\
S(x_{120}^{9}, \ldots, x_{123}^{9}) &= (y_{120}^{9}, \ldots, y_{123}^{9})
\end{aligned}$$

Nonlinear Constraint $\mathbb{E}_1^8$:

$$\begin{aligned}
y_{92}^{14} \oplus x_{52}^{15} &= 0\\
y_{86}^{14} \oplus x_{54}^{15} \oplus k_{114} &= 0\\
y_{84}^{14} \oplus x_{116}^{15} &= 0\\
y_{94}^{14} \oplus x_{118}^{15} \oplus k_{106} &= 0\\
S(x_{116}^{15}, \ldots, x_{119}^{15}) &= (y_{116}^{15}, \ldots, y_{119}^{15})\\
S(x_{84}^{14}, \ldots, x_{87}^{14}) &= (y_{84}^{14}, \ldots, y_{87}^{14})\\
S(x_{52}^{15}, \ldots, x_{55}^{15}) &= (y_{52}^{15}, \ldots, y_{55}^{15})\\
S(x_{92}^{14}, \ldots, x_{95}^{14}) &= (y_{92}^{14}, \ldots, y_{95}^{14})
\end{aligned}$$

Linear Constraint $\mathbb{E}_2^8$:

$$[y_{100}^{12}] \oplus [x_{120}^{13}] = 0$$

Nonlinear Constraint $\mathbb{E}_3^8$:

$$\begin{aligned}
y_{120}^2 \oplus x_{92}^3 &= 0\\
y_{121}^2 \oplus x_{125}^3 \oplus k_{32} &= 0\\
y_{93}^3 \oplus x_{85}^4 \oplus k_{10} &= 0\\
y_{125}^3 \oplus x_{93}^4 \oplus k_8 &= 0\\
y_{85}^4 \oplus x_{21}^5 \oplus k_{126} &= 0\\
[y_{95}^4] \oplus x_{23}^5 &= 0\\
y_{92}^4 \oplus x_{52}^5 &= 0\\
y_{86}^4 \oplus x_{54}^5 \oplus k_{54} &= 0\\
y_{93}^4 \oplus x_{85}^5 \oplus k_{104} &= 0\\
[y_{87}^4] \oplus x_{87}^5 &= 0\\
y_{84}^4 \oplus x_{116}^5 &= 0\\
y_{94}^4 \oplus x_{118}^5 \oplus k_{32} &= 0\\
y_{21}^5 \oplus x_5^6 \oplus k_{82} &= 0\\
y_{53}^5 \oplus x_{13}^6 \oplus k_{80} &= 0
\end{aligned}$$

$$
\begin{aligned}
y_{85}^{5} \oplus x_{21}^{6} \oplus k_{94} &= 0 \\
y_{117}^{5} \oplus x_{29}^{6} \oplus k_{92} &= 0 \\
y_{12}^{6} \oplus x_{32}^{7} &= 0 \\
y_{6}^{6} \oplus [x_{34}^{7}] \oplus k_{127} &= 0 \\
y_{28}^{6} \oplus x_{36}^{7} &= 0 \\
y_{22}^{6} \oplus [x_{38}^{7}] \oplus k_{126} &= 0 \\
y_{4}^{6} \oplus x_{96}^{7} &= 0 \\
y_{20}^{6} \oplus x_{100}^{7} &= 0 \\
[y_{34}^{7}] \oplus x_{74}^{8} \oplus k_{73} &= 0 \\
y_{39}^{7} \oplus x_{75}^{8} &= 0 \\
y_{98}^{7} \oplus x_{90}^{8} \oplus k_{69} &= 0 \\
y_{103}^{7} \oplus x_{91}^{8} &= 0 \\
S(x_{4}^{6}, \ldots, x_{7}^{6}) &= (y_{4}^{6}, \ldots, y_{7}^{6}) \\
S(x_{104}^{8}, \ldots, x_{107}^{8}) &= (y_{104}^{8}, \ldots, y_{107}^{8}) \\
S(x_{28}^{6}, \ldots, x_{31}^{6}) &= (y_{28}^{6}, \ldots, y_{31}^{6}) \\
S(x_{96}^{7}, \ldots, x_{99}^{7}) &= (y_{96}^{7}, \ldots, y_{99}^{7}) \\
S(x_{20}^{5}, \ldots, x_{23}^{5}) &= (y_{20}^{5}, \ldots, y_{23}^{5}) \\
S(x_{116}^{14}, \ldots, x_{119}^{14}) &= (y_{116}^{14}, \ldots, y_{119}^{14}) \\
S(x_{88}^{8}, \ldots, x_{91}^{8}) &= (y_{88}^{8}, \ldots, y_{91}^{8}) \\
S(x_{12}^{6}, \ldots, x_{15}^{6}) &= (y_{12}^{6}, \ldots, y_{15}^{6}) \\
S(x_{120}^{2}, \ldots, x_{123}^{2}) &= (y_{120}^{2}, \ldots, y_{123}^{2}) \\
y_{36}^{7} \oplus x_{104}^{8} &= 0 \\
y_{35}^{7} \oplus x_{107}^{8} &= 0 \\
y_{72}^{8} \oplus x_{80}^{9} &= 0 \\
y_{88}^{8} \oplus x_{84}^{9} &= 0 \\
y_{104}^{8} \oplus x_{88}^{9} &= 0 \\
y_{80}^{9} \oplus x_{20}^{10} &= 0 \\
y_{90}^{9} \oplus x_{22}^{10} \oplus k_{18} &= 0 \\
y_{88}^{9} \oplus x_{84}^{10} &= 0 \\
y_{82}^{9} \oplus x_{86}^{10} \oplus k_{6} &= 0 \\
y_{87}^{9} \oplus [x_{87}^{10}] &= 0 \\
y_{124}^{14} \oplus x_{60}^{15} &= 0 \\
y_{118}^{14} \oplus x_{62}^{15} \oplus k_{112} &= 0 \\
y_{116}^{14} \oplus x_{124}^{15} &= 0 \\
y_{126}^{14} \oplus x_{126}^{15} \oplus k_{104} &= 0 \\
S(x_{52}^{5}, \ldots, x_{55}^{5}) &= (y_{52}^{5}, \ldots, y_{55}^{5}) \\
S(x_{84}^{4}, \ldots, x_{87}^{4}) &= (y_{84}^{4}, \ldots, y_{87}^{4}) \\
S(x_{72}^{8}, \ldots, x_{75}^{8}) &= (y_{72}^{8}, \ldots, y_{75}^{8}) \\
S(x_{124}^{14}, \ldots, x_{127}^{14}) &= (y_{124}^{14}, \ldots, y_{127}^{14})
\end{aligned}
$$

$$
\begin{aligned}
S(x_{124}^{3},\ldots,x_{127}^{3}) &= (y_{124}^{3},\ldots,y_{127}^{3})\\
S(x_{80}^{9},\ldots,x_{83}^{9}) &= (y_{80}^{9},\ldots,y_{83}^{9})\\
S(x_{84}^{10},\ldots,x_{87}^{10}) &= (y_{84}^{10},\ldots,y_{87}^{10})\\
S(x_{20}^{6},\ldots,x_{23}^{6}) &= (y_{20}^{6},\ldots,y_{23}^{6})\\
S(x_{100}^{7},\ldots,x_{103}^{7}) &= (y_{100}^{7},\ldots,y_{103}^{7})\\
S(x_{20}^{10},\ldots,x_{23}^{10}) &= (y_{20}^{10},\ldots,y_{23}^{10})\\
S(x_{92}^{4},\ldots,x_{95}^{4}) &= (y_{92}^{4},\ldots,y_{95}^{4})\\
S(x_{84}^{5},\ldots,x_{87}^{5}) &= (y_{84}^{5},\ldots,y_{87}^{5})\\
S(x_{88}^{9},\ldots,x_{91}^{9}) &= (y_{88}^{9},\ldots,y_{91}^{9})\\
S(x_{36}^{7},\ldots,x_{39}^{7}) &= (y_{36}^{7},\ldots,y_{39}^{7})\\
S(x_{60}^{15},\ldots,x_{63}^{15}) &= (y_{60}^{15},\ldots,y_{63}^{15})\\
S(x_{124}^{15},\ldots,x_{127}^{15}) &= (y_{124}^{15},\ldots,y_{127}^{15})\\
S(x_{92}^{3},\ldots,x_{95}^{3}) &= (y_{92}^{3},\ldots,y_{95}^{3})\\
S(x_{84}^{9},\ldots,x_{87}^{9}) &= (y_{84}^{9},\ldots,y_{87}^{9})\\
S(x_{116}^{5},\ldots,x_{119}^{5}) &= (y_{116}^{5},\ldots,y_{119}^{5})\\
S(x_{32}^{7},\ldots,x_{35}^{7}) &= (y_{32}^{7},\ldots,y_{35}^{7})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_4^8$:

$$
\begin{aligned}
[y_{81}^{9}] \oplus x_{53}^{10} \oplus k_{90} &= 0\\
[y_{91}^{9}] \oplus x_{55}^{10} &= 0\\
[y_{89}^{9}] \oplus x_{117}^{10} \oplus k_{78} &= 0\\
[y_{83}^{9}] \oplus x_{119}^{10} &= 0\\
y_{53}^{10} \oplus x_{13}^{11} \oplus k_{52} &= 0\\
y_{117}^{10} \oplus x_{29}^{11} \oplus k_{48} &= 0\\
y_{12}^{11} \oplus x_{32}^{12} &= 0\\
y_{28}^{11} \oplus x_{36}^{12} &= 0\\
y_{14}^{11} \oplus [x_{98}^{12}] \oplus k_{65} &= 0\\
y_{30}^{11} \oplus [x_{102}^{12}] \oplus k_{64} &= 0\\
y_{34}^{12} \oplus x_{74}^{13} \oplus k_{39} &= 0\\
y_{39}^{12} \oplus x_{75}^{13} &= 0\\
y_{72}^{13} \oplus x_{80}^{14} &= 0\\
y_{83}^{14} \oplus [x_{119}^{15}] &= 0\\
S(x_{36}^{12},\ldots,x_{39}^{12}) &= (y_{36}^{12},\ldots,y_{39}^{12})\\
S(x_{28}^{11},\ldots,x_{31}^{11}) &= (y_{28}^{11},\ldots,y_{31}^{11})\\
S(x_{116}^{10},\ldots,x_{119}^{10}) &= (y_{116}^{10},\ldots,y_{119}^{10})\\
S(x_{32}^{12},\ldots,x_{35}^{12}) &= (y_{32}^{12},\ldots,y_{35}^{12})\\
S(x_{80}^{14},\ldots,x_{83}^{14}) &= (y_{80}^{14},\ldots,y_{83}^{14})\\
S(x_{12}^{11},\ldots,x_{15}^{11}) &= (y_{12}^{11},\ldots,y_{15}^{11})\\
S(x_{52}^{10},\ldots,x_{55}^{10}) &= (y_{52}^{10},\ldots,y_{55}^{10})\\
S(x_{72}^{13},\ldots,x_{75}^{13}) &= (y_{72}^{13},\ldots,y_{75}^{13})
\end{aligned}
$$

B.10 Nonlinear Constraints for Third 20-round GIFT-128 Characteristic from [JZZD21]

Nonlinear Constraint $\mathbb{E}_0^9$:

$$
\begin{aligned}
y_{120}^2 \oplus x_{92}^3 &= 0 \\
y_{121}^2 \oplus x_{125}^3 \oplus k_{32} &= 0 \\
y_{93}^3 \oplus x_{85}^4 \oplus k_{10} &= 0 \\
y_{125}^3 \oplus x_{93}^4 \oplus k_8 &= 0 \\
y_{85}^4 \oplus x_{21}^5 \oplus k_{126} &= 0 \\
[y_{95}^4] \oplus x_{23}^5 &= 0 \\
y_{92}^4 \oplus x_{52}^5 &= 0 \\
y_{86}^4 \oplus x_{54}^5 \oplus k_{54} &= 0 \\
y_{93}^4 \oplus x_{85}^5 \oplus k_{104} &= 0 \\
[y_{87}^4] \oplus x_{87}^5 &= 0 \\
y_{84}^4 \oplus x_{116}^5 &= 0 \\
y_{94}^4 \oplus x_{118}^5 \oplus k_{32} &= 0 \\
y_{21}^5 \oplus x_5^6 \oplus k_{82} &= 0 \\
y_{85}^5 \oplus x_{21}^6 \oplus k_{94} &= 0 \\
y_6^6 \oplus [x_{34}^7] \oplus k_{127} &= 0 \\
y_{22}^6 \oplus [x_{38}^7] \oplus k_{126} &= 0 \\
y_4^6 \oplus x_{96}^7 &= 0 \\
y_{20}^6 \oplus x_{100}^7 &= 0 \\
y_{98}^7 \oplus x_{90}^8 \oplus k_{69} &= 0 \\
y_{103}^7 \oplus x_{91}^8 &= 0 \\
y_{88}^8 \oplus x_{84}^9 &= 0 \\
y_{80}^9 \oplus x_{20}^{10} &= 0 \\
y_{90}^9 \oplus x_{22}^{10} \oplus k_{18} &= 0 \\
y_{88}^9 \oplus x_{84}^{10} &= 0 \\
y_{82}^9 \oplus x_{86}^{10} \oplus k_6 &= 0 \\
y_{87}^9 \oplus [x_{87}^{10}] &= 0 \\
y_{21}^{10} \oplus x_5^{11} \oplus k_{54} &= 0 \\
y_{85}^{10} \oplus x_{21}^{11} \oplus k_{50} &= 0 \\
y_4^{11} \oplus x_{96}^{12} &= 0 \\
y_{20}^{11} \oplus x_{100}^{12} &= 0 \\
[y_{98}^{12}] \oplus x_{90}^{13} \oplus k_{35} &= 0 \\
y_{103}^{12} \oplus x_{91}^{13} &= 0 \\
y_{100}^{12} \oplus x_{120}^{13} &= 0 \\
y_{99}^{12} \oplus x_{123}^{13} &= 0 \\
y_{88}^{13} \oplus x_{84}^{14} &= 0 \\
y_{120}^{13} \oplus x_{92}^{14} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{92}^{14} \oplus x_{52}^{15} &= 0 \\
y_{86}^{14} \oplus x_{54}^{15} \oplus k_{114} &= 0 \\
y_{124}^{14} \oplus x_{60}^{15} &= 0 \\
y_{118}^{14} \oplus x_{62}^{15} \oplus k_{112} &= 0 \\
y_{84}^{14} \oplus x_{116}^{15} &= 0 \\
y_{94}^{14} \oplus x_{118}^{15} \oplus k_{106} &= 0 \\
y_{116}^{14} \oplus x_{124}^{15} &= 0 \\
y_{126}^{14} \oplus x_{126}^{15} \oplus k_{104} &= 0 \\
S(x_{120}^{13}, \ldots, x_{123}^{13}) &= (y_{120}^{13}, \ldots, y_{123}^{13}) \\
S(x_{52}^{5}, \ldots, x_{55}^{5}) &= (y_{52}^{5}, \ldots, y_{55}^{5}) \\
S(x_{84}^{4}, \ldots, x_{87}^{4}) &= (y_{84}^{4}, \ldots, y_{87}^{4}) \\
S(x_{100}^{12}, \ldots, x_{103}^{12}) &= (y_{100}^{12}, \ldots, y_{103}^{12}) \\
S(x_{20}^{11}, \ldots, x_{23}^{11}) &= (y_{20}^{11}, \ldots, y_{23}^{11}) \\
S(x_{124}^{14}, \ldots, x_{127}^{14}) &= (y_{124}^{14}, \ldots, y_{127}^{14}) \\
S(x_{124}^{3}, \ldots, x_{127}^{3}) &= (y_{124}^{3}, \ldots, y_{127}^{3}) \\
S(x_{80}^{9}, \ldots, x_{83}^{9}) &= (y_{80}^{9}, \ldots, y_{83}^{9}) \\
S(x_{84}^{10}, \ldots, x_{87}^{10}) &= (y_{84}^{10}, \ldots, y_{87}^{10}) \\
S(x_{20}^{6}, \ldots, x_{23}^{6}) &= (y_{20}^{6}, \ldots, y_{23}^{6}) \\
S(x_{116}^{15}, \ldots, x_{119}^{15}) &= (y_{116}^{15}, \ldots, y_{119}^{15}) \\
S(x_{100}^{7}, \ldots, x_{103}^{7}) &= (y_{100}^{7}, \ldots, y_{103}^{7}) \\
S(x_{96}^{12}, \ldots, x_{99}^{12}) &= (y_{96}^{12}, \ldots, y_{99}^{12}) \\
S(x_{84}^{14}, \ldots, x_{87}^{14}) &= (y_{84}^{14}, \ldots, y_{87}^{14}) \\
S(x_{4}^{11}, \ldots, x_{7}^{11}) &= (y_{4}^{11}, \ldots, y_{7}^{11}) \\
S(x_{20}^{10}, \ldots, x_{23}^{10}) &= (y_{20}^{10}, \ldots, y_{23}^{10}) \\
S(x_{92}^{4}, \ldots, x_{95}^{4}) &= (y_{92}^{4}, \ldots, y_{95}^{4}) \\
S(x_{84}^{5}, \ldots, x_{87}^{5}) &= (y_{84}^{5}, \ldots, y_{87}^{5}) \\
S(x_{4}^{6}, \ldots, x_{7}^{6}) &= (y_{4}^{6}, \ldots, y_{7}^{6}) \\
S(x_{88}^{9}, \ldots, x_{91}^{9}) &= (y_{88}^{9}, \ldots, y_{91}^{9}) \\
S(x_{52}^{15}, \ldots, x_{55}^{15}) &= (y_{52}^{15}, \ldots, y_{55}^{15}) \\
S(x_{88}^{13}, \ldots, x_{91}^{13}) &= (y_{88}^{13}, \ldots, y_{91}^{13}) \\
S(x_{60}^{15}, \ldots, x_{63}^{15}) &= (y_{60}^{15}, \ldots, y_{63}^{15}) \\
S(x_{96}^{7}, \ldots, x_{99}^{7}) &= (y_{96}^{7}, \ldots, y_{99}^{7}) \\
S(x_{124}^{15}, \ldots, x_{127}^{15}) &= (y_{124}^{15}, \ldots, y_{127}^{15}) \\
S(x_{20}^{5}, \ldots, x_{23}^{5}) &= (y_{20}^{5}, \ldots, y_{23}^{5}) \\
S(x_{92}^{14}, \ldots, x_{95}^{14}) &= (y_{92}^{14}, \ldots, y_{95}^{14}) \\
S(x_{92}^{3}, \ldots, x_{95}^{3}) &= (y_{92}^{3}, \ldots, y_{95}^{3}) \\
S(x_{84}^{9}, \ldots, x_{87}^{9}) &= (y_{84}^{9}, \ldots, y_{87}^{9}) \\
S(x_{88}^{8}, \ldots, x_{91}^{8}) &= (y_{88}^{8}, \ldots, y_{91}^{8}) \\
S(x_{116}^{5}, \ldots, x_{119}^{5}) &= (y_{116}^{5}, \ldots, y_{119}^{5})
\end{aligned}
$$

$$S(x^2_{120}, \ldots, x^2_{123}) = (y^2_{120}, \ldots, y^2_{123})$$

Nonlinear Constraint $\mathbb{E}^9_1$:

$$\begin{aligned}
y^9_{112} \oplus x^{10}_{28} &= 0 \\
y^9_{122} \oplus x^{10}_{30} \oplus k_{16} &= 0 \\
y^9_{120} \oplus x^{10}_{92} &= 0 \\
y^9_{114} \oplus x^{10}_{94} \oplus k_4 &= 0 \\
S(x^9_{112}, \ldots, x^9_{115}) &= (y^9_{112}, \ldots, y^9_{115}) \\
S(x^{10}_{92}, \ldots, x^{10}_{95}) &= (y^{10}_{92}, \ldots, y^{10}_{95}) \\
S(x^{10}_{28}, \ldots, x^{10}_{31}) &= (y^{10}_{28}, \ldots, y^{10}_{31}) \\
S(x^9_{120}, \ldots, x^9_{123}) &= (y^9_{120}, \ldots, y^9_{123})
\end{aligned}$$

Nonlinear Constraint $\mathbb{E}^9_2$:

$$\begin{aligned}
[y^9_{81}] \oplus x^{10}_{53} \oplus k_{90} &= 0 \\
[y^9_{91}] \oplus x^{10}_{55} &= 0 \\
[y^9_{89}] \oplus x^{10}_{117} \oplus k_{78} &= 0 \\
[y^9_{83}] \oplus x^{10}_{119} &= 0 \\
y^{10}_{53} \oplus x^{11}_{13} \oplus k_{52} &= 0 \\
y^{10}_{117} \oplus x^{11}_{29} \oplus k_{48} &= 0 \\
y^{11}_{12} \oplus x^{12}_{32} &= 0 \\
y^{11}_{28} \oplus x^{12}_{36} &= 0 \\
y^{11}_{14} \oplus [x^{12}_{98}] \oplus k_{65} &= 0 \\
y^{11}_{30} \oplus [x^{12}_{102}] \oplus k_{64} &= 0 \\
y^{12}_{34} \oplus x^{13}_{74} \oplus k_{39} &= 0 \\
y^{12}_{39} \oplus x^{13}_{75} &= 0 \\
y^{13}_{72} \oplus x^{14}_{80} &= 0 \\
y^{14}_{83} \oplus [x^{15}_{119}] &= 0 \\
S(x^{12}_{36}, \ldots, x^{12}_{39}) &= (y^{12}_{36}, \ldots, y^{12}_{39}) \\
S(x^{11}_{28}, \ldots, x^{11}_{31}) &= (y^{11}_{28}, \ldots, y^{11}_{31}) \\
S(x^{10}_{116}, \ldots, x^{10}_{119}) &= (y^{10}_{116}, \ldots, y^{10}_{119}) \\
S(x^{12}_{32}, \ldots, x^{12}_{35}) &= (y^{12}_{32}, \ldots, y^{12}_{35}) \\
S(x^{14}_{80}, \ldots, x^{14}_{83}) &= (y^{14}_{80}, \ldots, y^{14}_{83}) \\
S(x^{11}_{12}, \ldots, x^{11}_{15}) &= (y^{11}_{12}, \ldots, y^{11}_{15}) \\
S(x^{10}_{52}, \ldots, x^{10}_{55}) &= (y^{10}_{52}, \ldots, y^{10}_{55}) \\
S(x^{14}_{116}, \ldots, x^{14}_{119}) &= (y^{14}_{116}, \ldots, y^{14}_{119}) \\
S(x^{13}_{72}, \ldots, x^{13}_{75}) &= (y^{13}_{72}, \ldots, y^{13}_{75})
\end{aligned}$$

B.11 Nonlinear Constraints for Fourth 20-round GIFT-128 Characteristic from [JZZD21]

Nonlinear Constraint $\mathbb{E}^{10}_0$:

$$y^2_{120} \oplus x^3_{92} = 0$$

$$
\begin{aligned}
y^2_{121} \oplus x^3_{125} \oplus k_{32} &= 0\\
y^3_{93} \oplus x^4_{85} \oplus k_{10} &= 0\\
y^3_{125} \oplus x^4_{93} \oplus k_{8} &= 0\\
y^4_{85} \oplus x^5_{21} \oplus k_{126} &= 0\\
[y^4_{95}] \oplus x^5_{23} &= 0\\
y^4_{92} \oplus x^5_{52} &= 0\\
y^4_{86} \oplus x^5_{54} \oplus k_{54} &= 0\\
y^4_{93} \oplus x^5_{85} \oplus k_{104} &= 0\\
[y^4_{87}] \oplus x^5_{87} &= 0\\
y^4_{84} \oplus x^5_{116} &= 0\\
y^4_{94} \oplus x^5_{118} \oplus k_{32} &= 0\\
y^5_{21} \oplus x^6_{5} \oplus k_{82} &= 0\\
y^5_{53} \oplus x^6_{13} \oplus k_{80} &= 0\\
y^5_{85} \oplus x^6_{21} \oplus k_{94} &= 0\\
y^5_{117} \oplus x^6_{29} \oplus k_{92} &= 0\\
y^6_{12} \oplus x^7_{32} &= 0\\
y^6_{6} \oplus [x^7_{34}] \oplus k_{127} &= 0\\
y^6_{28} \oplus x^7_{36} &= 0\\
y^6_{22} \oplus [x^7_{38}] \oplus k_{126} &= 0\\
y^6_{4} \oplus x^7_{96} &= 0\\
[y^6_{14}] \oplus x^7_{98} \oplus k_{99} &= 0\\
y^6_{20} \oplus x^7_{100} &= 0\\
[y^7_{34}] \oplus x^8_{74} \oplus k_{73} &= 0\\
y^7_{39} \oplus x^8_{75} &= 0\\
y^7_{98} \oplus x^8_{90} \oplus k_{69} &= 0\\
y^7_{103} \oplus x^8_{91} &= 0\\
y^7_{36} \oplus x^8_{104} &= 0\\
y^7_{35} \oplus x^8_{107} &= 0\\
y^8_{72} \oplus x^9_{80} &= 0\\
y^8_{88} \oplus x^9_{84} &= 0\\
y^8_{104} \oplus x^9_{88} &= 0\\
y^9_{80} \oplus x^{10}_{20} &= 0\\
y^9_{90} \oplus x^{10}_{22} \oplus k_{18} &= 0\\
y^9_{88} \oplus x^{10}_{84} &= 0\\
y^9_{82} \oplus x^{10}_{86} \oplus k_{6} &= 0\\
y^9_{87} \oplus [x^{10}_{87}] &= 0\\
y^{10}_{21} \oplus x^{11}_{5} \oplus k_{54} &= 0\\
y^{10}_{85} \oplus x^{11}_{21} \oplus k_{50} &= 0\\
y^{11}_{4} \oplus x^{12}_{96} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{20}^{11} \oplus x_{100}^{12} &= 0 \\
[y_{98}^{12}] \oplus x_{90}^{13} \oplus k_{35} &= 0 \\
y_{103}^{12} \oplus x_{91}^{13} &= 0 \\
y_{100}^{12} \oplus x_{120}^{13} &= 0 \\
y_{99}^{12} \oplus x_{123}^{13} &= 0 \\
y_{88}^{13} \oplus x_{84}^{14} &= 0 \\
y_{120}^{13} \oplus x_{92}^{14} &= 0 \\
y_{92}^{14} \oplus x_{52}^{15} &= 0 \\
y_{86}^{14} \oplus x_{54}^{15} \oplus k_{114} &= 0 \\
y_{124}^{14} \oplus x_{60}^{15} &= 0 \\
y_{118}^{14} \oplus x_{62}^{15} \oplus k_{112} &= 0 \\
y_{84}^{14} \oplus x_{116}^{15} &= 0 \\
y_{94}^{14} \oplus x_{118}^{15} \oplus k_{106} &= 0 \\
y_{116}^{14} \oplus x_{124}^{15} &= 0 \\
y_{126}^{14} \oplus x_{126}^{15} \oplus k_{104} &= 0 \\
S(x_{120}^{13}, \ldots, x_{123}^{13}) &= (y_{120}^{13}, \ldots, y_{123}^{13}) \\
S(x_{52}^{5}, \ldots, x_{55}^{5}) &= (y_{52}^{5}, \ldots, y_{55}^{5}) \\
S(x_{84}^{4}, \ldots, x_{87}^{4}) &= (y_{84}^{4}, \ldots, y_{87}^{4}) \\
S(x_{100}^{12}, \ldots, x_{103}^{12}) &= (y_{100}^{12}, \ldots, y_{103}^{12}) \\
S(x_{20}^{11}, \ldots, x_{23}^{11}) &= (y_{20}^{11}, \ldots, y_{23}^{11}) \\
S(x_{72}^{8}, \ldots, x_{75}^{8}) &= (y_{72}^{8}, \ldots, y_{75}^{8}) \\
S(x_{124}^{14}, \ldots, x_{127}^{14}) &= (y_{124}^{14}, \ldots, y_{127}^{14}) \\
S(x_{124}^{3}, \ldots, x_{127}^{3}) &= (y_{124}^{3}, \ldots, y_{127}^{3}) \\
S(x_{80}^{9}, \ldots, x_{83}^{9}) &= (y_{80}^{9}, \ldots, y_{83}^{9}) \\
S(x_{84}^{10}, \ldots, x_{87}^{10}) &= (y_{84}^{10}, \ldots, y_{87}^{10}) \\
S(x_{20}^{6}, \ldots, x_{23}^{6}) &= (y_{20}^{6}, \ldots, y_{23}^{6}) \\
S(x_{116}^{15}, \ldots, x_{119}^{15}) &= (y_{116}^{15}, \ldots, y_{119}^{15}) \\
S(x_{100}^{7}, \ldots, x_{103}^{7}) &= (y_{100}^{7}, \ldots, y_{103}^{7}) \\
S(x_{96}^{12}, \ldots, x_{99}^{12}) &= (y_{96}^{12}, \ldots, y_{99}^{12}) \\
S(x_{84}^{14}, \ldots, x_{87}^{14}) &= (y_{84}^{14}, \ldots, y_{87}^{14}) \\
S(x_{4}^{11}, \ldots, x_{7}^{11}) &= (y_{4}^{11}, \ldots, y_{7}^{11}) \\
S(x_{20}^{10}, \ldots, x_{23}^{10}) &= (y_{20}^{10}, \ldots, y_{23}^{10}) \\
S(x_{92}^{4}, \ldots, x_{95}^{4}) &= (y_{92}^{4}, \ldots, y_{95}^{4}) \\
S(x_{84}^{5}, \ldots, x_{87}^{5}) &= (y_{84}^{5}, \ldots, y_{87}^{5}) \\
S(x_{4}^{6}, \ldots, x_{7}^{6}) &= (y_{4}^{6}, \ldots, y_{7}^{6}) \\
S(x_{88}^{9}, \ldots, x_{91}^{9}) &= (y_{88}^{9}, \ldots, y_{91}^{9}) \\
S(x_{104}^{8}, \ldots, x_{107}^{8}) &= (y_{104}^{8}, \ldots, y_{107}^{8}) \\
S(x_{52}^{15}, \ldots, x_{55}^{15}) &= (y_{52}^{15}, \ldots, y_{55}^{15}) \\
S(x_{36}^{7}, \ldots, x_{39}^{7}) &= (y_{36}^{7}, \ldots, y_{39}^{7})
\end{aligned}
$$

$$
\begin{aligned}
S(x_{28}^{6},\ldots,x_{31}^{6}) &= (y_{28}^{6},\ldots,y_{31}^{6})\\
S(x_{88}^{13},\ldots,x_{91}^{13}) &= (y_{88}^{13},\ldots,y_{91}^{13})\\
S(x_{60}^{15},\ldots,x_{63}^{15}) &= (y_{60}^{15},\ldots,y_{63}^{15})\\
S(x_{96}^{7},\ldots,x_{99}^{7}) &= (y_{96}^{7},\ldots,y_{99}^{7})\\
S(x_{124}^{15},\ldots,x_{127}^{15}) &= (y_{124}^{15},\ldots,y_{127}^{15})\\
S(x_{20}^{5},\ldots,x_{23}^{5}) &= (y_{20}^{5},\ldots,y_{23}^{5})\\
S(x_{92}^{14},\ldots,x_{95}^{14}) &= (y_{92}^{14},\ldots,y_{95}^{14})\\
S(x_{92}^{3},\ldots,x_{95}^{3}) &= (y_{92}^{3},\ldots,y_{95}^{3})\\
S(x_{116}^{14},\ldots,x_{119}^{14}) &= (y_{116}^{14},\ldots,y_{119}^{14})\\
S(x_{84}^{9},\ldots,x_{87}^{9}) &= (y_{84}^{9},\ldots,y_{87}^{9})\\
S(x_{88}^{8},\ldots,x_{91}^{8}) &= (y_{88}^{8},\ldots,y_{91}^{8})\\
S(x_{116}^{5},\ldots,x_{119}^{5}) &= (y_{116}^{5},\ldots,y_{119}^{5})\\
S(x_{12}^{6},\ldots,x_{15}^{6}) &= (y_{12}^{6},\ldots,y_{15}^{6})\\
S(x_{32}^{7},\ldots,x_{35}^{7}) &= (y_{32}^{7},\ldots,y_{35}^{7})\\
S(x_{120}^{2},\ldots,x_{123}^{2}) &= (y_{120}^{2},\ldots,y_{123}^{2})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_1^{10}$:

$$
\begin{aligned}
y_{112}^{9} \oplus x_{28}^{10} &= 0\\
y_{122}^{9} \oplus x_{30}^{10} \oplus k_{16} &= 0\\
y_{120}^{9} \oplus x_{92}^{10} &= 0\\
y_{114}^{9} \oplus x_{94}^{10} \oplus k_{4} &= 0\\
S(x_{92}^{10},\ldots,x_{95}^{10}) &= (y_{92}^{10},\ldots,y_{95}^{10})\\
S(x_{112}^{9},\ldots,x_{115}^{9}) &= (y_{112}^{9},\ldots,y_{115}^{9})\\
S(x_{28}^{10},\ldots,x_{31}^{10}) &= (y_{28}^{10},\ldots,y_{31}^{10})\\
S(x_{120}^{9},\ldots,x_{123}^{9}) &= (y_{120}^{9},\ldots,y_{123}^{9})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2^{10}$:

$$
\begin{aligned}
[y_{81}^{9}] \oplus x_{53}^{10} \oplus k_{90} &= 0\\
[y_{91}^{9}] \oplus x_{55}^{10} &= 0\\
[y_{89}^{9}] \oplus x_{117}^{10} \oplus k_{78} &= 0\\
[y_{83}^{9}] \oplus x_{119}^{10} &= 0\\
y_{53}^{10} \oplus x_{13}^{11} \oplus k_{52} &= 0\\
y_{117}^{10} \oplus x_{29}^{11} \oplus k_{48} &= 0\\
y_{12}^{11} \oplus x_{32}^{12} &= 0\\
[y_{6}^{11}] \oplus x_{34}^{12} \oplus k_{83} &= 0\\
y_{28}^{11} \oplus x_{36}^{12} &= 0\\
y_{14}^{11} \oplus [x_{98}^{12}] \oplus k_{65} &= 0\\
y_{30}^{11} \oplus [x_{102}^{12}] \oplus k_{64} &= 0\\
y_{34}^{12} \oplus x_{74}^{13} \oplus k_{39} &= 0\\
y_{39}^{12} \oplus x_{75}^{13} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y_{72}^{13} \oplus x_{80}^{14} &= 0 \\
y_{83}^{14} \oplus [x_{119}^{15}] &= 0 \\
S(x_{36}^{12}, \ldots, x_{39}^{12}) &= (y_{36}^{12}, \ldots, y_{39}^{12}) \\
S(x_{28}^{11}, \ldots, x_{31}^{11}) &= (y_{28}^{11}, \ldots, y_{31}^{11}) \\
S(x_{116}^{10}, \ldots, x_{119}^{10}) &= (y_{116}^{10}, \ldots, y_{119}^{10}) \\
S(x_{32}^{12}, \ldots, x_{35}^{12}) &= (y_{32}^{12}, \ldots, y_{35}^{12}) \\
S(x_{80}^{14}, \ldots, x_{83}^{14}) &= (y_{80}^{14}, \ldots, y_{83}^{14}) \\
S(x_{12}^{11}, \ldots, x_{15}^{11}) &= (y_{12}^{11}, \ldots, y_{15}^{11}) \\
S(x_{52}^{10}, \ldots, x_{55}^{10}) &= (y_{52}^{10}, \ldots, y_{55}^{10}) \\
S(x_{72}^{13}, \ldots, x_{75}^{13}) &= (y_{72}^{13}, \ldots, y_{75}^{13})
\end{aligned}
$$

C Identified Bit-wise Constraints for SKINNY-128 Characteristic

C.1 Linear Constraints from 13-round SKINNY-128-128 Characteristic

The following bit-wise constraints render the trail infeasible:

$$
\begin{aligned}
[y_{19}^{5}] + [y_{67}^{5}] + [y_{123}^{5}] + [x_{19}^{6}] + k_{123} &= 0 \\
[y_{19}^{5}] + [x_{51}^{6}] + k_{123} &= 0
\end{aligned}
$$

which causes the value conflict on the master key k_{123}.

C.2 Nonlinear Constraints from 14-round SKINNY-128-128 Characteristic

Nonlinear Constraint $\mathbb{E}_0^{S1}$:

$$
\begin{aligned}
[y_{17}^{3}] \oplus [x_{49}^{4}] \oplus k_{73} &= 0 \\
[y_{57}^{3}] \oplus [y_{81}^{3}] \oplus x_{65}^{4} \oplus k_{105} &= 0 \\
[y_{63}^{3}] \oplus [y_{87}^{3}] \oplus x_{71}^{4} \oplus k_{111} &= 0 \\
[y_{7}^{4}] \oplus x_{39}^{5} \oplus k_{63} &= 0 \\
[y_{19}^{4}] \oplus [x_{51}^{5}] \oplus k_{11} &= 0 \\
[y_{19}^{4}] \oplus y_{67}^{4} \oplus [x_{115}^{5}] \oplus k_{11} &= 0 \\
[y_{23}^{4}] \oplus y_{71}^{4} \oplus x_{119}^{5} \oplus k_{15} &= 0 \\
y_{11}^{5} \oplus [y_{91}^{5}] \oplus y_{115}^{5} \oplus [x_{11}^{6}] \oplus k_{107} &= 0 \\
[y_{15}^{5}] \oplus [y_{95}^{5}] \oplus [y_{119}^{5}] \oplus x_{15}^{6} \oplus k_{111} &= 0 \\
y_{11}^{5} \oplus [x_{43}^{6}] \oplus k_{107} &= 0 \\
[y_{12}^{5}] \oplus x_{44}^{6} \oplus k_{108} &= 0 \\
y_{13}^{5} \oplus x_{45}^{6} \oplus k_{109} &= 0 \\
[y_{15}^{5}] \oplus x_{47}^{6} \oplus k_{111} &= 0 \\
y_{35}^{5} \oplus [y_{91}^{5}] \oplus [x_{75}^{6}] \oplus k_{75} &= 0 \\
y_{9}^{6} \oplus [x_{41}^{7}] \oplus k_{41} &= 0 \\
y_{11}^{6} \oplus [x_{43}^{7}] \oplus k_{43} &= 0
\end{aligned}
$$

$$
\begin{aligned}
y^4_{65} \oplus [x^5_{49}] \oplus [x^5_{113}] &= 0\\
y^5_{13} \oplus y^5_{37} \oplus y^5_{117} \oplus x^6_{13} \oplus x^6_{77} \oplus k_{77} \oplus k_{109} &= 0\\
y^5_{33} \oplus y^5_{113} \oplus [x^6_{9}] \oplus [x^6_{41}] \oplus [x^6_{73}] \oplus k_{73} &= 0\\
S(x^6_{40}, \ldots, x^6_{47}) &= (y^6_{40}, \ldots, y^6_{47})\\
S(x^6_{8}, \ldots, x^6_{15}) &= (y^6_{8}, \ldots, y^6_{15})\\
S(x^5_{32}, \ldots, x^5_{39}) &= (y^5_{32}, \ldots, y^5_{39})\\
S(x^5_{112}, \ldots, x^5_{119}) &= (y^5_{112}, \ldots, y^5_{119})\\
S(x^5_{8}, \ldots, x^5_{15}) &= (y^5_{8}, \ldots, y^5_{15})\\
S(x^4_{64}, \ldots, x^4_{71}) &= (y^4_{64}, \ldots, y^4_{71})\\
S(x^6_{72}, \ldots, x^6_{79}) &= (y^6_{72}, \ldots, y^6_{79})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_1^{S1}$:

$$
\begin{aligned}
[y^2_{29}] \oplus x^3_{61} \oplus k_{45} &= 0\\
[y^2_{31}] \oplus [x^3_{63}] \oplus k_{47} &= 0\\
[y^2_{29}] \oplus [y^2_{77}] \oplus x^3_{125} \oplus k_{45} &= 0\\
[y^2_{31}] \oplus [y^2_{79}] \oplus x^3_{127} \oplus k_{47} &= 0\\
y^3_{121} \oplus [x^4_{17}] \oplus [x^4_{113}] &= 0\\
S(x^3_{56}, \ldots, x^3_{63}) &= (y^3_{56}, \ldots, y^3_{63})\\
S(x^3_{120}, \ldots, x^3_{127}) &= (y^3_{120}, \ldots, y^3_{127})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2^{S1}$:

$$
\begin{aligned}
y^5_{19} \oplus [x^6_{51}] \oplus k_{123} &= 0\\
[y^5_{20}] \oplus x^6_{52} \oplus k_{124} &= 0\\
y^5_{21} \oplus x^6_{53} \oplus k_{125} &= 0\\
[y^5_{23}] \oplus x^6_{55} \oplus k_{127} &= 0\\
S(x^6_{48}, \ldots, x^6_{55}) &= (y^6_{48}, \ldots, y^6_{55})\\
S(x^5_{16}, \ldots, x^5_{23}) &= (y^5_{16}, \ldots, y^5_{23})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_3^{S1}$:

$$
\begin{aligned}
y^6_{27} \oplus [x^7_{59}] \oplus k_{35} &= 0\\
[y^6_{28}] \oplus x^7_{60} \oplus k_{36} &= 0\\
y^6_{29} \oplus x^7_{61} \oplus k_{37} &= 0\\
[y^6_{31}] \oplus x^7_{63} \oplus k_{39} &= 0\\
S(x^7_{56}, \ldots, x^7_{63}) &= (y^7_{56}, \ldots, y^7_{63})\\
S(x^6_{24}, \ldots, x^6_{31}) &= (y^6_{24}, \ldots, y^6_{31})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_4^{S1}$:

$$
\begin{aligned}
y^2_{127} \oplus [x^3_{23}] \oplus [x^3_{119}] &= 0\\
[y^1_{101}] \oplus [x^2_{29}] \oplus x^2_{125} &= 0\\
S(x^2_{120}, \ldots, x^2_{127}) &= (y^2_{120}, \ldots, y^2_{127})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_5^{S1}$:

$$\begin{aligned}
[y_{48}^0] \oplus [y_{72}^0] \oplus x_{88}^1 \oplus k_{48} &= 0 \\
[y_{37}^1] \oplus y_{93}^1 \oplus [x_{77}^2] \oplus k_{85} &= 0 \\
S(x_{88}^1, \ldots, x_{95}^1) &= (y_{88}^1, \ldots, y_{95}^1)
\end{aligned}$$

C.3 Nonlinear Constraints from 16-round SKINNY-128-256 Characteristic

Nonlinear Constraint $\mathbb{E}_0^{S2}$:

$$\begin{aligned}
y_2^4 \oplus [x_{34}^5] \oplus k1_{58} \oplus k2_{56} &= 0 \\
y_{99}^4 \oplus [x_{27}^5] \oplus [x_{123}^5] &= 0 \\
[y_{106}^3] \oplus x_2^4 \oplus x_{98}^4 &= 0 \\
[y_{110}^3] \oplus [x_6^4] \oplus x_{102}^4 &= 0 \\
y_{98}^4 \oplus [x_{26}^5] \oplus [x_{122}^5] &= 0 \\
S(x_0^4, \ldots, x_7^4) &= (y_0^4, \ldots, y_7^4) \\
S(x_{96}^4, \ldots, x_{103}^4) &= (y_{96}^4, \ldots, y_{103}^4)
\end{aligned}$$

Nonlinear Constraint $\mathbb{E}_1^{S2}$:

$$\begin{aligned}
[y_{12}^2] \oplus x_{44}^3 \oplus k1_{60} \oplus k2_{59} &= 0 \\
[y_{14}^2] \oplus x_{46}^3 \oplus k1_{62} \oplus k2_{61} &= 0 \\
[y_{59}^4] \oplus [y_{83}^4] \oplus x_{67}^5 \oplus k1_{43} \oplus k2_{41} &= 0 \\
[y_{20}^5] \oplus y_{68}^5 \oplus [y_{124}^5] \oplus x_{20}^6 \oplus k1_{124} \oplus k2_{121} &= 0 \\
[y_{22}^5] \oplus y_{70}^5 \oplus [y_{126}^5] \oplus x_{22}^6 \oplus k1_{126} \oplus k2_{123} &= 0 \\
[y_{20}^5] \oplus x_{52}^6 \oplus k1_{124} \oplus k2_{121} &= 0 \\
[y_{22}^5] \oplus x_{54}^6 \oplus k1_{126} \oplus k2_{123} &= 0 \\
[y_{20}^5] \oplus y_{68}^5 \oplus x_{116}^6 \oplus k1_{124} \oplus k2_{121} &= 0 \\
[y_{22}^5] \oplus y_{70}^5 \oplus x_{118}^6 \oplus k1_{126} \oplus k2_{123} &= 0 \\
[y_{44}^5] \oplus y_{68}^5 \oplus x_{84}^6 \oplus k1_{84} \oplus k2_{81} &= 0 \\
[y_{46}^5] \oplus y_{70}^5 \oplus x_{86}^6 \oplus k1_{86} \oplus k2_{83} &= 0 \\
y_{22}^6 \oplus [y_{70}^6] \oplus [x_{118}^7] \oplus k1_{62} \oplus k2_{59} &= 0 \\
S(x_{16}^6, \ldots, x_{23}^6) &= (y_{16}^6, \ldots, y_{23}^6) \\
S(x_{64}^5, \ldots, x_{71}^5) &= (y_{64}^5, \ldots, y_{71}^5) \\
S(x_{112}^6, \ldots, x_{119}^6) &= (y_{112}^6, \ldots, y_{119}^6) \\
S(x_{80}^6, \ldots, x_{87}^6) &= (y_{80}^6, \ldots, y_{87}^6) \\
S(x_{48}^6, \ldots, x_{55}^6) &= (y_{48}^6, \ldots, y_{55}^6) \\
S(x_{40}^3, \ldots, x_{47}^3) &= (y_{40}^3, \ldots, y_{47}^3)
\end{aligned}$$

Nonlinear Constraint $\mathbb{E}_2^{S2}$:

$$\begin{aligned}
[y_{36}^5] \oplus [y_{92}^5] \oplus x_{76}^6 \oplus k1_7 6 \oplus k2_7 3 &= 0 \\
[y_{38}^5] \oplus [y_{94}^5] \oplus x_{78}^6 \oplus k1_7 8 \oplus k2_7 5 &= 0 \\
[y_{50}^6] \oplus y_{74}^6 \oplus x_{90}^7 \oplus k1_2 \oplus k2_5 \oplus k2_7 &= 0
\end{aligned}$$

$$[y_{54}^6] \oplus y_{78}^6 \oplus [x_{94}^7] \oplus k1_6 \oplus k2_3 = 0$$
$$[y_{10}^7] \oplus y_{90}^7 \oplus [x_{106}^8] \oplus k1_{114} \oplus k2_{116} \oplus k2_{118} = 0$$
$$S(x_{88}^7, \ldots, x_{95}^7) = (y_{88}^7, \ldots, y_{95}^7)$$
$$S(x_{72}^6, \ldots, x_{79}^6) = (y_{72}^6, \ldots, y_{79}^6)$$

Nonlinear Constraint $\mathbb{E}_3^{S2}$:

$$y_{12}^4 \oplus x_{44}^5 \oplus k1_28 \oplus k2_26 = 0$$
$$y_{14}^4 \oplus x_{46}^5 \oplus k1_30 \oplus k2_28 = 0$$
$$y_{15}^4 \oplus x_{47}^5 \oplus k1_31 \oplus k2_29 = 0$$
$$[y_6^6] \oplus [x_{38}^7] \oplus k1_30 \oplus k2_27 = 0$$
$$S(x_{40}^5, \ldots, x_{47}^5) = (y_{40}^5, \ldots, y_{47}^5)$$
$$S(x_8^4, \ldots, x_{15}^4) = (y_8^4, \ldots, y_{15}^4)$$

Nonlinear Constraint $\mathbb{E}_4^{S2}$:

$$[y_{12}^5] \oplus x_{44}^6 \oplus k1_{108} \oplus k2_{105} = 0$$
$$[y_{14}^5] \oplus x_{46}^6 \oplus k1_{110} \oplus k2_{107} = 0$$
$$S(x_{40}^6, \ldots, x_{47}^6) = (y_{40}^6, \ldots, y_{47}^6)$$

Nonlinear Constraint $\mathbb{E}_5^{S2}$:

$$[y_{28}^5] \oplus x_{60}^6 \oplus k1_{100} \oplus k2_{97} = 0$$
$$[y_{30}^5] \oplus x_{62}^6 \oplus k1_{102} \oplus k2_{99} = 0$$
$$S(x_{56}^6, \ldots, x_{63}^6) = (y_{56}^6, \ldots, y_{63}^6)$$

Nonlinear Constraint $\mathbb{E}_6^{S2}$:

$$y_{26}^4 \oplus [x_{58}^5] \oplus k1_{50} \oplus k2_{48} = 0$$
$$S(x_{24}^4, \ldots, x_{31}^4) = (y_{24}^4, \ldots, y_{31}^4)$$

Nonlinear Constraint $\mathbb{E}_7^{S2}$:

$$[y_3^4] \oplus [x_{35}^5] \oplus k1_{59} \oplus k2_{57} = 0$$
$$[y_3^4] \oplus [y_{83}^4] \oplus [x_{99}^5] \oplus k1_{59} \oplus k2_{57} = 0$$

Block 9:

$$[y_{19}^1] \oplus [x_{51}^2] \oplus k1_{67} \oplus k2_{66} = 0$$

C.4 Constraints from 14-round RECTANGLE Characteristic

C.4.1 14-round RECTANGLE Characteristic of Stated Probability 2^{-63}

Nonlinear Constraint $\mathbb{E}_0^{REC}$:

$$x_3^7 \oplus k_3^7 = 0$$
$$y_0^7 \oplus k_0^8 = 1$$
$$y_1^7 \oplus x_5^8 \oplus k_5^8 = 0$$
$$x_7^8 \oplus k_7^8 = 0$$

$$
\begin{aligned}
y_4^8 \oplus k_4^9 &= 1 \\
y_5^8 \oplus x_9^9 \oplus k_9^9 &= 0 \\
x_{11}^9 \oplus k_{11}^9 &= 0 \\
y_8^9 \oplus k_8^{10} &= 1 \\
y_9^9 \oplus k_{13}^{10} &= 0 \\
S(x_8^9, \ldots, x_{11}^9) &= (y_8^9, \ldots, y_{11}^9) \\
S(x_0^7, \ldots, x_3^7) &= (y_0^7, \ldots, y_3^7) \\
S(x_4^8, \ldots, x_7^8) &= (y_4^8, \ldots, y_7^8)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_1^{REC}$:

$$
\begin{aligned}
y_{21}^8 \oplus x_{25}^9 \oplus k_{25}^9 &= 0 \\
y_{22}^8 \oplus x_6^9 \oplus k_6^9 &= 0 \\
y_5^9 \oplus x_9^{10} \oplus k_9^{10} &= 0 \\
y_{26}^9 \oplus x_{10}^{10} \oplus k_{10}^{10} &= 0 \\
y_{27}^9 \oplus x_{15}^{10} \oplus k_{15}^{10} &= 0 \\
y_9^{10} \oplus x_{13}^{11} \oplus k_{13}^{11} &= 0 \\
y_{11}^{10} \oplus x_{63}^{11} \oplus k_{63}^{11} &= 0 \\
y_{12}^{10} \oplus x_{12}^{11} \oplus k_{12}^{11} &= 0 \\
x_{62}^{11} \oplus k_{62}^{11} &= 1 \\
x_{62}^{12} \oplus k_{62}^{12} &= 0 \\
y_{60}^{11} \oplus x_{60}^{12} \oplus k_{60}^{12} &= 0 \\
y_{61}^{11} \oplus k_1^{12} &= 0 \\
y_{61}^{12} \oplus k_1^{13} &= 1 \\
S(x_{12}^{10}, \ldots, x_{15}^{10}) &= (y_{12}^{10}, \ldots, y_{15}^{10}) \\
S(x_{60}^{12}, \ldots, x_{63}^{12}) &= (y_{60}^{12}, \ldots, y_{63}^{12}) \\
S(x_4^9, \ldots, x_7^9) &= (y_4^9, \ldots, y_7^9) \\
S(x_{20}^8, \ldots, x_{23}^8) &= (y_{20}^8, \ldots, y_{23}^8) \\
S(x_8^{10}, \ldots, x_{11}^{10}) &= (y_8^{10}, \ldots, y_{11}^{10}) \\
S(x_{24}^9, \ldots, x_{27}^9) &= (y_{24}^9, \ldots, y_{27}^9) \\
S(x_{12}^{11}, \ldots, x_{15}^{11}) &= (y_{12}^{11}, \ldots, y_{15}^{11}) \\
S(x_{60}^{11}, \ldots, x_{63}^{11}) &= (y_{60}^{11}, \ldots, y_{63}^{11})
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_2^{REC}$:

$$
\begin{aligned}
x_0^4 \oplus k_0^4 &= 1 \\
y_3^4 \oplus k_{55}^5 &= 1 \\
S(x_0^4, \ldots, x_3^4) &= (y_0^4, \ldots, y_3^4)
\end{aligned}
$$

Nonlinear Constraint $\mathbb{E}_3^{REC}$:

$$
x_{20}^9 \oplus k_{20}^9 = 1
$$

$$y_{23}^{9} \oplus k_{11}^{10} = 1$$
$$S(x_{20}^{9}, \ldots, x_{23}^{9}) = (y_{20}^{9}, \ldots, y_{23}^{9})$$

Nonlinear Constraint $\mathbb{E}_4^{REC}$:

$$x_{16}^{8} \oplus k_{16}^{8} = 1$$
$$y_{19}^{8} \oplus k_{7}^{9} = 1$$
$$S(x_{16}^{8}, \ldots, x_{19}^{8}) = (y_{16}^{8}, \ldots, y_{19}^{8})$$

Nonlinear Constraint $\mathbb{E}_5^{REC}$:

$$x_{24}^{10} \oplus k_{24}^{10} = 0$$
$$y_{27}^{10} \oplus k_{15}^{11} = 0$$
$$S(x_{24}^{10}, \ldots, x_{27}^{10}) = (y_{24}^{10}, \ldots, y_{27}^{10})$$

Nonlinear Constraint $\mathbb{E}_6^{REC}$:

$$x_{52}^{1} \oplus k_{52}^{1} = 1$$
$$y_{55}^{1} \oplus k_{43}^{2} = 1$$
$$S(x_{52}^{1}, \ldots, x_{55}^{1}) = (y_{52}^{1}, \ldots, y_{55}^{1})$$

Nonlinear Constraint $\mathbb{E}_7^{REC}$:

$$x_{56}^{2} \oplus k_{56}^{2} = 1$$
$$y_{59}^{2} \oplus k_{47}^{3} = 1$$
$$S(x_{56}^{2}, \ldots, x_{59}^{2}) = (y_{56}^{2}, \ldots, y_{59}^{2})$$

Nonlinear Constraint $\mathbb{E}_8^{REC}$:

$$x_{60}^{3} \oplus k_{60}^{3} = 1$$
$$y_{63}^{3} \oplus k_{51}^{4} = 1$$
$$S(x_{60}^{3}, \ldots, x_{63}^{3}) = (y_{60}^{3}, \ldots, y_{63}^{3})$$

Nonlinear Constraint $\mathbb{E}_9^{REC}$:

$$x_{4}^{5} \oplus k_{4}^{5} = 1$$
$$y_{7}^{5} \oplus k_{59}^{6} = 1$$
$$S(x_{4}^{5}, \ldots, x_{7}^{5}) = (y_{4}^{5}, \ldots, y_{7}^{5})$$

Nonlinear Constraint $\mathbb{E}_{10}^{REC}$:

$$x_{8}^{6} \oplus k_{8}^{6} = 1$$
$$y_{11}^{6} \oplus k_{63}^{7} = 1$$
$$S(x_{8}^{6}, \ldots, x_{11}^{6}) = (y_{8}^{6}, \ldots, y_{11}^{6})$$

Nonlinear Constraint $\mathbb{E}_{11}^{REC}$:

$$x_{12}^{7} \oplus k_{12}^{7} = 1$$
$$y_{15}^{7} \oplus k_{3}^{8} = 1$$
$$S(x_{12}^{7}, \ldots, x_{15}^{7}) = (y_{12}^{7}, \ldots, y_{15}^{7})$$

C.4.2 14-round RECTANGLE Characteristic with Stated Probability 2^{-66}

Nonlinear Constraint $\mathbb{E}_0^{REC2}$:

$$
\begin{aligned}
x_7^8 \oplus k_7^8 &= 0\\
y_4^8 \oplus k_4^9 &= 1\\
y_5^8 \oplus x_9^9 \oplus k_9^9 &= 0\\
y_{21}^8 \oplus x_{25}^9 \oplus k_{25}^9 &= 0\\
y_{22}^8 \oplus x_6^9 \oplus k_6^9 &= 0\\
x_{11}^9 \oplus k_{11}^9 &= 0\\
y_5^9 \oplus x_9^{10} \oplus k_9^{10} &= 0\\
y_8^9 \oplus k_8^{10} &= 1\\
y_9^9 \oplus k_{13}^{10} &= 0\\
y_{11}^9 \oplus x_{63}^{10} \oplus k_{63}^{10} &= 0\\
y_{26}^9 \oplus x_{10}^{10} \oplus k_{10}^{10} &= 0\\
y_{27}^9 \oplus x_{15}^{10} \oplus k_{15}^{10} &= 0\\
y_9^{10} \oplus x_{13}^{11} \oplus k_{13}^{11} &= 0\\
y_{11}^{10} \oplus x_{63}^{11} \oplus k_{63}^{11} &= 0\\
y_{12}^{10} \oplus x_{12}^{11} \oplus k_{12}^{11} &= 0\\
x_{62}^{11} \oplus k_{62}^{11} &= 0\\
y_{15}^{10} \oplus x_3^{11} \oplus k_3^{11} &= 0\\
y_{60}^{10} \oplus x_{60}^{11} \oplus k_{60}^{11} &= 0\\
y_{61}^{10} \oplus k_1^{11} &= 0\\
y_0^{11} \oplus x_0^{12} \oplus k_0^{12} &= 0\\
x_{62}^{12} \oplus k_{62}^{12} &= 0\\
y_{15}^{11} \oplus x_3^{12} \oplus k_3^{12} &= 0\\
y_{60}^{11} \oplus x_{60}^{12} \oplus k_{60}^{12} &= 0\\
y_{61}^{11} \oplus k_1^{12} &= 1\\
y_{61}^{12} \oplus k_1^{13} &= 1\\
S(x_8^9, \ldots, x_{11}^9) &= (y_8^9, \ldots, y_{11}^9)\\
S(x_{12}^{10}, \ldots, x_{15}^{10}) &= (y_{12}^{10}, \ldots, y_{15}^{10})\\
S(x_{60}^{10}, \ldots, x_{63}^{10}) &= (y_{60}^{10}, \ldots, y_{63}^{10})\\
S(x_0^{12}, \ldots, x_3^{12}) &= (y_0^{12}, \ldots, y_3^{12})\\
S(x_{60}^{12}, \ldots, x_{63}^{12}) &= (y_{60}^{12}, \ldots, y_{63}^{12})\\
S(x_4^9, \ldots, x_7^9) &= (y_4^9, \ldots, y_7^9)\\
S(x_{20}^8, \ldots, x_{23}^8) &= (y_{20}^8, \ldots, y_{23}^8)\\
S(x_8^{10}, \ldots, x_{11}^{10}) &= (y_8^{10}, \ldots, y_{11}^{10})\\
S(x_4^8, \ldots, x_7^8) &= (y_4^8, \ldots, y_7^8)\\
S(x_0^{11}, \ldots, x_3^{11}) &= (y_0^{11}, \ldots, y_3^{11})\\
S(x_{24}^9, \ldots, x_{27}^9) &= (y_{24}^9, \ldots, y_{27}^9)\\
S(x_{12}^{11}, \ldots, x_{15}^{11}) &= (y_{12}^{11}, \ldots, y_{15}^{11})
\end{aligned}
$$

$$S(x_{60}^{11}, \ldots, x_{63}^{11}) = (y_{60}^{11}, \ldots, y_{63}^{11})$$

Nonlinear Constraint $\mathbb{E}_1^{REC2}$:

$$\begin{aligned} x_0^4 \oplus k_0^4 &= 1 \\ y_3^4 \oplus k_{55}^5 &= 1 \\ S(x_0^4, \ldots, x_3^4) &= (y_0^4, \ldots, y_3^4) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_2^{REC2}$:

$$\begin{aligned} x_{20}^9 \oplus k_{20}^9 &= 1 \\ y_{23}^9 \oplus k_{11}^{10} &= 1 \\ S(x_{20}^9, \ldots, x_{23}^9) &= (y_{20}^9, \ldots, y_{23}^9) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_3^{REC2}$:

$$\begin{aligned} x_{16}^8 \oplus k_{16}^8 &= 1 \\ y_{19}^8 \oplus k_7^9 &= 1 \\ S(x_{16}^8, \ldots, x_{19}^8) &= (y_{16}^8, \ldots, y_{19}^8) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_4^{REC2}$:

$$\begin{aligned} x_{24}^{10} \oplus k_{24}^{10} &= 0 \\ y_{27}^{10} \oplus k_{15}^{11} &= 0 \\ S(x_{24}^{10}, \ldots, x_{27}^{10}) &= (y_{24}^{10}, \ldots, y_{27}^{10}) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_5^{REC2}$:

$$\begin{aligned} x_{52}^1 \oplus k_{52}^1 &= 1 \\ y_{55}^1 \oplus k_{43}^2 &= 1 \\ S(x_{52}^1, \ldots, x_{55}^1) &= (y_{52}^1, \ldots, y_{55}^1) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_6^{REC2}$:

$$\begin{aligned} x_{56}^2 \oplus k_{56}^2 &= 1 \\ y_{59}^2 \oplus k_{47}^3 &= 1 \\ S(x_{56}^2, \ldots, x_{59}^2) &= (y_{56}^2, \ldots, y_{59}^2) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_7^{REC2}$:

$$\begin{aligned} x_{60}^3 \oplus k_{60}^3 &= 1 \\ y_{63}^3 \oplus k_{51}^4 &= 1 \\ S(x_{60}^3, \ldots, x_{63}^3) &= (y_{60}^3, \ldots, y_{63}^3) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_8^{REC2}$:

$$\begin{aligned} x_4^5 \oplus k_4^5 &= 1 \\ y_7^5 \oplus k_{59}^6 &= 1 \\ S(x_4^5, \ldots, x_7^5) &= (y_4^5, \ldots, y_7^5) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_9^{REC2}$:

$$\begin{aligned} x_8^6 \oplus k_8^6 &= 1 \\ y_{11}^6 \oplus k_{63}^7 &= 1 \\ S(x_8^6, \ldots, x_{11}^6) &= (y_8^6, \ldots, y_{11}^6) \end{aligned}$$

Nonlinear Constraint $\mathbb{E}_{10}^{REC2}$:

$$\begin{aligned} x_{12}^7 \oplus k_{12}^7 &= 1 \\ y_{15}^7 \oplus k_3^8 &= 1 \\ S(x_{12}^7, \ldots, x_{15}^7) &= (y_{12}^7, \ldots, y_{15}^7) \end{aligned}$$