On the Number of Restricted Solutions to Constrained Systems and their Applications

Benoît Cogliati[1], Ashwin Jha[2], Jordan Ethan[3], Mridul Nandi[4], and Abishanka Saha[5]

[1] Thales DIS France SAS, Meudon, France
benoit-michel.cogliati@thalesgroup.com
[2] Ruhr University Bochum, Bochum, Germany
ashwin.jha@rub.de
[3] University of Luxembourg, Esch-sur-Alzette, Luxembourg
jordan.naccache@uni.lu
[4] Indian Statistical Institute, Kolkata, India
mridul@isical.ac.in
[5] Eindhoven University of Technology, The Netherlands
a.saha1@tue.nl

Abstract. In this paper, we define a special class of systems of linear equations over finite fields that arise in the security analysis of various MAC and PRF modes. We establish lower bounds on the number of solutions for these systems under specific restrictions and use them to derive tight (up to logarithmic factors) PRF security for several constructions. Specifically, we prove security up to $O(2^{3n/4}/n^{1/4})$ queried blocks (i.e., the total number of blocks in all queries) for the single-keyed variant of the Double-block Hash-then-Sum (`DBHtS`) construction, called `1k-DBHtS`, assuming appropriate hash function properties. As instantiations, we show that single-keyed variants of `LightMAC+` and `PMAC+`, called `1k-LightMAC+` and `1k-PMAC+`, achieve the same bound (ignoring maximum message length) for all message lengths up to specified limits depending upon the irreducible polynomial used to define the field. Additionally, we show that the sum of r independent Even-Mansour ciphers is secure up to $O(2^{\frac{r}{r+1}n}/n)$ queries for any constant r.

Keywords: `PMAC+`, `LightMAC+`, Sum of Even-Mansour, tight security

1 Introduction

For $k \geq 2$, let $\Pi_1, \ldots, \Pi_k$ denote k independent uniform random permutations of $\{0,1\}^n$, and define the function $\mathtt{F} : \{0,1\}^n \to \{0,1\}^n$ by the mapping:

$$x \longmapsto \Pi_1(x) \oplus \Pi_2(x) \oplus \ldots \oplus \Pi_k(x),$$

for all $x \in \{0,1\}^n$. It is well-known [24,28] that $\mathtt{F}$ — the sum of k permutations — is statistically indistinguishable from the uniform random function $\Gamma : \{0,1\}^n \to \{0,1\}^n$, provided the permutations are secret and $q < 2^n$ queries are made. Over

the years, several proof techniques [3,39,42,28,20,18,26,24] have been used to prove this result, with various degrees of success. In particular, Patarin's mirror theory [46,47], has been the main tool in the combinatorial approach to this problem. Suppose $k = 2$ and the adversary makes q queries to the oracle. Let x_i denote the i-th query, then the output λ_i satisfies the equation $Y_1^i \oplus Y_2^i = \lambda_i$, where $Y_1^i = \Pi_1(x_i)$ and $Y_2^i = \Pi_2(x_i)$. This gives a system of equations $\{Y_1^i \oplus Y_2^i = \lambda_i : 1 \le i \le q\}$ with the added constraint that $Y_b^i \neq Y_b^j$ must also be satisfied for all $i \neq j$. Such *constrained* systems are the objects of central interest in mirror theory-based proofs. In particular, a typical proof lower bounds the number of *valid*[6] solutions. For random outputs, the expected number of solutions is $2^{2n}(2^n - 1)^2 \cdots (2^n - q + 1)^2/2^{nq}$. Dutta et al. [26] and Cogliati and Patarin [18] independently employed mirror theory to show that the number of valid solutions is very close to the expected value, while $q \le 2^{n-4.5}$, which translates into a proof of security up to roughly $2^{n-4.5}$ queries, when the permutations are secret. More generally, one can study a system of multivariate equations $A\boldsymbol{x} = \boldsymbol{\lambda}$ with an associated partition P of the variables set $\boldsymbol{x}$, such that any two variables in the same partition must be assigned distinct values.

Now, consider a variation where the adversary has bidirectional[7] oracle access to the permutations. A prominent example is the sum of Even-Mansour or $\mathtt{SOEM}^2$ construction [13,50], where $\mathtt{F}(x) := \Pi_1(x \oplus K_1) \oplus K_1 \oplus \Pi_2(x \oplus K_2) \oplus K_2$, and $(K_1, K_2) \in \{0,1\}^{2n}$ is the secret key. Suppose the adversary first makes q queries each to Π_1 and Π_2 (say $\mathcal{R}_1$ and $\mathcal{R}_2$ collects all the range points appearing in these queries), followed by q queries to the construction oracle. Then, in addition to the aforementioned inequality restriction, a valid solution must also exclude any element in $(\mathcal{R}_1 \times \{0,1\}^n) \cup (\{0,1\}^n \times \mathcal{R}_2)$. In Section 3, we extend this example to concretely show the link between security and the number of solutions to a constrained system. Unfortunately, the existing results cannot handle this problem of *restricted solutions*. Indeed, for $k = 2$, the best bounds [22,13,36,11] are within $(1 - O(q^3/2^{2n}))$-close to the expectation, provided $q \le 2^{2n/3}$. Moreover, to the best of our knowledge, the $k > 2$ case has not been explored yet.

A similar situation also arises in the secret permutations regime. For instance, all single-keyed attempts at `DBHtS`-based MACs, like `1k-PMAC+` [22], `1k-LightMAC+` [51] and `n1kf9` [49] are proven secure only up to $O(2^{2n/3})$ queries, primarily due to a (potentially) sub-optimal lower bound on the number of restricted solutions to the underlying constrained systems. Several works [22,17,36] cite this as the main obstacle towards an improved security bound for the single-keyed constructions.

Most of the known instances of constrained systems in symmetric cryptography fall into one of the two categories: (i) either all the variables are in a single partition (we call them *cliques*), (ii) no two variables in an equation share the same partition (we call them *partites*). For example, the single-keyed constructions result in clique systems, whereas the multi-keyed constructions give

[6] A solution $(y_1^i, y_2^i : 1 \le i \le q)$ is valid if $y_1^i \oplus y_2^i = \lambda_i$ for all $i \in \{1, \ldots, q\}$, and $y_b^i \neq y_b^j$ for all $1 \le i < j \le q$.

[7] The adversary can query both Π_i and Π_i^{-1}.

a partite system. In addition, almost always, the system is such that any two variables in the same partition share the same coefficient in any equation that they appear in (see Definition 8). While the coefficient matrix A is often just a binary matrix over $\mathbb{F}_{2^n}$, recent applications of symmetric primitives in advanced cryptographic protocols [25] highlight the urgent need to extend results from $\mathbb{F}_{2^n}$ to any general finite field $\mathbb{F}_N$. Accordingly, we take a pragmatic approach and restrict our exposition to a specific class of constrained systems that includes, among other things, all the known instances in symmetric-key cryptography. Nevertheless, our results will still be derived in a general field $\mathbb{F}_N$.

1.1 Related Works

Single-keyed `DBHtS`**.** The hash-then-PRP paradigm is a popular approach to construct message authentication codes (MACs) and pseudorandom functions (PRFs) using universal[8] hashing and block ciphers. Popular constructions such as `CBC-MAC` [4], `PMAC` [6], `OMAC` [33], and `LightMAC` [40] fall under this design paradigm. The security of such constructions is limited to the birthday bound on the hash output length, since a collision on the hash output implies a collision on the construction output. One can double the hash output size, which thwarts collision attacks. This, however, requires a bigger block cipher to encrypt the hash output. A more prudent and popular approach is the sum-of-permutations transformation, where each block is encrypted separately and the results are XORed. Datta et al. [21] formalized this as the *diblock hash-then-sum* (`DBHtS`) design, used in constructions like `SUM-ECBC` [52], `PMAC+` [53], `3kf9` [54], `LightMAC+` [45] etc. Leurent et al. [38] demonstrated a $O(2^{3n/4})$-query attack on `DBHtS`, while Kim et al. [37] and Jha and Nandi [35] proved security up to $O(2^{3n/4})$ queries. Though efficient, `DBHtS` typically requires three keys, which is not desirable for practical use. Datta et al. [22] proposed a single-keyed variant for `PMAC+`, called `1k-PMAC+`, with security up to $O(2^{2n/3})$ queries. Later, Song proposed [51] `1k-LightMAC+` and Shen and Sibleyras [49] proposed `n1kf9`, with similar security bounds as `1k-PMAC+`. With lack of matching attacks, these constructions are widely believed to offer the same security as their three-key counterparts.

Sum of Even-Mansour. All the constructions discussed so far are based on block ciphers. However, in recent years, several new designs have used cryptographic permutations or to use the theory parlance, a *public*[9] *random permutation*. Notable examples include `SipHash`[2] and keyed sponge constructions[1,43], both achieving birthday bound security. Chen et al. [13] were the first to propose a beyond-the-birthday bound candidate, the *sum of Even-Mansour* or `SOEM`^{2} construction. This approach replaces block ciphers in the sum of permutations with two independent Even-Mansour ciphers [29]. They showed that $\mathtt{SOEM}^2_{\Pi_1,\Pi_2}$ is secure up to $O(2^{2n/3})$ queries, provided the permutations and keys

[8] A keyed function is called universal if it is collision-resistant under a random key.
[9] The adversary is allowed black-box access to the permutation.

are independent. Without this independence, security degrades to birthday-bound levels. Since the initial proposal, several follow-up works [7,27,12,50] have introduced new variants, still maintaining security up to $O(2^{2n/3})$ queries. Most notably, Sibleyras et al. [50] demonstrated that while key and permutation independence is crucial, the post-addition of keys is redundant. They proposed a more efficient design, the *keyed sum of permutations* (KSoP), defined as $\mathsf{KSoP}_{\Pi_1,\Pi_2}(\mathsf{K}_1, \mathsf{K}_2, m) = \Pi_1(\mathsf{K}_1 \oplus m) \oplus \Pi_2(\mathsf{K}_2 \oplus m)$, which achieves a similar security bound. In this paper, we use $\texttt{SOEM}^2$ to refer to this modified construction.

1.2 Our Contributions

We first revisit the PRF security proof of $\texttt{SOEM}^2$ in Section 3 as a warm-up exercise to provide an intuition for the upcoming abstraction of the underlying combinatorial problem. The main technical contributions are twofold:

1. In Sections 4 and 5, we formalize the constrained systems problem over arbitrary finite fields, and derive lower bounds on the number of solutions for a large class of constrained systems encompassing all relevant instances.
2. As applications, we establish security bounds for several constructions, most of which are tight (up to a logarithmic factors):
   (a) *Tight bounds for single-keyed* `DBHtS`*:* We introduce `1k-DBHtS` (see Section 6), a single-key variant of `DBHtS`, proving security up to $O(2^{3n/4}/n^{1/4})$ queried blocks (i.e., the total number of blocks in all queries), provided the hash function meets specific properties (defined in Section 2.3). This addresses an open problem from [22]. This bound is tight up to a factor of $n^{1/4}$, as the Leurent-Nandi-Sibleyras attack [38] applies to `1k-DBHtS`. In Section 7, we propose two `1k-DBHtS` instances, called `1k-LightMAC+` and `1k-PMAC+`, and show that their respective hash functions satisfy these properties, thereby ensuring security up to $O(2^{3n/4}/n^{1/4})$ queried blocks (ignoring length factors), as long as the maximum message length satisfies some conditions depending upon the choice of the underlying irreducible polynomial.
   (b) *Security for Sum of Even-Mansour:* In Section 8, we generalize the sum of $r \geq 2$ Even-Mansour ciphers, an extension of the Sibleyras-Todo [50] variant, showing security up to $2^{\frac{r}{r+1}n}/n$ queries for any constant r. This result is also tight up to a logarithmic factor due to the key recovery attacks in [13,50].

   Table 1 summarizes and compares our security bounds with existing results.

1.3 Erratum

Apart from some expanded proofs and minor editorial and technical fixes, in this version, we have also corrected some technical errors in the published version [16] of the paper. We enumerate them below, along with any necessary updates:

Table 1. A comparison of our security bounds with the existing results. Here, ℓ, s, and n denote the message length in n-bit blocks, the counter size in bits, and the block size of the primitive, respectively. The security bounds ignore any length and logarithmic factors.

Construction	#Keys	#Calls	Security bound	Tightness
DBHtS [21]	3	$2^{\dagger}$	$O(2^{3n/4})$ [37]	• [38]
PMAC+ [53]	3	$\ell+2$	$O(2^{3n/4})$ [37]	• [38]
3kf9 [54]	3	$\ell+2$	$O(2^{3n/4})$ [37]	• [38]
LightMAC+ [45]	3	$\ell\left(1+\frac{s}{n-s}\right)+2$	$O(2^{3n/4})$ [37]	• [38]
1k-PMAC+ [22]	1	$\ell+2$	$O(2^{2n/3})$ [22]	–
1k-LightMAC+ [51]	1	$\ell\left(1+\frac{s+2}{n-s-2}\right)+2$	$O(2^{2n/3})$ [51]	–
n1kf9 [49]	1	$\ell+2$	$O(2^{2n/3})$ [49]	–
SOEM^2 [13,50]	2	2	$O(2^{2n/3})$ [13,50]	•
1k-DBHtS	1	$2^{\dagger}$	$O(2^{3n/4})$ [Sec. 6]	•
1k-PMAC+	1	$\ell\left(1+\frac{2}{n-2}\right)+2$	$O(2^{3n/4})$ [Sec. 7]	•
1k-LightMAC+	1	$\ell\left(1+\frac{s}{n-s}\right)+2$	$O(2^{3n/4})$ [Sec. 7]	•
SOEM^r	r	r	$O(2^{rn/(r+1)})$ [Sec. 8]	• [13,50]

†This excludes the primitive calls needed to compute the hash value.

- *1k-LightMAC+ and 1k-PMAC+.* Both of these instantiations were previously defined using an incorrect doubling step and a flawed truncation step, where both halves of the underlying hash function were truncated in the same way. This leads to a birthday-bound attack on the resulting instantiations (see Remark 3). In the current version, for both instantiations, we correct the doubling step (see Algorithm 1), truncate the two halves to $n-1$ and $n-2$ bits, respectively, and prove the desired hash bounds afresh (see Lemmata 9 and 10, and Appendix D).

- *Sum of Even-Mansour.* The analyses of SOEM^2 and SOEM^r missed a bad event (see the event DC on pg. 13 and 33). While revising the proof, we also noticed that some other parts of the proof (noticeably the expectation calculation) ignored the adaptivity of the adversary. In the current version, we have fixed all these issues in a revised proof. With these fixed, the security result (see Theorem 4) has slightly different terms, while still giving security up to $O(2^{rn/(r+1)}/n)$ queries.

- *Constrained systems.* The definition of acyclicity is relaxed to allow stars (which is required in latter applications). Some conditions and error terms in Theorems 1 and 2 are corrected. Corollaries 3 and 4 now state all the conditions used in their proofs. The published version did not include a proof of Corollary 4, which is now given over a general $\mathbb{F}_N$. Consequently, $\nabla_{\hat{\mathcal{R}}}$ now accounts for both sums and differences. The impact of these changes on the applications is limited to change in constants.

2 Preliminaries

For any $n \in \mathbb{N}^+$, $[n]$ denotes the set $\{1, \ldots, n\}$. For $k \leq n \in \mathbb{N}^+$, the falling factorial $(n)_k$ is defined as $(n)_k \coloneqq n(n-1)\ldots(n-k+1)$ and $(n)_0 \coloneqq 1$. For any $x, y \in \{0,1\}^*$, $|x|$ denotes the bit-length of x and $x \parallel y$ denotes the concatenation of x and y. For any $m, n \in \mathbb{N}^+$, let $\mathcal{F}(m;n)$ and $\mathcal{P}(n)$ denote the set of all functions $f : \{0,1\}^m \to \{0,1\}^n$ and permutations π of $\{0,1\}^n$, respectively. For any finite set $\mathcal{X}$ and $k \in \mathbb{N}^+$, we write $(\mathtt{X}_1, \ldots, \mathtt{X}_k) \twoheadleftarrow \mathcal{X}$ to denote sampling $\mathtt{X}_1, \ldots, \mathtt{X}_k$ from $\mathcal{X}$ with replacement.

For any prime power N, let $\mathbb{F}_N$ be the finite field of order N. We use $\oplus$, $\cdot$, and $\ominus$ to denote addition, multiplication, and subtraction in the given finite field. For $m, n \in \mathbb{N}^+$, let $\mathbb{F}_N^m$ and $\mathbb{F}_N^{m \times n}$ denote the m-dimensional vector space and the set of all $(m \times n)$ matrices over $\mathbb{F}_N$, respectively. For any $\boldsymbol{v} \in \mathbb{F}_N^m$, $\mathtt{H}(\boldsymbol{v})$ is the number of non-zero coordinates in $\boldsymbol{v}$. For any submatrix A' of $A \in \mathbb{F}_N^{m \times n}$, whenever convenient, we overload the notation $\mathrm{row}(A')$ (res. $\mathrm{col}(A')$) to denote the set of row (res. column) vectors as well as indices of A'.

Sum Capture: For some $k \geq 2$, let $\mathcal{A} = (a_1, \ldots, a_q)$ be a sequence of elements of $\mathbb{F}_N$ (possibly with repetitions), $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k \subseteq \mathbb{F}_N$ and $\boldsymbol{\alpha} \in \mathbb{F}_N^k$ such that $\mathtt{H}(\boldsymbol{\alpha}) = k$. Define

$$\begin{aligned} \mathcal{SC}_{\boldsymbol{\alpha}}(\mathcal{A}, \mathcal{B}) &\coloneqq \left\{ (j, b) \in [q] \times (\mathcal{B}_1 \times \ldots \times \mathcal{B}_k) : \bigoplus_{i=1}^{k} \alpha_i \cdot b_i = a_j \right\}, \\ \mu_{\boldsymbol{\alpha}}(\mathcal{A}, \mathcal{B}) &\coloneqq |\mathcal{SC}_{\boldsymbol{\alpha}}(\mathcal{A}, \mathcal{B})|, \end{aligned} \tag{1}$$

where $\mathcal{B} = (\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_k})$ denotes an arbitrary ordering of the constituent sets. For $\alpha = (1, 1, \ldots, 1)$, $\mu_{\boldsymbol{\alpha}}(\mathcal{A}, \mathcal{B}_{i_1}, \mathcal{B}_{i_2}, \ldots, \mathcal{B}_{i_k}) = \mu_{\boldsymbol{\alpha}}(\mathcal{A}, \mathcal{B}_{j_1}, \mathcal{B}_{j_2}, \ldots, \mathcal{B}_{j_k})$ for any two permutations $(i_1\, i_2\, \ldots\, i_k)$ and $(j_1\, j_2\, \ldots\, j_k)$ of $[k]$. We drop $\boldsymbol{\alpha}$ from the notations whenever $\boldsymbol{\alpha} = (1, 1, \ldots, 1)$. For any $k \geq 2$ and $p \geq 0$, we define

$$\mu_{\boldsymbol{\alpha}}(\mathcal{A}, p) \coloneqq \max_{\substack{\mathcal{B}_1, \ldots, \mathcal{B}_k \subseteq \mathbb{F}_N \\ |\mathcal{B}_i| \leq p}} \mu_{\boldsymbol{\alpha}}(\mathcal{A}, \mathcal{B}), \tag{2}$$

The following lemma is a restatement of [34, Theorem 2], which in turn is a simple generalization of a similar result proved for the $k = 2$ case in [19].

Lemma 1 (Theorem 2 in [34]). *For all but a $(4/N)$-fraction of sequences $\mathcal{A} \in \mathbb{F}_N^q$ and any $\boldsymbol{\alpha} \in \mathbb{F}_N^k$ with $H(\boldsymbol{\alpha}) \geq 2$, we have*

$$\mu_{\boldsymbol{\alpha}}(\mathcal{A}, p) \leq \left(\frac{qp^k}{N} + 2p^{k-1}\sqrt{\ln(N)q} \right).$$

2.1 Some Useful Results from Linear Algebra

In this section we present some linear algebraic definitions and results, which are largely inspired by standard texts in linear algebra [48] and coding theory [41].

Fix some $A \in \mathbb{F}_N^{q\times r}$. Any two rows $A_{i\bullet}$ and $A_{i'\bullet}$ are said to be *adjacent*[10], denoted $A_{i\bullet} \sim A_{i'\bullet}$ if they share at least one column index with non-zero entry. The relation $\sim$ on $\mathrm{row}(A)$ is reflexive and symmetric, but not transitive. We say that two rows $A_{i\bullet}$ and $A_{j\bullet}$ are *connected*, denoted $A_{i\bullet} \sim\!\!\sim A_{j\bullet}$, if and only if there exists a sequence of rows $A_{k_1\bullet}, \ldots, A_{k_l\bullet}$ satisfying

1. $A_{k_1\bullet} = A_{i\bullet}$ and $A_{k_l\bullet} = A_{j\bullet}$, and
2. $A_{k_1\bullet} \sim \cdots \sim A_{k_l\bullet}$.

$\sim\!\!\sim$ is an equivalence relation on $\mathrm{row}(A)$, and as such it effectively partitions $\mathrm{row}(A) = A_1 \sqcup \cdots \sqcup A_c$. For each block A_i of A, let $\overline{A}_i$ denote the *column-reduced form* of A_i, which is obtained by simply dropping all the zero columns from A_i. Then, $\sim\!\!\sim$ induces a block diagonalization on A:

$$\mathrm{BDF}(A) := \begin{pmatrix} \overline{A}_{i_1} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \overline{A}_{i_2} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{A}_{i_c} \end{pmatrix}$$

Unless stated otherwise, we assume that A is in its block diagonalized form.[11]

Definition 1 (Weight). *The weight of any $A \in \mathbb{F}_N^{q\times r}$ is defined as*

$$\mathtt{H}(A) := \min\{\mathtt{H}(\boldsymbol{v}) : \boldsymbol{v} \in \mathrm{rowsp}^+(A)\},$$

where $\mathrm{rowsp}^+(A) := \{a_1A_{1\bullet} \oplus \cdots \oplus a_qA_{q\bullet} : \forall(a_1, \ldots, a_q) \neq \mathbf{0}\}$ *and* $\mathtt{H}(\boldsymbol{v})$ *denotes the number of non-zero coordinates in v.*

The following fact relates the weight of a matrix with its row rank. A short proof is available in Appendix A.

Proposition 1. *Suppose $A \in \mathbb{F}_N^{q\times r}$ has $\mathtt{H}(A) = k > 0$. Then,*
(1) A has full row rank.
(2) for every $r' \geq r - k + 1$ and $1 \leq i_1 < \cdots < i_{r'} \leq r$, the matrix $A' = (A_{\bullet i_1}|\cdots|A_{\bullet i_{r'}})$ has full row rank, where $A_{\bullet i}$ denotes the i-th column of A viewed as a q-dimensional vector.
(3) $r - k + 1 \geq q$.

Definition 2 (Cyclic Matrix). *Any matrix A, with $\mathtt{H}(A) \geq 2$, is said to be cyclic if there exists a sequence of $k \geq 2$ distinct rows $A_{i_1\bullet}, A_{i_2\bullet}, \ldots, A_{i_k\bullet}$ and a sequence of k distinct column indices $j_1, \ldots, j_k$ such that $A_{i_lj_l} \neq 0$ and $A_{i_{l+1}j_l} \neq 0$ for all $l \in [k]$, where $i_{k+1} := i_1$. Otherwise, A is said to be acyclic.*

For $k = 2$, this simply means that $A_{i_1\bullet}$ and $A_{i_2\bullet}$ share at least two column indices with non-zero entries. The following proposition is a trivial consequence of acyclicity.

[10] The nomenclature hints to a graph theoretic connection. Any $q \times r$ matrix A can be viewed as an edge-labelled bipartite graph with rows and columns of A as the disjoint vertex sets. An edge with label α connects row i to column j if $A_{ij} = \alpha \neq 0$.

[11] There exists at least one such block diagonalized form for any matrix and it is unique up to a swapping of rows and columns.

Proposition 2. *Any acyclic matrix has full row rank.*

Note that the converse is not necessarily true.

Definition 3 (Regularity). *Any $A \in \mathbb{F}_N^{q \times r}$ is said to be k-regular if and only if $\mathtt{H}(A_{i\bullet}) = k$, for all $i \in [q]$.*

The following propositions show that acyclic and highly regular matrices have high weight.

Proposition 3. *For $k \geq 2$, any k-regular and acyclic $A \in \mathbb{F}_N^{q \times r}$ has $\mathtt{H}(A) = k$.*

A proof of this proposition is available in Appendix A.2.

Proposition 4. *For $q \geq 2$ and $k \geq 3$, let $A \in \mathbb{F}_N^{q \times r}$ be acyclic and k-regular. Then, for any $1 \leq i_1 < \ldots < i_k \leq r$, the matrix $A' = A \setminus \{A_{\bullet i_1}, \ldots, A_{\bullet i_k}\}$ has:*

$$\mathrm{rank}(A') = \begin{cases} q-1 & \text{if } \{i_1, \ldots, i_k\} = \mathrm{col}(\overline{A}_{j\bullet}) \text{ for some } j \in [q], \\ q & \text{otherwise.} \end{cases}$$

A proof of this proposition is available in Appendix A.3.

2.2 Some Useful Results from Probability Theory

The following well-known and simple results from probability theory will be useful in our analyses. For completeness, we provide proofs in Appendix A.

Proposition 5. *For any real-valued random variable $\mathtt{X}$, we have*

$$\mathbb{E}\left(|\mathtt{X} - \mathbb{E}\left(\mathtt{X}\right)|\right) \leq \sqrt{\mathbb{V}\left(\mathtt{X}\right)}.$$

Let $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_q)$ denote a sequence of $\mathbb{F}_{2^n}$-valued random variables. Define

$$\Delta \coloneqq \max_d |\{i \in [q] : \lambda_i = d\}| \qquad \nabla \coloneqq \max_{d \neq 0} |\{(i,j) : i \neq j \in [q],\, \lambda_i \oplus \lambda_j = d\}|$$

Proposition 6 ([44]). *For any $\boldsymbol{\lambda}$ sampled with replacement, $\mathbb{E}\left(\Delta\right) \leq 4n \left\lceil q/2^n \right\rceil$.*

Proposition 7 ([8]). *For $n \geq 2$ and any $\boldsymbol{\lambda}$ sampled without replacement with $q \leq 2^{n-1}$, $\mathbb{E}\left(\nabla\right) \leq 6n \left\lceil q^2/2^n \right\rceil$.*

Let $\sim$ denote an equivalence relation on $[q]$ such that $i \sim j$ if $\lambda_i = \lambda_j$. Let $\mathcal{P} = \{\mathcal{P}_1, \ldots, \mathcal{P}_c\}$ denote the corresponding partition. Let $\mathtt{NI} \subseteq [c]$ denote the set of indices corresponding to non-singleton blocks. Let $\nu_i = |\mathcal{P}_i|$ for all $i \in [c]$, and $\nu_{\max} = \max\{\nu_i : i \in [c]\}$.

Proposition 8 (Lemma 4.3 and Corollary 4.1 in [35]). *Suppose $\boldsymbol{\lambda}$ satisfies the condition: for distinct $i, j \in [q]$, $\Pr\left(\lambda_i = \lambda_j\right) \leq \epsilon$. Then, we have*

$$\mathbb{E}\left(\sum_{i \in \mathtt{NI}} \nu_i^2\right) \leq 2q^2\epsilon \qquad \Pr\left(\nu_{\max} \geq a\right) \leq \frac{2q^2\epsilon}{a^2}$$

2.3 Hash Functions

Fix some finite $\mathcal{X}, \mathcal{Y} \subseteq \{0,1\}^*$ and a finite $\mathcal{K}$. A $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$-keyed function H is a family of functions $H = (H_K : \mathcal{X} \to \mathcal{Y})_{K \in \mathcal{K}}$. We say that H is a *double-block hash function*, if we can write $\mathcal{Y} = \mathcal{Z}_1 \times \mathcal{Z}_2$, where $\mathcal{Z}_b = \{0,1\}^{k_b}$ for some $k_1, k_2 \in \mathbb{N}^+$. For any double-block hash function H, we write $(H_K^1(m), H_K^2(m)) \coloneqq (z_1, z_2)$, where $z_1 \in \mathcal{Z}_1$ and $z_2 \in \mathcal{Z}_2$, whenever $H_K(m) = y = (z_1, z_2)$.

Coverfree Hash Functions. For any $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$-double-block hash function H, any $s \geq 2$, and any tuple of q distinct inputs $\boldsymbol{m} \coloneqq (m_1, \ldots, m_q)$, we define the following events:

- $\mathsf{COLL}_H(\boldsymbol{m})$: $\exists$ distinct $i, j \in [q]$ such that $H_{\mathtt{K}}(m_i) = H_{\mathtt{K}}(m_j)$;
- $\mathsf{COLL1}_H(\boldsymbol{m})$: $\exists$ distinct $i, j \in [q]$ such that $H^1_{\mathtt{K}}(m_i) = H^1_{\mathtt{K}}(m_j)$;
- $\mathsf{COLL2}_H(\boldsymbol{m})$: $\exists$ distinct $i, j \in [q]$ such that $H^2_{\mathtt{K}}(m_i) = H^2_{\mathtt{K}}(m_j)$;
- $\mathsf{AP1}_H(\boldsymbol{m})$: $\exists$ distinct $i_1, \ldots, i_4 \in [q]$ such that

$$H^1_{\mathtt{K}}(m_{i_1}) = H^1_{\mathtt{K}}(m_{i_2}),\ H^2_{\mathtt{K}}(m_{i_2}) = H^2_{\mathtt{K}}(m_{i_3}),\ H^1_{\mathtt{K}}(m_{i_3}) = H^1_{\mathtt{K}}(m_{i_4})$$

- $\mathsf{AP2}_H(\boldsymbol{m})$: $\exists$ distinct $i_1, \ldots, i_4 \in [q]$ such that

$$H^2_{\mathtt{K}}(m_{i_1}) = H^2_{\mathtt{K}}(m_{i_2}),\ H^1_{\mathtt{K}}(m_{i_2}) = H^1_{\mathtt{K}}(m_{i_3}),\ H^2_{\mathtt{K}}(m_{i_3}) = H^2_{\mathtt{K}}(m_{i_4})$$

- $\mathsf{MC1}^s_H(\boldsymbol{m})$: $\exists$ distinct $i_1, \ldots, i_s \in [q]$ such that

$$H^1_{\mathtt{K}}(m_{i_1}) = H^1_{\mathtt{K}}(m_{i_2}) = \cdots = H^1_{\mathtt{K}}(m_{i_s})$$

- $\mathsf{MC2}^s_H(\boldsymbol{m})$: $\exists$ distinct $i_1, \ldots, i_s \in [q]$ such that

$$H^2_{\mathtt{K}}(m_{i_1}) = H^2_{\mathtt{K}}(m_{i_2}) = \cdots = H^2_{\mathtt{K}}(m_{i_s})$$

where the randomness is induced by $\mathtt{K} \twoheadleftarrow \mathcal{K}$.

Definition 4. *For some $\epsilon_1, \delta : \mathbb{N}^3 \to \mathbb{R}_{\geq 0}$, $\epsilon_2 : \mathbb{N}^3 \to \mathbb{R}_{\geq 0}$ and $\epsilon_3 : \mathbb{N}^4 \to \mathbb{R}_{\geq 0}$, a $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$-double-block hash function H is said to be an $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-Coverfree Hash or CfH if and only if for any $\rho = (q, \ell, \sigma) \in \mathbb{N}^3$, any tuple of q distinct inputs $\boldsymbol{m} \coloneqq (m_1, \ldots, m_q)$, each containing at most ℓ blocks and containing at most σ blocks in total, and any $s \geq 2$, it satisfies*

$$\Pr\left(\mathsf{COLL1}_H(\boldsymbol{m})\right) \leq \epsilon_1(\rho),\ \Pr\left(\mathsf{AP1}_H(\boldsymbol{m})\right) \leq \epsilon_2(\rho), \quad \Pr\left(\mathsf{MC1}^s_H(\boldsymbol{m})\right) \leq \epsilon_3(\rho, s),$$

$$\Pr\left(\mathsf{COLL2}_H(\boldsymbol{m})\right) \leq \epsilon_1(\rho),\ \Pr\left(\mathsf{AP2}_H(\boldsymbol{m})\right) \leq \epsilon_2(\rho), \quad \Pr\left(\mathsf{MC2}^s_H(\boldsymbol{m})\right) \leq \epsilon_3(\rho, s),$$

and $\Pr\left(\mathsf{COLL}_H(\boldsymbol{m})\right) \leq \delta(\rho)$.

Double-block Hash-then-Sum. Let H be a $(\mathcal{K}, \{0,1\}^*, \{0,1\}^{2n})$-double-block hash function. The *DiBlock Hash-then-Sum* construction is a $(\mathcal{K} \times \mathcal{P}(n)^2, \{0,1\}^*, \{0,1\}^n)$-keyed function $\mathtt{DBHtS}_H$, defined by the mapping:

$$(K, \pi_1, \pi_2, m) \mapsto \pi_1(H_K^1(m)) \oplus \pi_2(H_K^2(m)) \tag{3}$$

Several beyond-the-birthday bound MAC constructions, including SUM-ECBC [52], PMAC+ [53], LightMAC+ [45] etc. follow this paradigm.

Permutation-based Double-block Hash Function. A *permutation-based double-block hash function* H is a $(\mathcal{P}(n)^r, \mathcal{X}, \mathcal{Y})$-double-block hash function for some $r \in \mathbb{N}$. Any instantiation of such functions is viewed as an oracle-algorithm with oracle access to $\pi = (\pi_1, \ldots, \pi_r) \in \mathcal{P}(n)^r$. We define the rate function, $\beta_H : \mathbb{N} \to \mathbb{N}$, by the mapping:

$$\ell \longmapsto \max_{\substack{\pi \in \mathcal{P}(n)^r \\ m \in \mathcal{X} \\ m \text{ has } \ell \text{ blocks}}} \beta_{H_\pi(m)},$$

where $\beta_{H_\pi(m)}$ denotes the minimum number of oracle queries to π that H needs to compute $H_\pi(m)$, and an input m has $\max\{1, \lceil |m|/n \rceil\}$ blocks. In this paper, we fix $r = 1$, and assume that there exists an absolute constant $c \in \mathbb{R}^+$ such that $\beta_H(\ell) \leq c\ell$ for any $\ell \in \mathbb{N}$. As a side-effect we also assume independence from π. We refer to such an H as a *rate-c^{-1}* hash function. We remark that the underlying hash functions in almost all the popular constructions, including PMAC+, 3kf9 etc. make about one call per block (up to the padding and a constant number of additional calls), SUM-ECBC makes about two, and LightMAC+ with an s-bit counter makes about $n/(n-s)$. Thus, the above assumption is indeed plausible, and c is a small constant in most applications (see Section 7 for our instances).

2.4 Security Definitions

We write $\mathcal{A}^{\mathcal{O}}$ to denote a distinguisher $\mathcal{A}$ when run with oracle $\mathcal{O}$. For simplicity in security proofs, we assume the distinguisher is *computationally unbounded and deterministic* and it never issues duplicate queries or queries for already known responses. Any distinguisher $\mathcal{A}$ limited to q queries, each of length up to ℓ blocks, with a total of σ blocks is called a (q, ℓ, σ)-distinguisher. The advantage of $\mathcal{A}$ in distinguishing some oracle $\mathcal{O}_1$ from another oracle $\mathcal{O}_0$ is defined as

$$\Delta_{\mathcal{A}}[\mathcal{O}_1 ; \mathcal{O}_0] := \left| \Pr\left(\mathcal{A}^{\mathcal{O}_1} = 1\right) - \Pr\left(\mathcal{A}^{\mathcal{O}_0} = 1\right) \right|.$$

The Expectation Method. Let Θ_{re} (res. Θ_{id}) be the random transcript variable of $\mathcal{A}$'s interaction with the oracle $\mathcal{O}_1$ (respectively $\mathcal{O}_0$). Since $\mathcal{A}$ is deterministic, the probability that the respective transcripts are realized is only computed over the randomness of the respective oracles. A transcript ω is said to be *attainable* if $\Pr(\Theta_{\text{id}} = \omega) > 0$.

Lemma 2 (Fine-grained Expectation). *Let Ω be the set of all attainable transcripts. For some $\varepsilon_{\text{bad}} \geq 0$ and $\varepsilon_{\text{ratio}} : \Omega \to \mathbb{R}$, suppose there is a set $\Omega_{\text{bad}} \subseteq \Omega$ satisfying the following conditions:*

- $\Pr(\Theta_{\text{id}} \in \Omega_{\text{bad}}) \leq \varepsilon_{\text{bad}}$,
- $\varepsilon_{\text{ratio}}$ *is non-negative on* $\Omega_{\text{good}} = \Omega \setminus \Omega_{\text{bad}}$,
- *any* $\omega \in \Omega_{\text{good}}$ *satisfies* $\Pr(\Theta_{\text{re}} = \omega) \geq (1 - \varepsilon_{\text{ratio}}(\omega)) \times \Pr(\Theta_{\text{id}} = \omega)$.

Then, we have:

$$\Delta_{\mathcal{A}}\left[\mathcal{O}_1\,;\,\mathcal{O}_0\right] \leq \varepsilon_{\text{bad}} + \mathbb{E}_{\Theta_{\text{id}}}\left(1_{\text{good}}\varepsilon_{\text{ratio}}\right),$$

where 1_{good} *denotes the indicator variable corresponding to* Ω_{good}.

Proof. We have

$$\begin{aligned}\Delta_{\mathcal{A}}\left[\mathcal{O}_1\,;\,\mathcal{O}_0\right] &= \left|\Pr\left(\mathcal{A}^{\mathcal{O}_1}=1\right) - \Pr\left(\mathcal{A}^{\mathcal{O}_0}=1\right)\right| \\ &\leq \sum_{\omega\in\Omega}\Pr\left(\Theta_{\text{id}}=\omega\right)\cdot\max\left\{0, 1-\frac{\Pr\left(\Theta_{\text{re}}=\omega\right)}{\Pr\left(\Theta_{\text{id}}=\omega\right)}\right\} \\ &\leq \sum_{\omega\in\Omega_{\text{bad}}}\Pr\left(\Theta_{\text{id}}=\omega\right) + \sum_{\omega\in\Omega_{\text{good}}}\Pr\left(\Theta_{\text{id}}=\omega\right)\cdot\varepsilon_{\text{ratio}}(\omega)\end{aligned}$$

The first term in the right-hand-side of the last inequality is $\Pr\left(\Theta_{\text{id}}\in\Omega_{\text{bad}}\right) \leq \varepsilon_{\text{bad}}$ and the second term is $\mathbb{E}_{\Theta_{\text{id}}}\left(1_{\text{good}}\varepsilon_{\text{ratio}}\right)$, as needed. □

The expectation method due to Hoang and Tessaro [31] is a simple corollary of the above result, when $\varepsilon_{\text{ratio}}$ is non-negative over the entire transcript space.

Corollary 1 (Expectation Method). *In Lemma 2 if* $\varepsilon_{\text{ratio}}$ *is non-negative on* Ω *then* $\Delta_{\mathcal{A}}\left[\mathcal{O}_1\,;\,\mathcal{O}_0\right] \leq \varepsilon_{\text{bad}} + \mathbb{E}_{\Theta_{\text{id}}}\left(\varepsilon_{\text{ratio}}\right)$.

PRF Security: The PRF advantage of distinguisher $\mathcal{A}$ against a $(\mathcal{K},\mathcal{X},\mathcal{Y})$-keyed function $\mathtt{F}$ is defined as

$$\mathbf{Advt}^{\text{prf}}_{\mathtt{F}}\left(\mathcal{A}\right) = \Delta_{\mathcal{A}}\left[\mathtt{F}_{\mathtt{K}}\,;\,\Gamma\right], \tag{4}$$

where $\mathtt{K} \twoheadleftarrow \mathcal{K}$ and Γ is a uniform random function. In this paper, we also consider the security model where the distinguisher is given oracle access to the internal primitives of the construction. More specifically, suppose $\mathtt{F}$ has an oracle access $\Pi = (\Pi_1,\ldots,\Pi_k) \twoheadleftarrow \mathcal{P}\left(n\right)^k$, denoted $\mathtt{F}[\Pi]$. Then, the PRF advantage of $\mathcal{A}$ is defined as

$$\mathbf{Advt}^{\text{prf}}_{\mathtt{F}[\Pi]}\left(\mathcal{A}\right) = \Delta_{\mathcal{A}}\left[\left(\mathtt{F}_{\mathtt{K}}[\Pi],\Pi^{\pm}\right);\left(\Gamma,\Pi^{\pm}\right)\right], \tag{5}$$

where the superscript $\pm$ denotes a bidirectional access to Π.

3 Warm-up: PRF Security of Sum of 2 Even-Mansour

Let us revisit the security of the sum of two Even-Mansour, $\mathtt{SOEM}^2$, a PRF construction based on two public permutations, proposed by Chen et al. [13]. For the sake of simplicity, we focus in this section on the initial construction from [13], which includes the post-addition of keys. The more efficient keyed sum of permutation from [50] will be studied in Section 8.

Let $\pi = (\pi_1,\pi_2) \twoheadleftarrow \mathcal{P}\left(n\right)^2$ be a tuple of two permutations of $\{0,1\}^n$. For any key $K = (K_1,K_2) \in (\{0,1\}^n)^2$ and any $m \in \{0,1\}^n$, the 2-sum of Even-Mansour construction, denoted $\mathtt{SOEM}^2[\pi]$, is defined by the mapping

$$m \longmapsto \pi_1(m\oplus K_1)\oplus K_1 \oplus \pi_2(m\oplus K_2)\oplus K_2. \tag{6}$$

We will use the Expectation Method to do the analysis. To begin, let:

- $(\mathsf{M}^i, \mathsf{T}^i)$ denote the i-th query-response tuple corresponding to the construction oracle. Let $\mathsf{M} := \{\mathsf{M}^i : i \in [q]\}$ and $\mathsf{T} := \{\mathsf{T}^i : i \in [q]\}$.
- $(\mathsf{U}_j^i, \mathsf{V}_j^i)$ denote the i-th query-response tuple corresponding to the permutation Π_j. Unless stated otherwise, we assume that all these queries are in the forward direction. Let $\mathsf{U}_j := \{\mathsf{U}_j^i : i \in [p]\}$, $\mathsf{V}_j := \{\mathsf{V}_j^i : i \in [p]\}$, $\mathsf{U} := (\mathsf{U}_1, \mathsf{U}_2)$, and $\mathsf{V} := (\mathsf{V}_1, \mathsf{V}_2)$.
- $(\mathsf{X}_j^i, \mathsf{Y}_j^i)$ denote the input-output tuple to the j-th permutation, for all $j \in [2]$, within the i-th construction query in the real world, i.e., $\mathsf{X}_j^i = \mathsf{M}^i \oplus \mathsf{K}_j$. Let $\mathsf{X}^i := (\mathsf{X}_1^i, \mathsf{X}_2^i)$ and $\mathsf{Y}^i := (\mathsf{Y}_1^i, \mathsf{Y}_2^i)$. Let $\mathsf{X} := \{\mathsf{X}^i : i \in [q]\}$ and $\mathsf{Y} := \{\mathsf{Y}^i : i \in [q]\}$.

We study a modified game where the oracle releases (X, Y) to $\mathcal{A}$ once the query-response phase is over, but before $\mathcal{A}$ outputs. Accordingly, we must also define a sampling mechanism for (X, Y) in the ideal world.

In particular, Y must satisfy the equations $\mathsf{Y}_1^i \oplus \mathsf{Y}_2^i = \mathsf{T}^i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2$. Moreover, since the adversary has offline oracle access to the underlying permutations, we must have $\mathsf{X}_j^i = \mathsf{U}_{j'}^{i'} \iff \mathsf{Y}_j^i = \mathsf{V}_{j'}^{i'}$. In the real world, both of these conditions will be satisfied automatically. In the ideal world, however, the sampling of (X, Y) requires a more careful approach. For example, if there exist $i \in [q]$ and $j_1, j_2 \in [p]$ such that $\mathsf{X}_1^i = \mathsf{U}_1^{j_1}$ and $\mathsf{X}_2^i = \mathsf{U}_2^{j_2}$, then given that $\mathsf{K}_1, \mathsf{K}_2$ are sampled uniformly at random, it is highly unlikely that $\mathsf{V}_1^{j_1} \oplus \mathsf{V}_2^{j_2} = \mathsf{T}^i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2$ will hold, meaning the above equations are unlikely to be satisfied. On the other hand, suppose $\mathsf{X}_1^i = \mathsf{U}_1^{j_1}$ and $\mathsf{V}_1^{j_1} \oplus \mathsf{V}_2^{j_2} = \mathsf{T}^i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2$, then we must have $\mathsf{X}_2^i = \mathsf{U}_2^{j_1}$.

Consequently we use the following two-step sampling mechanism for (X, Y) in the ideal world:

1. First, a dummy key pair is sampled uniformly at random, i.e., $\mathsf{K}_1, \mathsf{K}_2 \xleftarrow{} \{0,1\}^n$, which determines $\mathsf{X}_1^i := \mathsf{M}^i \oplus \mathsf{K}_1$ and $\mathsf{X}_2^i := \mathsf{M}^i \oplus \mathsf{K}_2$. Consider the following predicates:

$$\begin{aligned}
\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K}) &: \exists\, i \in [q],\, j_1, j_2 \in [p] \text{ such that } (\mathsf{X}_1^i = \mathsf{U}_1^{j_1}) \wedge (\mathsf{X}_2^i = \mathsf{U}_2^{j_2}) \\
\mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) &: \exists\, i \in [q], j_1, j_2 \in [p], \{k, k'\} = [2] \text{ such that} \\
&\qquad (\mathsf{V}_1^{j_1} \oplus \mathsf{V}_2^{j_2} = \mathsf{T}^i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2) \wedge (\mathsf{X}_k^i \neq \mathsf{U}_k^{j_k}) \wedge (\mathsf{X}_{k'}^i = \mathsf{U}_{k'}^{j_{k'}}) \\
\mathsf{DC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) &: \exists\, i \neq i' \in [q], j \neq j' \in [p], k \in [2] \text{ such that} \\
&\qquad (\mathsf{X}_k^i = \mathsf{U}_k^j) \wedge (\mathsf{X}_k^{i'} = \mathsf{U}_k^{j'}) \wedge (\mathsf{V}_k^j \oplus \mathsf{V}_k^{j'} = \mathsf{T}^i \oplus \mathsf{T}^{i'})
\end{aligned}$$

   We remark that the event DC was missing in the published version of this paper [16]. A transcript $(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K})$ is considered *bad* if $\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K}) \vee \mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) \vee \mathsf{DC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K})$ is satisfied. Otherwise, it is considered *good*. Going forward, we assume the transcript is good. Thus, for each $i \in [q]$ if there exists $j \in [p]$ and $k \in [2]$, such that $\mathsf{X}_k^i = \mathsf{U}_k^j$, then we define $\mathsf{Y}_k^i := \mathsf{V}_k^j$. This concludes the first step.
2. Note that if Y_1^i is assigned a value, the value of Y_2^i is determined, and vice versa. Hence, after the first step, the only remaining undetermined Y-variables are those of the form $\mathsf{Y}_1^i, \mathsf{Y}_2^i$ for each $i \in \mathcal{I}$, where $\mathcal{I}$ is defined

as

$$\mathcal{I} = \{i \in [q] : (\mathsf{X}_1^i \notin \mathsf{U}_1) \wedge (\mathsf{X}_2^i \notin \mathsf{U}_2)\}.$$

Since the adversary is assumed to avoid redundant queries, we have $\mathsf{X}_1^i \neq \mathsf{X}_1^j$ and $\mathsf{X}_2^i \neq \mathsf{X}_2^j$ for any distinct $i, j \in [q]$. In order to maintain permutation property, the Y-variables must satisfy the following inequalities as well.

- $\mathsf{Y}_1^i \neq \mathsf{Y}_1^j$ and $\mathsf{Y}_2^i \neq \mathsf{Y}_2^j$ for any distinct $i, j \in [q]$.
- $\mathsf{Y}_1^i \notin \mathsf{V}_1$ and $\mathsf{Y}_2^i \notin \mathsf{V}_2$ for any $i \in \mathcal{I}$.

Therefore, here we sample a solution, $(y_1^i, y_2^i : i \in \mathcal{I})$, to the system of equations $\{\mathsf{Y}_1^i \oplus \mathsf{Y}_2^i = \mathsf{T}^i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2 : i \in \mathcal{I}\}$ satisfying

- $y_1^i \neq y_1^j$ and $y_2^i \neq y_2^j$ for distinct $i, j \in \mathcal{I}$
- $y_1^i \notin \mathcal{R}_1$ and $y_2^i \notin \mathcal{R}_2$ for all $i \in \mathcal{I}$, where

$$\mathcal{R}_1 \coloneqq \mathsf{V}_1 \cup \{\mathsf{Y}_1^i : i \in [q] \setminus \mathcal{I}\} \qquad \mathcal{R}_2 \coloneqq \mathsf{V}_2 \cup \{\mathsf{Y}_2^i : i \in [q] \setminus \mathcal{I}\}$$

and assign it to the Y^i variables for every $i \in \mathcal{I}$. At this stage the ideal world transcript is fully determined.

In Section 4, we will reformulate this system of equations as a $(|\mathcal{I}|, 2|\mathcal{I}|, 2)$-constrained system (see Definition 5), consisting of $|\mathcal{I}|$ equations, each involving two variables, one from each of the two equivalence classes corresponding to the input-output indices of the two underlying permutations. The specific solutions in which we are interested will later be defined as $\overline{\mathcal{R}}$-solutions (see Definition 7) to this $(|\mathcal{I}|, 2|\mathcal{I}|, 2)$-constrained system, where $\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_2)$.

Given the uniformity of K_1 and K_2, the probability of obtaining a bad transcript in the ideal world is given by $\Pr(\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K}) \vee \mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) \vee \mathsf{DC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K})) \leq (3qp^2 + 4q^2p)/2^{2n}$. Indeed, KG and SC cost at most $qp^2/2^{2n}$ and $2qp^2/2^{2n}$, respectively. For DC, fix $i \neq i'$, $j \neq j'$ and k. Consider the last of the four queries i, i', j, j'. If it is a construction query or a forward primitive query, its response satisfies the V-equation with probability at most $1/(2^n - p)$, and j determines j' via the U-equation. If it is a backward primitive query, its response satisfies the U-equation with probability at most $1/(2^n - p)$, and j determines j' via the V-equation. This gives at most $4q^2p/2^{2n}$, after accounting for the two choices of k, the unordered pairs $\{i, i'\}$ and $p \leq 2^{n-1}$.

For $j \in [2]$, let h_j denote the number of $i \in [q] \setminus \mathcal{I}$ such that $\mathsf{X}_j^i \in \mathsf{U}_j$. Since the transcript is good, each $i \in [q] \setminus \mathcal{I}$ is counted exactly once, and thus $h_1 + h_2 = q - |\mathcal{I}|$. Moreover, $|\mathcal{R}_1| = p + h_2$ and $|\mathcal{R}_2| = p + h_1$. The probability that a good transcript is realized in the real world is given by

$$\begin{aligned}
&\Pr(\Theta_{\mathrm{re}} = (K, U, V, X, Y, M, T)) \\
&\quad = \Pr_{\Theta_{\mathrm{re}}}(\mathsf{K} = K) \times \Pr_{\Theta_{\mathrm{re}}}((\mathsf{U}, \mathsf{V}) = (U, V)) \times \Pr_{\Theta_{\mathrm{re}}}((\mathsf{X}, \mathsf{Y}) = (X, Y) \mid \mathsf{K}, \mathsf{U}, \mathsf{V}) \\
&\quad = \frac{1}{2^{2n}} \times \frac{1}{((2^n)_p)^2} \times \frac{1}{(2^n - p)_{q-h_1} \times (2^n - p)_{q-h_2}}.
\end{aligned}$$

Similarly, the probability of a good transcript being realized in the ideal world can be calculated as

$$\Pr(\Theta_{\mathrm{id}} = (K, U, V, X, Y, M, T))$$

$$= \frac{1}{2^{2n}} \times \frac{1}{2^{nq}} \times \frac{1}{((2^n)_p)^2} \times \Pr_{\Theta_{\mathrm{id}}}((\mathsf{X},\mathsf{Y}) = (X,Y) \mid \mathsf{K},\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V})$$
$$= \frac{1}{2^{2n}} \times \frac{1}{2^{nq}} \times \frac{1}{((2^n)_p)^2} \times \frac{1}{\eta}$$

where η denotes the number of $\overline{\mathcal{R}}$-solutions to the $(|\mathcal{I}|, 2|\mathcal{I}|, 2)$-constrained system defined above.

We now give a heuristic sketch for finalizing the proof. See Section 8 for a more rigorous and general proof. Now, assuming that the constants for the equations above are sampled uniformly at random, the expected number of $\overline{\mathcal{R}}$-solutions for that system is given by $\mathbb{E} = \frac{(2^n-p-h_2)_{|\mathcal{I}|}(2^n-p-h_1)_{|\mathcal{I}|}}{2^{n|\mathcal{I}|}}$. Looking ahead, our results in the next section suggest that $\eta \geq (1 - O((q^3 + qp^2)/2^{2n}))\mathbb{E}$. Thus, using $(2^n - p)_{q-h_1} = (2^n - p)_{h_2}(2^n - p - h_2)_{|\mathcal{I}|}$ (and similarly for $q - h_2$) and $2^{n(h_1+h_2)} \geq (2^n - p)_{h_1}(2^n - p)_{h_2}$, the ratio between the probability of attaining a good transcript in the real world and the ideal world is greater than $1 - O((q^3 + qp^2)/2^{2n})$, whence the Expectation method dictates that the PRF advantage of the said adversary is upper bounded by $O(q^3/2^{2n} + qp^2/2^{2n})$, as $q^2p \leq q^3 + qp^2$.

4 Constrained System and its Solutions

Definition 5 (Constrained System). *For any positive integers q, r, t such that $q, t < r$, a (q, r, t)-constrained system $\mathbb{S} = (A|\boldsymbol{\lambda}; \mathsf{P})$ over $\mathbb{F}_N$ is the system $A|\boldsymbol{\lambda}$ of q equations in r variables, over $\mathbb{F}_N$, endowed with an equivalence relation P on $\mathrm{col}(A)$ resulting in the partition $\mathrm{col}(A) = \mathsf{P}_1 \sqcup \ldots \sqcup \mathsf{P}_t$.*

The dimension and rank of $\mathbb{S}$, denoted $\dim(\mathbb{S})$ and $\mathrm{rank}(\mathbb{S})$, are simply the dimension and rank of A, respectively.

We naturally extend the notion of adjacency relation $\sim$ associated with A to the augmented matrix $A|\boldsymbol{\lambda}$ as follows: we say that $A_{i\bullet}|\lambda_i \sim A_{j\bullet}|\lambda_j$ if $A_{i\bullet} \sim A_{j\bullet}$, and extend the notion of connectedness relation $\sim\!\!\sim$ similarly. Let $A_i|\boldsymbol{\lambda}_i$ denote the $q_i \times (r+1)$ submatrix (also referred to as a *block*) of $A|\boldsymbol{\lambda}$ corresponding to the equivalence class $A_i|\boldsymbol{\lambda}_i = \{A_{j_1\bullet}|\lambda_{j_1}, \ldots, A_{j_{q_i}\bullet}|\lambda_{j_{q_i}}\}$, i.e.

$$A_i|\boldsymbol{\lambda}_i = \begin{pmatrix} A_{j_1\bullet}|\lambda_{j_1} \\ \vdots \\ A_{j_{q_i}\bullet}|\lambda_{j_{q_i}} \end{pmatrix},$$

where $\sum_i q_i = q$. Let $r_i := |\mathrm{col}(\overline{A}_i)|$ and $\sum_i r_i = r$. For any $i \in [c]$, we say that $A_i|\boldsymbol{\lambda}_i$ is *isolated* if $q_i = 1$. By extension, $A|\boldsymbol{\lambda}$ is said to be isolated if $A_i|\boldsymbol{\lambda}_i$ is isolated for all $i \in [c]$. The block diagonalized form of the system is given by the block matrix

$$\mathrm{BDF}(A|\boldsymbol{\lambda}) := \begin{pmatrix} \overline{A}_1 & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda}_1 \\ \mathbf{0} & \overline{A}_2 & \cdots & \mathbf{0} & \boldsymbol{\lambda}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \overline{A}_{i_c} & \boldsymbol{\lambda}_c \end{pmatrix}$$

All other properties of the coefficient matrix A will also be inherited by $A|\boldsymbol{\lambda}$ without any ambiguity. For what follows, we fix a (q, r, t)-constrained system $\mathbb{S} = (A|\boldsymbol{\lambda}\,;\, \mathsf{P})$, where $A|\boldsymbol{\lambda}$ is in a block diagonalized form (BDF). Whenever convenient, we drop P from the notation. Since $\mathbb{S}$ is effectively a system of equations, all the notations and notions are analogously extended, unless stated otherwise.

The ordered sequence $(\mathbb{S}_1 \prec \cdots \prec \mathbb{S}_c)$ denotes the BDF of $\mathbb{S}$, denoted BDF($\mathbb{S}$), where each $\mathbb{S}_i$ is the (q_i, r_i, t_i)-constrained system $(\overline{A}_i|\boldsymbol{\lambda}_i\,;\, \mathsf{P}^{(i)})$, with $\mathsf{P}^{(i)} \subseteq \mathsf{P}$ being the equivalence relation on the set $\mathrm{col}(\overline{A}_i) \subseteq [r]$, that partitions $\mathrm{col}(\overline{A}_i)$ into t_i subsets $\mathsf{P}^{(i)}_1, \ldots, \mathsf{P}^{(i)}_{t_i}$. Since $\mathsf{P}^{(i)} \subseteq \mathsf{P}$, for brevity we continue to use P instead of $\mathsf{P}^{(i)}$ for all $i \in [c]$. Wlog we also assume that $\mathbb{S}$ is in the BDF.

Definition 6 (Clique and Partite). *The constrained system $\mathbb{S}$ is said to be:*

- *a clique if for all $j, j' \in \mathrm{col}(A)$, $(j, j') \in \mathsf{P}$. Thus, $t = 1$ in this case.*
- *a partite if for all $A_{i\bullet} \in \mathrm{row}(A)$, and for all $j, j' \in \mathrm{col}(\overline{A}_{i\bullet})$, $(j, j') \notin \mathsf{P}$.*

See Example 1 for a complete example summarizing the notations and definitions introduced thus far.

Example 1. Consider the following system of 6 equations in 15 variables over $\mathbb{F}_N$:

$$A|\boldsymbol{\lambda} = \left(\begin{array}{ccccccccccccccc|c}
\alpha_1 & \alpha_2 & \alpha_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 \\
0 & 0 & 0 & \alpha_4 & \alpha_5 & \alpha_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \\
\alpha_7 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_8 & \alpha_9 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 \\
0 & 0 & 0 & 0 & \alpha_{10} & 0 & \alpha_{11} & 0 & 0 & 0 & 0 & \alpha_{12} & 0 & 0 & 0 & \lambda_4 \\
0 & 0 & \alpha_{13} & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{14} & \alpha_{15} & 0 & 0 & 0 & 0 & \lambda_5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{16} & \alpha_{17} & \alpha_{18} & \lambda_6
\end{array}\right)$$

for non-zero $\alpha_1, \ldots, \alpha_{18} \in \mathbb{F}_N$. Here,

- $A_{3\bullet}|\lambda_3 \sim A_{1\bullet}|\lambda_1 \sim A_{5\bullet}|\lambda_5$ giving $A_1|\boldsymbol{\lambda}_1 = \{A_{1\bullet}|\lambda_1, A_{3\bullet}|\lambda_3, A_{5\bullet}|\lambda_5\}$,
- $A_{2\bullet}|\lambda_2 \sim A_{4\bullet}|\lambda_4$ giving $A_2|\boldsymbol{\lambda}_2 = \{A_{2\bullet}|\lambda_2, A_{4\bullet}|\lambda_4\}$, and
- $A_{6\bullet}|\lambda_6 \sim A_{6\bullet}|\lambda_6$ giving $A_3|\boldsymbol{\lambda}_3 = \{A_{6\bullet}|\lambda_6\}$,

resulting in the following BDF:

$$\left(\begin{array}{ccc|c}
\overline{A}_1 & \mathbf{0} & \mathbf{0} & \boldsymbol{\lambda}_1 \\
\mathbf{0} & \overline{A}_2 & \mathbf{0} & \boldsymbol{\lambda}_2 \\
\mathbf{0} & \mathbf{0} & \overline{A}_3 & \boldsymbol{\lambda}_3
\end{array}\right) = \left(\begin{array}{ccccccccccccccc|c}
\alpha_1 & \alpha_2 & \alpha_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1 \\
\alpha_7 & 0 & 0 & \alpha_8 & \alpha_9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 \\
0 & 0 & \alpha_{13} & 0 & 0 & \alpha_{14} & \alpha_{15} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_4 & \alpha_5 & \alpha_6 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{10} & 0 & \alpha_{11} & \alpha_{12} & 0 & 0 & 0 & \lambda_4 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{16} & \alpha_{17} & \alpha_{18} & \lambda_6
\end{array}\right)$$

The resulting system BDF($A|\boldsymbol{\lambda}$) is acyclic[12] and the same as $A|\boldsymbol{\lambda}$ up to a relabeling of variables and constants. Furthermore, one of the blocks $A_3|\boldsymbol{\lambda}_3$ is isolated, although the overall system itself is non-isolated.

[12] Although the matrix $A|\boldsymbol{\lambda}$ may not be acyclic (for instance when $\lambda_1 = \lambda_3$), it is important to remember that the acyclicity property of the system follows from the acyclicity of A alone.

Now, endow the system $A|\boldsymbol{\lambda}$ with an implicit equivalence relation P, resulting in the partition $\mathrm{col}(A) = \mathsf{P}_1 \sqcup \mathsf{P}_2 \sqcup \mathsf{P}_3$, where $\mathsf{P}_i = \{j \in [15] : j \equiv i \pmod 3\}$ for all $i \in [3]$. For the resulting $(6, 15, 3)$-constrained system $\mathbb{S} = (A|\boldsymbol{\lambda}\,;\,\mathsf{P})$, we have

- $\dim(\mathbb{S}) = 6 \times 15$, $\mathrm{rank}(\mathbb{S}) = 6$,
- $\mathrm{BDF}(\mathbb{S}) = (\mathbb{S}_1 \prec \mathbb{S}_2 \prec \mathbb{S}_3)$, where $\mathbb{S}_i = (\overline{A}_i|\boldsymbol{\lambda}_i\,;\,\mathsf{P})$,
- $\mathbb{S}_3$ is isolated, but $\mathbb{S}$ is not, and
- $\mathbb{S}$ is acyclic, partite and not a clique.

Definition 7 (Solution to a Constrained System). *Given a family of sets $\mathcal{R} = \{\mathcal{R}_i \subseteq \mathbb{F}_N\}_{i\in[t]}$, any $\boldsymbol{y} = (y_1, \ldots, y_r) \in \mathbb{F}_N^r$ is said to be an $\overline{\mathcal{R}}$-solution for $\mathbb{S}$ if and only if the following conditions are satisfied:*

1. *$\boldsymbol{y}$ satisfies the system $A|\boldsymbol{\lambda}$,*
2. *for any $i \in [t]$, and any $j \in \mathsf{P}_i$, $y_j \notin \mathcal{R}_i$,*
3. *for any $i \in [t]$, and any $j \neq j' \in \mathsf{P}_i$, $y_j \neq y_{j'}$.*

In words, all elements in $\mathcal{R}_1, \ldots, \mathcal{R}_t$ are forbidden or $\mathcal{R}_i$ are *forbidden sets*. Moreover, any two distinct variables related by P[13] must take distinct values. Let $(\mathbb{S} \,|\, \mathcal{R})$ denote the $\overline{\mathcal{R}}$-solution space of $\mathbb{S}$ and $\eta(\mathbb{S} \,|\, \mathcal{R}) := |(\mathbb{S} \,|\, \mathcal{R})|$, the number of $\overline{\mathcal{R}}$-solutions of $\mathbb{S}$. The central problem that we study in this work is to find a good lower bound on $\eta(\mathbb{S} \,|\, \mathcal{R})$ under some assumptions on A, $\boldsymbol{\lambda}$ and $\mathcal{R}$.

Throughout we will assume that the system is acyclic and regular, which is the case for a large class of constrained systems including all known instances in symmetric-key cryptography, particularly those discussed in this paper. Proposition 3 then ensures that the system has high weight, which will play a crucial role[14] towards establishing a good lower bound on $\eta(\mathbb{S} \,|\, \mathcal{R})$.

Definition 8 (Column-Uniform System). *Any k-regular system $\mathbb{S} = (A|\boldsymbol{\lambda}\,;\,\mathsf{P})$ is said to be a column-uniform system, if:*

1. *for each column j, there exists a unique α_j such that for all $i \in \mathrm{row}(A)$:*

$$A_{ij} = \begin{cases} \alpha_j & \text{if } A_{ij} \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

2. *for $k \geq 2$, if $j_1, j_2 \in \mathsf{P}_l$ then $\alpha_{j_1} = \alpha_{j_2} = \alpha_{(l)}$.*

This seemingly artificial property frequently appears in most of the known instances of constrained systems, including, the sum of k permutations [24], DBHtS [22], cascaded LRW2 [35] etc. So, in addition, to the system being acyclic and regular, we also restrict it to be column-uniform, and such a system will be referred to as a *column-uniform, acyclic and k-regular* (k-CAR) *system*. For any k-CAR system $\mathbb{S}$, we write $\alpha_{\mathbb{S}} := (\alpha_{(1)}, \ldots, \alpha_{(k)})$.

[13] The equivalence relation P on $\mathrm{col}(A)$ can be equivalently defined over the set of variables $\{x_1, \ldots, x_r\}$.

[14] Specifically, point (2) and (3) in Proposition 1 will be exploited freely.

5 Solutions to a CAR System

Fix a k-CAR (q, r, t)-constrained system $\mathbb{S} = (A|\boldsymbol{\lambda}; \mathsf{P})$ and a family of sets $\mathcal{R} = \{\mathcal{R}_i\}_{i\in[t]}$. Fix a BDF $(\mathbb{S}_1 \prec \ldots \prec \mathbb{S}_c)$ for $\mathbb{S}$, where for all $i \in [c]$, $q_i \coloneqq |\mathrm{row}(\overline{A}_i)|$ and $r_i \coloneqq |\mathrm{col}(\overline{A}_i)|$. For any $(i, j) \in [c] \times [t]$, let $r_{i,j} \coloneqq \left|\mathrm{col}(\overline{A}_i) \cap \mathsf{P}_j\right|$, and define $r_{\circ j} \coloneqq \sum_{i=1}^{c} r_{i,j}$. We will often use the following basic property which is easily verifiable using Definition 7.

Fact 1 *For any (q, r, t)-system $\mathbb{S}$ and any $\mathcal{R}' = (\mathcal{R}'_1, \ldots, \mathcal{R}'_t)$, where $\mathcal{R}'_i \subseteq \mathcal{R}_i$ for all $i \in [t]$, $\eta(\mathbb{S} \,|\, \mathcal{R}) \leq \eta(\mathbb{S} \,|\, \mathcal{R}')$.*

Wlog, we assume the system is consistent, i.e., $\mathrm{rank}(A|\boldsymbol{\lambda}) = \mathrm{rank}(A)$ and $|\mathcal{R}_i| = s_i \leq s$ for some $s < N$, or else, $(\mathbb{S} \,|\, \mathcal{R}) = \emptyset$. Then, under the assumption that $\boldsymbol{\lambda}$ is uniform at random, the expected number of $\overline{\mathcal{R}}$-solutions for $\mathbb{S}$ is approximately

$$\mathbb{E}\,(\mathbb{S} \,|\, \mathcal{R}) \coloneqq \frac{\prod_{j=1}^{t} (N - s_j)_{r_{\circ j}}}{N^q} \tag{7}$$

Of course, the assumption and the expression are both quite speculative at a first glance. However, as we show later, $\eta(\mathbb{S} \,|\, \mathcal{R})$ is very close to $\mathbb{E}\,(\mathbb{S} \,|\, \mathcal{R})$ for a large class of constrained systems. Indeed, for certain binary matrices A and $\mathcal{R} = \emptyset$ case, Cogliati et al. prove [15] exactly this result. We aim to prove it in a more general setting, where $\mathcal{R}$ may not be empty.

Additional Notations and Conventions: Without loss of generality assume a BDF $(\mathbb{S}_1 \prec \ldots \prec \mathbb{S}_c)$, such that all the isolated blocks appear before the non-isolated ones. Let $\mathtt{NI}(\mathbb{S})$ denote the set of indices of all the non-isolated blocks, $\xi_{\mathbb{S}} \coloneqq \max\{r_i : i \in [c]\}$, $\Delta_{\mathbb{S}} \coloneqq \max_d |\{i \in [q] : \lambda_i = d\}|$, and for any $i \in [c]$, let:

- $\mathbb{S}_{\leq i}$ denote the system $(\mathbb{S}_1 \prec \ldots \prec \mathbb{S}_i)$,
- $\boldsymbol{y}_{\leq i}$ denote some arbitrary solution in $(\mathbb{S}_{\leq i} \,|\, \mathcal{R})$,
- $\mathcal{P}$ and $\mathcal{F}$ define families of sets indexed by $j \in [t]$ such that

$$\mathcal{P}_j(\boldsymbol{y}_{\leq i}) \coloneqq \{y_k \in \boldsymbol{y}_{\leq i} : k \in \mathsf{P}_j\} \qquad \mathcal{F}_j(\boldsymbol{y}_{\leq i}) \coloneqq \mathcal{R}_j \sqcup \mathcal{P}_j(\boldsymbol{y}_{\leq i})\,.$$

  $\mathcal{P}_j(\boldsymbol{y}_{\leq i})$ is the set of values already assigned to variables from P_j in an earlier sub-system, making them unavailable for any $\mathbb{S}_k$ with $k > i$. $\mathcal{F}_j(\boldsymbol{y}_{\leq i})$ extends this by including $\mathcal{R}_j$, representing all forbidden values for variables from P_j in any later $\mathbb{S}_k$. Let $r_{\leq i,j} \coloneqq |\mathcal{P}_j(\boldsymbol{y}_{\leq i})|$ and $f_{\leq i,j} \coloneqq |\mathcal{F}_j(\boldsymbol{y}_{\leq i})| = s_j + r_{\leq i,j}$.

Extending the notation for $i = 0$, let $\boldsymbol{y}_{\leq 0}$ denote any empty sequence, and thus, $\mathcal{P}_j(\boldsymbol{y}_{\leq 0}) = \emptyset$ and $\mathcal{F}_j(\boldsymbol{y}_{\leq 0}) = \mathcal{R}_j$. Note that, $r_{\leq i,j}$ and hence $f_{\leq i,j}$ are independent of the actual elements in $\mathcal{P}_j(\boldsymbol{y}_{\leq i})$ and $\mathcal{F}_j(\boldsymbol{y}_{\leq i})$, respectively.

5.1 The Case of a CAR Partite System

For simplicity, we take $k = t \geq 3$. The case of $k = 2$ is more delicate, which we treat separately in section 5.2.

For any t-CAR and partite (t-CARP) (q,r,t)-system $\mathbb{S}$, we have the obvious[15] bijective map $\alpha_{(j)} \longmapsto \mathsf{P}_j$. With this in mind, we define three families of sets $\hat{\mathcal{R}}$, $\hat{\mathcal{P}}$ and $\hat{\mathcal{F}}$ indexed by $j \in [t]$ such that

$$\hat{\mathcal{R}}_j \coloneqq \alpha_{(j)} \cdot \mathcal{R}_j\,;\ \hat{\mathcal{P}}_j(\boldsymbol{y}_{\le i}) \coloneqq \{\alpha_{(j)} \cdot y_k \in \boldsymbol{y}_{\le i} : k \in \mathsf{P}_j\}\,;\ \hat{\mathcal{F}}_j(\boldsymbol{y}_{\le i}) \coloneqq \hat{\mathcal{R}}_j \sqcup \hat{\mathcal{P}}_j(\boldsymbol{y}_{\le i})\,.$$

This manipulation allows us to disregard the multiplicative nature of the field and focus solely on additivity in the analysis. It is obvious that $|\hat{\mathcal{R}}_j| = s_j$, $|\hat{\mathcal{P}}_j(\boldsymbol{y}_{\le i})| = r_{\le i,j}$ and $|\hat{\mathcal{F}}_j(\boldsymbol{y}_{\le i})| = f_{\le i,j}$. In particular, we have $r_{\le i,j} \le q_{\le i}$, where $q_{\le i} = q_1 + \ldots + q_i$, as each equation can have at most one variable in P_j. Thus, $f_{\le i,j} \le s_j + q_{\le i} \le s + q$.

Theorem 1 (Partite Bound). *Let $t \ge 3$, and $\mathcal{R}$ be a family of sets. For any (q,r,t)-constrained system $\mathbb{S}$ which is t-CARP and satisfies $\xi_{\mathbb{S}}(s+q) \le N/2$, we have $\eta(\mathbb{S}\,|\,\mathcal{R}) \ge (1-\varepsilon)\,\mathbb{E}\,(\mathbb{S}\,|\,\mathcal{R})$, where*

$$\varepsilon \le \frac{2\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda},\mathcal{R})}{N^{t-1}} + \frac{2q\Delta_{\mathbb{S}}}{N^{t-1}} + \frac{6q(s+q)^t}{N^t} + \sum_{i \in \mathtt{NI}(\mathbb{S})} \left(\frac{2tq_i^2}{N} + \frac{2r_i^t(s+q)^t}{N^t} + \varepsilon_{\mathrm{odd}}(q_i,r,s,t) \right),$$

where $\varepsilon_{\mathrm{odd}}(q_i,r,s,t) = 2q_i(s+q)^{t-1}N^{1-t}$ for odd t, and $\varepsilon_{\mathrm{odd}}(q_i r,s,t) = 0$ o.w.

Proof overview: The proof of this result proceeds in two main stages. First, in Lemma 4, we establish a bound for the isolated blocks. Then, in Corollary 2, we extend this to the non-isolated blocks, leading to Theorem 1. Each stage is further divided into two steps: first, deriving a conditional lower bound for a block given a solution for previous blocks (see Lemmas 3 and 5); and second, summing the error terms over all prior solutions.

The conditional lower bounds rely on the inclusion-exclusion principle, with careful applications of Propositions 1 and 3. We speculate that these bounds may be independently useful when the local[16] error terms are sufficiently small in expectation for a random constrained system. The error accumulation step has a mirror theoretic [46] flavour.

Consider the i-th block $\mathbb{S}_i = (\overline{A}_i|\boldsymbol{\lambda}_i\,;\,\mathsf{P})$. Since $\mathbb{S}$ is in BDF, $\mathrm{col}(\overline{A}_i) = \{r_{\le(i-1)} + 1, \ldots, r_{\le(i-1)} + r_i\}$, where $r_{\le(i-1)} = r_1 + \ldots + r_{(i-1)}$. For brevity, we ignore the $r_{\le(i-1)}$ shift in indexing. Observe that

$$\eta(\mathbb{S}_{\le i}\,|\,\mathcal{R}) = \sum_{\boldsymbol{y}_{\le(i-1)}} \eta(\mathbb{S}_i\,|\,\mathcal{F}(\boldsymbol{y}_{\le(i-1)}))\,, \tag{8}$$

where the sum is over all $\boldsymbol{y}_{\le(i-1)}$ in $(\mathbb{S}_{\le(i-1)}\,|\,\mathcal{R})$. For a fixed $\boldsymbol{y}_{\le(i-1)}$ define:

$$\mathcal{S}(\mathbb{S}_i\,|\,\mathcal{F}) \coloneqq \{y = (y_1,\ldots,y_{r_i}) \in \overline{\mathcal{F}}_{(1)} \times \ldots \times \overline{\mathcal{F}}_{(r_i)} : \overline{A}_i y = \boldsymbol{\lambda}_i\},$$

[15] This is made obvious by a (possible) relabelling of coefficient indices.
[16] Here, "local" refers to individual blocks.

where, for all $j \in [r_i]$, $\mathcal{F}_{(j)} \coloneqq \mathcal{F}_k(\boldsymbol{y}_{\leq(i-1)})$ if $r_{\leq(i-1)} + j \in \mathsf{P}_k$. Let $f_{(j)} = |\mathcal{F}_{(j)}|$, and thus $f_{(j)} = f_{\leq(i-1),k}$ for a unique $k \in [t]$. For each $k \in [t]$ and $j_1 \neq j_2 \in \mathrm{col}(\overline{A}_i) \cap \mathsf{P}_k$, define:

$$\mathsf{EQ}^k_{j_1,j_2}(\mathbb{S}_i \,|\, \mathcal{F}) \coloneqq \{y \in \mathcal{S}(\mathbb{S}_i \,|\, \mathcal{F}) \ : \ y_{j_1} = y_{j_2}\}.$$

Let $\mathsf{EQ}^k(\mathbb{S}_i \,|\, \mathcal{F}) \coloneqq \cup_{j_1,j_2 \in \mathrm{col}(\overline{A}_i) \cap \mathsf{P}_k} \mathsf{EQ}^k_{j_1,j_2}(\mathbb{S}_i \,|\, \mathcal{F})$. Then, the set of all $\overline{\mathcal{F}}$-solutions to $\mathbb{S}_i$ is given by

$$(\mathbb{S}_i \,|\, \mathcal{F}) \coloneqq \mathcal{S}(\mathbb{S}_i \,|\, \mathcal{F}) \setminus \left(\bigcup_{k \in [t]} \mathsf{EQ}^k(\mathbb{S}_i \,|\, \mathcal{F}) \right), \tag{9}$$

where the first set on the right hand side consists of all the solutions that do not overlap with the forbidden values, and the second set is a further refinement corresponding to within-the-block intra-partition equalities.

A bulk of the subsequent proofs will concentrate on deriving good bounds for $|\mathcal{S}(\mathbb{S}_i \,|\, \mathcal{F})|$, while $|\mathsf{EQ}^k_{j_1,j_2}(\mathbb{S}_i \,|\, \mathcal{F})|$ is bounded relatively loosely.

Let $\mathcal{A}_\emptyset \coloneqq \{y \in \mathbb{F}_N^{r_i} \ : \ \overline{A}_i y = \boldsymbol{\lambda}_i\}$. For each $j \in [r_i]$, we define $\mathcal{A}_{\{j\}} \coloneqq \mathcal{A}_\emptyset \bigcap (\mathbb{F}_N^{j-1} \times \mathcal{F}_{(j)} \times \mathbb{F}_N^{r_i - j})$. Then, we have

$$\mathcal{S}(\mathbb{S}_i \,|\, \mathcal{F}) = \mathcal{A}_\emptyset \setminus \left(\bigcup_{j \in \mathrm{col}(\overline{A}_i)} \mathcal{A}_{\{j\}} \right).$$

For any non-empty $\mathcal{J} \subseteq \mathrm{col}(\overline{A}_i)$, let $\mathcal{A}_\mathcal{J} \coloneqq \cap_{j \in \mathcal{J}} \mathcal{A}_{\{j\}}$. Using the principle of inclusion-exclusion, we have

$$|\mathcal{S}(\mathbb{S}_i \,|\, \mathcal{F})| = |\mathcal{A}_\emptyset| - \left| \left(\bigcup_{j \in [r_i]} \mathcal{A}_{\{j\}} \right) \right| = \sum_{\mathcal{J} \subseteq [r_i]} (-1)^{|\mathcal{J}|} |\mathcal{A}_\mathcal{J}| \tag{10}$$

Now, $|\mathcal{A}_\emptyset| = N^{r_i - q_i}$ follows from elementary[17] linear algebra; In fact, by virtue of $\mathbb{S}$ being an acyclic and t-regular system, Proposition 3 and 1 allows for an analogous argument to prevail for any $\mathcal{A}_\mathcal{J}$ with $|\mathcal{J}| \leq t - 1$. In particular, for any $\mathcal{J} = \{l_1, \ldots, l_{|\mathcal{J}|}\}$, and any $y_\mathcal{J} = (y_{l_1}, \ldots, y_{l_{|\mathcal{J}|}}) \in \mathcal{F}_{(l_1)} \times \ldots \times \mathcal{F}_{(l_{|\mathcal{J}|})}$, we obtain an equation in exactly $r_i - |\mathcal{J}| \geq r_i - t + 1 \geq q_i$ variables, which has exactly $N^{r_i - |\mathcal{J}| - q_i}$ solutions. There are exactly $f_{(\mathcal{J})} = f_{(l_1)} \ldots f_{(l_{|\mathcal{J}|})}$ such $y_\mathcal{J}$. Thus, we have $|\mathcal{A}_\mathcal{J}| = f_{(\mathcal{J})} \cdot N^{r_i - |\mathcal{J}| - q_i}$ for all $\mathcal{J} \subseteq \mathrm{col}(\overline{A}_i)$ with $|\mathcal{J}| \leq t - 1$.

[17] As $\overline{A}_i$ is acyclic, it has full row rank, so some q_i of its columns form an invertible submatrix. Once we fix a value for each of the other $r_i - q_i$ variables (and thus drop the corresponding columns), we are left with a reduced system of equations that has a unique solution.

Crude Bound. Digressing a little, from (10) and the above discussion, we have

$$N^{r_i-q_i} - r_i(s+q)N^{r_i-q_i-1} \le |\mathcal{S}(\mathbb{S}_i \,|\, \mathcal{F})| \le N^{r_i-q_i} \tag{11}$$

for any acyclic system $\mathbb{S}$ where we use the fact $f_{(j)} \le (s+q)$ for all $j \in [r_i]$. Let $\mathsf{EQ}^k_{j_1,j_2}(\mathbb{S}_i) \coloneqq \{y \in \mathbb{F}_N^{r_i} \,:\, \overline{A}_i y = \boldsymbol{\lambda}_i \wedge y_{j_1} = y_{j_2}\}$. Using Fact 1, we have that

$$|\mathsf{EQ}^k_{j_1,j_2}(\mathbb{S}_i \,|\, \mathcal{F})| \le |\mathsf{EQ}^k_{j_1,j_2}(\mathbb{S}_i)| \le N^{r_i-q_i-1}, \tag{12}$$

where, at the second inequality, we used Proposition 1 and 3 to ensure that the equation $x_{j_1} \ominus x_{j_2} = 0$ is independent of $\overline{A}_i y = \boldsymbol{\lambda}_i$, since $\mathtt{H}(A) = k \ge 3$.

Finally, (9), (11) and (12), along with (8) gives the following crude bound.

Fact 2 *Let $t \ge 3$. For any acyclic (q,r,t)-system and any $\mathcal{R} = (\mathcal{R}_1, \ldots, \mathcal{R}_t)$, we have*

$$N^{r_i-q_i-1}\left(N - r_i(s+q) - tq_i^2\right)\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) \le \eta(\mathbb{S}_{\le i} \,|\, \mathcal{R}) \le N^{r_i-q_i}\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})$$

Coming back to (10) for a proof of Theorem 1, we study the right hand side separately for isolated and non-isolated blocks, starting with an isolated block.

Lemma 3. *If $\mathbb{S}_i$ is isolated, then, for any $\boldsymbol{y}_{\le(i-1)} \in (\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})$, we have*

$$\eta(\mathbb{S}_i \,|\, \mathcal{F}) = \frac{1}{N}\left(\prod_{j=1}^{t}(N - f_{\le(i-1),j}) + (-1)^t N\left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) - \frac{\prod_{j=1}^{t} f_{\le(i-1),j}}{N}\right)\right).$$

A proof of this lemma follows from a refinement of the crude bound and can be found in Appendix B.1. Now, on to a lower bound on $\eta(\mathbb{S}_{\le i} \,|\, \mathcal{R})$ for isolated $\mathbb{S}_i$.

Lemma 4. *If $\mathbb{S}_i$ is isolated, then, we have*

$$\frac{\eta(\mathbb{S}_{\le i} \,|\, \mathcal{R})}{\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})} \ge \frac{\prod_{j=1}^{t}(N - f_{\le(i-1),j})}{N}\left(1 - \frac{2\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R})}{N^{t-1}} - \frac{2\Delta_{\mathbb{S}}}{N^{t-1}} - \frac{6(s+q)^t}{N^t}\right).$$

A proof of this lemma follows from (8) and Lemma 3 and can be found in Appendix B.2. We remark that the proofs of Lemma 3 and 4 never use $t \ge 3$ (the sets $\mathsf{EQ}^k(\mathbb{S}_i \,|\, \mathcal{F})$ are empty for an isolated partite block), and hence both lemmas hold for $t = 2$ as well. Moreover, $\Delta_{\mathbb{S}}$ is only used to bound the number of $j \le (i-1)$ such that $\lambda_j = \lambda_i$ (Case B2 in the proof of Claim (22)), so Lemma 4 also holds with $\Delta_{\mathbb{S}}$ replaced by this number. Next, we consider non-isolated blocks.

Lemma 5. *Let $t \ge 3$. If $\mathbb{S}_i$ is non-isolated, then, we have*

$$\eta(\mathbb{S}_i \,|\, \mathcal{F}) \ge \frac{\prod_{j=1}^{t}(N - f_{\le(i-1),j})^{r_{i,j}}}{N^{q_i}}\left(1 - \frac{2tq_i^2}{N} - \frac{2r_i^t(s+q)^t}{N^t} - \varepsilon_{\mathrm{odd}}(q,r,s,t)\right),$$

where $\varepsilon_{\mathrm{odd}}(q,r,s,t) = 2q_i(s+q)^{t-1}N^{1-t}$ for odd t, and $\varepsilon_{\mathrm{odd}}(q,r,s,t) = 0$ o.w.

A proof of this lemma follows from (10) and (12), which suggests using Bonferroni's inequality [30]. The even t case is relatively simpler where we can bound the terms simply using the facts $f_{(j)} \le (s+q)$ for any j and $r_i(s+q) \le \xi_{\mathbb{S}}(s+q) \le N/2$. For the odd t case the reasoning is more involved, in which case we need to additionally use Proposition 4. The full proof can be found in Appendix B.3. Since the bound in Lemma 5 is independent of $\boldsymbol{y}_{\le(i-1)}$, we have the following corollary.

Corollary 2. *Let $t \ge 3$. If $\mathbb{S}_i$ is non-isolated, then, we have*

$$\frac{\eta(\mathbb{S}_{\le i} \,|\, \mathcal{R})}{\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})} \ge \frac{\prod_{j=1}^{t}(N - f_{\le(i-1),j})^{r_{i,j}}}{N^{q_i}} \left(1 - \frac{2tq_i^2}{N} - \frac{2r_i^t(s+q)^t}{N^t} - \varepsilon_{\mathrm{odd}}(q_i, r_i, s, t)\right),$$

where $\varepsilon_{\mathrm{odd}}(q, r, s, t) = 2q_i(s+q)^{t-1}N^{1-t}$ for odd t, and $\varepsilon_{\mathrm{odd}}(q, r, s, t) = 0$ o.w.

Theorem 1 now follows from the appropriate recursive application of Lemma 4 and Corollary 2 for all i from c down to 1, carefully accumulating the bound for non-isolated blocks, and using $\sum_{i \notin \mathtt{NI}(\mathbb{S})} \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}) \le \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}, \mathcal{R})$.

Remark 1. An astute reader can observe that Lemma 4 and Corollary 2 actually imply a bound of the form:

$$\eta(\mathbb{S} \,|\, \mathcal{R}) \ge \frac{(1-\varepsilon)}{N^q} \prod_{i=1}^{c} \prod_{j=1}^{t} (N - f_{\le(i-1),j})^{r_{i,j}} \ge (1-\varepsilon)\mathbb{E}\,(\mathbb{S} \,|\, \mathcal{R})\,.$$

In fact, this improved bound seems to strengthen a conjecture [5, Conjecture 1] of Bhaumik et al. Indeed, this bound indicates that the conjecture might be true, even in the multivariate setting, albeit with an error factor.

In the end, we chose to use an inferior bound in Theorem 1 as we do not have an application for this result.

The Case of a CAR Clique System. Suppose $\mathbb{S}$ is k-CAR and clique (k-CARC) for some $k \ge 3$. The case of clique systems is similar to the partite case. Indeed we reuse the same notations and arguments to a large extent. First, we redefine $\mathbb{E}\,(\mathbb{S} \,|\, \mathcal{R}) \coloneqq (N-s)_r/N^q$. Next, we construct an arbitrary partite version of $\mathbb{S}$ by imposing an arbitrary (but valid) k-partitioning $\overline{\mathsf{P}}$ on $\overline{A}_i$ for all $i \in [c]$. Let this system be $\overline{\mathbb{S}}$. Clearly, $\overline{\mathbb{S}}$ is a k-CARP system. Next, set $\mathcal{R}_1 = \cdots = \mathcal{R}_k$, $s_1 = \ldots = s_k = s$, and reuse the definitions of $\mathcal{A}_\emptyset$ and $\mathcal{A}_{\{j\}}$ for any $j \in \mathrm{col}(\overline{A}_i)$.

Now, we can extend Theorem 1 to get the following clique counterpart.

Theorem 2 (Clique Bound). *Let $k \ge 3$ and $\mathcal{R}$ be a family of sets. For any $(q, r, 1)$-constrained system $\mathbb{S}$ which is k-CARC and which satisfies $\xi_{\mathbb{S}}(s+kq) \le N/2$, we have $\eta(\mathbb{S} \,|\, \mathcal{R}) \ge (1-\varepsilon)\,\mathbb{E}\,(\mathbb{S} \,|\, \mathcal{R})$, where*

$$\varepsilon \le \frac{2\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}, \mathcal{R})}{N^{k-1}} + \frac{2k!\,q\Delta_{\mathbb{S}}}{N^{k-1}} + \frac{6q(s+kq)^k}{N^k} + \frac{2qk^2}{N} + \sum_{i \in \mathtt{NI}(\mathbb{S})} \left(\frac{2r_i^k(s+kq)^k}{N^k} + \frac{2q_i(s+kq)^{k-1}}{N^{k-1}} + \frac{2r_i^2}{N}\right).$$

Proof. We follow the proof of Theorem 1 for $\overline{\mathbb{S}}$, and only describe the three changes. First, all the variables of $\mathbb{S}_{\leq(i-1)}$ are forbidden for $\mathbb{S}_i$, i.e., $\mathcal{F}_j(\boldsymbol{y}_{\leq(i-1)}) = \mathcal{R}_1 \sqcup \mathcal{P}(\boldsymbol{y}_{\leq(i-1)})$ for all $j \in [k]$, where $\mathcal{P}(\boldsymbol{y}_{\leq(i-1)})$ is the set of all values in $\boldsymbol{y}_{\leq(i-1)}$. Thus, $f_{(j)} \leq s + r \leq s + kq$, which explains the $s + kq$ terms and the condition $\xi_{\mathbb{S}}(s + kq) \leq N/2$. Second, any two variables in $\mathbb{S}_i$ must take distinct values. So the union in (9) runs over all the $\binom{r_i}{2}$ pairs $j_1 < j_2$ in $\mathrm{col}(\overline{A}_i)$, and each EQ_{j_1,j_2} has size at most $N^{r_i - q_i - 1}$ by (12), as $\mathtt{H}(A) \geq k \geq 3$. This costs at most r_i^2/N for a non-isolated block and k^2/N for an isolated block. Third, in the proof of Claim (22), all the k sets in $\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F})$ are equal to $\mathcal{F}_1(\boldsymbol{y}_{\leq(i-1)})$. So, (i) an earlier variable may appear at two positions of a tuple. There are at most $\binom{k}{2}$ choices for the two positions, at most kq choices for the variable, and at most $(s + kq)^{k-3}$ choices for the remaining $k - 2$ positions, as they must satisfy one linear equation. So there are at most $\binom{k}{2}(s+kq)^{k-2}$ such tuples for each $\boldsymbol{y}_{\leq(i-1)}$, which costs at most k^2/N for each isolated block. And (ii) in Case B2, the k positions may carry the variables of $\mathbb{S}_j$ in any of the $k!$ orders, which replaces $\Delta_{\mathbb{S}}$ by $k!\,\Delta_{\mathbb{S}}$. All other steps go through unchanged. □

5.2 Refinements for 2-Regular Systems

The case of 2-regular systems differs from the general case in the treatment of the sets $\mathsf{EQ}^k_{j_1,j_2}$. In particular, the argument behind (12) no longer applies when $k = 2$. We sidestep this issue by working with a special class of systems.

Any 2-regular system $\mathbb{S}$ is said to be *trivial* if and only if $(\boldsymbol{v}|0) \in \mathrm{rowsp}^+(A|\boldsymbol{\lambda})$ for some $\boldsymbol{v} \in \mathrm{rowsp}^+(A)$ with $H(\boldsymbol{v}) = 2$, and *non-trivial* otherwise. We only work with non-trivial 2-regular system and in this case it is easy to verify that (12) is applicable.

The Partite Case. For the special case of 2-CARP systems, we provide a finer version of Lemma 4, and hence, a finer version of Theorem 1. Let

$$\nabla_{\hat{\mathcal{R}}} \coloneqq \max_{\substack{a,b\in[2],\ d\in\mathbb{F}_N,\ \circ\in\{\oplus,\ominus\} \\ d\neq 0 \text{ if } a=b}} \left|\{(x_1, x_2) \in \hat{\mathcal{R}}_a \times \hat{\mathcal{R}}_b : x_1 \circ x_2 = d\}\right|.$$

Lemma 6. *Suppose $\mathbb{S}$ is 2-CARP and satisfies $s + q \leq N/4$. If $\mathbb{S}_i$ is isolated, then, we have*

$$\eta(\mathbb{S}_{\leq i} \,|\, \mathcal{R}) \geq \frac{\prod_{j=1}^{2}(N - f_{\leq(i-1),j})}{N}\,(1 - \epsilon)\,\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}),$$

where

$$\epsilon \leq \frac{2}{N}\left|\mu_{\alpha_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}) - \frac{|\mathcal{R}_1 \times \mathcal{R}_2|}{N}\right| + \frac{12(s+q)(\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}})}{N^2} + \frac{24(s+q)^3}{N^3}$$

A proof of this lemma is available in Appendix B.4. Note that it is not a coincidence that the bound in Lemma 6 is additionally parametrized by $\Delta_{\mathbb{S}}$ and

$\nabla_{\hat{\mathcal{R}}}$. This becomes evident when comparing them to the analogous definitions in Section 2.2. When $\mathbb{S}$ and $\hat{\mathcal{R}}$ are random, this fine-grained analysis yields a tighter bound. This is precisely why we preserved the sum-capture term as well.

Corollary 3. *If $\mathbb{S}$ is 2-CARP, non-trivial and satisfies $s+q \le N/4$ and $\xi_{\mathbb{S}}(s+q) \le N/2$, then, we have $\eta(\mathbb{S}\,|\,\mathcal{R}) \ge (1-\varepsilon)\,\mathbb{E}\,(\mathbb{S}\,|\,\mathcal{R})$, where*

$$\varepsilon \le \sum_{i \notin \mathtt{NI}(\mathbb{S})} \frac{2}{N} \left| \mu_{\alpha_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}) - \frac{|\mathcal{R}_1 \times \mathcal{R}_2|}{N} \right| + \frac{12q(s+q)(\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}})}{N^2} + \frac{24q(s+q)^3}{N^3} + \left(\frac{2(s+q)^2}{N^2} + \frac{1}{N} \right) \sum_{j \in \mathtt{NI}(\mathbb{S})} r_j^2.$$

The corollary follows from Lemma 6 for the isolated blocks. For a non-isolated block $\mathbb{S}_j$, the derivation of (24) (cf. Appendix B.3) with $t = 2$ applies verbatim, as $\mathtt{H}(\overline{A}_j) = 2$ by Proposition 3, and (12) applies to the at most $r_j^2/2$ pairs in EQ due to non-triviality. This gives the factor $1 - 2r_j^2(s+q)^2/N^2 - r_j^2/N$ for $\mathbb{S}_j$.

The Clique Case. Similarly, a refinement is possible for 2-CARC systems. Let

$$\nabla_{\hat{\mathcal{R}}} \coloneqq \max_{\substack{d \in \mathbb{F}_N \setminus \{0\} \\ \circ \in \{\oplus, \ominus\}}} \left| \{(x_1, x_2) \in \hat{\mathcal{R}}^2 : x_1 \circ x_2 = d\} \right|$$

Corollary 4. *If $\mathbb{S}$ is 2-CARC, non-trivial and satisfies $s+2q \le N/4$ and $\xi_{\mathbb{S}}(s+2q) \le N/2$, then, we have $\eta(\mathbb{S}\,|\,\mathcal{R}) \ge (1-\varepsilon)\,\mathbb{E}\,(\mathbb{S}\,|\,\mathcal{R})$, where*

$$\varepsilon \le \frac{4q}{N} + \frac{2}{N} \sum_{i \notin \mathtt{NI}(\mathbb{S})} \left| \mu_{\alpha_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}) - \frac{|\mathcal{R}|^2}{N} \right| + \frac{12q(s+2q)(\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}})}{N^2} + \frac{24q(s+2q)^3}{N^3} + \left(\frac{2(s+2q)^2}{N^2} + \frac{1}{N} \right) \sum_{j \in \mathtt{NI}(\mathbb{S})} r_j^2.$$

A proof of this corollary is available in Appendix B.5.

6 Single-keyed Double-block Hash-then-Sum

Let $\mathcal{X}_0, \mathcal{X}_1, \mathcal{X}_2 \subseteq \{0,1\}^*$ be finite sets, and let $e_j : \mathcal{X}_j \to \{0,1\}^n$, for $0 \le j \le 2$, be injective encodings with pairwise disjoint image sets. For a permutation π of $\{0,1\}^n$, we define three injective functions $\pi_j \coloneqq \pi \circ e_j : \mathcal{X}_j \to \{0,1\}^n$, for $0 \le j \le 2$. So, π_0, π_1 and π_2 are restrictions of a single permutation to disjoint parts of its domain.

For $0 \le j \le 2$, we define $\mathcal{I}_j(n) \coloneqq \{\pi_j : \pi \in \mathcal{P}(n)\}$. For some permutation π of $\{0,1\}^n$ and a rate-c^{-1} permutation-based diblock hash function $H : \mathcal{I}_0(n) \times \{0,1\}^* \to \mathcal{X}_1 \times \mathcal{X}_2$, we define the single-keyed $\mathtt{DBHtS}$ construction, denoted $\mathtt{1k\text{-}DBHtS}_{\pi,H}$, by the mapping:

$$m \mapsto \pi_1(H^1_{\pi_0}(m)) \oplus \pi_2(H^2_{\pi_0}(m)). \tag{13}$$

We drop the parameters π and H whenever they are clear from the context.

Remark 2. The definition of 1k-DBHtS in (13) uses the encodings e_0, e_1 and e_2 (in our instantiation, (up to) two bits) to separate the input domains of the permutation calls in the hash function and the two finalization calls. This slight deviation from the more conventional definition was made to simplify the analysis by avoiding additional hash-based bad events. For instance, in the absence of domain separation, a hash-half can potentially collide with a permutation input within the hash computation, or there can be cross-collisions between the two halves of the hash values. The analysis of these additional bad events would most likely require an integration of sophisticated techniques like reset-sampling [9,10] with the constrained system formalism, which is beyond the scope of this paper. As a side-effect of the domain separation, we are able to more closely mirror the elegant analyses [37] by Kim et al. of the PMAC+ and LightMAC+ hash functions. Note that, the analysis due to Dutta et al. [23] on two-keyed DBHtS seems inapplicable in our case due to its abstract hash assumptions.

Theorem 3 below shows that 1k-DBHtS is a secure PRF for $\overline{\sigma} \ll 2^{3n/4}/n^{1/4}$, assuming appropriate hash function bounds. While constants may be slightly improved, this bound on the number of queried blocks is tight up to a factor of $n^{1/4}$, as the attack [38] on DBHtS makes $O(2^{3n/4})$ queries, each of a constant number of blocks.

Theorem 3. *Let $c, q, \ell, \sigma \geq 0$ satisfying $q, \ell \leq \sigma$ and $\overline{\sigma} = c\sigma + 2q \leq 2^{n-3}$. Suppose $H : \mathcal{I}_0(n) \times \{0,1\}^* \to \mathcal{X}_1 \times \mathcal{X}_2$ is a rate-c^{-1} $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-CFH. Then, for $\rho = (q, \ell, \sigma)$ and $\rho' = (2, \ell, 2\ell)$, the PRF advantage of any ρ-distinguisher $\mathcal{A}$ against $\texttt{1k-DBHtS}_{\Pi,H}$ satisfies $\mathbf{Advt}^{\mathrm{prf}}_{\texttt{1k-DBHtS}_{\Pi,H}}(\mathcal{A}) \leq \varepsilon_1 + \varepsilon_2$, where*

$$\varepsilon_1 \coloneqq 2\epsilon_2(\rho) + \delta(\rho) + \frac{q + q^2\epsilon_1(\rho')}{2^n} + \frac{q^2\epsilon_1(\rho')}{4\overline{\sigma}} + 2\epsilon_3\left(\rho, \lceil 2^n/4\overline{\sigma} \rceil\right),$$
$$\varepsilon_2 \coloneqq \frac{18q^2\overline{\sigma}^2\epsilon_1(\rho')}{2^{2n}} + \frac{9q^2\epsilon_1(\rho')}{2^n} + \frac{q\overline{\sigma}}{2^{\frac{3n-4}{2}}} + \frac{126nq\overline{\sigma}}{2^{2n}} + \frac{96nq\overline{\sigma}^3}{2^{3n}} + \frac{4q}{2^n}.$$

Proof. Let

- $\mathsf{M}^i \coloneqq (\mathsf{M}^i_1, \ldots, \mathsf{M}^i_{\ell_i})$ denote the i-th query of the distinguisher.
- T^i denote the i-th response of the oracle.

The oracle releases additional information to the distinguisher, once the distinguisher is done querying the oracle, but before it outputs its decision bit.

In the real world, the oracle releases:

- $\mathsf{X}^i \coloneqq (\mathsf{X}^i_1, \mathsf{X}^i_2) = H_{\Pi_0}(\mathsf{M}^i)$ for each $i \in [q]$.
- $\mathsf{Y}^i \coloneqq (\mathsf{Y}^i_1, \mathsf{Y}^i_2) = (\Pi_1(\mathsf{X}^i_1), \Pi_2(\mathsf{X}^i_2))$ for each $i \in [q]$.
- $\mathcal{R}$, the set of all image points sampled during the computation of $H_{\Pi_0}(\mathsf{M}^i)$ for all $i \in [q]$, along with the corresponding input points. Since H is a rate-c^{-1} hash function, $|\mathcal{R}| \leq c\sigma$ for M.

Thus, the real world transcript is given by $\Theta_{\mathrm{re}} \coloneqq ((\mathsf{M}^i, \mathsf{T}^i, \mathsf{X}^i, \mathsf{Y}^i : i \in [q]), \mathcal{R})$.
In the ideal world, the oracle first samples a dummy random permutation Π', and then computes $\mathsf{X}^i \coloneqq H_{\Pi'_0}(\mathsf{M}^i)$ for all $i \in [q]$. In other words, X^i is generated

faithfully for all $i \in [q]$. Note that, $\mathcal{R}$ can be derived here as well, as the ideal oracle is faithfully generating the hash outputs.

Sampling Y in the ideal world: The sampling mechanism for Y^i is on the other hand a bit more sophisticated. The goal is to sample Y^i's in such a way that $(\mathsf{X}_1^i = \mathsf{X}_1^j \iff \mathsf{Y}_1^i = \mathsf{Y}_1^j)$ and $(\mathsf{X}_2^i = \mathsf{X}_2^j \iff \mathsf{Y}_2^i = \mathsf{Y}_2^j)$ is satisfied for all $i \neq j \in [q]$. We refer to this predicate as the *permutation compatibility* or PC *condition*.

For any $i \in [q]$, let $(i)_1 \coloneqq \min\{j \leq i \ : \ \mathsf{X}_1^i = \mathsf{X}_1^j\}$ and $(i)_2 \coloneqq \min\{j \leq i \ : \ \mathsf{X}_2^i = \mathsf{X}_2^j\}$. Let $r = |\{(i)_1 \ : \ i \in [q]\}| + |\{(i)_2 \ : \ i \in [q]\}|$. Consider the 2-regular and binary, $(q, r, 1)$-constrained system $\mathbb{S} \coloneqq \{\mathsf{Y}_1^{(i)_1} \oplus \mathsf{Y}_2^{(i)_2} = \mathsf{T}^i : i \in [q]\}$.

Any $\overline{\mathcal{R}}$-solution for $\mathbb{S}$ satisfies the PC condition, apart from fully defining Y. As long as the system is acyclic and non-trivial, we can use the results developed in the previous section. Keeping this in mind, we now define some bad predicates on the partial transcript $((\mathsf{M}^i, \mathsf{T}^i, \mathsf{X}^i : i \in [q]), \mathcal{R})$:

$$\mathsf{A}_1 : \exists \,\text{distinct}\, i,j,k,l \in [q],\ \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{X}_2^j = \mathsf{X}_2^k \wedge \mathsf{X}_1^k = \mathsf{X}_1^l.$$
$$\mathsf{A}_2 : \exists \,\text{distinct}\, i,j \in [q],\ \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{T}^i \oplus \mathsf{T}^j = 0^n.$$
$$\mathsf{A}_3 : \exists \,\text{distinct}\, k \geq 2^{n-2}/(c\sigma + 2q), i_1, \ldots, i_k \in [q],\ \mathsf{X}_1^{i_1} = \mathsf{X}_1^{i_2} = \ldots = \mathsf{X}_1^{i_k}.$$
$$\mathsf{B}_1 : \exists \,\text{distinct}\, i,j,k,l \in [q],\ \mathsf{X}_2^i = \mathsf{X}_2^j \wedge \mathsf{X}_1^j = \mathsf{X}_1^k \wedge \mathsf{X}_2^k = \mathsf{X}_2^l.$$
$$\mathsf{B}_2 : \exists \,\text{distinct}\, i,j \in [q],\ \mathsf{X}_2^i = \mathsf{X}_2^j \wedge \mathsf{T}^i \oplus \mathsf{T}^j = 0^n.$$
$$\mathsf{B}_3 : \exists \,\text{distinct}\, k \geq 2^{n-2}/(c\sigma + 2q), i_1, \ldots, i_k \in [q],\ \mathsf{X}_2^{i_1} = \mathsf{X}_2^{i_2} = \ldots = \mathsf{X}_2^{i_k}.$$
$$\mathsf{C} : \exists \,\text{distinct}\, i \in [q],\ \mathsf{T}^i = 0^n.$$
$$\mathsf{D} : \exists \,\text{distinct}\, i,j \in [q],\ \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{X}_2^i = \mathsf{X}_2^j.$$
$$\mathsf{E} : \exists \,\text{distinct}\, i,j,k \in [q],\ \mathsf{X}_1^i = \mathsf{X}_1^j \wedge \mathsf{X}_2^j = \mathsf{X}_2^k \wedge \mathsf{T}^i \oplus \mathsf{T}^j \oplus \mathsf{T}^k = 0^n.$$

Define $\mathsf{Cyclic} \coloneqq \mathsf{A}_1 \vee \mathsf{B}_1 \vee \mathsf{D}$, $\mathsf{Trivial} \coloneqq \mathsf{A}_2 \vee \mathsf{B}_2 \vee \mathsf{C} \vee \mathsf{E}$, and $\mathsf{Giant} \coloneqq \mathsf{A}_3 \vee \mathsf{B}_3$. It is not difficult to see that as long as Cyclic, $\mathsf{Trivial}$, and Giant are false, $\mathbb{S}$ is acyclic and non-trivial, and satisfies $\xi_{\mathbb{S}}\overline{\sigma} \leq 2^{n-1}$. Indeed, due to $\neg(\mathsf{A}_1 \vee \mathsf{B}_1)$, each block consists of at most two non-singleton equivalence classes (one for each half) that share at most one query, and thus has less than $2 \cdot 2^{n-2}/\overline{\sigma}$ variables due to $\neg\mathsf{Giant}$. For notational convenience, let $s = |\mathcal{R}|$, and note that $s + 2q \leq \overline{\sigma} \leq 2^{n-3}$.

Sampling Y*:* Onwards we describe the sampling of Y conditioned on the fact that $\neg(\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant})$ holds. Let $\mathrm{BDF}(\mathbb{S}) = (\mathbb{S}_1 \prec \ldots \prec \mathbb{S}_c)$ such that all the isolated components appear before the non-isolated ones. Let $\mathtt{NI}(\mathbb{S})$ denote the set of all non-isolated components. We define $\mathsf{Y} \twoheadleftarrow (\mathbb{S} \,|\, \mathcal{R})$. This concludes the sampling in the ideal world, and finally the ideal world transcript is given by $\Theta_{\mathrm{id}} \coloneqq ((\mathsf{M}^i, \mathsf{T}^i, \mathsf{X}^i, \mathsf{Y}^i : i \in [q]), \mathcal{R})$ where the PC condition is satisfied as long as $\neg(\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant})$ holds; otherwise the transcript is defined arbitrarily.

(Bad) Transcript Definition and Analysis: A transcript ω is said to be *bad*, i.e., $\omega \in \Omega_{\mathrm{bad}}$ if and only if it satisfies $\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant}$, and *good* otherwise.

Lemma 7. *Suppose H is an $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-CFH. Then*

$$\Pr\left(\Theta_{\mathrm{id}} \in \Omega_{\mathrm{bad}}\right) \leq 2\epsilon_2(\rho) + \delta(\rho) + \frac{q + q^2\epsilon_1(\rho')}{2^n} + \frac{q^2\epsilon_1(\rho')}{4\overline{\sigma}} + 2\epsilon_3\left(\rho, \left\lceil \frac{2^{n-2}}{\overline{\sigma}} \right\rceil\right).$$

A proof of this lemma follows from the coverfree property of H and uniformity of T, and can be found in Appendix C.1.

Lemma 8. *For any $\omega \in \Omega_{\mathrm{good}}$ we have $\Pr\left(\Theta_{\mathrm{re}} = \omega\right) \geq (1 - \varepsilon(\omega)) \Pr\left(\Theta_{\mathrm{id}} = \omega\right)$, where*

$$\varepsilon(\omega) \leq \frac{4q}{2^n} + \frac{2}{2^n} \sum_{i \notin \mathtt{NI}(\mathbb{S})} \left| \mu(\mathsf{T}^{(i)}, \mathcal{R}) - \frac{|\mathcal{R}|^2}{2^n} \right| + \frac{12q(s+2q)(\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}})}{2^{2n}} + \frac{24q(s+2q)^3}{2^{3n}} + \left(\frac{2(s+2q)^2}{2^{2n}} + \frac{1}{2^n}\right) \sum_{j \in \mathtt{NI}(\mathbb{S})} r_j^2.$$

The proof of this lemma follows from the bound for 2-CARC systems, Corollary 4. A detailed proof is available in Appendix C.2. To apply Corollary 1, we have to compute the following expectations

$$\mu := \mathbb{E}\left(\frac{2}{2^n} \sum_{i \notin \mathtt{NI}(\mathbb{S})} \left| \mu(\mathsf{T}^{(i)}, \mathcal{R}) - \frac{|\mathcal{R}|^2}{N} \right|\right) \qquad \delta := \mathbb{E}\left(\Delta_{\mathbb{S}}\right)$$

$$\nu := \left(\frac{2(s+2q)^2}{2^{2n}} + \frac{1}{2^n}\right) \mathbb{E}\left(\sum_{j \in \mathtt{NI}(\mathbb{S})} r_j^2\right) \qquad \gamma := \mathbb{E}\left(\nabla_{\mathcal{R}}\right)$$

Using Proposition 6, $q \leq 2^n$, and the fact that T is sampled with replacement, we have $\delta \leq 4n$. For γ, note that once T is fixed, the messages are fixed, and $\mathcal{R}$ is the set of outputs of Π'_0 at the s distinct inputs queried during the hash computation, where Π' is independent of T. Extending these queries by arbitrary fresh queries to exactly $\overline{\sigma}$ distinct inputs gives a set $\mathcal{R}^+ \supseteq \mathcal{R}$ of $\overline{\sigma}$ values sampled without replacement, and clearly $\nabla_{\mathcal{R}} \leq \nabla_{\mathcal{R}^+}$. Thus, $\gamma \leq 6n(\overline{\sigma}^2/2^n + 1)$ by Proposition 7, as $\overline{\sigma} \leq 2^{n-3}$. We claim

$$\nu \leq \frac{18q^2(s+2q)^2\epsilon_1(2, \ell, 2\ell)}{2^{2n}} + \frac{9q^2\epsilon_1(2, \ell, 2\ell)}{2^n}. \tag{14}$$

A proof of the claim in (14) is available in Appendix C.3. Next, we bound μ (here, $\varepsilon(\omega)$ is set to 0 on bad transcripts). On a good transcript, $\mathsf{T}^i \neq 0^n$ for all $i \in [q]$ due to $\neg\mathsf{C}$, so the diagonal pairs (a, a) do not contribute to $\mu(\mathsf{T}^i, \mathcal{R})$, i.e., $\mu(\mathsf{T}^i, \mathcal{R}) = \mu^*(\mathsf{T}^i, \mathcal{R}) := |\{(a, b) \in \mathcal{R}^2 : a \neq b, a \oplus b = \mathsf{T}^i\}|$. Moreover, each isolated component of $\mathbb{S}$ is a single equation with constant T^i for a distinct $i \in [q]$. As all the summands are non-negative, we have

$$\mu \leq \frac{2}{2^n} \sum_{i=1}^{q} \mathbb{E}\left(1_{\mathsf{T}^i \neq 0^n} \left| \mu^*(\mathsf{T}^i, \mathcal{R}) - \frac{|\mathcal{R}|^2}{2^n} \right|\right),$$

where the sum is now over a fixed index set. We claim that for all $i \in [q]$

$$\mathbb{E}\left(1_{\mathsf{T}^i \neq 0^n}\left|\mu^*(\mathsf{T}^i, \mathcal{R}) - \frac{|\mathcal{R}|^2}{2^n}\right|\right) \leq \frac{8\overline{\sigma}}{5 \cdot 2^{n/2}} + \frac{\overline{\sigma}}{2^n} + \frac{4\overline{\sigma}^3}{2^{2n}}. \tag{15}$$

A proof of the claim in (15) is given in Appendix C.4. Thus, $\mu \leq 16q\overline{\sigma}/(5{\cdot}2^{3n/2}) + 2q\overline{\sigma}/2^{2n} + 8q\overline{\sigma}^3/2^{3n}$, and $12q(s+2q)(\delta+\gamma)/2^{2n} \leq 120nq\overline{\sigma}/2^{2n} + 72nq\overline{\sigma}^3/2^{3n}$. Theorem 3 then follows from Lemma 7 and 8, and (14)-(15), using $s + 2q \leq \overline{\sigma} \leq 2^{n-3}$ and $n \geq 2$. □

7 Instantiations of Cover-free Hash functions

We identify $\{0,1\}^n$ with the field $\mathbb{F}_{2^n}$, defined by an irreducible polynomial $p(x)$ of degree n, where the first (leftmost) bit of a string is the coefficient of x^{n-1}, and 2 denotes the element x. For any $k \in \mathbb{N}^+$ and $i \in \{0, \ldots, 2^k - 1\}$, let $\langle i \rangle_k$ denote the unsigned k-bit representation of i. For any $x \in \{0,1\}^*$ and $k \in \mathbb{N}^+$, we write $(x[1], \ldots, x[m]) \leftarrow_k x$ to denote the k-bit parsing of $x\|1\|0^{k-1-|x| \mod k}$, where $x[1]\|x[2]\|\ldots\|x[m] = x\|1\|0^{k-1-|x| \mod k}$, and $|x[i]| = k$ for all $i \in [m]$.

The sets $\mathcal{X}_0$, $\mathcal{X}_1$ and $\mathcal{X}_2$ from section 6 are instantiated with $\mathcal{X}_0 = \mathcal{X}_2 = \{0,1\}^{n-2}$ and $\mathcal{X}_1 = \{0,1\}^{n-1}$, and the the three injective encodings are instantiated with $e_0(x) = 00\|x$,$e_1(y) = 1\|y$ and $e_2(x) = 01\|x$.

For a diblock hash function $H : \mathcal{I}_0(n) \times \{0,1\}^* \to \{0,1\}^n \times \{0,1\}^n$ we can construct the truncated diblock hash $\mathtt{T}H : \mathcal{I}_0(n) \times \{0,1\}^* \to \{0,1\}^{n-1} \times \{0,1\}^{n-2}$ as $\mathtt{T}H(x) := (\mathtt{Trunc}_1(H_1(x)), \mathtt{Trunc}_2(H_2(x)))$, where $\mathtt{Trunc}_1 : \{0,1\}^n \to \{0,1\}^{n-1}$ and $\mathtt{Trunc}_2 : \{0,1\}^n \to \{0,1\}^{n-2}$ truncate the first bit and the first two bits of their n-bit input, respectively.

7.1 TLightHash and TPHash

We define the functions $\mathtt{PHash} : \mathcal{I}_0(n) \times \{0,1\}^* \to \{0,1\}^n \times \{0,1\}^n$ and $\mathtt{LightHash} : \mathcal{I}_0(n) \times \{0,1\}^* \to \{0,1\}^n \times \{0,1\}^n$, in Algorithm 1.
Here, $3 \leq s \leq n-1$, and LightHash is only defined for messages whose padded length is $k \leq 2^{s-2} - 1$ blocks, so that the counter $\langle i \rangle_{s-2}$ is well defined. As in Section 2.3, ℓ and σ count n-bit blocks, whereas LightHash (res. PHash) parses a message of b bits into $\lfloor b/(n-s) \rfloor + 1$ (res. $\lfloor b/(n-2) \rfloor + 1$) blocks, which we call *parsed blocks*. As a message with k blocks has at most nk bits, for $\rho = (q, \ell, \sigma)$, the messages of a ρ-distinguisher have at most $\hat{\ell} := \lfloor n\ell/(n-s) \rfloor + 1$ parsed blocks each, and at most $\hat{\sigma} := \lfloor n\sigma/(n-s) \rfloor + q$ parsed blocks in total, for LightHash, and the same holds with $s = 2$ for PHash. Our analysis works with parsed blocks, so the conditions and bounds below are stated in terms of $\hat{\ell}$ and $\hat{\sigma}$. Note that $\hat{\ell} \leq 3\ell$ and $\hat{\sigma} \leq 3\sigma$ whenever $s \leq n/2$. LightHash makes one call to Π_0 per block, whereas PHash makes two additional calls, $\Pi_0(0)$ and $\Pi_0(1)$, which are the same for all messages. In PHash, 0 and 1 denote $\langle 0 \rangle_{n-2}$ and $\langle 1 \rangle_{n-2}$, and the masks are computed in $\mathbb{F}_{2^n}$ from the full outputs Δ_0 and Δ_1, and then truncated, so that $W[i]$ is an $(n-2)$-bit input of Π_0.

Algorithm 1 The `PHash` and `LightHash` functions.

function $\texttt{PHash}_{\Pi_0}(m)$
  $(m[1], \cdots, m[k]) \leftarrow_{n-2} m$
  $x[1] \leftarrow 0,\ x[2] \leftarrow 0$
  $\Delta_0 \leftarrow \Pi_0(0)$
  $\Delta_1 \leftarrow \Pi_0(1)$
  for $i = 1 \ldots k$ **do**
    $\Lambda_i \leftarrow 2^i \Delta_0 \oplus 2^{2i} \Delta_1$
    $W[i] \leftarrow m[i] \oplus \texttt{Trunc}_2(\Lambda_i)$
    $Z[i] \leftarrow \Pi_0(W[i])$
    $x[1] \leftarrow x[1] \oplus Z[i]$
    $x[2] \leftarrow 2 \cdot (x[2] \oplus Z[i])$
  return $(x[1], x[2])$

function $\texttt{LightHash}_{\Pi_0}(m)$
  $(m[1], \cdots, m[k]) \leftarrow_{n-s} m$
  $x[1] \leftarrow 0,\ x[2] \leftarrow 0$
  for $i = 1 \ldots k$ **do**
    $Z[i] \leftarrow \Pi_0(\langle i \rangle_{s-2} \| m[i])$
    $x[1] \leftarrow x[1] \oplus Z[i]$
    $x[2] \leftarrow 2 \cdot (x[2] \oplus Z[i])$
  return $(x[1], x[2])$

Remark 3. In the previous version of this paper, [16, Algorithm 1] used the accumulator $x[2] \leftarrow 2 \cdot x[2] \oplus Z[i]$ (after a typographical correction), finally truncating both halves to $n-2$ bits, and claimed CfH bounds for the resulting hash functions up to $2^{3n/4}/n^{1/4}$ blocks of queries. These claims are false, and we withdraw them. Indeed, consider two messages of the same length that differ only in their last (padded) block. In both hash functions, the last block output $Z[k]$ then entered both $x[1]$ and $x[2]$ with coefficient 1, and all the other terms are common to both messages. So, the two hash values differ by (δ, δ), where $\delta = Z[k] \oplus Z'[k]$ and $Z[k]$ and $Z'[k]$ are the outputs of Π_0 at two distinct inputs. As the same truncation was applied to both halves, the truncated hash values collide in both halves if and only if the last $n-2$ bits of δ are zero, which happens with probability about $3/2^n$. Since a full hash collision implies a tag collision, a distinguisher that makes roughly $2^{n/2}$ such queries and looks for a tag collision achieves a constant advantage. The flaw in our earlier analysis was in the rank argument for the double collision event, which overlooks messages differing in a single block.

A requirement on the underlying field. Our analyses compares coefficients of the form 2^e and their sums. Throughout, we assume that $p(x)$ is primitive, i.e., that 2 generates the multiplicative group of $\mathbb{F}_{2^n}$, so that the powers 2^e that we compare are pairwise distinct (as $\hat{\ell} \leq 2^{n-3}$). For $k \in \mathbb{N}^+$, we say that $p(x)$ satisfies:

- *trinomial-freeness*, denoted TF_k, if $p(x)$ does not divide any trinomial of degree at most $2k$.
- *strong-quadrinomial-freeness*, denoted SQF_k, if $p(x)$ satisfies TF_k, and additionally, it does not divide any quadrinomial of degree at most k.

For `TLightHash` and for `TPHash`, we require $\mathsf{TF}_{\hat{\ell}}$ and $\mathsf{SQF}_{\hat{\ell}}$, respectively. Clearly, $\mathsf{TF}_{\hat{\ell}}$ and $\mathsf{SQF}_{\hat{\ell}}$ holds whenever $2\hat{\ell} < n$. The standard primitive polynomials $p(x) = x^{128} \oplus x^7 \oplus x^2 \oplus x \oplus 1$ and $p(x) = x^{64} \oplus x^4 \oplus x^3 \oplus x \oplus 1$ satisfy $\mathsf{TF}_{\hat{\ell}}$ for all $\hat{\ell} \leq 2^{19}$ and $\mathsf{SQF}_{\hat{\ell}}$ for all $\hat{\ell} \leq 2^{18}$. In general, it can be shown that, for

every n, primitive polynomials satisfying these conditions exist for fairly large $\hat{\ell}$. Moreover, such conditions seem unavoidable. For instance, if $2^e = 1 \oplus 2^{-1}$ for some $e \leq \hat{\ell}$, then for two messages of e parsed blocks that differ only in their first block, both truncated halves collide with probability $1/(2^n - 1)$, and the birthday attack of Remark 3 applies.

Lemma 9. *Let $\rho = (q, \ell, \sigma)$ with $\hat{\ell} \leq \min\{2^{s-2} - 1, 2^{n-3}\}$, and suppose that $p(x)$ satisfies $\mathsf{TF}_{\hat{\ell}}$. Then, $\mathtt{TLightHash}^{\Pi_0}$ satisfies the conditions of an $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-CfH for ρ, where*

$$\epsilon_1(\rho) = \frac{4q^2}{2^n}, \qquad \epsilon_3(\rho, k) = \frac{16q^2}{k^2 \cdot 2^n}, \qquad \delta(\rho) = \frac{16q^2}{2^{2n}},$$
$$\epsilon_2(\rho) = \frac{256q^4}{2^{3n}} + \frac{22q^2}{2^{3n/2}} + \frac{2^{11}q^2}{2^{2n}}.$$

A proof of this result is given in Appendix D. It follows a rank-based approach similar to the one used in [53,37]. As the truncations ignore a few bits, each event in the CfH definition becomes the event that some linear combinations of the outputs of Π_0 lie in small subspaces (rather than being zero), and the main new step is to rule out the double collisions that invalidated the earlier construction (see Remark 3).

Lemma 10. *Let $\rho = (q, \ell, \sigma)$ with $\hat{\ell} \leq 2^{n-3} - 1$, and suppose that $p(x)$ satisfies $\mathsf{SQF}_{\hat{\ell}}$. Then, $\mathtt{TPHash}^{\Pi_0}$ satisfies the conditions of an $(\epsilon_1, \epsilon_2, \epsilon_3, \delta)$-CfH for ρ, where*

$$\epsilon_1(\rho) = \frac{20q^2}{2^n} + \frac{64\hat{\ell}^2q^2}{2^{2n}}, \qquad \epsilon_3(\rho, k) = \frac{1}{k^2}\left(\frac{80q^2}{2^n} + \frac{256\hat{\ell}^2q^2}{2^{2n}}\right),$$
$$\delta(\rho) = \frac{(4\hat{\ell} + 12)\hat{\sigma}}{2^n} + \frac{80q^2}{2^{2n}} + \frac{128\hat{\ell}^2q^2}{2^{3n}},$$
$$\epsilon_2(\rho) = \frac{(8\hat{\ell} + 24)\hat{\sigma}}{2^n} + \frac{68q^2}{2^{3n/2}} + \frac{1936q^2}{2^{2n}} + \frac{310\hat{\ell}^2q^2}{2^{5n/2}} + \frac{5120\hat{\ell}^2q^4}{2^{3n}}.$$

The proof (see Appendix D) reduces to that of Lemma 9. Unlike in `LightHash`, the masked inputs $W[i]$ of two messages can collide at distinct positions. Conditioned on $\Pi_0(0)$ and $\Pi_0(1)$, a set of messages without such collisions behaves exactly as in `LightHash`, and the remaining cases are handled using the randomness of the masks, as in [37].

7.2 Instantiating `1k-DBHtS`

For any $\pi \in \mathcal{P}(n)$, we define

$$\texttt{1k-PMAC+}_\pi := \texttt{1k-DBHtS}_{\pi,\texttt{TPHash}} \qquad \texttt{1k-LightMAC+}_\pi := \texttt{1k-DBHtS}_{\pi,\texttt{TLightHash}}$$

Using Lemma 9 in Theorem 3 (where we use $\epsilon_3(\rho, \lceil x \rceil) \leq \epsilon_3(\rho, x)$, as the bounds on $\epsilon_3(\rho, k)$ in Lemma 9 and 10 decrease in k) we have:

Corollary 5. *Let $q, \ell, \sigma \geq 0$ satisfying $q, \ell \leq \sigma$, $\hat{\ell} \leq 2^{s-2} - 1$ and $\overline{\sigma} = \hat{\sigma} + 2q \leq 2^{n-3}$, and suppose that $p(x)$ satisfies $\mathsf{TF}_{\hat{\ell}}$. Then, for $\rho = (q, \ell, \sigma)$, the PRF advantage of any ρ-distinguisher $\mathcal{A}$ against $\mathtt{1k\text{-}LightMAC+}_{\Pi}$ satisfies*

$$\mathbf{Advt}^{\mathrm{prf}}_{\mathtt{1k\text{-}LightMAC+}_{\Pi}}(\mathcal{A}) \leq \frac{7q}{2^n} + \frac{26q\overline{\sigma}}{2^{3n/2}} + \frac{4272q^2 + 126nq\overline{\sigma}}{2^{2n}} + \frac{928q^2\overline{\sigma}^2 + 96nq\overline{\sigma}^3}{2^{3n}}.$$

Here, $\overline{\sigma}$ plays the role of $c\sigma + 2q$ in Theorem 3, as its proof only uses that $|\mathcal{R}| + 2q \leq \overline{\sigma}$ (and $|\mathcal{R}| \leq \hat{\sigma}$), and we used $2q \leq \overline{\sigma}$ to simplify a few terms. As $\overline{\sigma} \leq 5\sigma$ for $s \leq n/2$, `1k-LightMAC+` is secure up to $O(2^{3n/4}/n^{1/4})$ blocks of queries, without any factor of ℓ, for all message lengths ℓ for which $\mathsf{TF}_{\hat{\ell}}$ holds. Similarly, using Lemma 10 in Theorem 3 we have:

Corollary 6. *Let $q, \ell, \sigma \geq 0$ satisfying $q, \ell \leq \sigma$, $\hat{\ell} \leq 2^{n-3}-1$ and $\overline{\sigma} = \hat{\sigma}+2q+2 \leq 2^{n-3}$, and suppose that $p(x)$ satisfies $\mathsf{SQF}_{\hat{\ell}}$. Then, for $\rho = (q, \ell, \sigma)$, the PRF advantage of any ρ-distinguisher $\mathcal{A}$ against $\mathtt{1k\text{-}PMAC+}_{\Pi}$ satisfies*

$$\begin{aligned}\mathbf{Advt}^{\mathrm{prf}}_{\mathtt{1k\text{-}PMAC+}_{\Pi}}(\mathcal{A}) \leq{}& \frac{(28\hat{\ell} + 85)\overline{\sigma}}{2^n} + \frac{140q\overline{\sigma}}{2^{3n/2}} + \frac{4752q^2 + 126nq\overline{\sigma}}{2^{2n}} + \frac{3308\hat{\ell}^2q^2}{2^{5n/2}} \\ &+ \frac{4000q^2\overline{\sigma}^2 + 96nq\overline{\sigma}^3 + 10240\hat{\ell}^2q^4}{2^{3n}} + \frac{12800\hat{\ell}^2q^2\overline{\sigma}^2}{2^{4n}}.\end{aligned}$$

Here, $\overline{\sigma}$ also accounts for the two calls $\Pi_0(0)$ and $\Pi_0(1)$, as the proof of Theorem 3 only uses that $|\mathcal{R}| + 2q \leq \overline{\sigma}$, and we used $q \leq \overline{\sigma}$ and $\hat{\ell} \leq 2^{n-3}$ to simplify a few terms. As $\hat{\ell} \leq 3\ell$ and $\overline{\sigma} \leq 7\sigma$, `1k-PMAC+` is secure as long as $\ell\sigma \ll 2^n$ and $\sigma \ll \min\{2^{3n/4}/n^{1/4}, 2^{3n/4}/\ell^{1/2}\}$, for all message lengths ℓ for which $\mathsf{SQF}_{\hat{\ell}}$ holds. The dependence on ℓ is similar to that of the bound for `PMAC+` in [37].

8 PRF Security of Sum of r Even-Mansour

For any $r \geq 2$, let $\pi = (\pi_1, \ldots, \pi_r) \twoheadleftarrow \mathcal{P}(n)^r$ be a tuple of r permutations of $\{0,1\}^n$. For any key $K = (K_1, \ldots, K_r) \in (\{0,1\}^n)^r$ and any $m \in \{0,1\}^n$, the r-sum of Even-Mansour construction, denoted $\mathtt{SOEM}^r[\pi]$, is defined by the mapping

$$m \longmapsto \bigoplus_{i=1}^{r} \pi_i(m \oplus K_i). \tag{16}$$

This construction is motivated by the $r = 2$ case proposed [50] by Sibleyras and Todo. We analyze the PRF security of the construction for any arbitrary $r \geq 2$.

Theorem 4. *Fix some $2 \leq r < n$, $q + p \leq 2^{\frac{r}{r+1}n - \log_2(n)}$, and $\Pi \twoheadleftarrow \mathcal{P}(n)^r$. For any (q,p)-distinguisher $\mathcal{A}$ we have*

$$\begin{aligned}\mathbf{Advt}^{\mathrm{prf}}_{\mathtt{SOEM}^r[\Pi]}(\mathcal{A}) \leq{}& \frac{4}{2^n} + \frac{4(r-1)q(2p+2q)^{r-1}}{2^{nr}} \\ &+ \frac{10\sqrt{nq}(2p+2q)^{r-1}}{2^{n(r-1)}} + \frac{(2r+15)q(2p+2q)^r}{2^{nr}}.\end{aligned}$$

For $q+p = 2^{\frac{r}{r+1}n}/n$, the last two terms are at most $10 \cdot 2^{r-1}/n^{r-1}$ and $(2r+15)2^r/n^{r+1}$, respectively (using $q \leq p+q$), and the second term is even smaller. So, for any constant r, Theorem 4 shows security up to $O(2^{\frac{r}{r+1}n})$ queries (ignoring logarithmic factors).

Proof. For the purpose of this proof let $\mathtt{F}_{\mathsf{K}}(\cdot) = \mathtt{SOEM}^r[\Pi]_{\mathsf{K}}(\cdot)$, and let $\Gamma \twoheadleftarrow \{0,1\}^n$. $\mathcal{A}$'s goal is to distinguish between the *real* oracle $(\mathtt{F}_{\mathsf{K}}, \Pi^{\pm})$ and the *ideal* oracle $(\Gamma, \Pi^{\pm})$, where $\mathtt{F}_{\mathsf{K}}$ and Γ are referred to as the construction oracle and $\Pi^{\pm}$ is referred to as the primitive oracle. Fix a (q,p)-distinguisher $\mathcal{A}$. Let

- $(\mathsf{M}^i, \mathsf{T}^i)$ denote the i-th query-response tuple corresponding to the construction oracle. Let $\mathsf{M} := (\mathsf{M}^i : i \in [q])$ and $\mathsf{T} := (\mathsf{T}^i : i \in [q])$ (a sequence, as the responses may repeat).
- $(\mathsf{U}_j^i, \mathsf{V}_j^i)$ denote the i-th query-response tuple corresponding to the permutation Π_j. Unless stated otherwise, we assume that all these queries are in the forward direction. Let $\mathsf{U}_j := \{\mathsf{U}_j^i : i \in [p]\}$, $\mathsf{V}_j := \{\mathsf{V}_j^i : i \in [p]\}$, $\mathsf{U} := (\mathsf{U}_1, \ldots, \mathsf{U}_r)$, and $\mathsf{V} := (\mathsf{V}_1, \ldots, \mathsf{V}_r)$.
- $(\mathsf{X}_j^i, \mathsf{Y}_j^i)$ denote the input-output tuple to the j-th permutation, for all $j \in [r]$, within the i-th construction query in the real world, i.e., $\mathsf{X}_j^i = \mathsf{M}^i \oplus \mathsf{K}_j$. Let $\mathsf{X}^i := (\mathsf{X}_j^i : j \in [r])$ and $\mathsf{Y}^i := (\mathsf{Y}_j^i : j \in [r])$. Let $\mathsf{X} := \{\mathsf{X}^i : i \in [q]\}$ and $\mathsf{Y} := \{\mathsf{Y}^i : i \in [q]\}$.

We study a modified game where the oracle releases (X, Y) to $\mathcal{A}$ once the query-response phase is over, but before $\mathcal{A}$ outputs.

Ideal World Transcript Extension: Naturally, in the ideal world, the sampling is extended to generate this additional information. We define a sum-capture-like set, as defined in (1), as follows:

$$\mathcal{SC}(\mathsf{T}, \mathsf{V}) = \left\{ (i, j_1, j_2, \ldots, j_r) \in [q] \times [p]^r : \bigoplus_{k=1}^{r} \mathsf{V}_k^{j_k} = \mathsf{T}^i \right\}.$$

Let $\mu(\mathsf{T}, \mathsf{V}) = |\mathcal{SC}(\mathsf{T}, \mathsf{V})|$. Since $\mu(\mathsf{T}, \cdot)$ is monotonically increasing, $\mu(\mathsf{T}, \mathsf{V}) \leq \mu(\mathsf{T}, p+q)$ (See (2)). We define the predicate

$$\mathsf{LSC}(\mathsf{T}, p+q) : \left(\mu(\mathsf{T}, p+q) > \frac{q(p+q)^r}{2^n} + 2(p+q)^{r-1}\sqrt{nq} \right)$$

The subsequent two-step sampling mechanism for (X, Y) in the ideal world is defined under the condition that $\neg\mathsf{LSC}(\mathsf{T}, p+q)$ holds:

1. In the first step, a dummy key tuple is sampled uniformly at random, i.e., $\mathsf{K} \twoheadleftarrow (\{0,1\}^n)^r$, which determines $\mathsf{X}_j^i := \mathsf{M}^i \oplus \mathsf{K}_j$. Consider the following predicates:

$$\mathsf{KG}(\mathsf{M}, \mathsf{U}, \mathsf{K}) : \exists\, i \in [q],\, j_1, \ldots, j_r \in [p] \text{ such that } \left(\forall k \in [r],\, \mathsf{X}_k^i = \mathsf{U}_k^{j_k} \right)$$

$$\mathsf{SC}(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V}, \mathsf{K}) : \exists\, (i, j_1, j_2, \ldots, j_r) \in \mathcal{SC}(\mathsf{T}, \mathsf{V}),\, k \in [r], \text{ such that}$$
$$(\mathsf{X}_k^i \neq \mathsf{U}_k^{j_k}) \text{ and } \left(\forall k' \neq k,\, \mathsf{X}_{k'}^i = \mathsf{U}_{k'}^{j_{k'}} \right)$$

$$\mathsf{DC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}):\ \exists\, i\neq i'\in[q],\, k\in[r],\, (j_l,j'_l\in[p])_{l\neq k} \text{ such that}$$
$$\left(\forall l\neq k,\, \mathsf{X}^i_l=\mathsf{U}^{j_l}_l\wedge \mathsf{X}^{i'}_l=\mathsf{U}^{j'_l}_l\right) \text{ and}$$
$$\bigoplus_{l\in[r]\setminus\{k\}}\left(\mathsf{V}^{j_l}_l\oplus\mathsf{V}^{j'_l}_l\right)=\mathsf{T}^i\oplus\mathsf{T}^{i'}$$

Note that DC captures the case where two construction queries determine the same output of Π_k (with distinct inputs) via the primitive queries. Going forward we assume that $\neg(\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K})\vee\mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K})\vee\mathsf{DC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}))$ holds. For each $i\in[q]$:

(a) if there exists $j\in[p]$ and $k\in[r]$, such that $\mathsf{X}^i_k=\mathsf{U}^j_k$, then define $\mathsf{Y}^i_k:=\mathsf{V}^j_k$;
(b) let $\mathcal{I}_i=\{j\in[r]\,:\,\mathsf{X}^i_j\notin\mathsf{U}_j\}$ to be the set of permutation indices with fresh input for the i-th construction query.
(c) let $\mathcal{Q}^{(j)}_{(0)}=\{i\in[q]:\mathcal{I}_i=\{j\}\}$ for $j\in[r]$. Let $\mathcal{J}_{(1)},\ldots,\mathcal{J}_{(c)}$ be the subsets of $[r]$ of size at least 2, ordered by decreasing size, with ties broken by a fixed rule (say, lexicographically), so that $c=\sum_{j=2}^{r}\binom{r}{j}\leq 2^r$ and $t_i:=|\mathcal{J}_{(i)}|$ is non-increasing in i. Let $\mathcal{Q}_{(i)}=\{k\in[q]:\mathcal{I}_k=\mathcal{J}_{(i)}\}$ (possibly empty). Then $\mathcal{Q}^{(1)}_{(0)}\sqcup\ldots\sqcup\mathcal{Q}^{(r)}_{(0)}\sqcup\mathcal{Q}_{(1)}\sqcup\ldots\sqcup\mathcal{Q}_{(c)}$ is a partitioning of $[q]$. Let $|\mathcal{Q}^{(j)}_{(0)}|=q^{(j)}_0$, $q_0:=\sum_{j\in[r]}q^{(j)}_0$ and $|\mathcal{Q}_{(i)}|=q_i$. Then $q_0+\sum_{i\in[c]}q_i=q$. Note that the classes and their order are indexed by fixed subsets of $[r]$, so that t_i is not random, whereas q_i is.
(d) for all $j\in[r]$ and $i\in\mathcal{Q}^{(j)}_{(0)}$, define $\mathsf{Y}^i_j:=\bigoplus_{l\in[r]\setminus\{j\}}\mathsf{Y}^i_l\oplus\mathsf{T}^i$ and

$$\mathsf{Y}^{(0)}=\{\mathsf{Y}^i_j\ :\ j\in[r],i\in\mathcal{Q}^{(j)}_{(0)}\}.$$

This concludes the first step. We encourage the readers to verify that at the end of this step Y^i_j is undefined for exactly the indices in $\mathcal{I}_i$ and $|\mathcal{I}_i|\geq 2$. Furthermore, due to $\neg(\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K})\vee\mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K})\vee\mathsf{DC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}))$, the partially defined (X,Y) is permutation-consistent.

Constrained system formulation: For each $i\in[c]$, $\mathcal{J}_{(i)}=\{j_1,\ldots,j_{t_i}\}$ is the set of permutation indices with fresh input for the i-th class $\mathcal{Q}_{(i)}$. Let $r_i=q_it_i$. Then, for each $i\in[c]$, we obtain a (q_i,r_i,t_i)-constrained system $\mathbb{S}^{(i)}$:

$$\mathbb{S}^{(i)}=\left\{\bigoplus_{k\in\mathcal{J}_{(i)}}\mathsf{Y}^j_k=\mathsf{T}^j\bigoplus_{k'\in[r]\setminus\mathcal{J}_{(i)}}\mathsf{Y}^j_{k'}\right\}_{j\in\mathcal{Q}_{(i)}}$$

which is binary, acyclic, partite, isolated and t_i-regular (and empty if $q_i=0$, in which case it has only the empty solution, and we simply skip it in the second step, with $\varepsilon^{(i)}(\omega)=0$ and $P_i=0$ below).

2. In the second step, we sample a solution for each of the c constrained systems. We process $\mathbb{S}^{(1)},\ldots,\mathbb{S}^{(c)}$ in this order, so that $t_1\geq\ldots\geq t_c$. Now, for the i-th system:

- let $\mathcal{R}^{(j)}_{\leq(i-1)} = \mathsf{V}_j \cup \{\mathsf{Y}^k_j \ : \ k \in \mathcal{Q}^{(j)}_{(0)}\} \cup \{\mathsf{Y}^k_j \ : \ k \in \mathcal{Q}_{(1)} \sqcup \ldots \sqcup \mathcal{Q}_{(i-1)}\}$, for all $j \in [r]$, and let $|\mathcal{R}^{(j)}_{\leq(i-1)}| = r^{(j)}_{\leq(i-1)} \leq (p+q)$,
- let $\mathcal{R}_{\leq(i-1)} = (\mathcal{R}^{(j)}_{\leq(i-1)} \ : \ j \in [r])$ and $\widehat{\mathcal{R}}_{\leq(i-1)} = (\mathcal{R}^{(j)}_{\leq(i-1)} \ : \ j \in \mathcal{J}_{(i)})$,
- let $\mathsf{T}^{(i)} = (\mathsf{T}^k \ : \ k \in \mathcal{Q}_{(i)})$ and $\widehat{\mathsf{T}}^{(i)} = (\mathsf{T}^k \bigoplus_{j \in [r] \setminus \mathcal{J}_{(i)}} \mathsf{Y}^k_j \ : \ k \in \mathcal{Q}_{(i)})$. Then, $|\mathsf{T}^{(i)}|, |\widehat{\mathsf{T}}^{(i)}| \leq q_i$.
- let $\mathsf{Y}^{(i)} = \{\mathsf{Y}^k_j \ : \ k \in \mathcal{Q}_{(i)}, j \in \mathcal{J}_{(i)}\}$. Then, $|\mathsf{Y}^{(i)}| = r_i$.

We sample $\mathsf{Y}^{(i)} \twoheadleftarrow (\mathbb{S}^{(i)} \,|\, \widehat{\mathcal{R}}_{\leq(i-1)})$. Since the solution for each system is sampled in a consistent manner given a consistent solution for the previous system, the cumulative sampling is also permutation-compatible. This completes the second step.

At this stage the ideal world transcript is fully determined.

Bad Transcript Definition and Analysis: A transcript $\omega = (M, T, U, V, K, Y) \in \Omega$ is said to be *bad* if $\mathsf{LSC}(T, p+q) \vee \mathsf{KG} \vee \mathsf{SC} \vee \mathsf{DC}$ holds.

Lemma 11.

$$\Pr\left(\mathtt{\Theta}_{\mathrm{id}} \in \Omega_{\mathrm{bad}}\right) \leq \frac{4}{2^n} + \frac{2r\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}} + \frac{(2r^2+r+1)q(p+q)^r}{2^{nr}}$$

A proof of this lemma is available in Appendix E.1.

Lemma 12. *For any good transcript ω, we have* $\Pr\left(\mathtt{\Theta}_{\mathrm{re}} = \omega\right) \geq \Pr\left(\mathtt{\Theta}_{\mathrm{id}} = \omega\right) \times (1 - \varepsilon_{\mathrm{ratio}}(\omega))$*, where* $\varepsilon_{\mathrm{ratio}}(\omega) = \sum_{i \in [c]} \varepsilon^{(i)}(\omega)$ *and*

$$\varepsilon^{(i)}(\omega) \leq \frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\leq(i-1)})}{2^{n(t_i-1)}} + \frac{2P_i}{2^{n(t_i-1)}} + \frac{6q_i(p+q)^{t_i}}{2^{nt_i}},$$

and P_i denotes the number of pairs $k < k'$ in $\mathcal{Q}_{(i)}$ such that $\widehat{\mathsf{T}}^k = \widehat{\mathsf{T}}^{k'}$.

A proof of this lemma is available in Appendix E.2. Now, we have

$$\begin{aligned}
\mathbb{E}\left(\mathtt{1}_{\mathrm{good}}\varepsilon_{\mathrm{ratio}}\right) &\leq \sum_{i \in [c]} \mathbb{E}\left(\mathtt{1}_{\mathrm{good}}(\mathtt{\Theta}_{\mathrm{id}}) \frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\leq(i-1)})}{2^{n(t_i-1)}}\right) + \sum_{i \in [c]} \frac{2\mathbb{E}\left(P_i\right)}{2^{n(t_i-1)}} \\
&\qquad + \sum_{i \in [c]} \frac{6\mathbb{E}\left(q_i\right)(p+q)^{t_i}}{2^{nt_i}} \\
&\leq \sum_{i \in [c]} \mathbb{E}\left(\mathtt{1}_{\mathrm{good}}(\mathtt{\Theta}_{\mathrm{id}}) \frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\leq(i-1)})}{2^{n(t_i-1)}}\right) + \frac{4(r-1)q(2p+2q)^{r-1}}{2^{nr}} \\
&\qquad + \frac{6q(2(p+q))^r}{2^{nr}} \qquad (17)
\end{aligned}$$

where the first inequality follows from linearity of expectation and the fact that $\mathbb{E}\left(\chi\mathtt{R}\right) \leq \mathbb{E}\left(\mathtt{R}\right)$ for any non-negative random variable $\mathtt{R}$ and indicator random variable χ. The third term in the second inequality follows from

$\mathbb{E}(q_i) \le qp^{r-t_i}/2^{n(r-t_i)} \le q(p+q)^{r-t_i}/2^{n(r-t_i)}$, $t_i \ge 2$, and the fact that there are at most $\binom{r}{t}$ classes with $t_i = t$. For the second term, let $t = t_i$. If $t = r$, then $\widehat{\mathsf{T}}^k = \mathsf{T}^k$, and thus $\mathbb{E}(P_i) \le q^2/2^{n+1}$ due to the uniformity of T. If $t < r$, then a pair $k < k'$ counted by P_i satisfies $\mathsf{X}_l^k = \mathsf{U}_l^{j_l}$ and $\mathsf{X}_l^{k'} = \mathsf{U}_l^{j'_l}$ for all $l \notin \mathcal{J}_{(i)}$ and some $j_l, j'_l \in [p]$, and $\bigoplus_{l \notin \mathcal{J}_{(i)}} (\mathsf{V}_l^{j_l} \oplus \mathsf{V}_l^{j'_l}) = \mathsf{T}^k \oplus \mathsf{T}^{k'}$. This is the event DC with $[r] \setminus \mathcal{J}_{(i)}$ in place of $[r] \setminus \{k\}$, and the argument for DC in Appendix E.1 gives $\mathbb{E}(P_i) \le (r-t+1)q^2p^{r-t}/2^{n(r-t+1)}$ (the factor $1/2$ accounts for the unordered pairs). In both cases, $2\mathbb{E}(P_i)/2^{n(t-1)} \le 2(r-t+1)q^2p^{r-t}/2^{nr} \le 2(r-1)q(p+q)^{r-1}/2^{nr}$, as $t \ge 2$, and the second term follows as there are at most 2^r classes. Now, when $t_i = r$, we have

$$\mathbb{E}\left(1_{\mathrm{good}}(\mathsf{\Theta}_{\mathrm{id}})\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\le(i-1)})}{2^{n(r-1)}}\right) \le \mathbb{E}\left(1_{\mathrm{good}}(\mathsf{\Theta}_{\mathrm{id}})\frac{2\mu^r(\mathsf{T}, p+q)}{2^{n(r-1)}}\right)$$
$$\le \frac{2q(p+q)^r}{2^{nr}} + \frac{4\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}}, \qquad (18)$$

where the first inequality holds as $\widehat{\mathsf{T}}^{(i)} = \mathsf{T}^{(i)}$ and each set in $\widehat{\mathcal{R}}_{\le(i-1)}$ has size at most $p+q$ (whatever be their dependence on K), and the last inequality follows from $\neg\mathsf{LSC}(\mathsf{T}, p+q)$. For $t_i < r$, let $t = t_i$ and $\mathcal{J} = \mathcal{J}_{(i)}$. For $j \in \mathcal{J}$, we have $\mathcal{R}^{(j)}_{\le(i-1)} = \mathsf{V}_j \sqcup \mathcal{D}^{(j)} \sqcup \mathcal{S}^{(j)}$, where $\mathcal{D}^{(j)} = \{\mathsf{Y}_j^k : k \in \mathcal{Q}^{(j)}_{(0)}\}$ is the set of derived values and $\mathcal{S}^{(j)}$ is the set of values sampled for $\mathbb{S}^{(1)}, \ldots, \mathbb{S}^{(i-1)}$. Note that both $\mathcal{D}^{(j)}$ and $\mathcal{S}^{(j)}$ depend on K. So, unlike the case $t_i = r$, we cannot simply combine the sum-capture bound with the uniformity of K. Instead, we write $\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\le(i-1)}) = \mu_{\mathsf{V}} + \mu_{\mathcal{D}} + \mu_{\mathcal{S}}$, where each of the three terms counts the tuples $(k, (z_j)_{j\in\mathcal{J}})$ with $k \in \mathcal{Q}_{(i)}$, $z_j \in \mathcal{R}^{(j)}_{\le(i-1)}$ and $\bigoplus_{j\in\mathcal{J}} z_j = \widehat{\mathsf{T}}^k$ (the entry of $\widehat{\mathsf{T}}^{(i)}$ for k), and

- μ_{V} counts the tuples with $z_j \in \mathsf{V}_j$ for all $j \in \mathcal{J}$,
- $\mu_{\mathcal{D}}$ counts the tuples with $z_j \in \mathcal{D}^{(j)}$ for some $j \in \mathcal{J}$,
- $\mu_{\mathcal{S}}$ counts the remaining tuples, i.e., $z_j \in \mathcal{S}^{(j)}$ for some $j \in \mathcal{J}$, and $z_j \notin \mathcal{D}^{(j)}$ for all $j \in \mathcal{J}$.

We bound the three terms separately. Throughout, we use that K is sampled independent of $(\mathsf{M}, \mathsf{T}, \mathsf{U}, \mathsf{V})$, and for any $k \in [q]$, $l \in [r]$, the expected number of $j \in [p]$ with $\mathsf{X}_l^k = \mathsf{U}_l^j$ is at most $p/2^n$. Moreover, for $k \ne k'$, the expected number of $j, j' \in [p]$ with $\mathsf{X}_l^k = \mathsf{U}_l^j$ and $\mathsf{X}_l^{k'} = \mathsf{U}_l^{j'}$ is also at most $p/2^n$, as K_l determines both.

The term μ_{V}: Each such tuple, together with the $r-t$ primitive queries matched by X^k outside $\mathcal{J}$, gives an element of $\mathcal{SC}(\mathsf{T}, \mathsf{V})$, and the $r-t$ matchings hold with probability $2^{-n(r-t)}$. Since $\mathsf{LSC}(\mathsf{T}, p+q)$ depends only on T, we get $\mathbb{E}(1_{\mathrm{good}}(\mathsf{\Theta}_{\mathrm{id}})\mu_{\mathsf{V}}) \le \mathbb{E}\left(1_{\neg\mathsf{LSC}(\mathsf{T},p+q)}\mu^r(\mathsf{T}, p+q)\right)/2^{n(r-t)}$.

The term $\mu_{\mathcal{D}}$: Fix $j_0 \in \mathcal{J}$ and $k' \in \mathcal{Q}^{(j_0)}_{(0)}$ such that $z_{j_0} = \mathsf{Y}_{j_0}^{k'}$. Then, $\mathsf{X}_l^k \in \mathsf{U}_l$ for all $l \notin \mathcal{J}$ and $\mathsf{X}_l^{k'} \in \mathsf{U}_l$ for all $l \ne j_0$. As $j_0 \in \mathcal{J}$, this costs a factor $p/2^n$ for each $l \ne j_0$. Given these, z_{j_0} is fixed, and there are at most $(p+q)^{t-2}$ choices for

the remaining coordinates, as the last one is determined by the equation. Thus, $\mathbb{E}(\mu_{\mathcal{D}}) \le tq^2p^{r-1}(p+q)^{t-2}/2^{n(r-1)}$.

The term $\mu_{\mathcal{S}}$: Let $i^* < i$ be the largest index such that some z_j is sampled for $\mathbb{S}^{(i^*)}$, and fix such a z_j. Let $k'' \in \mathcal{Q}_{(i^*)}$ be the index of the corresponding equation, $t^* = t_{i^*}$, and $\mathcal{T} = \{j \in \mathcal{J} : z_j = \mathsf{Y}_j^{k''}\}$. We have two cases:

- $\mathcal{T} \neq \mathcal{J}_{(i^*)}$: Condition on K, the transcript, the values sampled for $\mathbb{S}^{(1)}, \ldots, \mathbb{S}^{(i^*-1)}$, and the values of all equations in $\mathbb{S}^{(i^*)}$ other than the k''-th one. Then, $(\mathsf{Y}_j^{k''} : j \in \mathcal{J}_{(i^*)})$ is uniform over the solutions of the k''-th equation that avoid at most $p+q$ values for each j. There are at least $2^{n(t^*-1)} - t^*(p+q)2^{n(t^*-2)} \ge 2^{n(t^*-1)}/2$ such solutions, as $r(p+q) \le 2^{n-1}$ for $r < n$. On the other hand, the tuple fixes $\bigoplus_{j\in\mathcal{T}} \mathsf{Y}_j^{k''}$ (all the other coordinates are already fixed by the choice of i^*), which is linearly independent of the k''-th equation as $\mathcal{T} \neq \mathcal{J}_{(i^*)}$. So at most $2^{n(t^*-2)}$ of these solutions are consistent with the tuple, and the tuple is realized with probability at most $2/2^n$. There are at most q choices for k, which costs a factor $(p/2^n)^{r-t}$ for the matchings outside $\mathcal{J}$, and at most $(p+q)^t$ choices for the coordinates. So the expected number of such tuples is at most $2qp^{r-t}(p+q)^t/2^{n(r-t+1)}$.
- $\mathcal{T} = \mathcal{J}_{(i^*)}$: Then, $\mathcal{J}_{(i^*)} \subsetneq \mathcal{J}$ (as $\mathcal{T} \subseteq \mathcal{J}$ and $i^* \neq i$), and thus $t^* < t$. This is impossible, as $i^* < i$ gives $t^* \ge t$ by the choice of the order. So this case does not occur.

Combining the three bounds, and using $qp^{r-1} \le (p+q)^r$ and $p+q \le 2^n$, we have

$$\mathbb{E}\left(\mathsf{1}_{\mathrm{good}}(\Theta_{\mathrm{id}})\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\le(i-1)})}{2^{n(t_i-1)}}\right) \le \frac{2q(p+q)^r}{2^{nr}} + \frac{4\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}} + \frac{(2t+4)q(p+q)^r}{2^{nr}}$$
$$\le \frac{(2r+6)q(p+q)^r}{2^{nr}} + \frac{4\sqrt{nq}(p+q)^{r-1}}{2^{n(r-1)}}, \quad (19)$$

where the terms $2tq(p+q)^r/2^{nr}$ and $4q(p+q)^r/2^{nr}$ in the first line correspond to $\mu_{\mathcal{D}}$ and $\mu_{\mathcal{S}}$, respectively, and the last inequality uses $t \le r-1$. Using (18) and (19) in (17), we have

$$\mathbb{E}(\mathsf{1}_{\mathrm{good}}\varepsilon_{\mathrm{ratio}}) \le \frac{4(r-1)q(2p+2q)^{r-1}}{2^{nr}} + \frac{8\sqrt{nq}(2(p+q))^{r-1}}{2^{n(r-1)}} + \frac{(2r+12)q(2(p+q))^r}{2^{nr}} \quad (20)$$

Finally, Lemma 2, Lemma 11 and 12, and (20), gives Theorem 4, using $2r \le 2^r$ and $2r^2 + r + 1 \le 3 \cdot 2^r$. □

9 Conclusion and Future Directions

In this paper, we formulated a special class of systems of linear equations over finite fields that naturally arise in the security analysis of various symmetric-key primitives. We derived lower bounds on the number of solutions for these

systems under specific constraints and used them to strengthen the PRF security of several constructions. Specifically, under appropriate assumptions on the hash function, we proved that the 1k-DBHtS construction is secure up to $O(2^{3n/4}/n^{1/4})$ queried blocks. Additionally, we demonstrated two instances, namely 1k-LightMAC+ and 1k-PMAC+, where the underlying hash requirements are fulfilled and therefore they achieve security up to $O(2^{3n/4}/n^{1/4})$ queried blocks (ignoring length factors). In the public permutation setting, we proposed a sum of r independent Even-Mansour ciphers, called SOEM^r, extending Sibleyras and Todo's KSoP [50] for $r \geq 2$, and proved that it is secure up to $O(2^{\frac{r}{r+1}n}/n)$ queries for any constant r.

We believe that this work opens multiple new avenues for research.

First, the constrained system formalism and the subsequent analysis in this paper can be further extended in multiple directions. One can obviously study the problem in its full generality. While the cryptographic applications of this endeavour are not readily clear to us, it is nevertheless a challenging theoretical pursuit. At the same time, improving the bounds for cryptographically-relevant CAR systems or proving the tightness of current bounds could be highly relevant for cryptographic applications. Yet another direction is to extend the constrained system formalism to handle constructions involving tweakable block ciphers (TBCs). Indeed, there are several such mirror theory based results [35,14] — both where TBCs are used as primitives and where TBC constructions are considered as candidates for tweakable SPRPs.

Second, while we have shown that the restricted solutions to constrained systems are a crucial ingredient to study 1k-DBHtS construction, several open problems remain. Indeed, we use a domain-separated definition for 1k-DBHtS. Instead, one can study the original definition, without any domain-separation. In that case, the analysis of constrained systems is not the only source of complexity. As explained in Section 6, without domain separation, additional "badness" conditions must be addressed, which seems to require some additional techniques such as reset-sampling [9,10]. We leave this integration as an open problem. Even in the domain-separated world, it would be interesting to remove the factors of ℓ in our bound for 1k-PMAC+, and to avoid the conditions $\mathsf{TF}_{\hat{\ell}}$ and $\mathsf{SQF}_{\hat{\ell}}$ for long messages (the former is partly necessary for 1k-LightMAC+ as defined here). Our approach could potentially be extended to n1kf9 with appropriate domain separation in the hash analysis. However, the analysis of CBC-based hash functions tends to be more intricate.

Finally, we expect further cryptographic applications of Theorems 1 and 2, including to BBB security proofs for the single-keyed instances of constructions involving sum of permutations as a building block. A prime example for this would be the single-keyed variant of CHM [32] — an optimally secure nonce-based authenticated encryption scheme.

Acknowledgements. The authors would like to thank Avijit Dutta, Seongha Hwang and Mustafa Khairallah for their comments on earlier versions of this paper, and Sunyeop Kim for identifying a missing bad event in the earlier analysis of SOEM^{r}construction. This work was (in part) supported by the Eu-

ropean Research Council (ERC) project 101097056 (SYMTRUST). Ashwin Jha was supported by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States — EXC 2092 CaSa — 39078197. Mridul Nandi was supported by MATRICS scheme MTR/2023/000302 of Science and Engineering Research Board, India. Part of this work was done while Jordan Naccache and Abishanka Saha were PhD students at the CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, and Indian Statistical Institute, Kolkata, India, respectively. During this period, Abishanka Saha also visited the Chair of Symmetric Cryptography at Ruhr University Bochum.

References

1. Andreeva, E., Daemen, J., Mennink, B., Assche, G.V.: Security of keyed sponge constructions using a modular proof approach. In: Leander, G. (ed.) Fast Software Encryption - FSE 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9054, pp. 364–384. Springer (2015). https://doi.org/10.1007/978-3-662-48116-5_18
2. Aumasson, J., Bernstein, D.J.: Siphash: A fast short-input PRF. In: Galbraith, S.D., Nandi, M. (eds.) Progress in Cryptology - INDOCRYPT 2012. Proceedings. Lecture Notes in Computer Science, vol. 7668, pp. 489–508. Springer (2012). https://doi.org/10.1007/978-3-642-34931-7_28
3. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. IACR Cryptol. ePrint Arch. p. 24 (1999)
4. Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. J. Comput. Syst. Sci. **61**(3), 362–399 (2000). https://doi.org/10.1006/JCSS.1999.1694
5. Bhaumik, R., Chailloux, A., Frixons, P., Mennink, B., Naya-Plasencia, M.: Block cipher doubling for a post-quantum world. IACR Commun. Cryptol. **1**(3), 4 (2024). https://doi.org/10.62056/AV4FVUA5V
6. Black, J., Rogaway, P.: A block-cipher mode of operation for parallelizable message authentication. In: Knudsen, L.R. (ed.) Advances in Cryptology - EUROCRYPT 2002, Proceedings. Lecture Notes in Computer Science, vol. 2332, pp. 384–397. Springer (2002). https://doi.org/10.1007/3-540-46035-7_25
7. Chakraborti, A., Nandi, M., Talnikar, S., Yasuda, K.: On the composition of single-keyed tweakable even-mansour for achieving BBB security. IACR Trans. Symmetric Cryptol. **2020**(2), 1–39 (2020). https://doi.org/10.13154/TOSC.V2020.I2.1-39
8. Chakraborty, B., Jha, A., Nandi, M.: On the security of sponge-type authenticated encryption modes. IACR Trans. Symmetric Cryptol. **2020**(2), 93–119 (2020). https://doi.org/10.13154/TOSC.V2020.I2.93-119
9. Chattopadhyay, S., Jha, A., Nandi, M.: Fine-tuning the ISO/IEC standard light-mac. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13092, pp. 490–519. Springer (2021). https://doi.org/10.1007/978-3-030-92078-4_17

10. Chattopadhyay, S., Jha, A., Nandi, M.: Towards tight security bounds for omac, XCBC and TMAC. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13791, pp. 348–378. Springer (2022). https://doi.org/10.1007/978-3-031-22963-3_12
11. Chen, Y.L.: A modular approach to the security analysis of two-permutation constructions. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13791, pp. 379–409. Springer (2022). https://doi.org/10.1007/978-3-031-22963-3_13
12. Chen, Y.L., Dutta, A., Nandi, M.: Multi-user BBB security of public permutations based MAC. Cryptogr. Commun. **14**(5), 1145–1177 (2022). https://doi.org/10.1007/S12095-022-00571-W
13. Chen, Y.L., Lambooij, E., Mennink, B.: How to build pseudorandom functions from public random permutations. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11692, pp. 266–293. Springer (2019). https://doi.org/10.1007/978-3-030-26948-7_10
14. Choi, W., Lee, J., Lee, Y.: Building prfs from tprps: Beyond the block and the tweak length bounds. IACR Trans. Symmetric Cryptol. **2024**(1), 35–70 (2024). https://doi.org/10.46586/TOSC.V2024.I1.35-70
15. Cogliati, B., Dutta, A., Nandi, M., Patarin, J., Saha, A.: Proof of mirror theory for a wide range of $\xi _{\max }$. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology - EUROCRYPT 2023, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 470–501. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_16
16. Cogliati, B., Jha, A., Naccache, J.R.R., Nandi, M., Saha, A.: On the number of restricted solutions to constrained systems and their applications. In: Advances in Cryptology - ASIACRYPT 2025, Proceedings, Part I. Lecture Notes in Computer Science, vol. 16245, pp. 546–579. Springer (2025). https://doi.org/10.1007/978-981-95-5018-0_18
17. Cogliati, B., Jha, A., Nandi, M.: How to build optimally secure prfs using block ciphers. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 754–784. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_25
18. Cogliati, B., Patarin, J.: Mirror theory: A simple proof of the pi+pj theorem with xi_max=2. IACR Cryptol. ePrint Arch. p. 734 (2020), https://eprint.iacr.org/2020/734
19. Cogliati, B., Seurin, Y.: Analysis of the single-permutation encrypted davies-meyer construction. Des. Codes Cryptogr. **86**(12), 2703–2723 (2018). https://doi.org/10.1007/S10623-018-0470-9
20. Dai, W., Hoang, V.T., Tessaro, S.: Information-theoretic indistinguishability via the chi-squared method. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017, Proceedings, Part III. Lecture Notes in Computer Science, vol. 10403, pp. 497–523. Springer (2017). https://doi.org/10.1007/978-3-319-63697-9_17
21. Datta, N., Dutta, A., Nandi, M., Paul, G.: Double-block hash-then-sum: A paradigm for constructing BBB secure PRF. IACR Trans. Symmetric Cryptol. **2018**(3), 36–92 (2018). https://doi.org/10.13154/TOSC.V2018.I3.36-92

22. Datta, N., Dutta, A., Nandi, M., Paul, G., Zhang, L.: Single key variant of pmac_plus. IACR Trans. Symmetric Cryptol. **2017**(4), 268–305 (2017). https://doi.org/10.13154/TOSC.V2017.I4.268-305
23. Datta, N., Dutta, A., Nandi, M., Talnikar, S.: Tight multi-user security bound of dbhts. IACR Trans. Symmetric Cryptol. **2023**(1), 192–223 (2023). https://doi.org/10.46586/TOSC.V2023.I1.192-223
24. Dinur, I.: Tight indistinguishability bounds for the XOR of independent random permutations by fourier analysis. In: Joye, M., Leander, G. (eds.) Advances in Cryptology - EUROCRYPT 2024, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 33–62. Springer (2024). https://doi.org/10.1007/978-3-031-58716-0_2
25. Dinur, I., Goldfeder, S., Halevi, T., Ishai, Y., Kelkar, M., Sharma, V., Zaverucha, G.: Mpc-friendly symmetric cryptography from alternating moduli: Candidates, protocols, and applications. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 12828, pp. 517–547. Springer (2021). https://doi.org/10.1007/978-3-030-84259-8_18
26. Dutta, A., Nandi, M., Saha, A.: Proof of mirror theory for $\xi_{\max} = 2$. IEEE Trans. Inf. Theory **68**(9), 6218–6232 (2022). https://doi.org/10.1109/TIT.2022.3171178
27. Dutta, A., Nandi, M., Talnikar, S.: Permutation based EDM: an inverse free BBB secure PRF. IACR Trans. Symmetric Cryptol. **2021**(2), 31–70 (2021). https://doi.org/10.46586/TOSC.V2021.I2.31-70
28. Eberhard, S.: More on additive triples of bijections. CoRR **abs/1704.02407** (2017), http://arxiv.org/abs/1704.02407
29. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) Advances in Cryptology - ASIACRYPT 1991, Proceedings. Lecture Notes in Computer Science, vol. 739, pp. 210–224. Springer (1991). https://doi.org/10.1007/3-540-57332-1_17
30. Galambos, J., Simonelli, I.: Bonferroni-type Inequalities with Applications. Springer New York, 1 edn. (1996)
31. Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9814, pp. 3–32. Springer (2016). https://doi.org/10.1007/978-3-662-53018-4_1
32. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Robshaw, M.J.B. (ed.) Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers. Lecture Notes in Computer Science, vol. 4047, pp. 310–327. Springer (2006). https://doi.org/10.1007/11799313_20
33. Iwata, T., Kurosawa, K.: OMAC: one-key CBC MAC. In: Johansson, T. (ed.) Fast Software Encryption - FSE 2003, Revised Papers. Lecture Notes in Computer Science, vol. 2887, pp. 129–153. Springer (2003). https://doi.org/10.1007/978-3-540-39887-5_11
34. Jha, A.: A note on the generalized sum-capture problem for rings. Online: https://ashwin-jha.github.io/papers/gsc.pdf (2024)
35. Jha, A., Nandi, M.: Tight security of cascaded LRW2. J. Cryptol. **33**(3), 1272–1317 (2020). https://doi.org/10.1007/S00145-020-09347-Y

36. Jha, A., Nandi, M.: A survey on applications of h-technique: Revisiting security analysis of PRP and PRF. Entropy **24**(4), 462 (2022). https://doi.org/10.3390/E24040462
37. Kim, S., Lee, B., Lee, J.: Tight security bounds for double-block hash-then-sum macs. In: Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part I. pp. 435–465 (2020). https://doi.org/10.1007/978-3-030-45721-1_16
38. Leurent, G., Nandi, M., Sibleyras, F.: Generic attacks against beyond-birthday-bound macs. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology - CRYPTO 2018. Proceedings, Part I. Lecture Notes in Computer Science, vol. 10991, pp. 306–336. Springer (2018). https://doi.org/10.1007/978-3-319-96884-1_11
39. Lucks, S.: The sum of prps is a secure PRF. In: Preneel, B. (ed.) Advances in Cryptology - EUROCRYPT 2000, Proceeding. Lecture Notes in Computer Science, vol. 1807, pp. 470–484. Springer (2000). https://doi.org/10.1007/3-540-45539-6_34
40. Luykx, A., Preneel, B., Tischhauser, E., Yasuda, K.: A MAC mode for lightweight block ciphers. In: Peyrin, T. (ed.) Fast Software Encryption - FSE 2016, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9783, pp. 43–59. Springer (2016). https://doi.org/10.1007/978-3-662-52993-5_3
41. MacWilliams, F., Sloane, N. (eds.): The Theory of Error-Correcting Codes, North-Holland Mathematical Library, vol. 16. Elsevier (1977). https://doi.org/10.1016/S0924-6509(08)70527-0
42. Mennink, B., Preneel, B.: On the XOR of multiple random permutations. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) Applied Cryptography and Network Security - ACNS 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9092, pp. 619–634. Springer (2015). https://doi.org/10.1007/978-3-319-28166-7_30
43. Mennink, B., Reyhanitabar, R., Vizár, D.: Security of full-state keyed sponge and duplex: Applications to authenticated encryption. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology - ASIACRYPT 2015, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9453, pp. 465–489. Springer (2015). https://doi.org/10.1007/978-3-662-48800-3_19
44. Motwani, R., Raghavan, P.: Randomized Algorithms. Cambridge University Press (1995). https://doi.org/10.1017/CBO9780511814075
45. Naito, Y.: Blockcipher-based macs: Beyond the birthday bound without message length. In: Advances in Cryptology - ASIACRYPT 2017, Proceedings, Part III. pp. 446–470 (2017). https://doi.org/10.1007/978-3-319-70700-6_16
46. Patarin, J.: Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. IACR Cryptol. ePrint Arch. p. 287 (2010), http://eprint.iacr.org/2010/287
47. Patarin, J.: Mirror theory and cryptography. Appl. Algebra Eng. Commun. Comput. **28**(4), 321–338 (2017). https://doi.org/10.1007/S00200-017-0326-Y
48. Rao, A.R., Bhimasankaram, P.: Linear Algebra. Hindustan Book Agency (2000). https://doi.org/https://doi.org/10.1007/978-93-86279-01-9
49. Shen, Y., Sibleyras, F.: Key-reduced variants of 3kf9 with beyond-birthday-bound security. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13792, pp. 525–554. Springer (2022). https://doi.org/10.1007/978-3-031-22966-4_18
50. Sibleyras, F., Todo, Y.: Keyed sum of permutations: A simpler rp-based PRF. In: Rosulek, M. (ed.) Topics in Cryptology - CT-RSA 2023, Proceedings. Lecture

Notes in Computer Science, vol. 13871, pp. 573–593. Springer (2023). https://doi.org/10.1007/978-3-031-30872-7_22
51. Song, H.: A single-key variant of lightmac_plus. Symmetry **13**(10) (2021). https://doi.org/10.3390/sym13101818
52. Yasuda, K.: The sum of CBC macs is a secure PRF. In: Pieprzyk, J. (ed.) Topics in Cryptology - CT-RSA 2010. Proceedings. Lecture Notes in Computer Science, vol. 5985, pp. 366–381. Springer (2010). https://doi.org/10.1007/978-3-642-11925-5_25
53. Yasuda, K.: A new variant of PMAC: beyond the birthday bound. In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011. Proceedings. Lecture Notes in Computer Science, vol. 6841, pp. 596–609. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9_34
54. Zhang, L., Wu, W., Sui, H., Wang, P.: 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In: Wang, X., Sako, K. (eds.) Advances in Cryptology - ASIACRYPT 2012. Proceedings. Lecture Notes in Computer Science, vol. 7658, pp. 296–312. Springer (2012). https://doi.org/10.1007/978-3-642-34961-4_19

Appendices

A Results from Linear Algebra and Probability Theory

A.1 Proof of Proposition 1

(1) follows from the definition. For (2), suppose to the contrary that A' does not have full rank. Then, we must have $\mathbf{0} \in \mathrm{rowsp}^+(A')$. Specifically, one can find $(a_1, \ldots, a_q) \neq \mathbf{0} \in \mathbb{F}_N^q$, such that $a_1 A'_{1\bullet} \oplus \cdots \oplus a_q A'_{q\bullet} = \mathbf{0}$. Then, $\boldsymbol{v} = a_1 A_{1\bullet} \oplus \cdots \oplus a_q A_{q\bullet} \in \mathrm{rowsp}^+(A)$, and $\mathtt{H}(\boldsymbol{v}) \leq r - r' \leq k - 1$. Thus, $\mathtt{H}(A) < k$, which is a contradiction. Finally, (3) follows from (2). □

A.2 Proof of Proposition 3

The result is trivial for $q = 1$. Assume for contradiction that $\mathtt{H}(A) < k$ for some $q \geq 2$. Then, for some $2 \leq l \leq q$, there exists a sequence of rows $A_{i_1\bullet}, \ldots, A_{i_l\bullet}$ and a sequence of non-zero field elements $a_1, \ldots, a_l$, such that $\boldsymbol{v} = a_1 A_{i_1\bullet} \oplus \ldots \oplus a_l A_{i_l\bullet}$ has $H(\boldsymbol{v}) < k$. Since, A is acyclic, one can always find two distinct rows $A_{i_a\bullet}$ and $A_{i_b\bullet}$ such that each of them shares at most one column index with non-zero entries with the remaining rows in $\{A_{i_1\bullet}, \ldots, A_{i_l\bullet}\}$. Indeed, the bipartite graph associated with these l rows is a forest, as A is acyclic. If a connected component of this forest contains a single row, then this row shares no column with the remaining rows. Otherwise, consider a longest path between two rows in the component. Each of its two end rows shares at most one column with the remaining rows, as any other shared column would either extend the path or close a cycle. Then, using the k-regularity of A, at least $k - 1 \geq 1$ non-zero columns in each of $A_{i_a\bullet}$ and $A_{i_b\bullet}$ have a single non-zero entry. Therefore, these columns contribute non-zero coordinates to $\boldsymbol{v}$. Thus, $H(\boldsymbol{v}) \geq 2k - 2$ which is at least k for $k \geq 2$. □

A.3 Proof of Proposition 4

First consider the case: $\{i_1, \ldots, i_k\} = \mathrm{col}(\overline{A}_{j\bullet})$ for some $j \in [q]$, i.e., all the non-zero columns of $A_{j\bullet}$ are deleted, and hence $A_{j\bullet}$ can be dropped without affecting the rank of A'. Thus, $\mathrm{rank}(A') \leq q-1$. Furthermore, since the system is acyclic and A is k-regular, A' must be acyclic and any row $A'_{j'\bullet}$ must have $\mathtt{H}(A'_{j'\bullet}) \geq (k-1)$. In particular, without loss of generality we can assume that A' is $(k-1)$-regular.[18] In addition, A' is acyclic. Then, using Proposition 3, we have $\mathtt{H}(A') \geq k-1 \geq 2$, and thus using Proposition 1, $\mathrm{rank}(A') = q-1$.

Now suppose $\{i_1, \ldots, i_k\} \neq \mathrm{col}(\overline{A}_{j\bullet})$ for all $j \in [q]$. Thus, A' has q non-zero rows. Assume towards a contradiction that $\mathrm{rank}(A') < q$. Then one can find a sequence of distinct rows $A'_{j_1\bullet}, A'_{j_2\bullet}, \ldots, A'_{j_l\bullet} \in \mathrm{row}(A')$ and a sequence of non-zero coefficients $a_1, a_2, \ldots, a_l$ such that $\boldsymbol{v} = a_1 A'_{j_1\bullet} \oplus \ldots \oplus a_l A'_{j_l\bullet} = \mathbf{0}$. Let

$$A'' = \begin{pmatrix} A_{j_1\bullet} \\ A_{j_2\bullet} \\ \vdots \\ A_{j_l\bullet} \end{pmatrix}$$

If $l = 1$, then $a_1 A'_{j_1\bullet} = \mathbf{0}$ implies that all the non-zero columns of $A_{j_1\bullet}$ are deleted, i.e., $\{i_1, \ldots, i_k\} = \mathrm{col}(\overline{A}_{j_1\bullet})$, which is not the case. So $l \geq 2$. We claim that the number of columns in A'' with a single non-zero entry in each of these columns is at least $2k-2$. Indeed, as in the proof of Proposition 3, A'' has two distinct rows each of which shares at most one column index with non-zero entries with the remaining rows of A''. Since A'' is k-regular, each of these two rows contributes at least $k-1$ columns with a single non-zero entry. Now, even if one deletes k columns from A'', there are still at least $k-2 \geq 1$ columns that contribute non-zero entries in any linear combination, including $\boldsymbol{v} = a_1 A'_{j_1\bullet} \oplus \ldots \oplus a_l A'_{j_l\bullet}$. Therefore, $v \neq \mathbf{0}$, contradicting $\mathrm{rank}(A') < q$. □

A.4 Proof of Proposition 5

We have

$$\begin{aligned} \mathbb{E}\left(|\mathtt{X} - \mathbb{E}\left(\mathtt{X}\right)|\right) &= \sqrt{\left(\mathbb{E}\left(|\mathtt{X} - \mathbb{E}\left(\mathtt{X}\right)|\right)\right)^2} \\ &\leq \sqrt{\mathbb{E}\left((\mathtt{X} - \mathbb{E}\left(\mathtt{X}\right))^2\right)} = \sqrt{\mathbb{V}\left(\mathtt{X}\right)}, \end{aligned}$$

where the inequality also follows from Jensen's inequality among others. □

A.5 Proof of Proposition 6

First, assume $q \leq 2^n$. For any positive integer $k \leq q$, we have

$$\Pr\left(\Delta \geq k\right) \leq \sum_{x \in \mathbb{F}_{2^n}} \binom{q}{k} \frac{1}{2^{nk}} \leq 2^n \times \binom{q}{k} \frac{1}{2^{nk}} \leq 2^n \frac{q^k}{2^{nk} k!} \leq 2^n \left(\frac{qe}{k2^n}\right)^k,$$

[18] For if not, by dropping appropriate columns, we can find a $(k-1)$-regular sub-matrix.

where we use $k! \geq (k/e)^k$ for the last inequality. Then, since $\Delta \leq q$, we have

$$\mathbb{E}(\Delta) \leq (k-1) + q\Pr(\Delta \geq k) \leq (k-1) + q2^n \left(\frac{qe}{k2^n}\right)^k \leq (k-1) + 2^{2n}\left(\frac{e}{k}\right)^k.$$

For $q \leq 2^n$, the result then follows by setting $k = 4n$, as $2^{2n}(e/4n)^{4n} \leq 1$ for all $n \geq 1$. If $q < 4n$, the result is trivial as $\Delta \leq q$. For $q > 2^n$, divide the q sample into $\lceil q/2^n \rceil$ blocks, each of size at most 2^n. The result then follows by exploiting the linearity of expectation. □

A.6 Proof of Proposition 7

Let $k \coloneqq 3n\lceil q^2/2^n \rceil$. First, note that for any $d \neq 0$, and any $i \in [q]$, there is at most one $j \in [q]$ such that $\lambda_i \oplus \lambda_j = d$. So, $\nabla \leq q$, and the result is trivial if $2k > q$. Now, suppose $2k \leq q$. Since (i,j) and (j,i) are counted together, $\nabla \geq 2k$ implies that there exist some $d \neq 0$ and k pairwise disjoint pairs $\{i_1, j_1\}, \ldots, \{i_k, j_k\}$ such that $\lambda_{i_a} \oplus \lambda_{j_a} = d$ for all $a \in [k]$. For a fixed d and fixed pairs, this happens with probability at most $(2^n - 2k + 1)^{-k} \leq (2/2^n)^k$, as $\boldsymbol{\lambda}$ is sampled without replacement and $2k \leq q \leq 2^{n-1}$. There are at most $\binom{q^2/2}{k} \leq \left(\frac{q^2 e}{2k}\right)^k$ choices for the pairs, and thus

$$\Pr(\nabla \geq 2k) \leq 2^n \left(\frac{q^2 e}{2k}\right)^k \left(\frac{2}{2^n}\right)^k = 2^n \left(\frac{q^2 e}{k2^n}\right)^k \leq 2^n \left(\frac{e}{3n}\right)^k,$$

where the last inequality follows from $k \geq 3nq^2/2^n$. Then, since $\nabla \leq q \leq 2^n$ and $k \geq 3n$, we have

$$\mathbb{E}(\nabla) \leq (2k-1) + q\Pr(\nabla \geq 2k) \leq (2k-1) + 2^{2n}\left(\frac{e}{3n}\right)^{3n} \leq 2k,$$

where the last inequality holds for all $n \geq 2$. The result follows as $2k = 6n\lceil q^2/2^n \rceil$. □

B Deferred Proofs on Constrained Systems

B.1 Proof of Lemma 3

Since $\mathbb{S}_i$ is t-regular, partite and isolated, $r_i = t$ and $q_i = 1$. Then, recall from (10) and the subsequent discussion

$$\begin{aligned}
&\eta(\mathbb{S}_i \,|\, \mathcal{F}) \\
&= \sum_{\mathcal{J} \subseteq [t]} (-1)^{|\mathcal{J}|} |\mathcal{A}_{\mathcal{J}}| \\
&= \sum_{\mathcal{J} \subset [t]} (-1)^{|\mathcal{J}|} f_{(\mathcal{J})} N^{t-|\mathcal{J}|-1} + (-1)^t \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F})
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{N}\left(\sum_{\mathcal{J}\subset[t]} (-1)^{|\mathcal{J}|} f_{(\mathcal{J})} N^{t-|\mathcal{J}|} + (-1)^t \prod_{j=1}^{t} f_{\le(i-1),j} \right. \\
&\qquad\qquad \left. - (-1)^t \prod_{j=1}^{t} f_{\le(i-1),j} + (-1)^t N \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) \right) \\
&= \frac{1}{N}\left(\prod_{j=1}^{t} (N - f_{(j)}) + (-1)^t N \left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) - \frac{\prod_{j=1}^{t} f_{\le(i-1),j}}{N} \right) \right) \\
&= \frac{1}{N}\left(\prod_{j=1}^{t} (N - f_{\le(i-1),j}) + (-1)^t N \left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) - \frac{\prod_{j=1}^{t} f_{\le(i-1),j}}{N} \right) \right)
\end{aligned}
$$

where the second equality is due to (1) and the last equality is from a simple relabeling. □

B.2 Proof of Lemma 4

From (8) and Lemma 3, we have

$$
\begin{aligned}
&\eta(\mathbb{S}_{\le i} \,|\, \mathcal{R}) \\
&= \sum_{\boldsymbol{y}_{\le(i-1)}} \eta(\mathbb{S}_i \,|\, \mathcal{F}(\boldsymbol{y}_{\le(i-1)})) \\
&= \sum_{\boldsymbol{y}_{\le(i-1)}} \frac{1}{N}\left(\prod_{j=1}^{t} (N - f_{\le(i-1),j}) + (-1)^t N \left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) - \frac{\prod_{j=1}^{t} f_{\le(i-1),j}}{N} \right) \right) \\
&\ge \sum_{\boldsymbol{y}_{\le(i-1)}} \frac{1}{N}\left(\prod_{j=1}^{t} (N - f_{\le(i-1),j}) - N \left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) + \frac{\prod_{j=1}^{t} f_{\le(i-1),j}}{N} \right) \right) \\
&\ge \sum_{\boldsymbol{y}_{\le(i-1)}} \frac{\prod_{j=1}^{t} (N - f_{\le(i-1),j})}{N} \left(1 - \frac{2}{N^{t-1}} \left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) + \frac{\prod_{j=1}^{t} f_{\le(i-1),j}}{N} \right) \right) \\
&= \frac{\prod_{j=1}^{t} (N - f_{\le(i-1),j})}{N} \left(\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) - \frac{2 \prod_{j=1}^{t} f_{\le(i-1),j}}{N^t} \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) \right. \\
&\qquad\qquad \left. - \frac{2}{N^{t-1}} \sum_{\boldsymbol{y}_{\le(i-1)}} \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) \right),
\end{aligned}
\tag{21}
$$

where the first inequality follows from $(-1)^t(\mu - x) \ge -(\mu + x)$ for any $\mu, x \ge 0$, and the second inequality follows from the fact that $f_{\le(i-1),j} \le (s+q)$ and $t(s+q) \le \xi_{\mathbb{S}}(s+q) \le N/2$.

We claim

$$\sum_{\boldsymbol{y}_{\leq(i-1)}} \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) \leq \left(\mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}) + \Delta_{\mathbb{S}} + \frac{2(s+q)^t}{N}\right) \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \tag{22}$$

The lemma then follows by substituting the claimed bound in (21). □

Proof of Claim (22). We have

$$\begin{aligned}\sum_{\boldsymbol{y}_{\leq(i-1)}} \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{F}) &= \sum_{\boldsymbol{y}_{\leq(i-1)}} \sum_{\mathcal{I}\subseteq[t]} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_{\mathcal{I}}, \hat{\mathcal{R}}_{[t]\setminus\mathcal{I}}) \\ &= \sum_{\mathcal{I}\subseteq[t]} \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_{\mathcal{I}}, \hat{\mathcal{R}}_{[t]\setminus\mathcal{I}})\end{aligned}$$

where $\hat{\mathcal{P}}_{\mathcal{I}} = \hat{\mathcal{P}}_{j_1} \times \ldots \times \hat{\mathcal{P}}_{j_m}$ and $\hat{\mathcal{R}}_{[t]\setminus\mathcal{I}} = \hat{\mathcal{R}}_{k_1} \times \ldots \times \hat{\mathcal{R}}_{k_{m'}}$ for every $\mathcal{I} = \{j_1, \ldots, j_m\}$ and $[t] \setminus \mathcal{I} = \{k_1, \ldots, k_{m'}\}$. For brevity we simply write $\mathcal{I} = [m]$. Consider the following two cases:

- Case A: $\mathcal{I} = \emptyset$. In this case the definition straightaway gives

  $$\sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_{[t]}) = \mu_{\boldsymbol{\alpha}_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}) \times \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}).$$

  We remark that for $i = 1$ this is the only possible case.

- Case B: $\mathcal{I} \neq \emptyset \subseteq [t]$. Fix some $(a_{t-m+1}, \ldots, a_t) \in \hat{\mathcal{R}}_{[t]\setminus\mathcal{I}}$ and define $a_{\oplus} \coloneqq a_{t-m+1} \oplus \ldots \oplus a_t$, with $a_{\oplus} = 0$ whenever $\mathcal{I} = [t]$. Fix some $(y_{l_1}, \ldots, y_{l_m}) \in \hat{\mathcal{P}}_1 \times \ldots \times \hat{\mathcal{P}}_m$. Then, we have

  $$\sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, y_{l_1}, \ldots, y_{l_m}, a_{t-m+1}, \ldots, a_t) = \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i \ominus a_{\oplus}, y_{l_1}, \ldots, y_{l_m}) \tag{23}$$

  Thus, we want to count the number of solutions for $\mathbb{S}_{\leq(i-1)}$ that additionally satisfies the equation $\alpha_{l_1} \cdot \boldsymbol{x}_{l_1} \oplus \ldots \oplus \alpha_{l_m} \cdot \boldsymbol{x}_{l_m} = \boldsymbol{\lambda}_i \ominus a_{\oplus}$.
  Let $\mathbb{S}'_{\leq(i-1)} = \mathbb{S}_{\leq(i-1)} \cup \{\alpha_{l_1} \cdot \boldsymbol{x}_{l_1} \oplus \ldots \oplus \alpha_{l_m} \cdot \boldsymbol{x}_{l_m} = \boldsymbol{\lambda}_i \ominus a_{\oplus}\}$ be the constrained system $\mathbb{S}_{\leq(i-1)}$ extended with the additional equation $\alpha_{l_1} \cdot \boldsymbol{x}_{l_1} \oplus \ldots \oplus \alpha_{l_m} \cdot \boldsymbol{x}_{l_m} = \boldsymbol{\lambda}_i \ominus a_{\oplus}$. Then, by definition, we have

  $$\sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i \ominus a_{\oplus}, y_{l_1}, \ldots, y_{l_m}) = \eta(\mathbb{S}'_{\leq(i-1)} \,|\, \mathcal{R}).$$

  Let $A'_{\leq(i-1)}$ denote the corresponding coefficient matrix. We can have two cases based on the rank of $A'_{\leq(i-1)}$:

  - Case B1: $A'_{\leq(i-1)}$ has full row rank. Suppose $l_m \in \mathrm{col}_{\overline{A}_j}$ for some $j \leq (i-1)$ and let $\mathbb{S}_{\leq(i-1)\setminus j}$ denote the constrained system that excludes $\mathbb{S}_j$. Then, using the fact that $A'_{\leq(i-1)}$ is full rank, we have

    $$\eta(\mathbb{S}'_{\leq(i-1)} \,|\, \mathcal{R}) \leq N^{t-2} \times \eta(\mathbb{S}_{\leq(i-1)\setminus j} \,|\, \mathcal{R}),$$

and further, using the crude bound (Fact 2) for the isolated partite block $\mathbb{S}_j$ (where $r_j = t$, $q_j = 1$ and the EQ term vanishes), we have $\eta(\mathbb{S}_{\leq(i-1)} \mid \mathcal{R}) \geq (N^{t-1} - t(s+q)N^{t-2}) \times \eta(\mathbb{S}_{\leq(i-1)\setminus j} \mid \mathcal{R})$ holds as $\mathbb{S}_{\leq(i-1)}$ is acyclic and t-regular. Thus,

$$\eta(\mathbb{S}'_{\leq(i-1)} \mid \mathcal{R}) \leq \frac{2}{N}\eta(\mathbb{S}_{\leq(i-1)} \mid \mathcal{R}),$$

where we use the fact that $t(s+q) \leq N/2$. There are at most $\binom{t}{m}$ choices for $\mathcal{I}$ and for each such choice there are at most $q^m s^{t-m}$ choices for $(l_1, \ldots, l_m, a_{t-m+1}, \ldots, a_t)$, which finally gives

$$\sum_{\mathcal{I}\subseteq[t]} \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_{\mathcal{I}}, \hat{\mathcal{R}}_{[t]\setminus\mathcal{I}}) \leq \frac{2(s+q)^t}{N}\eta(\mathbb{S}_{\leq(i-1)} \mid \mathcal{R}).$$

- Case B2: $A'_{\leq(i-1)}$ does not have full row rank. This case is only possible if the additional equation is defined by the equations in $\mathbb{S}_{\leq(i-1)}$. Since $\mathbb{S}_{\leq(i-1)}$ is isolated, this case is only possible if the additional equation is redundant, i.e., $\mathcal{I} = [t]$, $\{l_1, \ldots, l_t\} = \mathrm{col}(\overline{A}_j)$ for some $j \leq (i-1)$, and $\lambda_j = \lambda_i$. Since there is only one choice for $\mathcal{I}$, and at most $\Delta_{\mathbb{S}}$ choices for j, the number of solutions in this case is bounded by $\Delta_{\mathbb{S}}\eta(\mathbb{S}_{\leq(i-1)} \mid \mathcal{R})$.

The claim then follows by combining the bounds in all cases. □

B.3 Proof of Lemma 5

From (9), (10) and (12), we have that

$$\eta(\mathbb{S}_i \mid \mathcal{F}) \geq \sum_{\mathcal{J}\subseteq[r_i]} (-1)^{|\mathcal{J}|}|\mathcal{A}_{\mathcal{J}}| - tq_i^2 N^{r_i - q_i - 1},$$

where we use that the number of pairs $j_1 < j_2$ in $\mathrm{col}(\overline{A}_i) \cap \mathsf{P}_k$ is $\binom{r_{i,k}}{2} \leq q_i^2/2$, as $\mathbb{S}$ is partite and thus each equation has at most one variable in P_k. First, for the even t case, by a simple application of Bonferroni's inequality [30] and the fact that $f_{(j)} \leq (s+q)$ for any j and $r_i(s+q) \leq \xi_{\mathbb{S}}(s+q) \leq N/2$, we have

$$\eta(\mathbb{S}_i \mid \mathcal{F}) \geq \frac{\prod_{j=1}^{r_i}(N - f_{(j)})}{N^{q_i}} \left(1 - \frac{2tq_i^2}{N} - \frac{2r_i^t(s+q)^t}{N^t}\right). \tag{24}$$

A short derivation is given after this proof. For the odd t case, using Bonferroni's inequality, we have

$$\begin{aligned}\sum_{\substack{\mathcal{J}\subseteq[r_i]\\|\mathcal{J}|\leq t}} (-1)^{|\mathcal{J}|}|\mathcal{A}_{\mathcal{J}}| &\geq \sum_{\substack{\mathcal{J}\subseteq[r_i]\\|\mathcal{J}|<t}} (-1)^{|\mathcal{J}|} f_{(\mathcal{J})} N^{r_i - |\mathcal{J}| - q_i} - \sum_{\substack{\mathcal{J}\subseteq[r_i]\\|\mathcal{J}|=t}} |\mathcal{A}_{\mathcal{J}}| \\ &\geq \frac{1}{N^{q_i}} \left(\sum_{\substack{\mathcal{J}\subseteq[r_i]\\|\mathcal{J}|<t}} (-1)^{|\mathcal{J}|} f_{(\mathcal{J})} N^{r_i - |\mathcal{J}|} - N^{q_i} \sum_{\substack{\mathcal{J}\subseteq[r_i]\\|\mathcal{J}|=t}} |\mathcal{A}_{\mathcal{J}}| \right)\end{aligned}$$

$$\geq \frac{1}{N^{q_i}} \left(\prod_{j=1}^{r_i} (N - f_{(j)}) - N^{q_i} \sum_{\substack{\mathcal{J} \subseteq [r_i] \\ |\mathcal{J}|=t}} |\mathcal{A}_{\mathcal{J}}| \right)$$

$$\geq \frac{\prod_{j=1}^{r_i} (N - f_{(j)})}{N^{q_i}} \left(1 - \frac{2}{N^{r_i - q_i}} \sum_{\substack{\mathcal{J} \subseteq [r_i] \\ |\mathcal{J}|=t}} |\mathcal{A}_{\mathcal{J}}| \right) \tag{25}$$

We claim $\sum_{\substack{\mathcal{J} \subseteq [r_i] \\ |\mathcal{J}|=t}} |\mathcal{A}_{\mathcal{J}}| \leq q_i (s+q)^{t-1} N^{r_i - t - q_i + 1} + r_i^t (s+q)^t N^{r_i - t - q_i}$.

Let $\mathcal{J} = \{l_1, \ldots, l_t\}$ and suppose $\mathbb{S}_i'$ denote the updated system after the removal of these t columns from $\mathbb{S}_i$. Using Proposition 4, we have two cases:

- Case A: $\mathcal{J} = \mathrm{col}(\overline{A}_{j\bullet})$ for some $A_{j\bullet} \in \mathrm{row}(A_i)$. From Proposition 4 we know that $\mathrm{rank}(\mathbb{S}_i') = q_i - 1$. Thus, we have

$$\sum_{\substack{\mathcal{J} = \mathrm{col}(\overline{A}_{j\bullet}) \\ A_{j\bullet} \in \mathrm{row}(A_i)}} |\mathcal{A}_{\mathcal{J}}| \leq q_i (s+q)^{t-1} N^{r_i - t - q_i + 1}.$$

- Case B: $\mathcal{J} \neq \mathrm{col}(\overline{A}_{j\bullet})$ for all $A_{j\bullet} \in \mathrm{row}(A_i)$. From Proposition 4 we know that $\mathrm{rank}(\mathbb{S}_i') = q_i$. Thus, we have

$$\sum_{\mathcal{J} \neq \mathrm{col}(\overline{A}_{j\bullet})} |\mathcal{A}_{\mathcal{J}}| \leq r_i^t (s+q)^t N^{r_i - t - q_i}.$$

This proves the claim. The result follows by substituting the claimed bound in (25), subtracting the term $tq_i^2 N^{r_i - q_i - 1} \leq \frac{2tq_i^2}{N} \cdot \frac{\prod_{j=1}^{r_i}(N - f_{(j)})}{N^{q_i}}$ as in the even case, and realizing that

$$\prod_{j=1}^{r_i} (N - f_{(j)}) = \prod_{k=1}^{t} (N - f_{\leq (i-1),k})^{r_{i,k}} \qquad \square$$

Derivation of (24). We have

$$\sum_{\substack{\mathcal{J} \subseteq [r_i] \\ |\mathcal{J}| \leq t-1}} (-1)^{|\mathcal{J}|} |\mathcal{A}_{\mathcal{J}}| \geq \sum_{\substack{\mathcal{J} \subseteq [r_i] \\ |\mathcal{J}| \leq t-1}} (-1)^{|\mathcal{J}|} f_{(\mathcal{J})} N^{r_i - |\mathcal{J}| - q_i}$$

$$\geq \frac{1}{N^{q_i}} \left(\sum_{\substack{\mathcal{J} \subseteq [r_i] \\ |\mathcal{J}| \leq t}} (-1)^{|\mathcal{J}|} f_{(\mathcal{J})} N^{r_i - |\mathcal{J}|} - \sum_{\substack{\mathcal{J}' \subseteq [r_i] \\ |\mathcal{J}'| = t}} f_{(\mathcal{J}')} N^{r_i - t} \right)$$

$$\geq \frac{1}{N^{q_i}} \left(\prod_{j=1}^{r_i} (N - f_{(j)}) - r_i^t (s+q)^t N^{r_i - t} \right)$$

$$\geq \frac{\prod_{j=1}^{r_i}(N - f_{(j)})}{N^{q_i}} \left(1 - \frac{2r_i^t(s+q)^t}{N^t}\right),$$

where the last inequality follows from the fact that $f_{(j)} \leq (s+q)$ for any j and $r_i(s+q) \leq \xi_{\mathbb{S}}(s+q) \leq N/2$.

B.4 Proof of Lemma 6

Since all the blocks before $\mathbb{S}_i$ are isolated, each of them contributes exactly one variable to each class, and thus $f_{\leq(i-1),j} = s_j + (i-1)$ for $j \in [2]$. From (8), Lemma 3 and $t = 2$, we have

$$\begin{aligned}
&\eta(\mathbb{S}_{\leq i} \,|\, \mathcal{R}) \\
&= \sum_{\boldsymbol{y}_{\leq(i-1)}} \eta(\mathbb{S}_i \,|\, \mathcal{F}(\boldsymbol{y}_{\leq(i-1)})) \\
&= \sum_{\boldsymbol{y}_{\leq(i-1)}} \frac{1}{N} \left(\prod_{j=1}^{2}(N - f_{\leq(i-1),j}) + N\left(\mu(\boldsymbol{\lambda}_i, \hat{\mathcal{F}}) - \frac{f_{\leq(i-1),1} f_{\leq(i-1),2}}{N}\right)\right)
\end{aligned}$$

Put $\delta(N) = N/\prod_{j=1}^{2}(N - f_{\leq(i-1),j})$ and continue

$$\begin{aligned}
&= \sum_{\boldsymbol{y}_{\leq(i-1)}} \frac{\prod_{j=1}^{2}(N - f_{\leq(i-1),j})}{N} \left(1 + \delta(N)\left(\mu(\boldsymbol{\lambda}_i, \hat{\mathcal{F}}) - \frac{f_{\leq(i-1),1} f_{\leq(i-1),2}}{N}\right)\right) \\
&= \sum_{\boldsymbol{y}_{\leq(i-1)}} \frac{\prod_{j=1}^{2}(N - f_{\leq(i-1),j})}{N} \Bigg(1 + \delta(N)\Bigg(\mu(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2) - \frac{s_1 s_2}{N} + \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2) \\
&\qquad - \frac{s_1(i-1)}{N} + \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{R}}_2) - \frac{(i-1)s_2}{N} + \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{P}}_2) - \frac{(i-1)^2}{N}\Bigg)\Bigg) \\
&\geq \frac{\prod_{j=1}^{2}(N - f_{\leq(i-1),j})}{N} \Bigg(\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \delta(N)\left|\mu_{\alpha_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R}_1, \mathcal{R}_2) - \frac{s_1 s_2}{N}\right| \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \\
&\qquad - \delta(N) \underbrace{\left(\frac{s_1(i-1)}{N}\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2)\right)}_{\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2)} \\
&\qquad - \delta(N) \underbrace{\left(\frac{(i-1)s_2}{N}\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{R}}_2)\right)}_{\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{R}}_2)}
\end{aligned}$$

$$- \delta(N) \underbrace{\left(\frac{(i-1)^2}{N} \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{P}}_2) \right)}_{\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{P}}_2)} \Bigg) \tag{26}$$

Claim. We claim

$$\begin{aligned}
\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2) &\leq \left(\frac{2(s+q)}{N} (\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}}) + \frac{4(s+q)q^2}{N^2} \right) \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \\
\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{R}}_2) &\leq \left(\frac{2(s+q)}{N} (\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}}) + \frac{4(s+q)q^2}{N^2} \right) \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \\
\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{P}}_2) &\leq \left(\frac{2q\Delta_{\mathbb{S}}}{N} + \frac{4q^2(q+s)}{N^2} \right) \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R})
\end{aligned}$$

Proof. Let $\boldsymbol{x}_k^1, \boldsymbol{x}_k^2$ denote the variables corresponding to the k-th equations. Analogously, for $k \leq (i-1)$, we write y_k^1, y_k^2 to denote the solution assigned to the variables corresponding to the k-th equation. Let

$$\begin{aligned}
\mathcal{M}_1 &:= \left\{ (x,j) \in \mathcal{R}_1 \times [i-1] \,:\, \boldsymbol{\lambda}_j \neq \boldsymbol{\lambda}_i,\, \boldsymbol{\lambda}_i \ominus \alpha_1 \cdot x \notin \hat{\mathcal{R}}_2,\, \boldsymbol{\lambda}_j \ominus \boldsymbol{\lambda}_i \oplus \alpha_1 \cdot x \notin \hat{\mathcal{R}}_1 \right\} \\
\mathcal{M}_2 &:= \left\{ (j,x) \in [i-1] \times \mathcal{R}_2 \,:\, \boldsymbol{\lambda}_j \neq \boldsymbol{\lambda}_i,\, \boldsymbol{\lambda}_i \ominus \alpha_2 \cdot x \notin \hat{\mathcal{R}}_1,\, \boldsymbol{\lambda}_j \ominus \boldsymbol{\lambda}_i \oplus \alpha_2 \cdot x \notin \hat{\mathcal{R}}_2 \right\} \\
\mathcal{M}_3 &:= \{ (j,j') \in [i-1]^2 \,:\, j \neq j',\, \boldsymbol{\lambda}_j, \boldsymbol{\lambda}_{j'} \neq \boldsymbol{\lambda}_i \}
\end{aligned}$$

Let g_i be the number of $j \in [i-1]$ such that $\boldsymbol{\lambda}_j \neq \boldsymbol{\lambda}_i$. As at most $\Delta_{\mathbb{S}}$ constants are equal to $\boldsymbol{\lambda}_i$, including $\boldsymbol{\lambda}_i$ itself, we have $d_i := i - 1 - g_i \leq \Delta_{\mathbb{S}} - 1$. Then, it is easy to see that

$$\begin{aligned}
g_i(s_1 - 2\nabla_{\hat{\mathcal{R}}}) \leq |\mathcal{M}_1| &\leq (i-1)s_1 \\
g_i(s_2 - 2\nabla_{\hat{\mathcal{R}}}) \leq |\mathcal{M}_2| &\leq (i-1)s_2 \\
|\mathcal{M}_3| = g_i(g_i - 1) &\leq (i-1)^2
\end{aligned}$$

Indeed, for each of the g_i indices j with $\boldsymbol{\lambda}_j \neq \boldsymbol{\lambda}_i$, the second condition in $\mathcal{M}_1$ fails for at most $\nabla_{\hat{\mathcal{R}}}$ values of x, as it asks for a sum in $\hat{\mathcal{R}}_1 \times \hat{\mathcal{R}}_2$ to equal $\boldsymbol{\lambda}_i$, and the third condition fails for at most $\nabla_{\hat{\mathcal{R}}}$ values of x, as it asks for a difference in $\hat{\mathcal{R}}_1 \times \hat{\mathcal{R}}_1$ to equal $\boldsymbol{\lambda}_j \ominus \boldsymbol{\lambda}_i \neq 0$. We prove the first and third inequality. As for the second inequality, it can be argued in a similar fashion as the first one.
First consider

$$\begin{aligned}
\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2) &\leq \frac{s_1(i-1)}{N} \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2) \\
&\leq \frac{s_1(i-1)}{N} \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \sum_{(x,j) \in \mathcal{M}_1} \mu(\boldsymbol{\lambda}_i, \alpha_1 \cdot x, \alpha_2 \cdot y_j^2)
\end{aligned}$$

$$= \frac{s_1(i-1)}{N}\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) - \sum_{(x,j)\in\mathcal{M}_1} \sum_{\boldsymbol{y}_{\le(i-1)}} \mu(\boldsymbol{\lambda}_i, \alpha_1 \cdot x, \alpha_2 \cdot y_j^2)$$

Thus, we have to count the number of solutions $\boldsymbol{y}_{\le(i-1)}$ that additionally satisfy $\alpha_1 \cdot x \oplus \alpha_2 \cdot y_j^2 = \boldsymbol{\lambda}_i$ for all valid (x, j). Let $\mathbb{S}_{\le(i-1)\setminus\{j\}}$ denote the system that excludes $\mathbb{S}_j$. Then, the second summand on the right hand side can be rewritten as

$$\sum_{(x,j)\in\mathcal{M}_1} \sum_{\boldsymbol{y}_{\le(i-1)}} \mu(\boldsymbol{\lambda}_i, \alpha_1 \cdot x, \alpha_2 \cdot y_j^2) = \sum_{(x,j)\in\mathcal{M}_1} \eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}'(x,j)),$$

where $\mathcal{R}'(x,j) := (\mathcal{R}'_1(x,j), \mathcal{R}'_2(x,j))$, $\mathcal{R}'_1(x,j) := \mathcal{R}_1 \cup \left\{\frac{\boldsymbol{\lambda}_j \ominus \boldsymbol{\lambda}_i \oplus \alpha_1 \cdot x}{\alpha_1}\right\}$, and $\mathcal{R}'_2(x,j) := \mathcal{R}_2 \cup \left\{\frac{\boldsymbol{\lambda}_i \ominus \alpha_1 \cdot x}{\alpha_2}\right\}$. Using Fact 1, it is obvious that

$$\eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}'(x,j)) \le \eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}),$$

since $(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}'(x,j)) \subseteq (\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R})$.

Now, a solution in $(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R})$ is not in $(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}'(x,j))$ if and only if there exists a $k \in [i-1]\setminus\{j\}$ such that $y_k^1 = \frac{\boldsymbol{\lambda}_j \ominus \boldsymbol{\lambda}_i \oplus \alpha_1 \cdot x}{\alpha_1}$ or $y_k^2 = \frac{\boldsymbol{\lambda}_i \ominus \alpha_1 \cdot x}{\alpha_2}$. Using Fact 2, such solutions are at most $2\eta(\mathbb{S}_{\le(i-1)\setminus\{j,k\}} \,|\, \mathcal{R})$ for each k, where $\mathbb{S}_{\le(i-1)\setminus\{j,k\}}$ denote the system excluding $\mathbb{S}_j$ and $\mathbb{S}_k$. Thus, we have

$$\begin{aligned}
\eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}'(x,j)) &\ge \eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}) - 2 \sum_{k\in[i-1]\setminus\{j\}} \eta(\mathbb{S}_{\le(i-1)\setminus\{j,k\}} \,|\, \mathcal{R}) \\
&\ge \eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R}) - 2 \sum_{k\in[i-1]\setminus\{j\}} \frac{\eta(\mathbb{S}_{\le(i-1)\setminus\{j\}} \,|\, \mathcal{R})}{N - 2s - 2(i-1)} \\
&\ge \frac{\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})}{N} \left(1 - \frac{2i}{N - 2s - 2(i-1)}\right),
\end{aligned}$$

where the second and third inequalities follow from Fact 2, and $s_1 + s_2 \le 2s$. Finally, using $2(s + i - 1) \le N/2$, we have

$$\begin{aligned}
\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{R}}_1, \hat{\mathcal{P}}_2) &\le \frac{s_1(i-1)}{N}\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) - \frac{|\mathcal{M}_1|}{N}\left(1 - \frac{4i}{N}\right)\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) \\
&\le \left(\frac{s+q}{N}(\Delta_{\mathbb{S}} + 2\nabla_{\hat{\mathcal{R}}}) + \frac{4(s+q)q^2}{N^2}\right)\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}), \qquad (27)
\end{aligned}$$

and similarly,

$$\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{R}}_2) \le \left(\frac{s+q}{N}(\Delta_{\mathbb{S}} + 2\nabla_{\hat{\mathcal{R}}}) + \frac{4(s+q)q^2}{N^2}\right)\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}). \qquad (28)$$

Now, consider

$$\varepsilon(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{P}}_2) \le \frac{(i-1)^2}{N}\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\le(i-1)}} \mu(\boldsymbol{\lambda}_i, \hat{\mathcal{P}}_1, \hat{\mathcal{P}}_2)$$

$$\leq \frac{(i-1)^2}{N}\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \sum_{(j,j')\in\mathcal{M}_3} \mu(\boldsymbol{\lambda}_i, \alpha_1 \cdot y_j^1, \alpha_2 \cdot y_{j'}^2)$$

$$= \frac{(i-1)^2}{N}\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{(j,j')\in\mathcal{M}_3} \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \alpha_1 \cdot y_j^1, \alpha_2 \cdot y_{j'}^2)$$

We want to count the number of solutions $\boldsymbol{y}_{\leq(i-1)}$ that additionally satisfy $\alpha_1 \cdot y_j^1 \oplus \alpha_2 \cdot y_{j'}^2 = \boldsymbol{\lambda}_i$ for all valid (j, j'). Let $\mathbb{S}_{\leq(i-1)\cup\{j-j'\}}$ denote the system $\mathbb{S}_{\leq(i-1)} \cup \{\alpha_1 \cdot \boldsymbol{x}_j^1 \oplus \alpha_2 \cdot \boldsymbol{x}_{j'}^2 = \boldsymbol{\lambda}_i\}$. Then, we can rewrite the second summand on the right hand side as

$$\sum_{(j,j')\in\mathcal{M}_3} \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \alpha_1 \cdot y_j^1, \alpha_2 \cdot y_{j'}^2) = \sum_{(j,j')\in\mathcal{M}_3} \eta(\mathbb{S}_{\leq(i-1)\cup\{j-j'\}} \,|\, \mathcal{R}).$$

Let $\mathbb{S}_{\leq(i-1)\setminus\{j'\}}$ denote the system after excluding $\mathbb{S}_{j'} \cup \{\alpha_1 \cdot \boldsymbol{x}_j^1 \oplus \alpha_2 \cdot \boldsymbol{x}_{j'}^2 = \boldsymbol{\lambda}_i\}$. Then, it is obvious that

$$\eta(\mathbb{S}_{\leq(i-1)\cup\{j-j'\}} \,|\, \mathcal{R}) \leq \eta(\mathbb{S}_{\leq(i-1)\setminus\{j'\}} \,|\, \mathcal{R})$$

Now, a solution in $(\mathbb{S}_{\leq(i-1)\setminus\{j'\}} \,|\, \mathcal{R})$ does not extend to a solution in $(\mathbb{S}_{\leq(i-1)\cup\{j-j'\}} \,|\, \mathcal{R})$ if and only if $\frac{\boldsymbol{\lambda}_i \ominus \alpha_1 \cdot y_j^1}{\alpha_2} \in \mathcal{R}_2$, or $\frac{\boldsymbol{\lambda}_{j'} \ominus \boldsymbol{\lambda}_i \oplus \alpha_1 \cdot y_j^1}{\alpha_1} \in \mathcal{R}_1$, or there exists a $k \in [i-1] \setminus \{j'\}$ such that $y_k^2 = \frac{\boldsymbol{\lambda}_i \ominus \alpha_1 \cdot y_j^1}{\alpha_2}$ or $y_k^1 = \frac{\boldsymbol{\lambda}_{j'} \ominus \boldsymbol{\lambda}_i \oplus \alpha_1 \cdot y_j^1}{\alpha_1}$. The first two events fix y_j^1 to one of at most $s_1 + s_2 \leq 2s$ values, and thus such solutions are at most $2s\eta(\mathbb{S}_{\leq(i-1)\setminus\{j',j\}} \,|\, \mathcal{R})$. For the last event, such solutions are at most $2\eta(\mathbb{S}_{\leq(i-1)\setminus\{j',k\}} \,|\, \mathcal{R})$ for each k, where $\mathbb{S}_{\leq(i-1)\setminus\{j',k\}}$ denote the system excluding $\mathbb{S}_{j'}$ and $\mathbb{S}_k$. Thus, we have

$$\begin{aligned}
\eta(\mathbb{S}_{\leq(i-1)\cup\{j-j'\}} \,|\, \mathcal{R}) &\geq \eta(\mathbb{S}_{\leq(i-1)\setminus\{j'\}} \,|\, \mathcal{R}) - 2s\eta(\mathbb{S}_{\leq(i-1)\setminus\{j',j\}} \,|\, \mathcal{R}) \\
&\qquad - 2 \sum_{k\in[i-1]\setminus\{j'\}} \eta(\mathbb{S}_{\leq(i-1)\setminus\{j',k\}} \,|\, \mathcal{R}) \\
&\geq \eta(\mathbb{S}_{\leq(i-1)\setminus\{j'\}} \,|\, \mathcal{R}) - 2(s+i)\frac{\eta(\mathbb{S}_{\leq(i-1)\setminus\{j'\}} \,|\, \mathcal{R})}{N - 2s - 2(i-1)} \\
&\geq \frac{\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R})}{N}\left(1 - \frac{2(s+i)}{N - 2s - 2(i-1)}\right),
\end{aligned}$$

where the second and third inequalities follow from Fact 2, and $s_1 + s_2 \leq 2s$. Finally, using $2(s+i-1) \leq N/2$ and $(i-1)^2 - g_i(g_i-1) = (2d_i+1)(i-1) - d_i(d_i+1) \leq 2(i-1)\Delta_{\mathbb{S}}$, we have

$$\begin{aligned}
\varepsilon(\boldsymbol{\lambda}_i, \mathcal{P}_1, \mathcal{P}_2) &\leq \frac{(i-1)^2}{N}\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \frac{|\mathcal{M}_3|}{N}\left(1 - \frac{4(s+i)}{N}\right)\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \\
&\leq \left(\frac{2q\Delta_{\mathbb{S}}}{N} + \frac{4q^2(q+s)}{N^2}\right)\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \qquad (29)
\end{aligned}$$

Lemma 6 now follows by combining (26) with (27)-(29), and taking $\delta(N) \leq 2/N$. □

B.5 Proof of Corollary 4

Since $\mathbb{S}$ is column-uniform with a single class, we have $\alpha_{\mathbb{S}} = (\alpha, \alpha)$ for some $\alpha \neq 0$. Dividing every equation by α changes neither the solutions, nor $\Delta_{\mathbb{S}}$, nor $\mu_{\alpha_{\mathbb{S}}}(\boldsymbol{\lambda}_i, \mathcal{R})$ (which becomes $\mu(\boldsymbol{\lambda}_i/\alpha, \mathcal{R}, \mathcal{R})$). So, without loss of generality, we assume $\alpha = 1$. Then $\hat{\mathcal{R}} = \mathcal{R}$, and every equation is of the form $x^1 \oplus x^2 = \lambda$. Since $\mathbb{S}$ is non-trivial, we have $\lambda \neq 0$ for every isolated equation. As before, we order the blocks so that the isolated blocks $\mathbb{S}_1, \ldots, \mathbb{S}_m$ come first. For $i \leq m$, we write y_k^1, y_k^2 for the values assigned to the two variables of $\mathbb{S}_k$, and let $\mathcal{P} = \mathcal{P}(\boldsymbol{y}_{\leq(i-1)})$ be the set of all values in $\boldsymbol{y}_{\leq(i-1)}$. Then $\mathcal{F} = \mathcal{R} \sqcup \mathcal{P}$, and $f := |\mathcal{F}| = s + 2(i-1) \leq s + 2q \leq N/4$ for every $\boldsymbol{y}_{\leq(i-1)}$.

Isolated blocks. Fix some $i \leq m$. The number of $(y_1, y_2) \in (\mathbb{F}_N \setminus \mathcal{F})^2$ such that $y_1 \oplus y_2 = \boldsymbol{\lambda}_i$ is exactly $N - 2f + \mu(\boldsymbol{\lambda}_i, \mathcal{F}, \mathcal{F})$, and at most one such pair has $y_1 = y_2$ (none in characteristic 2, as $\boldsymbol{\lambda}_i \neq 0$). Put $\delta(N) = N/(N-f)^2 \leq 2/N$. Then, similar to (26), and using $\mu(\boldsymbol{\lambda}_i, \mathcal{P}, \mathcal{R}) = \mu(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{P})$, we have

$$\begin{aligned}
\eta(\mathbb{S}_{\leq i} \,|\, \mathcal{R}) &\geq \sum_{\boldsymbol{y}_{\leq(i-1)}} \frac{(N-f)^2}{N} \left(1 + \delta(N) \left(\mu(\boldsymbol{\lambda}_i, \mathcal{F}, \mathcal{F}) - \frac{f^2}{N} - 1\right)\right) \\
&\geq \frac{(N-f)^2}{N} \Bigg(\eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \delta(N) \left(\left|\mu(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{R}) - \frac{s^2}{N}\right| + 1\right) \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) \\
&\quad - 2\delta(N) \underbrace{\left(\frac{2s(i-1)}{N} \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{P}) \right)}_{\varepsilon(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{P})} \\
&\quad - \delta(N) \underbrace{\left(\frac{4(i-1)^2}{N} \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R}) - \sum_{\boldsymbol{y}_{\leq(i-1)}} \mu(\boldsymbol{\lambda}_i, \mathcal{P}, \mathcal{P}) \right)}_{\varepsilon(\boldsymbol{\lambda}_i, \mathcal{P}, \mathcal{P})} \Bigg).
\end{aligned}$$

We will repeatedly use the following two simple observations. First, $\eta(\mathbb{S}_{\leq(i-1)\setminus\mathcal{K}} \,|\, \mathcal{R}) \geq \eta(\mathbb{S}_{\leq(i-1)} \,|\, \mathcal{R})/N^{|\mathcal{K}|}$ for any $\mathcal{K} \subseteq [i-1]$, as each block has at most N solutions. Second, $\eta(\mathbb{S}_{\leq(i-1)\setminus\{k,k'\}} \,|\, \mathcal{R}) \leq \eta(\mathbb{S}_{\leq(i-1)\setminus\{k\}} \,|\, \mathcal{R})/(N-2f)$, as any solution of the former extends to at least $N - 2f$ solutions of the latter. First consider $\varepsilon(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{P})$. Let

$$\mathcal{M} := \{(x, k, b) \in \mathcal{R} \times [i-1] \times [2] \,:\, \boldsymbol{\lambda}_i \ominus x \notin \mathcal{R},\, \boldsymbol{\lambda}_k \ominus \boldsymbol{\lambda}_i \oplus x \notin \mathcal{R},\, \boldsymbol{\lambda}_i \ominus x \neq \boldsymbol{\lambda}_k \ominus \boldsymbol{\lambda}_i \oplus x\}\,.$$

If $(x, k, b) \notin \mathcal{M}$, then no solution has $y_k^b = \boldsymbol{\lambda}_i \ominus x$, as y_k^b and $y_k^{3-b} = \boldsymbol{\lambda}_k \ominus \boldsymbol{\lambda}_i \oplus x$ must be distinct and both lie outside $\mathcal{R}$. Now, for each (k, b), the first condition fails for at most $\nabla_{\hat{\mathcal{R}}}$ values of x, as $\boldsymbol{\lambda}_i \neq 0$. The second condition fails for at most $\nabla_{\hat{\mathcal{R}}}$ values of x if $\boldsymbol{\lambda}_k \neq \boldsymbol{\lambda}_i$, and for all s values of x otherwise. The third condition fails for at most one value of x (and for none in characteristic 2, as $\boldsymbol{\lambda}_k \neq 0$). There are at most $\Delta_{\mathbb{S}}$ choices of k with $\boldsymbol{\lambda}_k = \boldsymbol{\lambda}_i$. Thus, $|\mathcal{M}| \geq 2(i-1)(s - 2\nabla_{\hat{\mathcal{R}}} - 1) - 2\Delta_{\mathbb{S}} s$. For $(x, k, b) \in \mathcal{M}$, the number of solutions with

$y_k^b = \boldsymbol{\lambda}_i \ominus x$ is $\eta(\mathbb{S}_{\le(i-1)\setminus\{k\}} \,|\, \mathcal{R}')$, where $\mathcal{R}' = \mathcal{R} \cup \{\boldsymbol{\lambda}_i \ominus x, \boldsymbol{\lambda}_k \ominus \boldsymbol{\lambda}_i \oplus x\}$. A solution of $\mathbb{S}_{\le(i-1)\setminus\{k\}}$ is not an $\overline{\mathcal{R}'}$-solution if and only if some $y_{k'}^{b'}$ takes one of these two values. There are four choices for b' and the value, and each of them fixes $\mathbb{S}_{k'}$. So, using the two observations and $N - 2f \ge N/2$, we have

$$\begin{aligned}\eta(\mathbb{S}_{\le(i-1)\setminus\{k\}} \,|\, \mathcal{R}') &\ge \eta(\mathbb{S}_{\le(i-1)\setminus\{k\}} \,|\, \mathcal{R}) - 4 \sum_{k' \in [i-1]\setminus\{k\}} \eta(\mathbb{S}_{\le(i-1)\setminus\{k,k'\}} \,|\, \mathcal{R}) \\ &\ge \frac{\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})}{N} \left(1 - \frac{8i}{N}\right).\end{aligned}$$

Therefore, we have

$$\begin{aligned}\varepsilon(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{P}) &\le \frac{2s(i-1)}{N} \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) - \frac{|\mathcal{M}|}{N} \left(1 - \frac{8i}{N}\right) \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) \\ &\le \left(\frac{4q\nabla_{\hat{\mathcal{R}}} + 2q + 2s\Delta_{\mathbb{S}}}{N} + \frac{16q^2 s}{N^2}\right) \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}).\end{aligned}$$

Now, consider $\varepsilon(\boldsymbol{\lambda}_i, \mathcal{P}, \mathcal{P})$. The pairs $(y_k^b, y_{k'}^{b'})$ with $k = k'$ contribute non-negatively to $\mu(\boldsymbol{\lambda}_i, \mathcal{P}, \mathcal{P})$, and we simply drop them. Let

$$\begin{aligned}\mathcal{M}' \coloneqq \big\{((k,b),(k',b')) \,:\, & k \ne k' \in [i-1],\, b, b' \in [2], \\ & \boldsymbol{\lambda}_k \ne \boldsymbol{\lambda}_i,\, \boldsymbol{\lambda}_{k'} \ne \boldsymbol{\lambda}_i,\, \boldsymbol{\lambda}_i \oplus \boldsymbol{\lambda}_k \ominus \boldsymbol{\lambda}_{k'} \ne 0\big\}.\end{aligned}$$

Each of the three conditions fails for at most $4(i-1)\Delta_{\mathbb{S}}$ tuples, and thus $|\mathcal{M}'| \ge 4(i-1)(i-2) - 12(i-1)\Delta_{\mathbb{S}}$. Fix some $((k,b),(k',b')) \in \mathcal{M}'$, and let $z = y_k^b$. A solution with $y_k^b \oplus y_{k'}^{b'} = \boldsymbol{\lambda}_i$ is determined by a solution of $\mathbb{S}_{\le(i-1)\setminus\{k,k'\}}$ and a value z such that the four values z, $\boldsymbol{\lambda}_k \ominus z$, $\boldsymbol{\lambda}_i \ominus z$ and $\boldsymbol{\lambda}_{k'} \ominus \boldsymbol{\lambda}_i \oplus z$ are pairwise distinct and avoid $\mathcal{R}$ and all the other values. Due to the conditions in $\mathcal{M}'$, two of the six pairs of these values are never equal. In each of the remaining four pairs, z appears with coefficients 1 and -1, and thus the pair is equal for at most one value of z (and never in characteristic 2, due to the conditions in $\mathcal{M}'$ and $\boldsymbol{\lambda}_i, \boldsymbol{\lambda}_{k'} \ne 0$). So there are at least $N - 4(s + 2(i-1)) - 4 \ge N - 4s - 8i$ choices for z, and the number of such solutions is at least

$$(N - 4s - 8i)\eta(\mathbb{S}_{\le(i-1)\setminus\{k,k'\}} \,|\, \mathcal{R}) \ge \frac{\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})}{N} \left(1 - \frac{4s + 8i}{N}\right).$$

Therefore, we have

$$\begin{aligned}\varepsilon(\boldsymbol{\lambda}_i, \mathcal{P}, \mathcal{P}) &\le \frac{4(i-1)^2}{N} \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) - \frac{|\mathcal{M}'|}{N} \left(1 - \frac{4s + 8i}{N}\right) \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}) \\ &\le \left(\frac{4q + 12q\Delta_{\mathbb{S}}}{N} + \frac{16q^2(s + 2q)}{N^2}\right) \eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R}).\end{aligned}$$

Combining the above bounds with $\delta(N) \le 2/N$, we get $\eta(\mathbb{S}_{\le i} \,|\, \mathcal{R}) \ge \frac{(N-f)^2}{N}(1 - \epsilon_i)\eta(\mathbb{S}_{\le(i-1)} \,|\, \mathcal{R})$, where

$$\epsilon_i \le \frac{2}{N} \left|\mu(\boldsymbol{\lambda}_i, \mathcal{R}, \mathcal{R}) - \frac{s^2}{N}\right| + \frac{12(s + 2q)(\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}})}{N^2} + \frac{24(s + 2q)^3}{N^3} + \frac{2}{N} + \frac{16q}{N^2}.$$

Note that $(N-f)^2 \geq (N-s-2(i-1))(N-s-2(i-1)-1)$.

Non-isolated blocks. For $i > m$, we follow the derivation of (24) with $t = 2$, as in the proof of Corollary 3, with the changes described in the proof of Theorem 2. In particular, $\mathcal{F}_j(\boldsymbol{y}_{\leq(i-1)}) = \mathcal{R} \sqcup \mathcal{P}(\boldsymbol{y}_{\leq(i-1)})$ for all the variables of $\mathbb{S}_i$, $f_{(j)} \leq s + r \leq s + 2q$, and the at most $r_i^2/2$ pairs in EQ cost at most r_i^2/N due to non-triviality. This gives the factor $1 - 2r_i^2(s+2q)^2/N^2 - r_i^2/N$ for $\mathbb{S}_i$, under the condition $\xi_{\mathbb{S}}(s+2q) \leq N/2$.

The corollary now follows by multiplying the bounds for all the blocks, and using $\sum_{i \leq m}(2/N + 16q/N^2) \leq 2q/N + 16q^2/N^2 \leq 4q/N$, as $8q \leq N$. □

C Miscellaneous Proofs related to Theorem 3

C.1 Proof of Lemma 7

Let $s' = 2^{n-2}/\overline{\sigma}$. We have

$$
\begin{aligned}
&\Pr\left(\theta_{\mathrm{id}} \in \Omega_{\mathrm{bad}}\right) \\
&= \Pr\left(\mathsf{Cyclic} \vee \mathsf{Trivial} \vee \mathsf{Giant}\right) \\
&\leq \Pr\left(\mathsf{Cyclic}\right) + \Pr\left(\mathsf{Trivial}\right) + \Pr\left(\mathsf{Giant}\right) \\
&\leq \Pr\left(\mathsf{A}_1\right) + \Pr\left(\mathsf{B}_1\right) + \Pr\left(\mathsf{D}\right) + \Pr\left(\mathsf{A}_2\right) + \Pr\left(\mathsf{B}_2\right) + \Pr\left(\mathsf{C}\right) \\
&\quad + \Pr\left(\mathsf{E} \wedge \neg \mathsf{B}_3\right) + \Pr\left(\mathsf{A}_3\right) + \Pr\left(\mathsf{B}_3\right) \\
&\leq \Pr\left(\mathsf{AP1}_H(\mathsf{M})\right) + \Pr\left(\mathsf{AP2}_H(\mathsf{M})\right) + \Pr\left(\mathsf{COLL}_H(\mathsf{M})\right) + \frac{q^2\epsilon_1(\rho')}{2^{n+1}} \\
&\quad + \frac{q^2\epsilon_1(\rho')}{2^{n+1}} + \frac{q}{2^n} + \frac{q^2\epsilon_1(\rho')s'}{2^n} + \Pr\left(\mathsf{MC1}_H^{\lceil s' \rceil}(\mathsf{M})\right) + \Pr\left(\mathsf{MC2}_H^{\lceil s' \rceil}(\mathsf{M})\right) \\
&\leq 2\epsilon_2(\rho) + \delta + \frac{q + q^2\epsilon_1(\rho')}{2^n} + \frac{q^2\epsilon_1(\rho')}{4\overline{\sigma}} + 2\epsilon_3(\rho, \lceil s' \rceil),
\end{aligned}
$$

where the first three (in)equalities follow from the definition and a trivial application of union bound, the fourth inequality maps the bad predicates to corresponding coverfree hash events, and finally the fifth inequality follows from the coverfree bound of H. Here, $\rho' = (2, \ell, 2\ell)$ as in Theorem 3. As the messages are fixed once T is fixed, and Π' is independent of T, we have $\Pr\left(\mathsf{X}_1^i = \mathsf{X}_1^j\right) \leq \epsilon_1(\rho')$ for each pair $i < j$ (apply the CfH bound to the two messages M^i and M^j). So, the expected number of pairs $i < j$ with $\mathsf{X}_1^i = \mathsf{X}_1^j$ (res. $\mathsf{X}_2^i = \mathsf{X}_2^j$) is at most $q^2\epsilon_1(\rho')/2$. Also, for any $m \in [q]$, the messages $\mathsf{M}^1, \ldots, \mathsf{M}^m$, and hence $\mathsf{X}^1, \ldots, \mathsf{X}^m$, are determined by Π' and $\mathsf{T}^1, \ldots, \mathsf{T}^{m-1}$, whereas T^m is uniform and independent of them. For A_2 (and similarly for B_2), we use this with $m = j$: for each pair $i < j$, $\mathsf{X}_1^i = \mathsf{X}_1^j$ and $\mathsf{T}^i \oplus \mathsf{T}^j = 0^n$ hold together with probability $\Pr\left(\mathsf{X}_1^i = \mathsf{X}_1^j\right)/2^n$. For $\mathsf{E} \wedge \neg \mathsf{B}_3$, fix distinct i, j, k (note that $i \neq k$ due to $\neg \mathsf{D}$) and let $m = \max\{i, j, k\}$. Due to $\neg \mathsf{B}_3$, k is among the first $\lceil s' \rceil - 1$ elements of $\{k' \leq m : \mathsf{X}_2^j = \mathsf{X}_2^{k'}\}$, which is determined by Π' and $\mathsf{T}^1, \ldots, \mathsf{T}^{m-1}$, and then $\mathsf{T}^i \oplus \mathsf{T}^j \oplus \mathsf{T}^k = 0^n$ holds with probability $1/2^n$. Thus, each of the at most

$q^2\epsilon_1(\rho')$ ordered pairs (i,j) with $\mathsf{X}_1^i = \mathsf{X}_1^j$ (in expectation) contributes at most $(\lceil s' \rceil - 1)/2^n \le s'/2^n$, and $s'/2^n = 1/(4\overline{\sigma})$. □

C.2 Proof of Lemma 8

Fix a good transcript $\omega \in \Omega_{\text{good}}$. We will recycle notations from the sampling phase. In the real world, Π is sampled exactly $s+r$ times ($|\mathcal{R}| = s$ and $|\{(i)_1 \,:\, i \in [q]\}| + |\{(i)_2 \,:\, i \in [q]\}| = r$), due to the domain separation. Thus, we have

$$\Pr\left(\Theta_{\text{re}} = \omega\right) = \frac{1}{(2^n)_{s+r}} \tag{30}$$

In the ideal world, first T is sampled uniformly from a set of size 2^{nq}, followed by $\mathcal{R}$ which is sampled faithfully via Π. Finally, Y is sampled uniformly from $(\mathbb{S} \,|\, \mathcal{R})$. Using Corollary 4 (with $N = 2^n$), we have

$$\Pr\left(\Theta_{\text{id}} = \omega\right) = \frac{1}{2^{nq}} \times \frac{1}{(2^n)_s} \times \frac{1}{\eta(\mathbb{S} \,|\, \mathcal{R})} \le \frac{1}{2^{nq}} \times \frac{1}{(2^n)_s} \times \frac{1}{(1-\varepsilon)\mathbb{E}\left(\mathbb{S} \,|\, \mathcal{R}\right)} \tag{31}$$

where

$$\varepsilon \le \frac{4q}{2^n} + \frac{2}{2^n} \sum_{i \notin \mathtt{NI}(\mathbb{S})} \left| \mu(\mathsf{T}^{(i)}, \mathcal{R}) - \frac{|\mathcal{R}|^2}{2^n} \right| + \frac{12q(s+2q)(\Delta_{\mathbb{S}} + \nabla_{\hat{\mathcal{R}}})}{2^{2n}} + \frac{24q(s+2q)^3}{2^{3n}} + \left(\frac{2(s+2q)^2}{2^{2n}} + \frac{1}{2^n} \right) \sum_{j \in \mathtt{NI}(\mathbb{S})} r_j^2.$$

The result then follows on dividing (30) by (31), as $\mathbb{E}\left(\mathbb{S} \,|\, \mathcal{R}\right) = (2^n - s)_r / 2^{nq}$. □

C.3 Proof of Claims in (14)

Let $\sim_1$ (res. $\sim_2$) be equivalence relations on $[q]$, such that $i \sim_1 j$ (res. $i \sim_2 j$) if and only if $\mathsf{X}_1^i = \mathsf{X}_1^j$ (res. $\mathsf{X}_2^i = \mathsf{X}_2^j$). Let $\mathcal{C}_1^1, \ldots, \mathcal{C}_{t_1}^1$ and $\mathcal{C}_1^2, \ldots, \mathcal{C}_{t_2}^2$ denote the non-singleton equivalence classes of $[q]$ with respect to $\sim_1$ and $\sim_2$, respectively. For $i \in [t_1]$ and $j \in [t_2]$, let $\mathtt{mc}_i^{(1)} = |\mathcal{C}_i^1|$ and $\mathtt{mc}_j^{(2)} = |\mathcal{C}_j^2|$.

$$\begin{aligned}
\nu &= \left(\frac{2(s+2q)^2}{2^{2n}} + \frac{1}{2^n} \right) \mathbb{E}\left(\sum_{i' \in \mathtt{NI}(\mathbb{S})} r_{i'}^2 \right) \\
&\le \left(\frac{2(s+2q)^2}{2^{2n}} + \frac{1}{2^n} \right) \times \frac{9}{4} \left(\sum_{j=1}^{t_1} \mathbb{E}\left(\left(\mathtt{mc}_j^{(1)} \right)^2 \right) + \sum_{j'=1}^{t_2} \mathbb{E}\left(\left(\mathtt{mc}_{j'}^{(2)} \right)^2 \right) \right) \\
&\le \frac{18q^2(s+2q)^2\epsilon_1(2,\ell,2\ell)}{2^{2n}} + \frac{9q^2\epsilon_1(2,\ell,2\ell)}{2^n}.
\end{aligned}$$

Here, the first inequality holds as each non-isolated block consists of at most two non-singleton classes $\mathcal{C}$ and $\mathcal{C}'$, one from each $\sim_b$, that share at most one query

(see the proof of Theorem 3). So, the block has at most $|\mathcal{C}| + |\mathcal{C}'|$ variables, and $(|\mathcal{C}| + |\mathcal{C}'|)^2 \leq 2(|\mathcal{C}|^2 + |\mathcal{C}'|^2)$. If the block has a single non-singleton class $\mathcal{C}$, then it has $|\mathcal{C}| + 1$ variables, and $(|\mathcal{C}| + 1)^2 \leq \frac{9}{4}|\mathcal{C}|^2$ as $|\mathcal{C}| \geq 2$. The second inequality holds as $\mathtt{mc}^2 \leq 2\mathtt{mc}(\mathtt{mc} - 1)$ for $\mathtt{mc} \geq 2$, and thus $\sum_{j=1}^{t_1} (\mathtt{mc}_j^{(1)})^2$ is at most four times the number of pairs $i < i'$ with $\mathsf{X}_1^i = \mathsf{X}_1^{i'}$, which has expectation at most $\frac{q^2}{2}\epsilon_1(2, \ell, 2\ell)$ (and similarly for $\sim_2$). □

C.4 Proof of the Claim in (15)

Fix $i \in [q]$ and write $N = 2^n$. We first condition on T, and assume $t \coloneqq \mathsf{T}^i \neq 0^n$ (otherwise there is nothing to prove). As noted before, this fixes the messages, and the hash computation becomes a deterministic (possibly adaptive) procedure querying Π_0', which is independent of T. Let $\mathtt{Z}_1, \ldots, \mathtt{Z}_s$ denote the outputs of Π_0' at the distinct inputs queried during the hash computation, in the order of their first appearance, so that $\mathcal{R} = \{\mathtt{Z}_1, \ldots, \mathtt{Z}_s\}$. Note that $s \leq \overline{\sigma} \leq N/8$ is itself random. However, for any $k \geq 1$, the event $s \geq k$ is determined by $\mathtt{Z}_1, \ldots, \mathtt{Z}_{k-1}$, and conditioned on $\mathtt{Z}_1, \ldots, \mathtt{Z}_{k-1}$ and $s \geq k$, $\mathtt{Z}_k$ is uniform over the remaining $N - k + 1$ values.

Let $\mathtt{U}$ denote the number of pairs $j < k \leq s$ such that $\mathtt{Z}_j \oplus \mathtt{Z}_k = t$, so that $\mu^*(t, \mathcal{R}) = 2\mathtt{U}$. For $k \geq 1$, let $\mathtt{Y}_k$ denote the number of $j < k$ such that $\mathtt{Z}_j \oplus \mathtt{Z}_k = t$ if $s \geq k$, and $\mathtt{Y}_k = 0$ otherwise. Then $\mathtt{U} = \sum_k \mathtt{Y}_k$, and $\mathtt{Y}_k \in \{0, 1\}$ as the $\mathtt{Z}_j$'s are distinct. Let $\mathtt{U}_k \coloneqq \sum_{k' \leq k} \mathtt{Y}_{k'}$. For $j < k$, $\mathtt{Z}_j \oplus t \in \{\mathtt{Z}_1, \ldots, \mathtt{Z}_{k-1}\}$ if and only if j belongs to one of the $\mathtt{U}_{k-1}$ pairs among the first $k - 1$ values, and each such pair contains exactly two indices. Thus, we have

$$\mathtt{E}_k \coloneqq \mathbb{E}\left(\mathtt{Y}_k \mid \mathtt{Z}_1, \ldots, \mathtt{Z}_{k-1}\right) = 1_{s \geq k} \frac{k - 1 - 2\mathtt{U}_{k-1}}{N - k + 1}.$$

Let $\mathtt{A} \coloneqq \sum_k \mathtt{E}_k$ and $\mathtt{D}_k \coloneqq \mathtt{Y}_k - \mathtt{E}_k$. For $k' < k$, $\mathtt{D}_{k'}$ is determined by $\mathtt{Z}_1, \ldots, \mathtt{Z}_{k-1}$, and $\mathtt{D}_k$ has zero mean conditioned on $\mathtt{Z}_1, \ldots, \mathtt{Z}_{k-1}$. So $\mathbb{E}\left(\mathtt{D}_k \mathtt{D}_{k'}\right) = 0$ for $k \neq k'$, and

$$\mathbb{E}\left((\mathtt{U} - \mathtt{A})^2\right) = \sum_k \mathbb{E}\left(\mathtt{D}_k^2\right) \leq \sum_k \mathbb{E}\left(\mathtt{E}_k\right) \leq \mathbb{E}\left(\sum_{k=1}^{s} \frac{k - 1}{N - s}\right) \leq \frac{\overline{\sigma}^2}{2(N - \overline{\sigma})} \leq \frac{4\overline{\sigma}^2}{7N},$$

where the first inequality holds as $\mathtt{Y}_k \in \{0, 1\}$. In particular, $\mathbb{E}\left(\mathtt{U}\right) = \mathbb{E}\left(\mathtt{A}\right) \leq 4\overline{\sigma}^2/7N$. Next, we compare $\mathtt{A}$ with $s^2/2N$. On the one hand, $\mathtt{A} \leq s(s-1)/2(N - s) \leq s^2/2N + 4s^3/7N^2$. On the other hand, $\mathtt{U}_{k-1} \leq \mathtt{U}$ gives $\mathtt{A} \geq s(s-1)/2N - 2s\mathtt{U}/N$. Thus,

$$\mathbb{E}\left(\left|\mathtt{A} - \frac{s^2}{2N}\right|\right) \leq \frac{\overline{\sigma}}{2N} + \frac{4\overline{\sigma}^3}{7N^2} + \frac{2\overline{\sigma}\mathbb{E}\left(\mathtt{U}\right)}{N} \leq \frac{\overline{\sigma}}{2N} + \frac{12\overline{\sigma}^3}{7N^2}.$$

Finally, using $\mathbb{E}\left(|\mathtt{X}|\right) \leq \sqrt{\mathbb{E}\left(\mathtt{X}^2\right)}$, we have

$$\mathbb{E}\left(\left|\mu^*(t, \mathcal{R}) - \frac{s^2}{N}\right|\right) \leq 2\sqrt{\mathbb{E}\left((\mathtt{U} - \mathtt{A})^2\right)} + 2\mathbb{E}\left(\left|\mathtt{A} - \frac{s^2}{2N}\right|\right) \leq \frac{4\overline{\sigma}}{\sqrt{7N}} + \frac{\overline{\sigma}}{N} + \frac{24\overline{\sigma}^3}{7N^2},$$

and (15) follows on taking the expectation over T, as $4/\sqrt{7} \leq 8/5$. □

D Proofs of Lemma 9 and 10

Throughout this section, we only count parsed blocks, so we write ℓ and σ for the bounds $\hat{\ell}$ and $\hat{\sigma}$ of Section 7. Moreover, $N = 2^n$, $p(x)$ is primitive and satisfies TF_ℓ, and we fix q distinct messages, whose parsed (padded) forms are $m_u = (m_u[1], \ldots, m_u[\ell_u])$ with $\ell_u \le \ell$, for $u \in [q]$. We call a pair $v = (a, x) \in [\ell] \times \{0,1\}^{n-s}$ a *point* at position a, and write $Z_v \coloneqq \Pi_0(\langle a \rangle_{s-2} \| x)$. As Π_0 is injective, for any set T of t points, $(Z_v)_{v \in T}$ is uniformly distributed over the t-tuples of distinct n-bit strings. The message m_u has exactly one point at each position $a \in [\ell_u]$, and we write $V_u \coloneqq \{(a, m_u[a]) : a \in [\ell_u]\}$. Note that distinct messages have distinct point sets.

We consider vectors $\mathbf{y} = (y_v)_v$ over $\mathbb{F}_{2^n}$ indexed by points, and write $\mathbf{y} \cdot \mathbf{Z} \coloneqq \bigoplus_v y_v \cdot Z_v$. Let $\mathbf{e}_v$ denote the unit vector at v, and $\mathbf{1}_V \coloneqq \bigoplus_{v \in V} \mathbf{e}_v$ for a set of points V. By Algorithm 1, $\mathtt{LightHash}_{\Pi_0}(m_u) = (\mathbf{1}_{V_u} \cdot \mathbf{Z}, \beta_u \cdot \mathbf{Z})$, where $\beta_u \coloneqq \bigoplus_{(a,x) \in V_u} 2^{\ell_u + 1 - a}\, \mathbf{e}_{(a,x)}$. For distinct $u, w \in [q]$, let

$$\mathbf{a}_{uw} \coloneqq \mathbf{1}_{V_u} \oplus \mathbf{1}_{V_w} = \mathbf{1}_{V_u \triangle V_w}, \qquad \mathbf{b}_{uw} \coloneqq \beta_u \oplus \beta_w,$$

both supported on $V_u \cup V_w$, i.e., on at most 2ℓ points. Let $K_1 \coloneqq \{0, 2^{n-1}\}$ and $K_2 \coloneqq \{0, 2^{n-1}, 2^{n-2}, 2^{n-1} \oplus 2^{n-2}\}$. As $\mathtt{Trunc}_1$ (res. $\mathtt{Trunc}_2$) ignores the first bit (res. the first two bits), we have

$$\begin{aligned} \mathtt{TLightHash}^1_{\Pi_0}(m_u) = \mathtt{TLightHash}^1_{\Pi_0}(m_w) &\iff \mathbf{a}_{uw} \cdot \mathbf{Z} \in K_1, \\ \mathtt{TLightHash}^2_{\Pi_0}(m_u) = \mathtt{TLightHash}^2_{\Pi_0}(m_w) &\iff \mathbf{b}_{uw} \cdot \mathbf{Z} \in K_2. \end{aligned}$$

Thus, all the events in the CfH definition are events that a few linear combinations of the Z_v's lie in K_1 or K_2. We use three simple tools.

Lemma 13. *Let $\mathbf{y}_1, \ldots, \mathbf{y}_k$ be linearly independent vectors supported on a set of $t \le N/2$ points. Then, for any $\kappa_1, \ldots, \kappa_k \in \mathbb{F}_{2^n}$, we have*

$$\Pr\left(\mathbf{y}_i \cdot \mathbf{Z} = \kappa_i \text{ for all } i \in [k]\right) \le \prod_{i=1}^{k} \frac{1}{N - t + i} \le \left(\frac{2}{N}\right)^k.$$

Proof. Fix k points such that the restrictions of $\mathbf{y}_1, \ldots, \mathbf{y}_k$ to these points form an invertible matrix. Conditioned on the values of the other $t - k$ variables, the k fixed variables are uniformly distributed over the k-tuples of distinct values outside a set of size $t - k$, whereas the system determines them uniquely. □

Lemma 14. *For any $c \neq 0$, $c \cdot K_1 \cap K_2 \neq \{0\}$ if and only if $c \in \{1, 2^{-1}, 1 \oplus 2^{-1}\}$. In particular, $2^e \cdot K_1 \cap K_2 = \{0\}$ for $1 \le e \le \ell$.*

Proof. The first claim is immediate from $K_2 = 2^{n-1} \cdot \{0, 1, 2^{-1}, 1 \oplus 2^{-1}\}$. For the second claim, $2^e = 1$, $2^e = 2^{-1}$ and $2^e = 1 \oplus 2^{-1}$ would be vanishing sums of at most three powers of 2 with distinct exponents in $[-1, \ell]$, which TF_ℓ rules out. □

Lemma 15. *For distinct $u, w \in [q]$, $\mathbf{b}_{uw} \neq 0$. Moreover, $\mathbf{b}_{uw}$ is constant on its support if and only if $\ell_u = \ell_w$ and m_u and m_w differ at exactly one position a, in which case $\mathbf{b}_{uw} = 2^{\ell_u+1-a} \cdot \mathbf{a}_{uw}$. In particular, $\mathbf{a}_{uw}$ and $\mathbf{b}_{uw}$ are linearly independent unless this is the case.*

Proof. If $\ell_u = \ell_w$, then β_u and β_w agree on $V_u \cap V_w$, so $\mathbf{b}_{uw} = \bigoplus_{(a,x)\in V_u \triangle V_w} 2^{\ell_u+1-a}\, \mathbf{e}_{(a,x)} \neq 0$, and it is constant on its support if and only if all the points in $V_u \triangle V_w$ have the same position. Now, let $\ell_u < \ell_w$. The point of m_w at position ℓ_w has coefficient 2 in $\mathbf{b}_{uw}$, so $\mathbf{b}_{uw} \neq 0$. If $\ell_w \geq \ell_u + 2$, then the point of m_w at position $\ell_w - 1$ has coefficient 2^2. Otherwise, $\ell_w = \ell_u + 1$, and at each position $a \leq \ell_u$, either m_u and m_w have two distinct points, with the distinct coefficients 2^{ℓ_u+1-a} and 2^{ℓ_u+2-a}, or they share a point, with coefficient $(1 \oplus 2) \cdot 2^{\ell_u+1-a}$. If $\ell_u \geq 2$, these shared coefficients differ for $a = 1$ and $a = 2$. If $\ell_u = 1$, the shared coefficient $(1 \oplus 2) \cdot 2$ differs from the coefficient 2 of the point of m_w at position 2. In all cases, $\mathbf{b}_{uw}$ is not constant on its support. Finally, $\mathbf{a}_{uw}$ is a 0/1-vector, so $\mathbf{b}_{uw} = c \cdot \mathbf{a}_{uw}$ implies that $\mathbf{b}_{uw}$ is constant on its support. □

D.1 Collisions and Multicollisions

Let $u \neq w \in [q]$. By Lemma 13 (with $k = 1$ and $t \leq 2\ell \leq N/2$) and Lemma 15, we have $\Pr(\mathbf{a}_{uw} \cdot \mathbf{Z} \in K_1) \leq 4/N$ and $\Pr(\mathbf{b}_{uw} \cdot \mathbf{Z} \in K_2) \leq 8/N$. Summing over the $q(q-1)/2$ pairs shows that $\epsilon_1(\rho) = 4q^2/N$ bounds the expected number of colliding pairs in either half, and Proposition 8 with $\epsilon = 8/N$ gives $\epsilon_3(\rho, k) = 16q^2/(k^2 N)$.

For the double collision, suppose first that $\mathbf{a}_{uw}$ and $\mathbf{b}_{uw}$ are linearly independent. Then, by Lemma 13, each of the 8 choices of $(\mathbf{a}_{uw} \cdot \mathbf{Z}, \mathbf{b}_{uw} \cdot \mathbf{Z}) \in K_1 \times K_2$ has probability at most $4/N^2$. Otherwise, by Lemma 15, m_u and m_w have points $v \neq v'$ at some position a and agree elsewhere, and $\mathbf{b}_{uw} = 2^e \cdot \mathbf{a}_{uw}$ with $e = \ell_u + 1 - a \in [1, \ell]$. A double collision would then give $0 \neq Z_v \oplus Z_{v'} = \mathbf{a}_{uw} \cdot \mathbf{Z} \in K_1$ with $2^e \cdot (Z_v \oplus Z_{v'}) \in K_2$, which is impossible by Lemma 14. So, $\Pr\left(\mathsf{COLL}_{\mathtt{TLightHash}_{\Pi_0}}(\boldsymbol{m})\right) \leq (q^2/2) \cdot 32/N^2 = \delta(\rho)$.

D.2 Alternating Paths

Let $\mathcal{Q}$ denote the set of all $(i, j, r, s) \in [q]^4$ such that $i \neq j$, $j \neq r$, $r \neq s$, $i \neq r$ and $j \neq s$ (we allow $i = s$). In the event $\mathsf{AP1}_{\mathtt{TLightHash}_{\Pi_0}}(\boldsymbol{m})$, if $i = r$ or $j = s$, then the path contains a double collision. So, $\Pr\left(\mathsf{AP1}_{\mathtt{TLightHash}_{\Pi_0}}(\boldsymbol{m})\right) \leq \delta(\rho) + \Pr\left(\bigvee_{(i,j,r,s)\in\mathcal{Q}} \mathsf{E}_1(i, j, r, s)\right)$, and similarly for $\mathsf{AP2}_{\mathtt{TLightHash}_{\Pi_0}}(\boldsymbol{m})$ with E_2, where

$$\mathsf{E}_1(i, j, r, s): \ \mathbf{a}_{ij} \cdot \mathbf{Z} \in K_1 \wedge \mathbf{b}_{jr} \cdot \mathbf{Z} \in K_2 \wedge \mathbf{a}_{rs} \cdot \mathbf{Z} \in K_1,$$
$$\mathsf{E}_2(i, j, r, s): \ \mathbf{b}_{ij} \cdot \mathbf{Z} \in K_2 \wedge \mathbf{a}_{jr} \cdot \mathbf{Z} \in K_1 \wedge \mathbf{b}_{rs} \cdot \mathbf{Z} \in K_2.$$

All the vectors involved are supported on at most $4\ell \leq N/2$ points. We first record a consequence of Lemma 15: for $(i,j,r,s) \in \mathcal{Q}$,

$$\mathbf{b}_{jr} \notin \mathbb{F}_{2^n} \cdot \mathbf{a}_{ij} \cup \mathbb{F}_{2^n} \cdot \mathbf{a}_{rs} \quad \text{and} \quad \mathbf{a}_{jr} \notin \mathbb{F}_{2^n} \cdot \mathbf{b}_{ij} \cup \mathbb{F}_{2^n} \cdot \mathbf{b}_{rs}, \tag{32}$$

where $\mathbb{F}_{2^n} \cdot \mathbf{y}$ denotes the set of multiples of $\mathbf{y}$. Indeed, if $\mathbf{b}_{jr} = c \cdot \mathbf{a}_{ij}$, then $\mathbf{b}_{jr}$ is constant on its support, so by Lemma 15, m_j and m_r differ at a single position and $V_i \triangle V_j = V_j \triangle V_r$, i.e., $V_i = V_r$ and $i = r$. Similarly, the other three cases give $j = s$, $i = r$ and $j = s$, respectively.

Lemma 16. $\Pr\left(\bigvee_{(i,j,r,s)\in\mathcal{Q}} \mathsf{E}_1(i,j,r,s)\right) \leq \frac{128q^4}{N^3} + \frac{12q^2}{N^{3/2}} + \frac{96q^2}{N^2}$.

Proof. Let $\mathtt{J}_1$ be the set of $(i,j,r,s) \in \mathcal{Q}$ such that $\mathbf{a}_{ij}$, $\mathbf{b}_{jr}$ and $\mathbf{a}_{rs}$ are linearly independent, $\mathtt{J}_2$ the set of those with $\mathbf{a}_{ij} = \mathbf{a}_{rs}$, and $\mathtt{J}_3$ the rest.
Case $\mathtt{J}_1$*:* The right hand side takes 16 values in $K_1 \times K_2 \times K_1$, each with probability at most $8/N^3$ by Lemma 13. So, $\mathtt{J}_1$ contributes at most $128q^4/N^3$.
Case $\mathtt{J}_2$*:* For a set of points D, let C_D be the set of unordered pairs $\{u,w\}$ with $V_u \triangle V_w = D$. Given u and D, V_w is determined, so $\sum_D |C_D| \leq q^2/2$. For $(i,j,r,s) \in \mathtt{J}_2$, both $\{i,j\}$ and $\{r,s\}$ lie in C_D for $D = V_i \triangle V_j$, and E_1 implies $\mathbf{1}_D \cdot \mathbf{Z} \in K_1$, which has probability at most $4/N$. On the other hand, the rank is 2 by (32), and the right hand side takes 8 values (the first and third coordinates coincide), so $\Pr(\mathsf{E}_1(i,j,r,s)) \leq 32/N^2$ for each of the at most $4|C_D|^2$ tuples with pairs in C_D. Using $\min\{x,y\} \leq \sqrt{xy}$, $\mathtt{J}_2$ contributes at most

$$\sum_D \min\left\{\frac{4}{N}, \frac{128|C_D|^2}{N^2}\right\} \leq \frac{\sqrt{512}}{N^{3/2}} \sum_D |C_D| \leq \frac{12q^2}{N^{3/2}}.$$

Case $\mathtt{J}_3$*:* Here, $\mathbf{a}_{ij} \neq \mathbf{a}_{rs}$ are non-zero 0/1-vectors, hence linearly independent, and the rank is 2. So, $\mathbf{b}_{jr} = c_1 \cdot \mathbf{a}_{ij} \oplus c_2 \cdot \mathbf{a}_{rs}$, where $c_1, c_2 \neq 0$ by (32). Let $P = V_i \triangle V_j$ and $P' = V_r \triangle V_s$, so that $\mathbf{b}_{jr} = c_1 \cdot \mathbf{1}_{P \setminus P'} \oplus c_2 \cdot \mathbf{1}_{P' \setminus P} \oplus (c_1 \oplus c_2) \cdot \mathbf{1}_{P \cap P'}$.

If $c_1 = c_2$, then $\mathbf{b}_{jr}$ is constant on its support, so by Lemma 15, m_j and m_r have points $v \neq v'$ at some position a and agree elsewhere, and $\mathbf{b}_{jr} = 2^e \cdot \mathbf{a}_{jr}$ with $e \in [1,\ell]$. Then, $\mathbf{a}_{ij} \oplus \mathbf{a}_{rs} = c_1^{-1} \cdot \mathbf{b}_{jr}$ is a 0/1-vector with the same support as $\mathbf{a}_{jr}$, i.e., $\mathbf{a}_{ij} \oplus \mathbf{a}_{rs} = \mathbf{a}_{jr}$, which gives $\mathbf{1}_{V_i} = \mathbf{1}_{V_s}$ and $i = s$. But then, E_1 gives $0 \neq Z_v \oplus Z_{v'} = \mathbf{a}_{ij} \cdot \mathbf{Z} \oplus \mathbf{a}_{ri} \cdot \mathbf{Z} \in K_1$ and $2^e \cdot (Z_v \oplus Z_{v'}) = \mathbf{b}_{jr} \cdot \mathbf{Z} \in K_2$, which is impossible by Lemma 14.

If $c_1 \neq c_2$, then c_1, c_2 and $c_1 \oplus c_2$ are distinct and non-zero, so $P \setminus P'$, $P' \setminus P$ and $P \cap P'$ are exactly the (non-empty) level sets of $\mathbf{b}_{jr}$ on its support. As $\mathbf{b}_{jr}$ takes at most three distinct non-zero values, given (j,r), there are at most $3! = 6$ choices for (P,P'), and then $V_i = V_j \triangle P$ and $V_s = V_r \triangle P'$ determine (i,s). So, there are at most $6q^2$ such tuples. For each of them, the first and third coordinates of the right hand side determine the second one, so $\Pr(\mathsf{E}_1(i,j,r,s)) \leq 4 \cdot 4/N^2$, and $\mathtt{J}_3$ contributes at most $96q^2/N^2$. □

Lemma 17. $\Pr\left(\bigvee_{(i,j,r,s)\in\mathcal{Q}} \mathsf{E}_2(i,j,r,s)\right) \leq \frac{256q^4}{N^3} + \frac{22q^2}{N^{3/2}} + \frac{1664q^2}{N^2}$.

Proof. Let $\mathtt{J}_1$ be the set of $(i,j,r,s) \in \mathcal{Q}$ such that $\mathbf{b}_{ij}$, $\mathbf{a}_{jr}$ and $\mathbf{b}_{rs}$ are linearly independent, $\mathtt{J}_2$ the set of those with $\mathbf{b}_{rs} = c \cdot \mathbf{b}_{ij}$ for some c, and $\mathtt{J}_3$ the rest. As in Lemma 16, $\mathtt{J}_1$ contributes at most $32 \cdot 8q^4/N^3$.

Case $\mathtt{J}_2$*:* We claim that $\ell_i = \ell_j$, $\ell_r = \ell_s$ and $V_i \triangle V_j = V_r \triangle V_s$. If $\ell_r = \ell_s$, then at each position, $\mathbf{b}_{rs}$ has either no point or two points with equal coefficients. If $\ell_i \neq \ell_j$, then at position 1, $\mathbf{b}_{ij}$ has either one point or two points with the distinct coefficients 2^{ℓ_i} and 2^{ℓ_j}. So, $\ell_i = \ell_j$ if and only if $\ell_r = \ell_s$, and in this case, the claim follows as the supports of $\mathbf{b}_{ij}$ and $\mathbf{b}_{rs}$ coincide. Now, suppose $\ell_i < \ell_j$ and $\ell_r < \ell_s$ (the other cases are symmetric). As the supports coincide, $\ell_j = \ell_s =: L$, and comparing the coefficients at position L (both equal to 2) gives $c = 1$, i.e., $\beta_i \oplus \beta_j \oplus \beta_r \oplus \beta_s = 0$. If $\ell_i < \ell_r$, then at position ℓ_r, m_i has no point, the point of m_r has coefficient 2 in β_r, and the points of m_j and m_s have coefficient $2^{L+1-\ell_r} \neq 2$. So, the total coefficient of the point of m_r is 2 or $2 \oplus 2^{L+1-\ell_r}$, which is non-zero, a contradiction. By symmetry, $\ell_i = \ell_r$. Then, at each position $a \leq \ell_i$, the points of m_i and m_r have coefficient $\alpha = 2^{\ell_i+1-a}$, and those of m_j and m_s have coefficient $\alpha' = 2^{L+1-a}$, where α, α' and $\alpha \oplus \alpha'$ are non-zero. So, the total coefficient of a point vanishes only if it lies in both or none of V_i and V_r. Hence, $V_i = V_r$, and $i = r$, a contradiction. This proves the claim.

Now, for a set of points D and $L \in [\ell]$, let $C_{D,L}$ be the set of unordered pairs $\{u,w\}$ with $\ell_u = \ell_w = L$ and $V_u \triangle V_w = D$, and let q_L be the number of messages of length L. As before, $\sum_D |C_{D,L}| \leq q_L^2/2$. For $\{u,w\} \in C_{D,L}$, we have $\mathbf{b}_{uw} = 2^{L+1} \cdot \gamma_D$, where $\gamma_D \coloneqq \bigoplus_{(a,x)\in D} 2^{-a}\, \mathbf{e}_{(a,x)}$. If $\{i,j\} \in C_{D,L_1}$ and $\{r,s\} \in C_{D,L_2}$, then E_2 implies $\gamma_D \cdot \mathbf{Z} \in 2^{-L_1-1} \cdot K_2$, which has probability at most $8/N$. On the other hand, the rank is 2 by (32), and the right hand side takes at most 8 values (the third coordinate is $2^{L_2-L_1}$ times the first one), so $\Pr\left(\mathsf{E}_2(i,j,r,s)\right) \leq 32/N^2$ for each of the at most $4|C_{D,L_1}||C_{D,L_2}|$ such tuples. Using $\min\{x,y\} \leq \sqrt{xy}$ and the Cauchy-Schwarz inequality, $\mathtt{J}_2$ contributes at most

$$\sum_{L_1,L_2} \sum_{D} \frac{32\sqrt{|C_{D,L_1}||C_{D,L_2}|}}{N^{3/2}} \leq \sum_{L_1,L_2} \frac{16 q_{L_1} q_{L_2}}{N^{3/2}} = \frac{16q^2}{N^{3/2}}.$$

Case $\mathtt{J}_3$*:* Here, $\mathbf{b}_{ij}$ and $\mathbf{b}_{rs}$ are linearly independent and $\mathbf{a}_{jr} = c_1 \cdot \mathbf{b}_{ij} \oplus c_2 \cdot \mathbf{b}_{rs}$, where $c_1, c_2 \neq 0$ by (32). We call such a tuple *exceptional* if $i \neq s$, $\ell_i = \ell_s$, m_i and m_s differ at a single position, and $V_i \triangle V_s = V_j \triangle V_r$. For a set of points D, let C_D be as in the proof of Lemma 16. For an exceptional tuple, $\{i,s\}$ and $\{j,r\}$ lie in C_D, where $D = V_j \triangle V_r$ consists of two points $v \neq v'$ at the same position, and E_2 implies $Z_v \oplus Z_{v'} = \mathbf{a}_{jr} \cdot \mathbf{Z} = 2^{n-1}$, which has probability at most $2/N$. On the other hand, the rank is 2, and the right hand side takes at most 4 values (the second coordinate is 2^{n-1}, and the first two determine the third one), so $\Pr\left(\mathsf{E}_2(i,j,r,s)\right) \leq 16/N^2$ for each of the at most $4|C_D|^2$ exceptional tuples with pairs in C_D. As in Lemma 16, the exceptional tuples contribute at most

$$\sum_D \min\left\{\frac{2}{N}, \frac{64|C_D|^2}{N^2}\right\} \leq \frac{\sqrt{128}}{N^{3/2}} \sum_D |C_D| \leq \frac{6q^2}{N^{3/2}}.$$

By Lemma 18 below, $\mathsf{E}_2(i,j,r,s)$ is impossible for all but at most $26q^2$ of the other tuples in J_3. For each of them, the first and third coordinates of the right hand side determine the second one, so $\Pr(\mathsf{E}_2(i,j,r,s)) \le 16 \cdot 4/N^2$, and these tuples contribute at most $1664q^2/N^2$. □

For two messages u and w, let $\Delta(u,w)$ denote the set of positions at which m_u and m_w do not have the same point (i.e., either both have a point and the points differ, or exactly one of them has a point).

Lemma 18. *There are at most $26q^2$ tuples $(i,j,r,s) \in \mathsf{J}_3$ that are not exceptional and for which $\mathsf{E}_2(i,j,r,s)$ is possible.*

Proof. Fix $(i,j,r,s) \in \mathsf{J}_3$ with $\mathbf{a}_{jr} = c_1 \cdot \mathbf{b}_{ij} \oplus c_2 \cdot \mathbf{b}_{rs}$. We first consider the case $i \neq s$. Let $h_u := c_1 2^{\ell_u+1}$ for $u \in \{i,j\}$, and $h_u := c_2 2^{\ell_u+1}$ for $u \in \{r,s\}$. For $S \subseteq \{i,j,r,s\}$, let $h(S) := \bigoplus_{u \in S} h_u$, and let $\chi(S) = 1$ if S contains exactly one of j and r, and $\chi(S) = 0$ otherwise. For a point v at position p, let $S_v := \{u : v \in V_u\}$ be its *profile*. Comparing the coefficients of $\mathbf{e}_v$ on both sides gives

$$h(S_v) = 2^p \cdot \chi(S_v). \tag{33}$$

At position 1, every message has exactly one point, so the profiles of these points partition $\{i,j,r,s\}$, and either zero or two of them have $\chi = 1$. Summing (33) over these points gives

$$h_i \oplus h_j \oplus h_r \oplus h_s = 0. \tag{34}$$

As $h_u \neq 0$, (33) and (34) rule out the profiles $\{i\}$, $\{s\}$, $\{i,j,r\}$ and $\{j,r,s\}$. So, every profile with $\chi = 0$ is one of $\{i,s\}$, $\{j,r\}$ and $\{i,j,r,s\}$, and every profile with $\chi = 1$ belongs to one of the following lines, where the value of h is computed using (34):

$$\begin{array}{ll} (1)\ \{j\},\ \{i,r,s\}\colon h = h_j; & (2)\ \{r\},\ \{i,j,s\}\colon h = h_r; \\ (3)\ \{i,j\},\ \{r,s\}\colon h = h_i \oplus h_j; & (4)\ \{i,r\},\ \{j,s\}\colon h = h_i \oplus h_r. \end{array}$$

We call a position *special* if one of its points has $\chi = 1$. By (33), and as the value 2^p determines p, all the profiles with $\chi = 1$ at a special position share one value of h, and distinct special positions have distinct values.

Case $h_i \neq h_s$: By (34), $h_j \neq h_r$, so the profiles $\{i,s\}$ and $\{j,r\}$ do not occur, and using (34) and $h_u \neq 0$, the four values in (1)-(4) are distinct. Hence, at a non-special position, either all four messages share a point or none of them has a point. At a special position, all the profiles come from a single line (as $\{i,j,r,s\}$ is the only remaining profile with $\chi = 0$), and as each of them contains exactly one of j and r, the position lies in $\Delta(j,r)$. So, $\Delta(j,r)$ is the set of special positions, and $|\Delta(j,r)| \le 4$. Moreover, m_i and m_s agree with m_j outside $\Delta(j,r)$, and at $p \in \Delta(j,r)$, the line determines the points of m_i and m_s: both are those of m_r in (1), both are those of m_j in (2), they are those of m_j and m_r in (3), and those of m_r and m_j in (4) (where "no point" is allowed). As distinct special positions use distinct lines, given (j,r), there are at most $4! = 24$ choices of (i,s).

Case $h_i = h_s$: By (34), $h_j = h_r$, so the lines (1) and (2) share the value h_j, and the lines (3) and (4) share the value $h_i \oplus h_j$. Moreover, $h_i = h_s$ and $h_j = h_r$

give $2^{\ell_i-\ell_s} = c_2/c_1 = 2^{\ell_j-\ell_r}$, i.e., $\ell_i - \ell_s = \ell_j - \ell_r$. At a non-special position and at a position of value h_j, i and s lie in a common profile, or have no point. As $m_i \neq m_s$, they differ at the unique position p of value $h_i \oplus h_j$, and agree at all the other positions. Suppose first that $\ell_i \neq \ell_s$, so that $p = \max\{\ell_i, \ell_s\} = \min\{\ell_i, \ell_s\} + 1$. Exchanging (i, j) with (s, r) if necessary, we may assume that $\ell_i = p$ and $\ell_s = p - 1$, so that $\ell_j = \ell_r + 1$. At p, the profile of the point of m_i is $\{i, j\}$ or $\{i, r\}$, and as the profiles $\{j\}$ and $\{r\}$ have the value $h_j \neq h_i \oplus h_j$, no other profile at p contains exactly one of j and r. If the profile is $\{i, j\}$, then m_r has no point at p, so $\ell_r < p \leq \ell_j = \ell_r + 1$, which gives $\ell_j = p = \ell_i$ and $h_i = h_j$, contradicting $h_i \oplus h_j = 2^p$. If it is $\{i, r\}$, then m_j has no point at p, so $\ell_j < p \leq \ell_r$, which contradicts $\ell_j = \ell_r + 1$. So, $\ell_i = \ell_s$, which gives $\ell_j = \ell_r$ and $c_1 = c_2$, and the profiles of the points of m_i and m_s at p are $\{i, j\}$ and $\{r, s\}$, or $\{i, r\}$ and $\{j, s\}$. In particular, $V_i \triangle V_s$ consists of the points of m_j and m_r at p. If m_j and m_r also differed at a position $p' \neq p$, then p' would have the value h_j, so $2^{p'} = c_1 2^{\ell_j+1}$ and $2^p = c_1(2^{\ell_i+1} \oplus 2^{\ell_j+1})$, i.e., $2^{p-p'} = 2^{\ell_i-\ell_j} \oplus 1$, where $\ell_i \neq \ell_j$ as $2^p \neq 0$. This is a vanishing sum of three powers of 2 with distinct exponents in an interval of length $2\ell - 2$, which TF_ℓ rules out. So, $V_j \triangle V_r = V_i \triangle V_s$, and the tuple is exceptional.

Case $i = s$: If $c_1 = c_2$, then $\mathbf{a}_{jr} = c_1 \cdot (\mathbf{b}_{ij} \oplus \mathbf{b}_{ri}) = c_1 \cdot \mathbf{b}_{jr}$, so $\mathbf{b}_{jr}$ is constant on its support, and E_2 is impossible as in Case $\mathtt{J}_3$ of Lemma 16. Otherwise, we proceed as above with $h_i := (c_1 \oplus c_2)2^{\ell_i+1} \neq 0$, $h_j := c_1 2^{\ell_j+1}$, $h_r := c_2 2^{\ell_r+1}$ and profiles in $\{i, j, r\}$. Now, (34) reads $h_i \oplus h_j \oplus h_r = 0$, which rules out the profiles $\{i\}$ and $\{j, r\}$, and the profiles with $\chi = 1$ are $\{j\}$, $\{i, r\}$ (value h_j) and $\{r\}$, $\{i, j\}$ (value $h_r \neq h_j$). As in the case $h_i \neq h_s$, $\Delta(j, r)$ consists of at most two special positions, m_i agrees with m_j elsewhere, and at $p \in \Delta(j, r)$, m_i has the point of m_r (value h_j) or of m_j (value h_r). So, given (j, r), there are at most 2 choices of i.

Altogether, $\mathsf{E}_2(i, j, r, s)$ is possible for at most $(24 + 2)q^2$ tuples in $\mathtt{J}_3$ that are not exceptional. □

Lemma 9 now follows by combining the bounds on ϵ_1, ϵ_3 and δ above with Lemma 16 and 17, which give

$$\Pr\left(\mathsf{AP1}_{\mathtt{TLightHash}_{\Pi_0}}(\boldsymbol{m})\right), \Pr\left(\mathsf{AP2}_{\mathtt{TLightHash}_{\Pi_0}}(\boldsymbol{m})\right) \leq \delta(\rho) + \frac{256q^4}{N^3} + \frac{22q^2}{N^{3/2}} + \frac{1664q^2}{N^2} \leq \epsilon_2(\rho).$$

D.3 Proof of Lemma 10

We now fix q distinct messages for $\mathtt{PHash}$, with parsed forms $m_u = (m_u[1], \ldots, m_u[\ell_u])$, $\ell_u \leq \ell$, and we assume that $p(x)$ satisfies SQF_ℓ. Here, a point is a pair $v = (a, x) \in [\ell] \times \{0, 1\}^{n-2}$, and V_u, $\Delta(u, w)$, β_u, $\mathbf{a}_{uw}$, $\mathbf{b}_{uw}$, K_1, K_2, $\mathcal{Q}$, E_1 and E_2 are defined as before. Let $Y_0 := \Pi_0(0)$, $Y_1 := \Pi_0(1)$, and $\mu_a := \mathtt{Trunc}_2(2^a \cdot Y_0 \oplus 2^{2a} \cdot Y_1)$ for $a \in [\ell]$. For a point $v = (a, x)$, let $W(v) := x \oplus \mu_a$ and $Z_v := \Pi_0(W(v))$. By Algorithm 1, we again have $\mathtt{PHash}_{\Pi_0}(m_u) = (\mathbf{1}_{V_u} \cdot \mathbf{Z}, \beta_u \cdot \mathbf{Z})$, so all the events in the CfH definition are given by the same linear conditions as before. The difference is that distinct points

may have the same input, so the Z_v's are not distinct. We say that two points $v = (a, x)$ and $v' = (b, y)$ *collide* if $a \neq b$ and $W(v) = W(v')$, i.e., $\mu_a \oplus \mu_b = x \oplus y$ (two distinct points at the same position never have the same input), and that v is *special* if $W(v) \in \{0, 1\}$, i.e., $\mu_a \in \{x, x \oplus 1\}$.

Lemma 19. *For $a \neq b \in [\ell]$ and $\kappa \in \{0,1\}^{n-2}$, we say that the event $\mu_a \oplus \mu_b = \kappa$ (res. $\mu_a = \kappa$) has position set $\{a, b\}$ (res. $\{a\}$). Each such event has probability at most $4/(N-1)$, and any two such events with distinct position sets hold simultaneously with probability at most $16/(N(N-1))$.*

Proof. As $\mathtt{Trunc}_2$ is linear, $\mu_a \oplus \mu_b = \mathtt{Trunc}_2(t \cdot Y_0 \oplus t^2 \cdot Y_1)$ with $t = 2^a \oplus 2^b$, and $\mu_a = \mathtt{Trunc}_2(t \cdot Y_0 \oplus t^2 \cdot Y_1)$ with $t = 2^a$. By SQF_ℓ (all positions lie in $[\ell]$), $t \neq 0$, and distinct position sets give distinct values of t. For a fixed Y_1, $Y_0 \mapsto t \cdot Y_0 \oplus t^2 \cdot Y_1$ is a bijection, so at most 4 values of Y_0 satisfy the event, whereas Y_0 is uniformly distributed over $N-1$ values. For two events with $t \neq t'$, the map $(Y_0, Y_1) \mapsto (tY_0 \oplus t^2 Y_1, t'Y_0 \oplus t'^2 Y_1)$ is a bijection, as its determinant $tt'(t \oplus t')$ is non-zero, so at most 16 of the $N(N-1)$ equally likely pairs (Y_0, Y_1) satisfy both events. □

Moreover, conditioned on (Y_0, Y_1), the outputs of Π_0 at any t distinct inputs outside $\{0, 1\}$ are uniformly distributed over the t-tuples of distinct strings outside $\{Y_0, Y_1\}$. So, Lemma 13 holds conditionally on (Y_0, Y_1) for vectors indexed by such inputs, with $N-2$ in place of N, and the bound $(2/N)^k$ remains valid as $t + 2 \leq 4\ell + 2 \leq N/2$. For a vector $\mathbf{y}$ indexed by points, let $\overline{\mathbf{y}}$ denote the vector indexed by inputs, given by $\overline{y}_x \coloneqq \bigoplus_{v:W(v)=x} y_v$. Then, $\mathbf{y} \cdot \mathbf{Z} = \overline{\mathbf{y}} \cdot \overline{\mathbf{Z}}$, where $\overline{Z}_x \coloneqq \Pi_0(x)$.

Collisions and multicollisions. Let $u \neq w \in [q]$, and let $\mathbf{y}$ be $\mathbf{a}_{uw}$ or $\mathbf{b}_{uw}$, with support S. If, given (Y_0, Y_1), some non-special input has a non-zero coefficient in $\overline{\mathbf{y}}$, then $\overline{\mathbf{y}} \cdot \overline{\mathbf{Z}} \in K_1$ (res. K_2) has conditional probability at most $8/N$ (the special inputs only contribute a known constant). Otherwise, every non-special point $v \in S$ has the same input as another point of S, which lies at a different position. Indeed, all the points of S have non-zero coefficients in $\mathbf{y}$, and distinct points at the same position have distinct inputs. So, for a fixed point $v_1 \in S$ at position a_1, at least one of at most 2ℓ events holds: v_1 is special (2 events), or v_1 collides with a point of S at another position (at most $2(\ell - 1)$ events). Each of them has probability at most $4/(N-1)$ by Lemma 19, and its position set P_1 contains a_1. If S occupies at most two positions, then only 4 of these events are possible, which gives at most $16/(N-1)$. Otherwise, for each of these events, we fix a point $v_2 \in S$ at a position outside P_1, and one of at most 2ℓ similar events holds for v_2, whose position set is different from P_1. By Lemma 19, this gives at most $16(2\ell)^2/(N(N-1))$. So, the two halves of the hash values of m_u and m_w collide with probability at most

$$\frac{8}{N} + \frac{16}{N-1} + \frac{64\ell^2}{N(N-1)} \leq \frac{40}{N} + \frac{128\ell^2}{N^2}.$$

Summing over the pairs gives $\epsilon_1(\rho)$, and Proposition 8 gives $\epsilon_3(\rho, k)$.

Masked inputs. Let Aux be the event that some message m_u has two colliding points or a special point. As $\sum_u \ell_u \le \sigma$ and $\ell_u \le \ell$, by Lemma 19, we have

$$\Pr(\mathsf{Aux}) \le \sum_{u\in[q]} \left(\frac{\ell_u(\ell_u-1)}{2} + 2\ell_u\right)\frac{4}{N-1} \le \frac{(4\ell+12)\sigma}{N}.$$

Suppose that Aux does not hold. Then, for each u, the inputs $W_u[a] \coloneqq W(a, m_u[a])$, $a \in [\ell_u]$, are distinct and non-special. Let $P_u \coloneqq \{W_u[a] : a \in [\ell_u]\}$, so that $\overline{\mathbf{a}}_{uw} = \mathbf{1}_{P_u \triangle P_w}$ and $\overline{\mathbf{b}}_{uw} = \overline{\beta}_u \oplus \overline{\beta}_w$, where $\overline{\beta}_u = \bigoplus_{a\in[\ell_u]} 2^{\ell_u+1-a}\,\mathbf{e}_{W_u[a]}$. We call a pair (u, w) of distinct messages

- a *single-difference pair* if $\ell_u = \ell_w$ and m_u and m_w differ at exactly one position a. Then, $W_u[a] \notin P_w$ (it differs from $W_w[a]$, and from $W_w[b] = W_u[b]$ for $b \ne a$), and similarly $W_w[a] \notin P_u$, so that $\overline{\mathbf{a}}_{uw} = \mathbf{e}_{W_u[a]} \oplus \mathbf{e}_{W_w[a]}$ and $\overline{\mathbf{b}}_{uw} = 2^{\ell_u+1-a} \cdot \overline{\mathbf{a}}_{uw}$;
- *degenerate* if $P_u = P_w$, i.e., $\overline{\mathbf{a}}_{uw} = 0$;
- a *swap pair* if $\ell_u = \ell_w$, m_u and m_w differ exactly at two positions a and b, $W_u[a] = W_w[b]$ and $W_u[b] = W_w[a]$. Then, (u, w) is degenerate, and $\overline{\mathbf{b}}_{uw} = (2^{\ell_u+1-a} \oplus 2^{\ell_u+1-b})(\mathbf{e}_{W_u[a]} \oplus \mathbf{e}_{W_u[b]})$;
- a *shift pair* if, up to exchanging u and w, $\ell_w = \ell_u + 1$ and $W_u[a] = W_w[a+1]$ for all $a \in [\ell_u]$. Then, $\overline{\mathbf{a}}_{uw} = \mathbf{e}_{W_w[1]} = 2^{-\ell_w} \cdot \overline{\mathbf{b}}_{uw}$.

Lemma 20. *Suppose that* Aux *does not hold, and let* $u \ne w \in [q]$. *Then,* $\overline{\mathbf{b}}_{uw} \ne 0$. *Moreover, if* $\overline{\mathbf{b}}_{uw}$ *is constant on its support, then* (u, w) *is a single-difference pair, a swap pair or a shift pair, and if* (u, w) *is degenerate, then* $\ell_u = \ell_w$, *and either* (u, w) *is a swap pair or* m_u *and* m_w *differ at three or more positions.*

Proof. For $x = W_u[a]$, let $e_u(x) \coloneqq \ell_u + 1 - a \in [1, \ell]$, and similarly for w. The coefficient of x in $\overline{\mathbf{b}}_{uw}$ is $2^{e_u(x)}$, $2^{e_w(x)}$ or $2^{e_u(x)} \oplus 2^{e_w(x)}$, according as x lies in $P_u \setminus P_w$, $P_w \setminus P_u$ or $P_u \cap P_w$. We call $x \in P_u \cap P_w$ *aligned* if $e_u(x) = e_w(x)$. If $\overline{\mathbf{b}}_{uw} = 0$, then $P_u = P_w$ and all inputs are aligned, so $\ell_u = |P_u| = \ell_w$ and $W_u[a] = W_w[a]$ for all a, i.e., $m_u = m_w$, a contradiction.

Suppose that $\overline{\mathbf{b}}_{uw}$ is constant on its support. If $P_u \ne P_w$, then the constant is some 2^g, so by SQF_ℓ, all the inputs in $P_u \cap P_w$ are aligned, and $P_u \setminus P_w$ (res. $P_w \setminus P_u$) has at most one element, at position $\ell_u + 1 - g$ (res. $\ell_w + 1 - g$). If $\ell_u = \ell_w$, aligned inputs are at the same position in both messages, so m_u and m_w agree at all positions but $\ell_u + 1 - g$, and (u, w) is a single-difference pair. If $\ell_u < \ell_w$ (the case $\ell_u > \ell_w$ is symmetric), then $\ell_w \le |P_u \cap P_w| + 1 \le \ell_u + 1$, so $\ell_w = \ell_u + 1$, $P_u \subseteq P_w$, and as all inputs of P_u are aligned, (u, w) is a shift pair. If $P_u = P_w$, then $\ell_u = \ell_w$, and by SQF_ℓ, the unordered pair $\{e_u(x), e_w(x)\}$ is the same for all the non-aligned inputs x. As each message has one input at each position, there are at most two of them, and not exactly one (its position in m_u would be occupied in m_w by another non-aligned input). So, exactly two inputs are not aligned, and they are at swapped positions a and b, whereas all the other positions carry the same input, i.e., the same block. Hence, (u, w) is a swap pair.

Finally, let (u, w) be degenerate, so that $\ell_u = \ell_w$. If m_u and m_w differ at a position a, then $W_u[a] = W_w[b]$ for some $b \neq a$, and they differ at b as well, as otherwise $W_u[a] = W_w[b] = W_u[b]$, which contradicts $\neg\mathsf{Aux}$. So, the positions at which they differ are permuted without fixed points. Hence, there are at least two of them, and if there are exactly two, then (u, w) is a swap pair. □

Lemma 21. *For $u \neq w \in [q]$, the probability that* Aux *does not hold and (u, w) is a swap pair (res. a degenerate pair but not a swap pair, res. a shift pair) is at most $4/(N-1)$ (res. $16\ell^2/(N(N-1))$, res. $4/(N-1)$).*

Proof. If $\ell_u = \ell_w$ and m_u and m_w differ exactly at positions a and b, then the condition $W_u[a] = W_w[b]$ is the event $\mu_a \oplus \mu_b = m_u[a] \oplus m_w[b]$. If (u, w) is degenerate but not a swap pair, then by Lemma 20, m_u and m_w differ at three or more positions, which are permuted without fixed points. Let $a_1 < a_2 < a_3$ be the first three of them. Then, $W_u[a_1] = W_w[b_1]$ for some $b_1 \neq a_1$, and $W_u[a'] = W_w[b']$ for some $b' \neq a'$, where a' is the smallest element of $\{a_2, a_3\} \setminus \{b_1\}$. As $a' \notin \{a_1, b_1\}$, the two position sets are distinct, and Lemma 19 applies to each of the at most ℓ^2 choices of (b_1, b'). For a shift pair, $W_u[1] = W_w[2]$. □

We say that a set of messages is *aligned* if no two of their points collide. In the absence of Aux, a set of at most four messages is not aligned only if a point of one of them collides with a point of another one, at a different position. So, by Lemma 19, this happens with probability at most $6\ell^2 \cdot 4/(N-1) \leq 48\ell^2/N$. If a set of messages is aligned and Aux does not hold, then W is injective on their points, with non-special values, so for vectors supported on these points, $\overline{\mathbf{y}}$ is just a relabeling of $\mathbf{y}$, and the arguments of the previous subsections apply conditionally on (Y_0, Y_1).

Double collisions. Let $u \neq w \in [q]$, and suppose that Aux does not hold. If $\overline{\mathbf{a}}_{uw}$ and $\overline{\mathbf{b}}_{uw}$ are linearly independent, then both halves collide with conditional probability at most $32/N^2$. Otherwise, as $\overline{\mathbf{b}}_{uw} \neq 0$, either $\overline{\mathbf{a}}_{uw} = 0$, or $\overline{\mathbf{b}}_{uw}$ is constant on its support, so by Lemma 20, (u, w) is a single-difference pair, a degenerate pair or a shift pair. For a single-difference pair at position a, with $\overline{\mathbf{a}}_{uw} = \mathbf{e}_x \oplus \mathbf{e}_y$, a double collision would give $0 \neq \overline{Z}_x \oplus \overline{Z}_y \in K_1$ and $2^{\ell_u+1-a} \cdot (\overline{Z}_x \oplus \overline{Z}_y) \in K_2$, which is impossible by Lemma 14. In the other cases, the collision of the second half has conditional probability at most $8/N$. By Lemma 21, we get

$$\begin{aligned}\Pr\left(\mathsf{COLL}_{\mathtt{TPHash}_{\Pi_0}}(\boldsymbol{m})\right) &\leq \Pr(\mathsf{Aux}) + \frac{q^2}{2}\left(\frac{32}{N^2} + \left(\frac{8}{N-1} + \frac{16\ell^2}{N(N-1)}\right)\frac{8}{N}\right) \\ &\leq \delta(\rho).\end{aligned}$$

Alternating paths. As before, $\Pr\left(\mathsf{AP1}_{\mathtt{TPHash}_{\Pi_0}}(\boldsymbol{m})\right) \leq \delta(\rho) + \Pr(\mathsf{Aux}) + \Pr\left(\neg\mathsf{Aux} \wedge \bigvee_{(i,j,r,s)\in\mathcal{Q}} \mathsf{E}_1(i,j,r,s)\right)$, and similarly for $\mathsf{AP2}_{\mathtt{TPHash}_{\Pi_0}}(\boldsymbol{m})$ with E_2.

Lemma 22. *For $b \in \{1, 2\}$, we have*

$$\Pr\left(\neg\mathsf{Aux} \wedge \bigvee_{(i,j,r,s)\in\mathcal{Q}} \mathsf{E}_b(i,j,r,s)\right) \leq \frac{(256 + 4864\ell^2)q^4}{N^3} + \frac{68q^2}{N^{3/2}} + \frac{1856q^2}{N^2} + \frac{182\ell^2q^2}{N^{5/2}}.$$

$$+ \frac{91\ell^2 q^2}{N^{5/2}}.$$

Proof. For $T = (i, j, r, s) \in \mathcal{Q}$, we split $\mathsf{E}_b(T)$ according to whether the set $\{m_i, m_j, m_r, m_s\}$ is aligned or not.

Aligned tuples: The proofs of Lemma 16 and 17 (including Lemma 18) only use the structure of the sets V_u, Lemma 14, and Lemma 13 for vectors supported on the points of the messages of a single tuple. So, they remain valid if we replace $\mathsf{E}_b(T)$ by the event that $\mathsf{E}_b(T)$ holds, Aux does not hold, and the messages of T are aligned. Indeed, conditioned on (Y_0, Y_1), Lemma 13 applies to these vectors, and in the case J_2 (res. for the exceptional tuples of Lemma 17), we intersect the event $\mathbf{1}_D \cdot \mathbf{Z} \in K_1$ or $\gamma_D \cdot \mathbf{Z} \in 2^{-L_1-1} \cdot K_2$ (res. $Z_v \oplus Z_{v'} = 2^{n-1}$) with the event that W is injective on D, which holds whenever one of the tuples in question is aligned, and still has probability at most $4/N$ or $8/N$ (res. $2/N$). So, the aligned tuples contribute at most $256q^4/N^3 + 22q^2/N^{3/2} + 1664q^2/N^2$.

For the other tuples, we fix (Y_0, Y_1) such that Aux does not hold, and consider the rank $\rho_b(T)$ of $(\overline{\mathbf{a}}_{ij}, \overline{\mathbf{b}}_{jr}, \overline{\mathbf{a}}_{rs})$ (for $b = 1$) or $(\overline{\mathbf{b}}_{ij}, \overline{\mathbf{a}}_{jr}, \overline{\mathbf{b}}_{rs})$ (for $b = 2$). These vectors are supported on at most 4ℓ non-special inputs.

Non-aligned tuples with $\rho_b(T) \geq 2$: Here, $\mathsf{E}_b(T)$ has conditional probability at most $64/N^2$, and the messages of T are not aligned with probability at most $48\ell^2/N$. So, these tuples contribute at most $3072\ell^2 q^4/N^3$.

Tuples with $\rho_b(T) \leq 1$: As the $\overline{\mathbf{b}}$'s are non-zero and the $\overline{\mathbf{a}}$'s are 0/1-vectors, by Lemma 20, $\rho_1(T) \leq 1$ only if $\overline{\mathbf{a}}_{ij} = \overline{\mathbf{a}}_{rs} = 0$, or (j, r) is a single-difference, swap or shift pair, and $\rho_2(T) \leq 1$ only if (i, j) is a single-difference, swap or shift pair, or $\overline{\mathbf{a}}_{jr} = 0$ and $\overline{\mathbf{b}}_{rs} = c \cdot \overline{\mathbf{b}}_{ij}$ for some c. If (j, r) (for $b = 1$) or (i, j) (for $b = 2$) is a single-difference pair, then the $\overline{\mathbf{a}}$'s of T are 0/1-multiples of $\mathbf{e}_x \oplus \mathbf{e}_y$, where $\overline{\mathbf{b}}_{jr}$ (res. $\overline{\mathbf{b}}_{ij}$) is $2^e \cdot (\mathbf{e}_x \oplus \mathbf{e}_y)$ with $e \in [1, \ell]$. If one of them is non-zero, then $\mathsf{E}_b(T)$ is impossible by Lemma 14, as for the double collisions, and otherwise, T falls into the case (1) or (3) below. Let G be the set of $u \in [q]$ such that (u, w) is degenerate for some $w \neq u$. By Lemma 21, the expectation of $|G|$ (on $\neg\mathsf{Aux}$) is at most $q^2(4/(N-1) + 16\ell^2/(N(N-1))) \leq 8q^2/N + 32\ell^2 q^2/N^2$.

1. If $\overline{\mathbf{a}}_{ij} = \overline{\mathbf{a}}_{rs} = 0$, then $j, r \in G$, and $\mathsf{E}_1(T)$ implies $\overline{\mathbf{b}}_{jr} \cdot \overline{\mathbf{Z}} \in K_2$. The conditional probability that $\overline{\mathbf{b}}_{uw} \cdot \overline{\mathbf{Z}} \in K_2$ for some distinct $u, w \in G$ is at most $\min\{1, 8|G|^2/N\} \leq \sqrt{8/N}\,|G|$. Taking the expectation, these tuples contribute at most $23q^2/N^{3/2} + 91\ell^2 q^2/N^{5/2}$.
2. If (j, r) (for $b = 1$) or (i, j) (for $b = 2$) is a swap or shift pair, then $\mathsf{E}_b(T)$ implies $\overline{\mathbf{b}}_{jr} \cdot \overline{\mathbf{Z}} \in K_2$ (res. $\overline{\mathbf{b}}_{ij} \cdot \overline{\mathbf{Z}} \in K_2$). By Lemma 21, summing over the unordered pairs, these tuples contribute at most $(q^2/2) \cdot 8/(N-1) \cdot 8/N \leq 64q^2/N^2$.
3. Let $b = 2$, $\overline{\mathbf{a}}_{jr} = 0$ and $\overline{\mathbf{b}}_{rs} = c \cdot \overline{\mathbf{b}}_{ij}$, so that (j, r) is degenerate, and $\mathsf{E}_2(T)$ implies $\overline{\mathbf{b}}_{ij} \cdot \overline{\mathbf{Z}} \in K_2$. If (j, r) is not a swap pair, then by Lemma 21, each such tuple contributes at most $16\ell^2/(N(N-1)) \cdot 8/N$, i.e., at most $256\ell^2 q^4/N^3$ in total. Now, let (j, r) be a swap pair at positions $p < p'$. If $c = 1$, then $\overline{\mathbf{b}}_{is} = \overline{\mathbf{b}}_{jr} = (2^{\ell_j+1-p} \oplus 2^{\ell_j+1-p'})(\mathbf{e}_x \oplus \mathbf{e}_y)$ for some inputs $x \neq y$ (in particular, $i \neq s$). So, by Lemma 20, (i, s) is a single-difference, swap or shift pair. It is not a shift pair, as the support has two elements, and not

a single-difference pair, as $2^e = 2^{\ell_j+1-p} \oplus 2^{\ell_j+1-p'}$ with $e \in [1,\ell]$ is ruled out by TF_ℓ. Hence, (i,s) is a swap pair, and $i,j \in G$. As in (1), these tuples contribute at most $23q^2/N^{3/2} + 91\ell^2q^2/N^{5/2}$. If $c \neq 1$ and two points of the messages of T at positions $a \neq b$ with $\{a,b\} \neq \{p,p'\}$ collide, then by Lemma 19, for each of the at most $6\ell^2$ such pairs of points, this and the swap condition hold simultaneously with probability at most $16/(N(N-1))$. So, these tuples contribute at most $1536\ell^2q^4/N^3$. Finally, if $c \neq 1$ and there is no such collision, then by Lemma 23 below, m_i and m_r differ exactly at positions p and p', and m_j agrees with m_i at all positions but one of p and p', where its block is determined by $m_j[p] \oplus m_j[p'] = m_r[p] \oplus m_r[p']$ (adding the two swap conditions). So, given (i,r), there are at most 2 choices of j, and as the event Aux does not hold, (j,r) is a swap pair and $\overline{\mathbf{b}}_{ij} \cdot \overline{\mathbf{Z}} \in K_2$ only depends on (i,j,r), these tuples contribute at most $2q^2 \cdot 4/(N-1) \cdot 8/N \leq 128q^2/N^2$.

Adding up all the contributions proves the claim for $b = 2$. For $b = 1$, the same bound holds a fortiori, as the aligned tuples contribute at most $128q^4/N^3 + 12q^2/N^{3/2} + 96q^2/N^2$, and only the cases (1) and (2) occur among the tuples with $\rho_1(T) \leq 1$. □

Lemma 23. *Suppose that* Aux *does not hold, let* $(i,j,r,s) \in \mathcal{Q}$*, and let* (j,r) *be a swap pair at positions* $p < p'$*. Suppose that any two colliding points of* m_i*,* m_j*,* m_r *and* m_s *are at positions* p *and* p'*. If* $\overline{\mathbf{b}}_{rs} = c \cdot \overline{\mathbf{b}}_{ij}$ *for some* $c \neq 1$*, then* $\ell_i = \ell_s = \ell_j$*,* (i,s) *is a swap pair at positions* p *and* p'*, and* m_i *has the same block as* m_j *at all positions but one of* p *and* p'*. In particular,* m_i *and* m_r *differ exactly at positions* p *and* p'*.*

Proof. Let $L \coloneqq \ell_j = \ell_r$. We call p and p' the inner positions, and all the other positions outer. By assumption, the input of a point at an outer position is not the input of any other point, and V_j and V_r agree at outer positions. Note that $c \neq 0$ as $\overline{\mathbf{b}}_{rs} \neq 0$. The coefficients of $\overline{\beta}_u$ add up to $\bigoplus_{a\in[\ell_u]} 2^{\ell_u+1-a} = 2(2^{\ell_u} \oplus 1)/(1 \oplus 2)$. So, adding up the coefficients on both sides of $\overline{\beta}_r \oplus \overline{\beta}_s = c(\overline{\beta}_i \oplus \overline{\beta}_j)$ gives

$$2^{\ell_s} \oplus 2^L = c\,(2^{\ell_i} \oplus 2^L). \tag{35}$$

Comparing the coefficients of the input of a point $v = (a,x)$ at an outer position, and dividing by 2^{1-a}, gives

$$[v \in V_s]\, 2^{\ell_s} \oplus [v \in V_j]\, (1 \oplus c) 2^L \oplus [v \in V_i]\, c\, 2^{\ell_i} = 0,$$

where $[\cdot]$ is 1 if the condition holds and 0 otherwise. The three terms are non-zero (as $c \notin \{0,1\}$), and by (35), they add up to zero, so no two of them add up to zero. Hence, every outer point lies in all or none of V_s, V_j and V_i. So, at an outer position $a \leq L$, m_i and m_s have the same point as m_j, and at an outer position $a > L$, none of them has a point. In particular, $\ell_i, \ell_s \leq L$, and all the positions in $[\ell_i + 1, L] \cup [\ell_s + 1, L]$ are inner.

Suppose that $\ell_i \neq L$. Then, by (35) and $c \neq 1$, $\ell_s \notin \{L, \ell_i\}$, so ℓ_i and ℓ_s are the two elements of $\{L-2, L-1\}$, and $\{p,p'\} = \{L-1, L\}$. Let $x \coloneqq W_j[L-1] = W_r[L]$ and $y \coloneqq W_j[L] = W_r[L-1]$, with coefficients 2^2 and 2 in

$\overline{\beta}_j$. If $(\ell_i, \ell_s) = (L-1, L-2)$, then $c = (1 \oplus 2^{-2})/(1 \oplus 2^{-1}) = 1 \oplus 2^{-1}$, m_s has no inner point, and the only inner point of m_i is at position $L-1$, with coefficient 2. So, comparing the coefficients of x gives $2 = (1 \oplus 2^{-1})(2^2 \oplus \lambda)$, where $\lambda = 2$ if $W_i[L-1] = x$ and $\lambda = 0$ otherwise. If $(\ell_i, \ell_s) = (L-2, L-1)$, then $c = (1 \oplus 2^{-1})^{-1}$, m_i has no inner point, and the only inner point of m_s is at position $L-1$, with coefficient 2. So, comparing the coefficients of y gives $(1 \oplus 2^{-1})(2^2 \oplus \lambda) = 2$, where $\lambda = 2$ if $W_s[L-1] = y$ and $\lambda = 0$ otherwise. In both cases, we get $2^2 = 0$ or $1 \oplus 2 \oplus 2^2 = 0$, which is impossible as $p(x)$ does not divide $x^2 \oplus x \oplus 1$ (recall that $n \geq 3$).

So, $\ell_i = L$, and by (35), $\ell_s = L$. Hence, m_i and m_s agree with m_j at outer positions, and $\overline{\mathbf{b}}_{ij}$ and $\overline{\mathbf{b}}_{rs}$ vanish at the inputs of outer points. Let $\alpha \coloneqq 2^{L+1-p}$ and $\alpha' \coloneqq 2^{L+1-p'}$, and for $u \in \{i, j, r, s\}$, let $x_u \coloneqq W_u[p]$ and $y_u \coloneqq W_u[p']$, so that $x_r = y_j$ and $y_r = x_j$. Then, $\overline{\mathbf{b}}_{ij} = \alpha \cdot \mathbf{1}_G \oplus \alpha' \cdot \mathbf{1}_{G'}$ and $\overline{\mathbf{b}}_{rs} = \alpha \cdot \mathbf{1}_F \oplus \alpha' \cdot \mathbf{1}_{F'}$, where $G \coloneqq \{x_i\} \triangle \{x_j\}$, $G' \coloneqq \{y_i\} \triangle \{y_j\}$, $F \coloneqq \{x_r\} \triangle \{x_s\}$ and $F' \coloneqq \{y_r\} \triangle \{y_s\}$. Each of these sets is empty or has two elements, and $\overline{\mathbf{b}}_{ij}$ takes the values α, α' and $\alpha \oplus \alpha'$ on $G \setminus G'$, $G' \setminus G$ and $G \cap G'$, respectively, and similarly for $\overline{\mathbf{b}}_{rs}$. As α, α' and $\alpha \oplus \alpha'$ are distinct and non-zero, and $\overline{\mathbf{b}}_{rs} = c \cdot \overline{\mathbf{b}}_{ij}$, the two vectors have the same support and the same level sets on it.

- If G and G' are disjoint and non-empty, then the support has four elements, so F and F' are disjoint and non-empty as well, and c maps $\{\alpha, \alpha'\}$ onto itself. As $c \neq 1$, we get $c\alpha = \alpha'$ and $c\alpha' = \alpha$, i.e., $c^2 = 1$, a contradiction.
- If $|G \cap G'| = 1$, then the support has three elements, with three distinct values, so $|F \cap F'| = 1$ as well, and c permutes $\{\alpha, \alpha', \alpha \oplus \alpha'\}$. Let $t \coloneqq \alpha'/\alpha = 2^{p-p'}$. As $c \neq 1$, $c\alpha \neq \alpha$, so either $c = t$, and then $c\alpha' = t^2\alpha \in \{\alpha, \alpha \oplus \alpha'\}$, or $c = 1 \oplus t$, and then $c\alpha' = (t \oplus t^2)\alpha \in \{\alpha, \alpha'\}$. So, $t^2 = 1$, $t^2 = 1 \oplus t$, $t \oplus t^2 = 1$ or $t^2 = 0$. The first one contradicts the primitivity of $p(x)$ (as $0 < 2(p'-p) < 2^n - 1$), the last one is impossible, and the other two give $1 \oplus 2^{p'-p} \oplus 2^{2(p'-p)} = 0$, which is ruled out by TF_ℓ.
- Otherwise, $\overline{\mathbf{b}}_{ij}$ is constant on a two-element set D, and so is $\overline{\mathbf{b}}_{rs}$. If $G = G' = D$, then $\{x_i, x_j\} = \{y_i, y_j\}$, and as $x_i \neq y_i$ and $x_j \neq y_j$ (by $\neg\mathsf{Aux}$), we get $x_i = y_j = x_r$ and $y_i = x_j = y_r$, i.e., $V_i = V_r$, a contradiction. If $G = \emptyset$ and $G' = D$, then $x_i = x_j$ and $D = \{y_i, y_j\}$, and $\overline{\mathbf{b}}_{rs}$ takes the value $c\alpha' \neq \alpha'$ on D. So, either $F = F' = D$, which gives $x_i = x_j = y_r \in D$, a contradiction as above, or $F = D$ and $F' = \emptyset$, i.e., $y_s = y_r = x_i$ and $\{x_r, x_s\} = \{y_i, y_j\}$, which gives $x_s = y_i$ as $x_r = y_j$. Hence, (i, s) is a swap pair at positions p and p', and m_i has the same block as m_j at p, but not at p'. The case $G' = \emptyset$ and $G = D$ is symmetric, with the roles of p and p' exchanged.

Finally, m_i differs from m_r at both inner positions, as $\{x_i, y_i\}$ and $\{x_r, y_r\} = \{x_j, y_j\}$ share exactly one input, which is at different positions in m_i and m_r. □

Lemma 10 now follows by combining the bounds on ϵ_1, ϵ_3 and δ above with Lemma 22, which shows that both $\Pr\left(\mathsf{AP1}_{\mathtt{TPHash}\Pi_0}(\boldsymbol{m})\right)$ and $\Pr\left(\mathsf{AP2}_{\mathtt{TPHash}\Pi_0}(\boldsymbol{m})\right)$ are at most

$$\delta(\rho) + \Pr(\mathsf{Aux}) + \frac{(256 + 4864\ell^2)q^4}{N^3} + \frac{68q^2}{N^{3/2}} + \frac{1856q^2}{N^2} + \frac{182\ell^2q^2}{N^{5/2}} \leq \epsilon_2(\rho)$$

where we used $\ell \geq 1$ and $N^{-3} \leq N^{-5/2}$.

E Miscellaneous Proofs related to Theorem 4

E.1 Proof of Lemma 11

We have

$$\begin{aligned}
&\Pr\left(\mathsf{\theta}_{\mathrm{id}} \in \Omega_{\mathrm{bad}}\right) \\
&= \Pr\left(\mathsf{LSC}(\mathsf{T}, p+q) \vee \mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K}) \vee \mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}) \vee \mathsf{DC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K})\right) \\
&\leq \Pr\left(\mathsf{LSC}(\mathsf{T}, p+q)\right) + \Pr\left(\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K})\right) + \Pr\left(\mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}) \mid \neg\mathsf{LSC}(\mathsf{T}, p+q)\right) \\
&\qquad + \Pr\left(\mathsf{DC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K})\right) \\
&\leq \frac{4}{2^n} + \frac{qp^r}{2^{nr}} + \frac{rq(p+q)^r}{2^{nr}} + \frac{2r(p+q)^{r-1}\sqrt{nq}}{2^{n(r-1)}} + \frac{2r^2q^2p^{r-1}}{2^{nr}},
\end{aligned}$$

where the first term on the right hand side corresponds to $\Pr\left(\mathsf{LSC}(\mathsf{T}, p+q)\right)$ and follows from Lemma 1, the second term corresponds to $\Pr\left(\mathsf{KG}(\mathsf{M},\mathsf{U},\mathsf{K})\right)$ and follows from the uniformity of K. The last two terms correspond to $\Pr\left(\mathsf{SC}(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V},\mathsf{K}) \mid \neg\mathsf{LSC}(\mathsf{T}, p+q)\right)$. To argue this, first notice that given $\neg\mathsf{LSC}(\mathsf{T}, p+q)$, we have

$$\mu(\mathsf{T},\mathsf{V}) \leq \frac{q(p+q)^r}{2^n} + 2(p+q)^{r-1}\sqrt{nq}.$$

For each choice of $k \in [r]$, the predicate $\forall k' \neq k$, $\mathsf{X}^i_{k'} = \mathsf{U}^{j_{k'}}_{k'}$ is satisfied with at most $2^{-n(r-1)}$ probability. Now, we get the desired terms using union bound over the at most $\mu(\mathsf{T},\mathsf{V})$ tuples and the r choices of k. Finally, for DC, recall that K is sampled independent of $(\mathsf{M},\mathsf{T},\mathsf{U},\mathsf{V})$. Fix $i \neq i'$, k and $(j_l, j'_l)_{l\neq k}$. Then, $\mathsf{X}^i_l = \mathsf{U}^{j_l}_l$ and $\mathsf{X}^{i'}_l = \mathsf{U}^{j'_l}_l$ hold for all $l \neq k$ with probability $2^{-n(r-1)}$ if $\mathsf{U}^{j_l}_l \oplus \mathsf{U}^{j'_l}_l = \mathsf{M}^i \oplus \mathsf{M}^{i'}$ for all $l \neq k$, and with probability 0 otherwise. So, $\Pr\left(\mathsf{DC}\right) \leq \mathbb{E}\left(\mathtt{N}\right)/2^{n(r-1)}$, where $\mathtt{N}$ denotes the number of tuples $\tau = (i, i', k, (j_l, j'_l)_{l\neq k})$ satisfying

$$\mathsf{E}_l: \ \mathsf{U}^{j_l}_l \oplus \mathsf{U}^{j'_l}_l = \mathsf{M}^i \oplus \mathsf{M}^{i'} \text{ for all } l \neq k, \qquad \mathsf{E}_0: \ \bigoplus_{l\neq k}\left(\mathsf{V}^{j_l}_l \oplus \mathsf{V}^{j'_l}_l\right) = \mathsf{T}^i \oplus \mathsf{T}^{i'}.$$

Note that $j_l \neq j'_l$ as $\mathsf{M}^i \neq \mathsf{M}^{i'}$. Since the queries are adaptive, we cannot simply use the uniformity of T for E_0. Instead, we consider the query in τ (among its $2r$ construction and primitive queries) that is made last by $\mathcal{A}$, and condition on all the queries made before it. If it is a construction query or a forward primitive query, then the events E_l are already fixed, and its response (uniform over at least $2^n - p$ values) satisfies E_0 with probability at most $1/(2^n - p)$. If it is a backward primitive query to $\mathsf{\Pi}_l$, then E_0 and $\mathsf{E}_{l'}$ for all $l' \notin \{k, l\}$ are already fixed, and its response satisfies E_l with probability at most $1/(2^n - p)$. On the other hand, for fixed (i, i', k), there are at most p^{r-1} choices of $(j_l, j'_l)_{l\neq k}$ satisfying E_l for all $l \neq k$, as j_l determines j'_l. Similarly, for fixed (i, i', k) and $l \neq k$, there are at most

p^{r-1} choices satisfying E_0 and $\mathsf{E}_{l'}$ for all $l' \notin \{k, l\}$, as j_l then determines j'_l via E_0. Thus, using $p \leq 2^{n-1}$, we have $\mathbb{E}(\mathtt{N}) \leq (rq^2p^{r-1} + r(r-1)q^2p^{r-1})/(2^n - p) \leq 2r^2q^2p^{r-1}/2^n$, and we get $2r^2q^2p^{r-1}/2^{nr}$ (the factor $1/2$ for unordered pairs is ignored). The result follows as $qp^r + 2r^2q^2p^{r-1} \leq (2r^2+1)q(p+q)^r$. □

E.2 Proof of Lemma 12

Let $\omega = (M, T, U, V, K, Y)$. Since the transcript is good, $\neg(\mathsf{LSC}(T, p+q) \vee \mathsf{KG} \vee \mathsf{SC} \vee \mathsf{DC})$ holds. Before moving forward, recall the notations introduced while discussing the sampling in the ideal world. We assume analogous notations for any arbitrary transcript. We also ignore the probability computation of obvious events, such as: the message tuple being realized.

Real World: In the real world, we have

$$\begin{aligned}\Pr(\mathtt{\Theta}_{\mathrm{re}} = \omega) &= \Pr\left(\mathtt{\Theta}^{\mathrm{key}}_{\mathrm{re}} = K, \mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{re}} = (U,V), \mathtt{\Theta}^{\mathrm{int}}_{\mathrm{re}} = (X,Y), \mathtt{\Theta}^{\mathrm{con}}_{\mathrm{re}} = (M,T)\right) \\ &= \Pr\left(\mathtt{\Theta}^{\mathrm{key}}_{\mathrm{re}} = K\right) \times \Pr\left(\mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{re}} = (U,V)\right) \times \Pr\left(\mathtt{\Theta}^{\mathrm{int}}_{\mathrm{re}} = (X,Y) \,\middle|\, \mathtt{\Theta}^{\mathrm{key}}_{\mathrm{re}}, \mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{re}}\right) \\ &= \frac{1}{2^{nr}} \times \frac{1}{((2^n)_p)^r} \times \Pr\left(\mathtt{\Theta}^{\mathrm{int}}_{\mathrm{re}} = (X,Y) \,\middle|\, \mathtt{\Theta}^{\mathrm{key}}_{\mathrm{re}}, \mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{re}}\right),\end{aligned}$$

where the first term on the right hand side follows from the uniformity of K, the second term follows from the uniformity of $\mathsf{\Pi} = (\mathsf{\Pi}_1, \ldots, \mathsf{\Pi}_r)$.

As for the last term, consider the classes $\mathcal{Q}^{(j)}_{(0)}$ and $\mathcal{Q}_{(1)}, \ldots, \mathcal{Q}_{(c)}$ (in the order fixed above), and also the associated notations introduced earlier. Then, conditioned on $(\mathtt{\Theta}^{\mathrm{key}}_{\mathrm{re}}, \mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{re}})$, we have

$$\Pr\left(\mathtt{\Theta}^{\mathrm{int}}_{\mathrm{re}} = (X,Y) \,\middle|\, \mathtt{\Theta}^{\mathrm{key}}_{\mathrm{re}}, \mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{re}}\right) = \prod_{j=1}^{r} \frac{1}{(2^n - p)_{q^{(j)}_0}} \times \prod_{\substack{i \in [c] \\ j' \in \mathcal{J}_{(i)}}} \frac{1}{(2^n - r^{(j')}_{\leq (i-1)})_{q_i}}.$$

Indeed, the first product term corresponds to the query indices with exactly one fresh primitive input, i.e. the ones in $\mathcal{Q}^{(j)}_{(0)}$ for some $j \in [r]$, and the second product correspond to the query indices with at least two fresh primitive inputs, computed using a simple application of chain rule over the partitions $\mathcal{Q}_{(1)}, \ldots, \mathcal{Q}_{(c)}$. By combining everything, we have

$$\Pr(\mathtt{\Theta}_{\mathrm{re}} = \omega) = \frac{1}{2^{nr}} \times \frac{1}{((2^n)_p)^r} \times \prod_{j=1}^{r} \frac{1}{(2^n - p)_{q^{(j)}_0}} \times \prod_{\substack{i \in [c] \\ j' \in \mathcal{J}_{(i)}}} \frac{1}{(2^n - r^{(j')}_{\leq (i-1)})_{q_i}}, \quad (36)$$

Ideal World: In the ideal world, we have

$$\begin{aligned}\Pr(\mathtt{\Theta}_{\mathrm{id}} = \omega) &= \Pr\left(\mathtt{\Theta}^{\mathrm{key}}_{\mathrm{id}} = K, \mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{id}} = (U,V), \mathtt{\Theta}^{\mathrm{int}}_{\mathrm{id}} = (X,Y), \mathtt{\Theta}^{\mathrm{con}}_{\mathrm{id}} = (M,T)\right) \\ &= \Pr\left(\mathtt{\Theta}^{\mathrm{key}}_{\mathrm{id}} = K\right) \times \Pr\left(\mathtt{\Theta}^{\mathrm{con}}_{\mathrm{id}} = (M,T)\right) \times \Pr\left(\mathtt{\Theta}^{\mathrm{prim}}_{\mathrm{id}} = (U,V)\right)\end{aligned}$$

$$\times \Pr\left(\Theta_{\mathrm{id}}^{\mathrm{int}} = (X,Y) \,\middle|\, \Theta_{\mathrm{id}}^{\mathrm{key}}, \Theta_{\mathrm{id}}^{\mathrm{prim}}, \Theta_{\mathrm{id}}^{\mathrm{con}}\right)$$
$$= \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{((2^n)_p)^r} \times \Pr\left(\Theta_{\mathrm{id}}^{\mathrm{int}} = (X,Y) \,\middle|\, \Theta_{\mathrm{id}}^{\mathrm{key}}, \Theta_{\mathrm{id}}^{\mathrm{prim}}, \Theta_{\mathrm{id}}^{\mathrm{con}}\right)$$
$$= \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{((2^n)_p)^r} \times \prod_{i\in[c]} \Pr\left(\mathsf{Y}^{(i)} = Y^{(i)} \,\middle|\, \widehat{\mathcal{R}}_{\le(i-1)}\right)$$
$$= \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{((2^n)_p)^r} \times \prod_{i\in[c]} \frac{1}{\eta(\mathbb{S}^{(i)} \mid \widehat{\mathcal{R}}_{\le(i-1)})}$$

where the first three terms are obvious. The fourth term corresponds to the indices in $\mathcal{Q}_{(i)}$ for all $i \in [c]$. Further, since $\mathbb{S}^{(i)}$ is isolated, we can apply Lemma 4 (which also holds for $t_i = 2$) to each of its q_i equations, with $\Delta_{\mathbb{S}}$ replaced by the number of earlier equations in $\mathcal{Q}_{(i)}$ with the same constant (see the remark after Lemma 4). These numbers sum to P_i, and we get

$$\Pr(\Theta_{\mathrm{id}} = \omega) \le \frac{1}{2^{nr}} \times \frac{1}{2^{nq}} \times \frac{1}{((2^n)_p)^r} \times \prod_{i\in[c]} \frac{2^{nq_i}}{(1-\varepsilon^{(i)}) \prod_{j'\in\mathcal{J}_{(i)}} (2^n - r_{\le(i-1)}^{(j')})_{q_i}}$$
$$= \frac{1}{2^{nr}} \times \frac{1}{2^{nq_0}} \times \frac{1}{((2^n)_p)^r} \times \prod_{i\in[c]} \frac{1}{(1-\varepsilon^{(i)}) \prod_{j'\in\mathcal{J}_{(i)}} (2^n - r_{\le(i-1)}^{(j')})_{q_i}}, \tag{37}$$

where the equality follows from the fact that $q = q_0 + \sum_{i\in[c]} q_i$.

The Ratio: On dividing (36) by (37), we have

$$\frac{\Pr(\Theta_{\mathrm{re}} = \omega)}{\Pr(\Theta_{\mathrm{id}} = \omega)} \ge \frac{2^{nq_0}}{\prod_{j=1}^{r} (2^n - p)_{q_0^{(j)}}} \prod_{i\in[c]} \left(1 - \varepsilon^{(i)}\right) \ge \prod_{i\in[c]} \left(1 - \varepsilon^{(i)}\right)$$
$$\ge 1 - \sum_{i\in[c]} \varepsilon^{(i)}$$
$$\ge 1 - \underbrace{\sum_{i\in[c]} \left(\frac{2\mu(\widehat{\mathsf{T}}^{(i)}, \widehat{\mathcal{R}}_{\le(i-1)})}{2^{n(t_i-1)}} + \frac{2P_i}{2^{n(t_i-1)}} + \frac{6q_i(p+q)^{t_i}}{2^{nt_i}} \right)}_{\varepsilon_{\mathrm{ratio}}(\omega)}. \quad \square$$