# Security of Single-permutation-based Compression Functions

Jooyoung Lee and Daesung Kwon

The Attached Institute of Electronics and Telecommunications Research Institute
Yuseong-gu, Daejeon, Korea 305-390
{jlee05,ds_kwon}@ensec.re.kr

**Abstract.** In this paper, we study security for a certain class of permutation-based compression functions. Denoted lp231 in [12], they are $2n$-bit to $n$-bit compression functions using three calls to a single $n$-bit random permutation. We prove that lp231 is asymptotically preimage resistant up to $(2^{\frac{2n}{3}}/n)$ queries, adaptive preimage resistant up to $(2^{\frac{n}{2}}/n)$ queries/commitments, and collision resistant up to $(2^{\frac{n}{2}}/n^{1+\epsilon})$ queries for $\epsilon > 0$.

## 1 Introduction

A cryptographic hash function takes a message of arbitrary length, and returns a bit string of fixed length. The most common way of hashing variable length messages is to iterate a fixed-size compression function according to the Merkle-Damgård paradigm. The underlying compression function can either be constructed from scratch, or be built upon off-the-shelf cryptographic primitives. For example, the Whirlpool hash function, adopted as ISO/IEC 10118-3 standard, is based on the Miyaguchi-Preneel construction using a modified version of AES [1]. Compression functions based on blockciphers have been widely studied [4, 6, 7, 9, 10, 16, 17]. Recently, researchers has begun to pay attention to building compression functions from fixed key blockciphers, where just a small number of constants are used as keys [2, 3, 11, 12, 14, 15]. Since each key of a blockcipher defines an independent random permutation in the ideal cipher model, such compression functions are often called *permutation-based*. Permutation-based compression functions have an obvious advantage over conventional blockcipher-based ones, since fixing the keys allows to save computational overload for key scheduling.

In earlier work, Black, Cochran and Shrimpton showed that any "highly-efficient" compression function using exactly one permutation call for each message block allows a query-efficient collision-finding attack [3]. Rogaway and Shrimpton extended this result to a wide class of compression functions that map $mn$ bits to $rn$ bits using $k$ calls to $n$-bit permutations [13]. Such compression functions, denoted $m \xrightarrow{k} r$, allow collision-finding attacks with about $2^{n(1-(m-0.5r)/k)}$ queries, and preimage finding attacks with about $2^{n(1-(m-r)/k)}$ queries.

In [12], the authors focused on the security of a special class of permutation-based compression functions, where the input to each permutation is given by a linear combination of the inputs to the compression function and the outputs of the previously called permutations. Such compression functions are called *linearly-dependent permutation-based*, and denoted by LP$mkr$ if the compression function is based on independent random permutations, and by lp$mkr$ if the compression function is based on a single random permutation. Taking into account the attacks presented in [13], they investigated the security of LP231, LP241, LP352, LP362 and their "lp variants". From a practical point of view, it is obvious that lp compression functions are more efficient compared to LP ones since an lp compression function uses its basing blockcipher with only one fixed key. However, [12] gives a concrete analysis only for

LP231. The analysis of the other compression functions rest on computer-aided approximation. Especially, the authors say that analyzing lp231 by hand would require about 30 times as much paper as LP231.

In this paper, we give a concrete analysis for the security of lp231 in terms of preimage resistance, adaptive preimage resistance and collision resistance. Specifically, we prove preimage resistance up to $(2^{\frac{2n}{3}}/n)$ queries, adaptive preimage resistance up to $(2^{\frac{n}{2}}/n)$ queries/commitments, and collision resistance up to $(2^{\frac{n}{2}}/n^{1+\epsilon})$ queries for $\epsilon > 0$. Our analysis is not only simpler than the authors of [12] estimated, but also elegant based on a recursive approach.

The notion of adaptive preimage resistance is first introduced in [8]. A compression function that is collision resistant and adaptive preimage resistant can be composed with a public random function to yield a hash function that is indifferentiable from a random oracle. In addition, the Merkle-Damgård transform preserves adaptive preimage resistance as long as the underlying compression function is collision resistant. For this reason, we believe that adaptive preimage resistance would be one of the desirable properties of a secure compression function. We note that a similar security notion, called *preimage awareness*, was independently introduced in [5]. Since any compression function that is both collision resistant and adaptive preimage resistant is preimage aware, our result can be regarded as the proof of preimage awareness for lp231.

## 2 Preliminaries

**General Notations** For a positive integer $n$, let $I_n = \{0,1\}^n$ and $[1,n] = \{1,2,\ldots,n\}$. We write $\mathit{\Pi}_n$ for the set of permutations on $I_n$. We let $\mathbb{F}_{2^n}$ denote a finite field of order $2^n$. Throughout our work, we will identify $\mathbb{F}_{2^n}$ and $I_n$, assuming a fixed mapping between the two sets.

For positive integers $s$ and $t$, we let $\mathcal{M}_{\mathbb{F}_{2^n}}^{s\times t}$ denote the set of all $s \times t$ matrices over $\mathbb{F}_{2^n}$. Given $s \times t$ matrices $A$ and $B$, $[A,B]$ denotes the $s \times 2t$ matrix obtained by the concatenation of $A$ and $B$. The concatenation is similarly denoted for more than two matrices. For a nonzero matrix $A \in \mathcal{M}_{\mathbb{F}_{2^n}}^{2\times 1}$, $A^*$ denotes a nonzero matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}^{1\times 2}$ such that $A^*A = 0$. Such a matrix is unique up to scalar multiplication. Note that $[A,B]$ is invertible if and only if $A^*B \neq 0$ for $A$, $B \in \mathcal{M}_{\mathbb{F}_{2^n}}^{2\times 1}$.

For a set $U$, $\overline{U}$ denotes the complement of $U$. We write $u \xleftarrow{\$} U$ to denote uniform random sampling from the set $U$ and assignment to $u$. For a miltiset $U$, $\mathsf{mult}(U,u)$ is the multiplicity of $u$ in $U$, and $\mathsf{mult}(U) = \max_{u\in U} \mathsf{mult}(U,u)$.

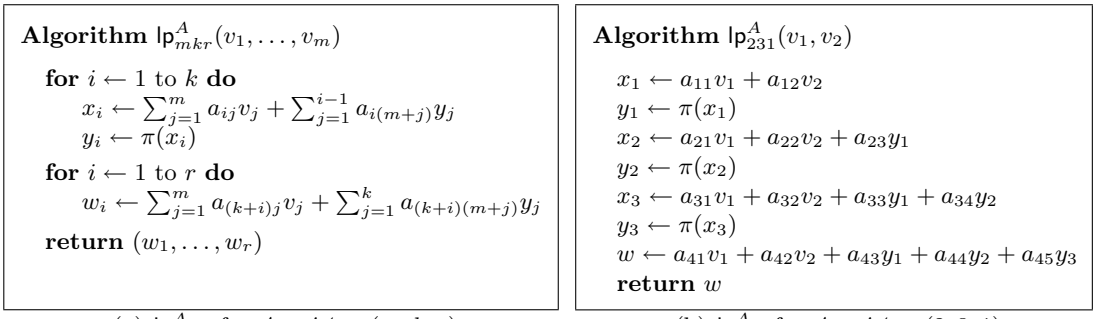
**Linearly-dependent Permutation-based Compression Functions** For positive integers $m$, $k$ and $r$ with $m > r$, let $\mathcal{M}_{\mathbb{F}_{2^n}}(m,k,r)$ be a set of $(k+r)\times(m+k)$ matrices $A = (a_{ij})$ over $\mathbb{F}_{2^n}$ such that

$$a_{ij} = 0 \text{ for } 1 \le i \le k \text{ and } j \ge m+i.$$

Then each matrix $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(m,k,r)$ defines a compression function $\mathsf{lp}_{mkr}^A$ with oracle access to a random permutation $\pi \in \mathit{\Pi}_n$ as follows.

$$\begin{array}{c} \mathsf{lp}_{mkr}^A : I_n^m \longrightarrow I_n^r \\ (v_1,\ldots,v_m) \longmapsto (w_1,\ldots,w_r), \end{array} \tag{1}$$

where $(w_1, \ldots, w_r)$ is computed by the algorithm described in Figure 1(a). A function $\mathsf{lp}^A_{mkr}$ is called *linearly-dependent single-permutation-based*, and often simply denoted as $\mathsf{lp}mkr$ or $\mathsf{lp}^A$. A compression function $\mathsf{lp}^A_{231}$ for $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$ is separately described in Figure 1(b).




(a) $\mathsf{lp}^A_{mkr}$ for $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(m,k,r)$ (b) $\mathsf{lp}^A_{231}$ for $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$

**Fig. 1.** Compression function $\mathsf{lp}^A_{mkr}$

**Collision Resistance and Preimage Resistance** For simplicity of notations, we will define security notions including collision resistance, preimage resistance and adaptive preimage resistance for linearly-dependent single-permutation-based compression functions. However, we note that these security notions can be extended in an obvious way to any hash function based on public ideal primitives.

Let $\mathsf{lp}^A_{mkr}$ be a compression function for $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(m,k,r)$. Given an information-theoretic adversary $\mathcal{A}$ with oracle access to $\pi$ and $\pi^{-1}$, we execute the experiment $\mathbf{Exp}^{\mathsf{coll}}_{\mathcal{A}}$ described in Figure 2(a) in order to quantify the collision resistance of $\mathsf{lp}^A_{mkr}$. The experiment records the query-response pairs that the adversary $\mathcal{A}$ obtains into a *query history* $\mathcal{Q}$. A pair $(x,y)$ is in the query history if $\mathcal{A}$ makes $\pi(x)$ and gets back $y$, or it makes $\pi^{-1}(y)$ and gets back $x$. Given a query history $\mathcal{Q}$, then $\mathsf{Map}_{\mathsf{lp}^A}(\mathcal{Q}) \subset I_n^m \times I_n^r$ is defined to be the set of pairs $(v,w)$ such that there exist evaluations $(x_i, y_i) \in \mathcal{Q}$ satisfying the following equations.

$$\begin{aligned} x_i &= \sum_{j=1}^{m} a_{ij} v_j + \sum_{j=1}^{i-1} a_{i(m+j)} y_j, && i = 1, \ldots, k, \\ w_i &= \sum_{j=1}^{m} a_{(k+i)j} v_j + \sum_{j=1}^{k} a_{(k+i)(m+j)} y_j, && i = 1, \ldots, r, \end{aligned} \tag{2}$$

where we write $v = (v_1, \ldots, v_m)$ and $w = (w_1, \ldots, w_r)$. Informally, $\mathsf{Map}_{\mathsf{lp}^A}(\mathcal{Q})$ is the set of the evaluations of $\mathsf{lp}^A_{mkr}$ that are determined by the query history $\mathcal{Q}$. Now the *collision-finding advantage* of $\mathcal{A}$ is defined to be

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{lp}^A}(\mathcal{A}) = \mathbf{Pr}\left[\mathbf{Exp}^{\mathsf{coll}}_{\mathcal{A}} = 1\right]. \tag{3}$$

The probability is taken over the random permutation $\pi$, and $\mathcal{A}$'s coins (if any). For $q > 0$, we define $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{lp}^A}(q)$ as the maximum of $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{lp}^A}(\mathcal{A})$ over all adversaries $\mathcal{A}$ making at most $q$ queries.

The preimage resistance of $\mathsf{lp}^A_{mkr}$ is quantified similarly using the experiment $\mathbf{Exp}^{\mathsf{pre}}_{\mathcal{A}}$ described in Figure 2(b). The adversary $\mathcal{A}$ takes as input a random $w \in I^r_n$ before it begins making queries to $\pi^{\pm 1}$. The *preimage-finding advantage* of $\mathcal{A}$ is defined to be

$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}(\mathcal{A}) = \mathbf{Pr}\left[\mathbf{Exp}^{\mathsf{pre}}_{\mathcal{A}} = 1\right]. \tag{4}$$

For $q > 0$, $\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}(q)$ is the maximum of $\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}(\mathcal{A})$ over all adversaries $\mathcal{A}$ making at most $q$ queries.

**Experiment** $\mathbf{Exp}^{\mathsf{coll}}_{\mathcal{A}}$
$\pi \xleftarrow{\$} \Pi_n$
$\mathcal{A}^{\pi^{\pm 1}}$ updates $\mathcal{Q}$
**if** $\exists\, v \neq v'$, $w$ s.t. $(v, w)$, $(v', w) \in \mathsf{Map}_{\mathsf{lp}^A}(\mathcal{Q})$ **then**
output 1
**else**
output 0

(a) Quantification of collision resistance

**Experiment** $\mathbf{Exp}^{\mathsf{pre}}_{\mathcal{A}}$
$\pi \xleftarrow{\$} \Pi_n$
$w \xleftarrow{\$} I^r_n$
$\mathcal{A}^{\pi^{\pm 1}}(w)$ updates $\mathcal{Q}$
**if** $\exists\, v$ s.t. $(v, w) \in \mathsf{Map}_{\mathsf{lp}^A}(\mathcal{Q})$ **then**
output 1
**else**
output 0

(b) Quantification of preimage resistance

**Fig. 2.** Experiments for quantification of collision resistance and preimage resistance

**Adaptive Preimage Resistance** In this section, we define a notion of *adaptive preimage resistance*. Given a compression function $\mathsf{lp}^A_{mkr}$ for $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(m, k, r)$ and an information-theoretic adversary $\mathcal{A}$ with oracle access to $\pi^{\pm 1}$, the adaptive preimage resistance of $\mathsf{lp}^A_{mkr}$ is quantified by the experiment $\mathbf{Exp}^{\mathsf{a-pre}}_{\mathcal{A}}$ described in Figure 3. At any point during the experiment, the adversary $\mathcal{A}$ can choose a "commitment" point $w \in I^r_n \backslash \mathsf{Range}_{\mathsf{lp}^A}(\mathcal{Q})$, where

$$\mathsf{Range}_{\mathsf{lp}^A}(\mathcal{Q}) = \left\{ w \in I^r_n : (v, w) \in \mathsf{Map}_{\mathsf{lp}^A}(\mathcal{Q}) \text{ for some } v \in I^m_n \right\}.$$

Then the experiment $\mathbf{Exp}^{\mathsf{a-pre}}_{\mathcal{A}}$ records the element $w$ into a *commitment list* $\mathcal{L} \subset I^r_n$. At the end of the experiment, $\mathcal{A}$ would like to succeed in finding a preimage of some element in the commitment list. Now the *adaptive preimage-finding advantage* of $\mathcal{A}$ is defined to be

$$\mathbf{Adv}^{\mathsf{a-pre}}_{\mathsf{lp}^A}(\mathcal{A}) = \mathbf{Pr}\left[\mathbf{Exp}^{\mathsf{a-pre}}_{\mathcal{A}} = 1\right]. \tag{5}$$

For $q_1, q_2 > 0$, we define $\mathbf{Adv}^{\mathsf{a-pre}}_{\mathsf{lp}^A}(q_1, q_2)$ as the maximum of $\mathbf{Adv}^{\mathsf{a-pre}}_{\mathsf{lp}^A}(\mathcal{A})$ over all adversaries $\mathcal{A}$ that makes at most $q_1$ queries to $\pi$ and $\pi^{-1}$ and makes at most $q_2$ commitments.

## 3 Auxiliary Events

In order to analyze the security of lp231, we need to define some auxiliary events. Suppose that an adversary $\mathcal{A}$ makes $q$ adaptive queries to a random permutation $\pi$ and its inverse

**Experiment** $\mathbf{Exp}^{\mathsf{a-pre}}_{\mathcal{A}}$

$\pi \xleftarrow{\$} \Pi_n$

$\mathcal{A}^{\pi^{\pm 1}}$ updates $\mathcal{Q}$ and $\mathcal{L}$ (in an arbitrarily interleaved order)

**if** $\exists\ v$ such that $(v, w) \in \mathsf{Map}_{\mathsf{lp}^{\mathcal{A}}}(\mathcal{Q})$ for some $w \in \mathcal{L}$ **then**

  output 1

**else**

  output 0

**Fig. 3.** Experiment for quantification of adaptive preimage resistance

$\pi^{-1}$, and records a query history $\mathcal{Q} = \{(x^j, y^j) \in I_n^2 : 1 \le j \le q\}$, where $(x^j, y^j)$ denotes the query-response pair obtained by the $j$-th query. Then we define the following multisets.

$$U^t\left(a_1, b_1, \ldots, a_t, b_t\right) = \left\{ \sum_{i=1}^{t} \left(a_i x^{j_i} + b_i y^{j_i}\right) : (j_1, \ldots, j_t) \in [1, q]^t \right\}, \tag{6}$$

$$U^t_{\neq}\left(a_1, b_1, \ldots, a_t, b_t\right) = U^t\left(a_1, b_1, \ldots, a_t, b_t\right) \setminus U^1\left(\sum_{i=1}^{t} a_i, \sum_{i=1}^{t} b_i\right), \tag{7}$$

$$V^t\left(A_1, B_1, \ldots, A_t, B_t\right) = \left\{ \sum_{i=1}^{t} \left(A_i x^{j_i} + B_i y^{j_i}\right) : (j_1, \ldots, j_t) \in [1, q]^t \right\}, \tag{8}$$

where $t > 0$ and, $a_i$, $b_i \in \mathbb{F}_{2^n}$ and $A_i$, $B_i \in \mathcal{M}^{2\times 1}_{\mathbb{F}_{2^n}}$ for $i \in [1, t]$. For a positive integer $l$, these multisets are associated with the following events.

$$\mathcal{E}^t(a_1, b_1, \ldots, a_t, b_t; l) \Leftrightarrow \mathcal{A} \text{ sets } \mathsf{mult}(U^t(a_1, b_1, \ldots, a_t, b_t)) > l, \tag{9}$$

$$\mathcal{E}^t_{\neq}(a_1, b_1, \ldots, a_t, b_t; l) \Leftrightarrow \mathcal{A} \text{ sets } \mathsf{mult}(U^t_{\neq}(a_1, b_1, \ldots, a_t, b_t)) > l, \tag{10}$$

$$\mathcal{F}^t(A_1, B_1, \ldots, A_t, B_t; l) \Leftrightarrow \mathcal{A} \text{ sets } \mathsf{mult}(V^t(A_1, B_1, \ldots, A_t, B_t)) > l. \tag{11}$$

We often write $\mathcal{E}^t(l) = \mathcal{E}^t(a_1, b_1, \ldots, a_t, b_t; l)$, $\mathcal{E}^t_{\neq}(l) = \mathcal{E}^t_{\neq}(a_1, b_1, \ldots, a_t, b_t; l)$ and $\mathcal{F}^t(l) = \mathcal{F}^t(A_1, B_1, \ldots, A_t, B_t; l)$. The rest of this section is devoted to the estimation of the probability of auxiliary events needed for the analysis of $\mathsf{lp231}$. First, we prove recursive formulas for the probability of the auxiliary events $\mathcal{E}^t$, $\mathcal{E}^t_{\neq}$ and $\mathcal{F}^t$.

**Theorem 1.** *Suppose that an adversary $\mathcal{A}$ makes $q$ ($\le 2^{n-1}$) adaptive queries to a random permutation $\pi$ and its inverse $\pi^{-1}$, and records a query history $\mathcal{Q}$. For $t > 1$, let $(l_0, l_1, \ldots, l_{t-1}, l_t)$ be a sequence of positive integers with $l_0 = 1$, and let $\Delta = \sum_{s=0}^{t-1} \binom{t}{s} l_s$. Let $a_i$ and $b_i$, $i \in [1, t]$, be elements in $\mathbb{F}_{2^n}$ that satisfy the following conditions for every nonempty subset $I = \{i_1, \ldots, i_s\} \subsetneq [1, t]$.*

**A1**. $\sum_{i \notin I} a_i \neq 0$ *and* $\sum_{i \notin I} b_i \neq 0$.

**A2**. $\mathbf{Pr}\left[\mathcal{E}^s\left(a_{i_1}, b_{i_1}, \ldots, a_{i_s}, b_{i_s}; l_s\right)\right] \le \mathsf{p}_s\left(l_s\right)$.

*Then,*

$$\mathbf{Pr}\left[\mathcal{E}^t_{\neq}\left(a_1, b_1, \ldots, a_t, b_t; l_t\right)\right] \le 2^n \binom{q}{\left\lceil \frac{l_t+1}{\Delta-1} \right\rceil} \left(\frac{2^t q^{t-1}}{2^{n-1}}\right)^{\left\lceil \frac{l_t+1}{\Delta-1} \right\rceil} + \sum_{s=1}^{t-1} \binom{t}{s} \mathsf{p}_s(l_s). \tag{12}$$

*If* $\sum_{i=1}^{t} a_i \neq 0$ *and* $\sum_{i=1}^{t} b_i \neq 0$*, then*

$$\mathbf{Pr}\left[\mathcal{E}^t\left(a_1, b_1, \ldots, a_t, b_t; l_t\right)\right] \leq 2^n \binom{q}{\left\lceil \frac{l_t+1}{\Delta} \right\rceil} \left(\frac{2^t q^{t-1}}{2^{n-1}}\right)^{\left\lceil \frac{l_t+1}{\Delta} \right\rceil} + \sum_{s=1}^{t-1} \binom{t}{s} \mathsf{p}_s(l_s). \tag{13}$$

*Proof.* Here we give a proof for inequality (13). Inequality (12) can be proved similarly. For $c \in \mathbb{F}_{2^n}$ and $j \in [1, q]$, we define events

$$\mathcal{E}^t(c, j) \Leftrightarrow \mathcal{A} \text{ sets } \sum_{i=1}^{t} \left(a_i x^{j_i} + b_i y^{j_i}\right) = c, \text{ where } j \in \{j_1, \ldots, j_t\} \subset [1, j], \tag{14}$$

$$\mathcal{E}^t(c; l_t) \Leftrightarrow \mathcal{A} \text{ sets } \mathsf{mult}(U^t, c) > l_t, \tag{15}$$

where we simply write $U^t = U^t(a_1, b_1, \ldots, a_t, b_t)$. Note that $\mathcal{E}^t(c, j)$ occurs when the $j$-th query increases the multiplicity of $c$ in $U^t$ at least by one. In order to estimate $\mathbf{Pr}\left[\mathcal{E}^t(l_t)\right]$, we decompose $\mathcal{E}^t(l_t)$ as follows.

$$\mathcal{E}^t(l_t) = \bigcup_{c \in \mathbb{F}_{2^n}} \mathcal{E}^t(c; l_t) \subset \bigcup_{c \in \mathbb{F}_{2^n}} \left(\mathcal{E}^t(c; l_t) \cap \overline{\mathcal{E}_{ex}}\right) \cup \mathcal{E}_{ex}, \tag{16}$$

where

$$\mathcal{E}_{ex} = \bigcup_{1 \leq s \leq t-1} \mathcal{E}_{ex}^s \quad \text{and} \quad \mathcal{E}_{ex}^s = \bigcup_{\{i_1, \ldots, i_s\} \subset [1,t]} \mathcal{E}^s(a_{i_1}, b_{i_1}, \ldots, a_{i_s}, b_{i_s}; l_s). \tag{17}$$

From condition **A2**, it follows that

$$\mathbf{Pr}\left[\mathcal{E}_{ex}\right] \leq \sum_{s=1}^{t-1} \binom{t}{s} \mathsf{p}_s(l_s). \tag{18}$$

We now analyze the event $\mathcal{E}^t(\hat{c}; l_t) \cap \overline{\mathcal{E}_{ex}}$ for a fixed $\hat{c} \in \mathbb{F}_{2^n}$. Since each query increases the multiplicity $\mathsf{mult}(U^t, \hat{c})$ at most by

$$\Delta = \sum_{s=0}^{t-1} \binom{t}{s} l_s, \tag{19}$$

without the occurrence of $\mathcal{E}_{ex}$, the number of queries that increase $\mathsf{mult}(U^t, \hat{c})$ should be at least

$$d = \left\lceil \frac{l_t + 1}{\Delta} \right\rceil. \tag{20}$$

Therefore, we obtain

$$\mathcal{E}^t(\hat{c}; l_t) \cap \overline{\mathcal{E}_{ex}} \subset \bigcup_{\substack{J \subset [1,q] \\ |J| = d}} \left( \bigcap_{j \in J} \left(\mathcal{E}^t(\hat{c}, j) \cap \overline{\mathcal{E}_{ex}}\right) \right). \tag{21}$$

In order to compute $\mathbf{Pr}\left[\bigcap_{j \in \hat{J}} \left(\mathcal{E}^t(\hat{c}, j) \cap \overline{\mathcal{E}_{ex}}\right)\right]$ for a fixed $\hat{J} = \{\hat{j}_1, \ldots, \hat{j}_d\} \subset [1, q]$, suppose that $\mathcal{A}$ makes the $\hat{j}$-th query $\pi(\hat{x})$ for $\hat{j} \in \hat{J}$. Then we upper-bound the number of $y = \pi(\hat{x})$ that contributes the equation

$$\sum_{i=1}^{t} \left(a_i x^{j_i} + b_i y^{j_i}\right) = \hat{c}, \tag{22}$$

with $\hat{\jmath} \in \{j_1, \ldots, j_t\} \subset [1, \hat{\jmath}]$. Consider the case where the $\hat{\jmath}$-th query-response pair contributes $t - s$ terms in equation (22) for $s \in [0, t-1]$. Taking into account symmetry, assume that $j_i = \hat{\jmath}$ for $i \in [s+1, t]$. Then the equation (22) is reduced to

$$\sum_{i=1}^{s} \left(a_i x^{j_i} + b_i y^{j_i}\right) + \bar{a}\hat{x} + \bar{b}y = \hat{c}, \tag{23}$$

where $\bar{a} = \sum_{i=s+1}^{t} a_i \neq 0$ and $\bar{b} = \sum_{i=s+1}^{t} b_i \neq 0$ by condition **A1**. The number of $y$ satisfying (23) is at most $q^s$. With an analogous argument for $\pi^{-1}$, we conclude that

$$\mathbf{Pr}\left[\bigcap_{j \in \hat{J}} \left(\mathcal{E}^t(\hat{c}, j) \cap \overline{\mathcal{E}_{ex}}\right)\right] \leq \left(\frac{\Delta'}{2^{n-1}}\right)^d, \tag{24}$$

where

$$\Delta' = \sum_{s=0}^{t-1} \binom{t}{s} q^s < \left(\sum_{s=0}^{t} \binom{t}{s}\right) q^{t-1} = 2^t q^{t-1}. \tag{25}$$

Now the proof is complete from (16), (18), (21), (24) and (25). □

**Theorem 2.** *Suppose that an adversary $\mathcal{A}$ makes $q$ ($\leq 2^{n-1}$) adaptive queries to a random permutation $\pi$ and its inverse $\pi^{-1}$, and records a query history $\mathcal{Q}$. For $t > 1$, let $(l_0, \ldots, l_t)$ and $(l'_0, \ldots, l'_{t-1})$ be sequences of positive integers with $l_0 = l'_0 = 1$. Let $A_i$ and $B_i$, $i \in [1, t]$, be matrices in $\mathcal{M}^{2\times 1}_{\mathbb{F}_{2^n}}$ that satisfy the following conditions for every nonempty subset $I = \{i_1, \ldots, i_s\} \subsetneq [1, t]$.*

**B1**. $\bar{A}_I = \sum_{i \notin I} A_i \neq 0$ *and* $\bar{B}_I = \sum_{i \notin I} B_i \neq 0$.

**B2**. $\mathbf{Pr}\left[\mathcal{F}^s\left(A_{i_1}, B_{i_1}, \ldots, A_{i_s}, B_{i_s}; l_s\right)\right] \leq \mathsf{P}_s\left(l_s\right)$.

**B3**. $\mathbf{Pr}\left[\mathcal{E}^s\left(\bar{A}_I^* A_{i_1}, \bar{A}_I^* B_{i_1}, \ldots, \bar{A}_I^* A_{i_s}, \bar{A}_I^* B_{i_s}; l'_s\right)\right] \leq \mathsf{p}_s\left(l'_s\right)$.

**B4**. $\mathbf{Pr}\left[\mathcal{E}^s\left(\bar{B}_I^* A_{i_1}, \bar{B}_I^* B_{i_1}, \ldots, \bar{B}_I^* A_{i_s}, \bar{B}_I^* B_{i_s}; l'_s\right)\right] \leq \mathsf{p}_s\left(l'_s\right)$.

*If $\sum_{i=1}^{t} A_i \neq 0$ and $\sum_{i=1}^{t} B_i \neq 0$, then*

$$\mathbf{Pr}\left[\mathcal{F}^t\left(A_1, B_1, \ldots, A_t, B_t; l_t\right)\right] \leq 2^{2n} \binom{q}{\left\lceil \frac{l_t+1}{\Delta} \right\rceil} \left(\frac{\Delta'}{2^{n-1}}\right)^{\left\lceil \frac{l_t+1}{\Delta} \right\rceil} + \sum_{s=1}^{t-1} \binom{t}{s} \left(\mathsf{P}_s(l_s) + 2\mathsf{p}_s(l'_s)\right), \tag{26}$$

*where*

$$\Delta = \sum_{s=0}^{t-1} \binom{t}{s} l_s \qquad \text{and} \qquad \Delta' = \sum_{s=0}^{t-1} \binom{t}{s} l'_s. \tag{27}$$

*Proof.* The proof is essentially the same as Theorem 1. For $C \in \mathcal{M}^{2\times 1}_{\mathbb{F}_{2^n}}$ and $j \in [1, q]$, we define events

$$\mathcal{F}^t(C, j) \Leftrightarrow \mathcal{A} \text{ sets } \sum_{i=1}^{t} \left(A_i x^{j_i} + B_i y^{j_i}\right) = C, \text{ where } j \in \{j_1, \ldots, j_t\} \subset [1, j], \tag{28}$$

$$\mathcal{F}^t(C; l_t) \Leftrightarrow \mathcal{A} \text{ sets } \mathsf{mult}(V^t, C) > l_t, \tag{29}$$

where we simply write $V^t = V^t(A_1, B_1, \ldots, A_t, B_t)$. The event $\mathcal{F}^t(C, j)$ occurs when the $j$-th query increases the multiplicity of $C$ in $V^t$ at least by one. In order to estimate $\mathbf{Pr}\left[\mathcal{F}^t(l_t)\right]$, we decompose $\mathcal{F}^t(l_t)$ as follows.

$$\mathcal{F}^t(l_t) = \bigcup_{C \in \mathcal{M}_{\mathbb{F}_{2^n}}^{2\times 1}} \mathcal{F}^t(C; l_t) \subset \bigcup_{C \in \mathcal{M}_{\mathbb{F}_{2^n}}^{2\times 1}} \left(\mathcal{F}^t(C; l_t) \cap \overline{\mathcal{F}_{ex}}\right) \cup \mathcal{F}_{ex}, \tag{30}$$

where

$$\mathcal{F}_{ex} = \left(\bigcup_{1 \le s \le t-1} \mathcal{F}_{ex}^s\right) \cup \left(\bigcup_{1 \le s \le t-1} \mathcal{E}_{ex}^s\right), \tag{31}$$

$$\mathcal{F}_{ex}^s = \bigcup_{\{i_1,\ldots,i_s\} \subset [1,t]} \mathcal{F}^s(A_{i_1}, B_{i_1}, \ldots, A_{i_s}, B_{i_s}; l_s), \tag{32}$$

$$\begin{aligned}\mathcal{E}_{ex}^s = &\bigcup_{I=\{i_1,\ldots,i_s\} \subset [1,t]} \mathcal{E}^s\left(\bar{A}_I^* A_{i_1}, \bar{A}_I^* B_{i_1}, \ldots, \bar{A}_I^* A_{i_s}, \bar{A}_I^* B_{i_s}; l_s'\right) \\ \cup &\bigcup_{I=\{i_1,\ldots,i_s\} \subset [1,t]} \mathcal{E}^s\left(\bar{B}_I^* A_{i_1}, \bar{B}_I^* B_{i_1}, \ldots, \bar{B}_I^* A_{i_s}, \bar{B}_I^* B_{i_s}; l_s'\right).\end{aligned} \tag{33}$$

From conditions **B2**, **B3** and **B4**, it follows that

$$\mathbf{Pr}\left[\mathcal{F}_{ex}\right] \le \sum_{s=1}^{t-1} \binom{t}{s} \left(\mathsf{P}_s(l_s) + 2\mathsf{p}_s(l_s)\right). \tag{34}$$

We now analyze the event $\mathcal{F}^t(\hat{C}; l_t) \cap \overline{\mathcal{F}_{ex}}$ for a fixed $\hat{C} \in \mathcal{M}_{\mathbb{F}_{2^n}}^{2\times 1}$. Since each query increases the multiplicity $\mathsf{mult}(V^t, \hat{C})$ at most by

$$\Delta = \sum_{s=0}^{t-1} \binom{t}{s} l_s, \tag{35}$$

without the occurrence of $\bigcup_{s=1}^{t-1} \mathcal{F}_{ex}^s$, the number of queries that increase $\mathsf{mult}(V^t, \hat{C})$ should be at least

$$d = \left\lceil \frac{l_t + 1}{\Delta} \right\rceil. \tag{36}$$

Therefore, we obtain

$$\mathcal{F}^t(\hat{C}; l_t) \cap \overline{\mathcal{F}_{ex}} \subset \bigcup_{\substack{J \subset [1,q] \\ |J| = d}} \left(\bigcap_{j \in J} \left(\mathcal{F}^t(\hat{C}, j) \cap \overline{\mathcal{F}_{ex}}\right)\right). \tag{37}$$

In order to compute $\mathbf{Pr}\left[\bigcap_{j \in \hat{J}} \left(\mathcal{F}^t(\hat{C}, j) \cap \overline{\mathcal{F}_{ex}}\right)\right]$ for a fixed $\hat{J} = \{\hat{j}_1, \ldots, \hat{j}_d\} \subset [1, q]$, suppose that $\mathcal{A}$ makes the $\hat{j}$-th query $\pi(\hat{x})$ for $\hat{j} \in \hat{J}$. Then we upper-bound the number of $y = \pi(\hat{x})$ that contributes the equation

$$\sum_{i=1}^{t} \left(A_i x^{j_i} + B_i y^{j_i}\right) = \hat{C}, \tag{38}$$

with $\hat{\jmath} \in \{j_1, \ldots, j_t\} \subset [1, \hat{\jmath}]$. Consider the case where the $\hat{\jmath}$-th query-response pair contributes $t - s$ terms in equation (38) for $s \in [0, t-1]$. Taking into account symmetry, we can assume that $j_i = \hat{\jmath}$ for $i \in [s+1, t]$. Then the equation (38) is reduced to

$$\sum_{i=1}^{s} \left(A_i x^{j_i} + B_i y^{j_i}\right) + \bar{A}\hat{x} + \bar{B}y = \hat{C}, \tag{39}$$

where $\bar{A} = \sum_{i=s+1}^{t} A_i \neq 0$ and $\bar{B} = \sum_{i=s+1}^{t} B_i \neq 0$ by condition **B1**. By multiplying $\bar{B}^*$ on both sides of (39), we observe that each $y$ satisfying (39) is associated with a solution $(j_1, \ldots, j_s) \in [1, \hat{\jmath} - 1]^s$ to the following equation.

$$\sum_{i=1}^{s} \left(\bar{B}^* A_i x^{j_i} + \bar{B}^* B_i y^{j_i}\right) = \bar{B}^* \hat{C} + \bar{B}^* \bar{A}\hat{x}. \tag{40}$$

The number of solutions $(j_1, \ldots, j_s)$ to (40) is at most $l'_s$ without the occurrence of $\mathcal{E}^s_{ex}$. With an analogous argument for $\pi^{-1}$, we conclude that

$$\mathbf{Pr}\left[\bigcap_{j \in \hat{J}} \left(\mathcal{F}^t(\hat{C}, j) \cap \overline{\mathcal{F}_{ex}}\right)\right] \leq \left(\frac{\Delta'}{2^{n-1}}\right)^d, \tag{41}$$

where

$$\Delta' = \sum_{s=0}^{t-1} \binom{t}{s} l'_s. \tag{42}$$

Now the proof is complete from (30), (34), (37) and (41). □

**Corollary 1.** *Suppose that an adversary $\mathcal{A}$ makes $q$ ($\leq 2^{n-1}$) adaptive queries to a random permutation $\pi$ and its inverse $\pi^{-1}$, and records a query history $\mathcal{Q}$. Let $a_i$ and $b_i$, $1 \leq i \leq 3$, be nonzero elements in $\mathbb{F}_{2^n}$, and let*

$$f_1 = f_1(l_1) = 2^n \binom{q}{l_1 + 1} \left(\frac{2}{2^n}\right)^{l_1+1}, \tag{43}$$

$$f_2 = f_2(l_1, l_2) = 2^n \binom{q}{\left\lceil \frac{l_2+1}{2l_1+1} \right\rceil} \left(\frac{8q}{2^n}\right)^{\left\lceil \frac{l_2+1}{2l_1+1} \right\rceil}, \tag{44}$$

$$f_3 = f_3(l_1, l_2, l_3) = 2^n \binom{q}{\left\lceil \frac{l_3+1}{3l_1+3l_2+1} \right\rceil} \left(\frac{16q^2}{2^n}\right)^{\left\lceil \frac{l_3+1}{3l_1+3l_2+1} \right\rceil}, \tag{45}$$

*for positive integers $l_1$, $l_2$ and $l_3$. Then the following hold.*

1. $\mathbf{Pr}\left[\mathcal{E}^1(a_1, b_1; l_1)\right] \leq f_1(l_1)$.
2. $\mathbf{Pr}\left[\mathcal{E}^2_{\neq}(a_1, b_1, a_2, b_2; l_2)\right] \leq f_2 + 2f_1$.
3. *If $a_1 + a_2 \neq 0$ and $b_1 + b_2 \neq 0$, then*

$$\mathbf{Pr}\left[\mathcal{E}^2(a_1, b_1, a_2, b_2; l_2)\right] \leq f_2 + 2f_1.$$

**4**. *If* $a_1 + a_2 \neq 0$, $a_2 + a_3 \neq 0$, $a_3 + a_1 \neq 0$, $b_1 + b_2 \neq 0$, $b_2 + b_3 \neq 0$ *and* $b_3 + b_1 \neq 0$, *then*

$$\mathbf{Pr}\left[\mathcal{E}^3_{\neq}(a_1, b_1, a_2, b_2, a_3, b_3; l_3)\right] \leq f_3 + 3f_2 + 9f_1.$$

*Proof.* Here we only give a proof for the first inequality. The other inequalities can be proved by recursive application of Theorem 1.

Fix $\hat{c} \in \mathbb{F}_{2^n}$. When $\mathcal{A}$ makes the $j$-th query $\pi(\hat{x})$, the probability that $a\hat{x}+b\pi(\hat{x}) = \hat{c}$, which is equivalent to $\pi(\hat{x}) = b^{-1}(\hat{c} + a\hat{x})$, is not greater than $1/(2^n - (j-1))$. Similarly, when $\mathcal{A}$ makes the $j$-th query $\pi^{-1}(\hat{y})$, the probability that $a\pi^{-1}(\hat{y}) + b\hat{y} = \hat{c}$ is not greater than $1/(2^n - (j-1))$. The event $\mathcal{E}^1(a_1, b_1; l_1)$ occurs when there exists a set $\{j_1, \ldots, j_{l+1}\} \subset [1, q]$ such that

$$a_1 x^{j_1} + b_1 y^{j_1} = \ldots = a_1 x^{j_{l+1}} + b_1 y^{j_{l+1}} = c,$$

for some $c \in \mathbb{F}_{2^n}$. Since $1/(2^n - (j-1)) \leq 1/(2^n - q) \leq 2/2^n$, it follows that

$$\mathbf{Pr}\left[\mathcal{E}^1(a_1, b_1; l_1)\right] \leq 2^n \binom{q}{l_1 + 1} \left(\frac{2}{2^n}\right)^{l_1+1}.$$

□

**Definition 1.** *For* $t > 0$, *a matrix* $M = [A_1, B_1, \ldots, A_t, B_t] \in \mathcal{M}^{2\times 2t}_{\mathbb{F}_{2^n}}$ *is called* column-sum independent *if* $M$ *satisfies the following conditions.*

1. $\left[\sum_{i\in I_1} A_i, \sum_{i\in I_2} A_i\right]$, $\left[\sum_{i\in I_1} A_i, \sum_{i\in I_2} B_i\right]$ *and* $\left[\sum_{i\in I_1} B_i, \sum_{i\in I_1} B_i\right]$ *are invertible for every pair* $(I_1, I_2)$ *of nonempty subsets of* $[1, t]$ *such that* $I_1 \cap I_2 = \emptyset$.
2. $[A_i, B_i]$ *are invertible for* $i = 1, \ldots, t$.

Definition 1 is needed for compact statement of the following corollary. We point out some useful properties of column-sum independent matrices.

- If $[A_1, B_1, \ldots, A_t, B_t]$ is column-sum independent, then $[A_{i_1}, B_{i_1}, \ldots, A_{i_s}, B_{i_s}]$ is also column-sum independent for every subset $\{i_1, \ldots, i_s\} \subset [1, t]$.
- If $[A_1, B_1, \ldots, A_t, B_t]$ is column-sum independent, then $\sum_{i\in I} A_i \neq 0$ and $\sum_{i\in I} B_i \neq 0$ for every nonempty subset $I \subset [1, t]$.
- Column-sum independence of $M$ stipulates nonsigularity of $\left(2 \cdot 3^t - 4 \cdot 2^t + t + 2\right)$ matrices determined by $M$.

**Corollary 2.** *Suppose that an adversary* $\mathcal{A}$ *makes* $q$ $(\leq 2^{n-1})$ *adaptive queries to a random permutation* $\pi$ *and its inverse* $\pi^{-1}$, *and records a query history* $\mathcal{Q}$. *Let* $[A_1, B_1, A_2, B_2, A_3, B_3]$ *be a column-sum independent matrix in* $\mathcal{M}^{2\times 6}_{\mathbb{F}_{2^n}}$, *and let*

$$f_1 = f_1(l'_1),\ f_2 = f_2(l'_1, l'_2),\ f_3 = f_3(l'_1, l'_2, l'_3), \tag{46}$$

$$g_2 = g_2(l'_1, l_2) = 2^{2n} \binom{q}{\left\lceil \frac{l_2+1}{3} \right\rceil} \left(\frac{4l'_1 + 2}{2^n}\right)^{\left\lceil \frac{l_2+1}{3} \right\rceil}, \tag{47}$$

$$g_3 = g_3(l'_1, l'_2, l_2, l_3) = 2^{2n} \binom{q}{\left\lceil \frac{l_3+1}{3l_2+4} \right\rceil} \left(\frac{6l'_1 + 6l'_2 + 2}{2^n}\right)^{\left\lceil \frac{l_3+1}{3l_2+4} \right\rceil}, \tag{48}$$

*for positive integers* $l'_1$, $l'_2$, $l'_3$, $l_2$ *and* $l_3$. *Then the following hold.*

**1**. $\mathbf{Pr}\left[\mathcal{F}^1(A_1, B_1; 1)\right] = 0$.

**2**. $\mathbf{Pr}\left[\mathcal{F}^2(A_1, B_1, A_2, B_2; l_2)\right] \leq g_2 + 4f_1$.

**3**. *If* $[A_1 + A_2, B_1]$, $[A_1 + A_2, B_2]$, $[B_1 + B_2, A_1]$ *and* $[B_1 + B_2, A_2]$ *are invertible, then*

$$\mathbf{Pr}\left[\mathcal{F}^2(A_1, B_1, A_2, B_2; 1)\right] \leq \frac{\left(4q^2 + 2q\right) l_2'}{2^n} + 6f_2 + 12f_1.$$

**4**. $\mathbf{Pr}\left[\mathcal{F}^3(A_1, B_1, A_2, B_2, A_3, B_3; l_3)\right] \leq g_3 + 3g_2 + 6f_2 + 30f_1$.

*Proof.* The proof of the first equality is straightforward. Due to the first equality, we can always set $l_1 = 1$ in recursive application of Theorem 2. Here we only give a proof for the third inequality, since the proof of the other inequalities is straightforward.

First, we define the following events.

$$\mathcal{F}^2_{\mathsf{coll}}(j) \Leftrightarrow \mathcal{A} \text{ sets } A_1x^{j_1} + B_1x^{j_1} + A_2x^{j_2} + B_2x^{j_2} = A_1x^{j_3} + B_1x^{j_3} + A_2x^{j_4} + B_2x^{j_4} \\ \text{where } j_3 < j_1 \leq j,\ j_4 < j_2 \leq j, \text{ and } j \in \{j_1, j_2\}, \quad (49)$$

and

$$\begin{aligned}\mathcal{E}_{ex} = {} & \mathcal{E}^2_{\neq}\left((B_1 + B_2)^*A_1, (B_1 + B_2)^*B_1, (B_1 + B_2)^*A_2, (B_1 + B_2)^*B_2; l_2'\right) \\ & \cup \mathcal{E}^2_{\neq}\left((A_1 + A_2)^*A_1, (A_1 + A_2)^*B_1, (A_1 + A_2)^*A_2, (A_1 + A_2)^*B_2; l_2'\right) \\ & \cup \mathcal{E}^2_{\neq}\left(B_1^*A_2, B_1^*B_2, B_1^*A_2, B_1^*B_2; l_2'\right) \cup \mathcal{E}^2_{\neq}\left(A_1^*A_2, A_1^*B_2, A_1^*A_2, A_1^*B_2; l_2'\right) \\ & \cup \mathcal{E}^2_{\neq}\left(B_2^*A_1, B_2^*B_1, B_2^*A_1, B_2^*B_1; l_2'\right) \cup \mathcal{E}^2_{\neq}\left(A_2^*A_1, A_2^*B_1, A_2^*A_1, A_2^*B_1; l_2'\right). \end{aligned} \quad (50)$$

Then, it follows that

$$\mathcal{F}^2(A_1, B_1, A_2, B_2; 1) \subset \bigcup_{1 \leq j \leq q} \mathcal{F}^2_{\mathsf{coll}}(j) \subset \bigcup_{1 \leq j \leq q} \left(\mathcal{F}^2_{\mathsf{coll}}(j) \cap \overline{\mathcal{E}_{ex}}\right) \cup \mathcal{E}_{ex}, \quad (51)$$

and

$$\mathbf{Pr}\left[\mathcal{E}_{ex}\right] \leq 6\left(f_2 + 2f_1\right), \quad (52)$$

by Corollary 1.

We now estimate the probability $\mathbf{Pr}\left[\mathcal{F}^2_{\mathsf{coll}}(j) \cap \overline{\mathcal{E}_{ex}}\right]$. Suppose that $\mathcal{A}$ makes the $j$-th query $\pi(\hat{x})$, and consider the following three cases where $y = \pi(\hat{x})$ contributes the equation

$$A_1x^{j_1} + B_1x^{j_1} + A_2x^{j_2} + B_2x^{j_2} = A_1x^{j_3} + B_1x^{j_3} + A_2x^{j_4} + B_2x^{j_4}. \quad (53)$$

*Case 1:* $j_1 = j_2 = j$. The equality (53) is reduced to

$$(A_1 + A_2)\hat{x} + (B_1 + B_2)y = A_1x^{j_3} + B_1y^{j_3} + A_2x^{j_4} + B_2y^{j_4}. \quad (54)$$

Any response $y$ satisfying (54) corresponds to a pair $(j_3, j_4) \in [1, j-1]^2$ such that

$$(B_1 + B_2)^*A_1x^{j_3} + (B_1 + B_2)^*B_1y^{j_3} + (B_1 + B_2)^*A_2x^{j_4} + (B_1 + B_2)^*B_2y^{j_4} \\ = (B_1 + B_2)^*(A_1 + A_2)\hat{x}. \quad (55)$$

The number of such pairs is at most $l_2'$ without the occurrence of $\mathcal{E}_{ex}$. Note that if $j_3 = j_4$, then (55) is reduced to $(B_1 + B_2)^*(A_1 + A_2)x^{j_3} = (B_1 + B_2)^*(A_1 + A_2)\hat{x}$, which contradicts to the condition $x^{j_3} \neq \hat{x}$.

*Case 2:* $j_1 = j$ *and* $j_2 \neq j$. The equality (53) is reduced to

$$A_1\hat{x} + B_1 y = A_2 x^{j_2} + B_2 y^{j_2} + A_1 x^{j_3} + B_1 y^{j_3} + A_2 x^{j_4} + B_2 y^{j_4}. \tag{56}$$

Any response $y$ satisfying (56) corresponds to a triple $(j_2, j_3, j_4) \in [1, j-1]^3$ such that

$$B_1^* A_1 x^{j_3} + (B_1^* A_2 x^{j_2} + B_1^* B_2 y^{j_2} + B_1^* A_2 x^{j_4} + B_1^* B_2 y^{j_4}) = B_1^* A_1 \hat{x}. \tag{57}$$

For each $j_3 \in [1, j-1]$, the number of pairs $(j_2, j_4) \in [1, j-1]^2$ satisfying (57) is at most $l_2'$ without the occurrence of $\mathcal{E}_{ex}$. Therefore the number of the triples satisfying (56) is at most $ql_2'$ without the occurrence of $\mathcal{E}_{ex}$.

*Case 3:* $j_2 = j$ *and* $j_1 \neq j$. The analysis of this case is essentially the same as Case 2.

To summarize, we conclude that

$$\mathbf{Pr}\left[\mathcal{F}^2_{\mathsf{coll}}(j) \cap \overline{\mathcal{E}_{ex}}\right] \leq \frac{(2q+1)\, l_2'}{2^{n-1}}. \tag{58}$$

The proof is complete from (51), (52) and (58). □

## 4 Concrete Security Bounds for lp231

For $A \in \mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$, the system of equations (2) is rewritten as follows.

$$\begin{aligned} x_1 &= a_{11}v_1 + a_{12}v_2 \\ x_2 &= a_{21}v_1 + a_{22}v_2 + a_{23}y_1 \\ x_3 &= a_{31}v_1 + a_{32}v_2 + a_{33}y_1 + a_{34}y_2 \\ w &= a_{41}v_1 + a_{42}v_2 + a_{43}y_1 + a_{44}y_2 + a_{45}y_3. \end{aligned} \tag{59}$$

If we regard every variable in the system of equations (59) as constant except $v_1$, $v_2$, $x_3$ and $y_3$, then we obtain the following system of equations in the four variables.

$$\begin{bmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ a_{31} & a_{32} & 1 & 0 \\ a_{41} & a_{42} & 0 & a_{45} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ x_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 + a_{23}y_1 \\ a_{33}y_1 + a_{34}y_2 \\ a_{43}y_1 + a_{44}y_2 + w \end{bmatrix}. \tag{60}$$

If $a_{11}a_{22} + a_{12}a_{21} \neq 0$ and $a_{45} \neq 0$, then we can solve the system of equations (60) to obtain an equation of the following form.

$$A_1 x_1 + B_1 y_1 + A_2 x_2 + B_2 y_2 + A_3 x_3 + B_3 y_3 = Cw, \tag{61}$$

where $A_i$, $B_i$ and $C$ are matrices in $\mathcal{M}^{2\times 1}_{\mathbb{F}_{2^n}}$. We write $M(A) = [A_1, B_1, A_2, B_2, A_3, B_3]$ and $C(A) = C$, since these matrices are determined by the matrix $A$. Note that $B_3 = \lambda C$ for some $\lambda \in \mathbb{F}_{2^n}$. When $(x_i, y_i)$, $i = 1, 2, 3$, and $w$ satisfy the equation (61), we write

$$(x_1, y_1; x_2, y_2; x_3, y_3) \vdash w. \tag{62}$$

Assuming that $M(A)$ is column-sum independent, we will use the following events in the analysis of lp231.

$$\begin{aligned}\mathcal{G}_{ex}(l_1', l_2') = &\bigcup_{1\le i\le 3} \mathcal{E}^1\left((A_{i+1}+A_{i+2})^*A_i, (A_{i+1}+A_{i+2})^*B_i; l_1'\right)\\ &\cup \bigcup_{1\le i\le 3} \mathcal{E}^1\left((B_{i+1}+B_{i+2})^*A_i, (B_{i+1}+B_{i+2})^*B_i; l_1'\right)\\ &\cup \bigcup_{1\le i\le 3} \mathcal{E}^2\left(A_i^*A_{i+1}, A_i^*B_{i+1}, A_i^*A_{i+2}, A_i^*B_{i+2}; l_2'\right)\\ &\cup \bigcup_{1\le i\le 3} \mathcal{E}^2\left(B_i^*A_{i+1}, B_i^*B_{i+1}, B_i^*A_{i+2}, B_i^*B_{i+2}; l_2'\right),\end{aligned} \tag{63}$$

where $l_1'$ and $l_2'$ are positive integers and indices $i$ are interpreted up to modulo 3. Note that

$$\begin{aligned}\mathbf{Pr}\left[\mathcal{G}_{ex}(l_1', l_2')\right] &\le 6f_2(l_1', l_2') + 18f_1(l_1')\\ &= 6\cdot 2^n\binom{q}{d}\left(\frac{8q}{2^n}\right)^d + 18\cdot 2^n\binom{q}{l_1'+1}\left(\frac{2}{2^n}\right)^{l_1'+1}\\ &\le 6\cdot 2^n\left(\frac{24q^2}{d2^n}\right)^d + 18\cdot 2^n\left(\frac{6q}{(l_1'+1)2^n}\right)^{l_1'+1},\end{aligned} \tag{64}$$

for $d = \left\lceil \frac{l_2'+1}{2l_1'+1} \right\rceil$.

### 4.1 Preimage Resistance

**Theorem 3.** *Suppose that an adversary $\mathcal{A}$ makes a total of $q(\le 2^{n-1})$ queries to a random permutation $\pi$ and its inverse $\pi^{-1}$, and records a query history $\mathcal{Q}$. Let $A = (a_{ij})$ be a matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$ such that $a_{11}a_{22}+a_{12}a_{21} \ne 0$ and $a_{45} \ne 0$. If $M(A)$ is column-sum independent, then for positive integers $l_1'$ and $l_2'$,*

$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}(\mathcal{A}) \le \frac{q(3l_1'+3l_2'+1)}{2^{n-1}} + 6f_2(l_1', l_2') + 18f_1(l_1'). \tag{65}$$

*Proof.* For $w \in \mathbb{F}_{2^n}$ and $j \in [1, q]$, we define events

$$\mathcal{P}(w, j) \Leftrightarrow \mathcal{A} \text{ sets } (x^{j_1}, y^{j_1}; x^{j_2}, y^{j_2}; x^{j_3}, y^{j_3}) \vdash w, \text{ where } j \in \{j_1, j_2, j_3\} \subset [1, j]. \tag{66}$$

The events $\mathcal{P}(w, j)$ are identical with $\mathcal{F}^3(Cw, j)$ as defined in (28). Since the occurrence of $\mathcal{P}(w, j)$ means that the $j$-th query determines a preimage of $w$, it follows that

$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}(\mathcal{A}) \le \max_{w\in\mathbb{F}_{2^n}} \mathbf{Pr}\left[\bigcup_{1\le j\le q} \mathcal{P}(w, j)\right]. \tag{67}$$

For a fixed $\hat{w} \in \mathbb{F}_{2^n}$, we have

$$\mathbf{Pr}\left[\bigcup_{1\le j\le q} \mathcal{P}(\hat{w}, j)\right] \le \mathbf{Pr}\left[\bigcup_{1\le j\le q} \left(\mathcal{P}(\hat{w}, j) \cap \overline{\mathcal{G}_{ex}(l_1', l_2')}\right)\right] + \mathbf{Pr}\left[\mathcal{G}_{ex}(l_1', l_2')\right]. \tag{68}$$

Since the number of responses that determine a preimage of $\hat{w}$ is at most $3l'_1 + 3l'_2 + 1$ for each query without the occurrence of $\mathcal{G}_{ex}(l'_1, l'_2)$, we obtain

$$\mathbf{Pr}\left[\bigcup_{1\le j\le q}\left(\mathcal{P}(\hat{w}, j)\cap\overline{\mathcal{G}_{ex}(l'_1, l'_2)}\right)\right] \le \frac{q(3l'_1 + 3l'_2 + 1)}{2^{n-1}}. \tag{69}$$

The proof is complete from (64), (67), (68) and (69). □

**Corollary 3.** *Let $A = (a_{ij})$ be a matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}(2, 3, 1)$ such that $a_{11}a_{22} + a_{12}a_{21} \neq 0$ and $a_{45} \neq 0$. If $M(A)$ is column-sum independent, then*

$$\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}\left(2^{\frac{2n}{3}}/n\right) = 0. \tag{70}$$

*Proof.* Let $q = 2^{\frac{2n}{3}}/n$, $l'_1 = 2$ and $l'_2 = 5 \cdot 2^{\frac{n}{3}} - 1$. Then it follows that

$$\lim_{n\to 0} \frac{q(3l'_1 + 3l'_2 + 1)}{2^{n-1}} = \lim_{n\to 0} f_2(l'_1, l'_2) = \lim_{n\to 0} f_1(l'_1) = 0. \tag{71}$$

The proof is complete from Theorem 3. □

### 4.2 Adaptive Preimage Resistance

**Theorem 4.** *Suppose that an adversary $\mathcal{A}$ makes a total of $q_1 (\le 2^{n-1})$ queries to a random permutation $\pi$ and its inverse $\pi^{-1}$, and makes $q_2$ commitments. Let $A = (a_{ij})$ be a matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}(2, 3, 1)$ such that $a_{11}a_{22} + a_{12}a_{21} \neq 0$ and $a_{45} \neq 0$. If $M(A)$ is column-sum independent, then for positive integers $l'_1$ and $l'_2$,*

$$\mathbf{Adv}^{\mathsf{pre}}_{\mathsf{lp}^A}(\mathcal{A}) \le \frac{q_1 q_2(3l'_1 + 3l'_2 + 1)}{2^{n-1}} + 6f_2(l'_1, l'_2) + 18f_1(l'_1). \tag{72}$$

*Proof.* Let $\mathcal{Q} = \{(x^j, y^j) \in I_n^2 : 1 \le j \le q_1\}$ and $\mathcal{L}$ denote the query history and the commitment list, respectively. Let $\mathcal{L}_j$ denote the set of commitments made before the $j$-th query. For $w \in \mathbb{F}_{2^n}$ and $j \in [1, q_1]$, we define events

$$\mathcal{D}(j) \Leftrightarrow \mathcal{A} \text{ sets } (x^{j_1}, y^{j_1}; x^{j_2}, y^{j_2}; x^{j_3}, y^{j_3}) \vdash w, \quad \text{where } j \in \{j_1, j_2, j_3\} \subset [1, j] \text{ and } w \in \mathcal{L}_j. \tag{73}$$

Since the occurrence of $\mathcal{D}(j)$ means that the $j$-th query determines a preimage of an element in $\mathcal{L}$, it follows that

$$\begin{aligned}\mathbf{Adv}^{\mathsf{a-pre}}_{\mathsf{lp}^A}(\mathcal{A}) &= \mathbf{Pr}\left[\bigcup_{1\le j\le q_1}\mathcal{D}(j)\right] \\ &\le \mathbf{Pr}\left[\bigcup_{1\le j\le q_1}\left(\mathcal{D}(j)\cap\overline{\mathcal{G}_{ex}(l'_1, l'_2)}\right)\right] + \mathbf{Pr}\left[\mathcal{G}_{ex}(l'_1, l'_2)\right].\end{aligned} \tag{74}$$

For a fixed $\hat{j} \in [1, q_1]$, we have

$$\mathbf{Pr}\left[\mathcal{D}(\hat{j})\cap\overline{\mathcal{G}_{ex}(l'_1, l'_2)}\right] \le \frac{q_2(3l'_1 + 3l'_2 + 1)}{2^{n-1}}, \tag{75}$$

with a similar argument as the analysis of preimage resistance. Therefore it follows that

$$\mathbf{Pr}\left[\bigcup_{1\le j\le q_1}\left(\mathcal{D}(j)\cap\overline{\mathcal{G}_{ex}(l_1',l_2')}\right)\right]\le\frac{q_1q_2(3l_1'+3l_2'+1)}{2^{n-1}}. \tag{76}$$

The proof is complete from (64), (74) and (76). □

**Corollary 4.** *Let $A=(a_{ij})$ be a matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$ such that $a_{11}a_{22}+a_{12}a_{21}\neq 0$ and $a_{45}\neq 0$. If $M(A)$ is column-sum independent, then*

$$\lim_{n\to\infty}\mathbf{Adv}^{\mathsf{a-pre}}_{\mathsf{lp}^A}\left(2^{\frac{n}{2}}/n,2^{\frac{n}{2}}/n\right)=0. \tag{77}$$

*Proof.* Let $q_1=q_2=2^{\frac{n}{2}}/n$, $l_1'=1$ and $l_2'=3n-1$. Then it follows that

$$\lim_{n\to 0}\frac{q_1q_2(3l_1'+3l_2'+1)}{2^{n-1}}=\lim_{n\to 0}f_2(l_1',l_2')=\lim_{n\to 0}f_1(l_1')=0. \tag{78}$$

The proof is complete from Theorem 4. □

### 4.3 Collision Resistance

**Theorem 5.** *Suppose that an adversary $\mathcal{A}$ makes a total of $q(\le 2^{n-1})$ queries to a random permutation $\pi$ and its inverse $\pi^{-1}$, and records a query history $\mathcal{Q}$. Let $A=(a_{ij})$ be a matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$ such that $a_{11}a_{22}+a_{12}a_{21}\neq 0$ and $a_{45}\neq 0$, and let $M(A)=[A_1,B_1,A_2,B_2,A_3,B_3]$ and $C(A)=C$ satisfy the following conditions.*

1. *$M(A)$ is column-sum independent.*
2. *$[A_1+A_2,B_1]$, $[A_1+A_2,B_2]$, $[A_2+A_3,B_2]$, $[A_2+A_3,B_3]$, $[A_3+A_1,B_3]$ and $[A_3+A_1,B_1]$ are invertible.*
3. *$[B_1+B_2,A_1]$, $[B_1+B_2,A_2]$, $[B_2+B_3,A_2]$, $[B_2+B_3,A_3]$, $[B_3+B_1,A_3]$ and $[B_3+B_1,A_1]$ are invertible.*
4. *$\left[\bar{A},B_1\right]$, $\left[\bar{A},B_2\right]$, $\left[\bar{A},B_3\right]$, $\left[\bar{A},B_1+B_2\right]$, $\left[\bar{A},B_2+B_3\right]$ and $\left[\bar{A},B_3+B_1\right]$ are invertible, where $\bar{A}=A_1+A_2+A_3$.*
5. *$\left[\bar{B},A_1\right]$, $\left[\bar{B},A_2\right]$, $\left[\bar{B},A_3\right]$, $\left[\bar{B},A_1+A_2\right]$, $\left[\bar{B},A_2+A_3\right]$ and $\left[\bar{B},A_3+A_1\right]$ are invertible, where $\bar{B}=B_1+B_2+B_3$.*
6. *$[A_1,C]$, $[A_2,C]$, $[A_3,C]$, $[B_1,C]$ and $[B_2,C]$ are invertible.*
7. *The following $2\times 6$ matrices are column-sum independent.*

$$\begin{aligned}
D^1&=\left[[A_3,C]^{-1}[A_1,B_1],[A_3,C]^{-1}[A_2,B_2],[A_1,C]^{-1}[A_3,B_3]\right],\\
D^2&=\left[[A_3,C]^{-1}[A_1,B_1],[A_3,C]^{-1}[A_2,B_2],[A_2,C]^{-1}[A_3,B_3]\right],\\
D^3&=\left[[A_2,C]^{-1}[A_1,B_1],[A_1,C]^{-1}[A_2,B_2],[A_1,C]^{-1}[A_3,B_3]\right],\\
D^4&=\left[[B_2,C]^{-1}[A_1,B_1],[B_1,C]^{-1}[A_2,B_2],[B_1,C]^{-1}[A_3,B_3]\right].
\end{aligned}$$

*Then for positive integers $l'_1$, $l'_2$, $l'_3$, $l_2$ and $l_3$,*

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{lp}^A}(\mathcal{A}) \le 2^n q^2 \left(\frac{3l'_1 + 3l'_2 + 1}{2^{n-1}}\right)^2 + \frac{3q(l'_3 + q) + 3q\max(ql_3, l'_2)}{2^{n-1}} + \frac{\left(12q^2 + 6q\right) l'_2}{2^n} + 4g_3 + 12g_2 + 2f_3 + 37f_2 + 194f_1, \tag{79}$$

*where $f_1 = f_1(l'_1)$, $f_2 = f_2(l'_1, l'_2)$, $f_3 = f_3(l'_1, l'_2, l'_3)$, $g_2 = g_2(l'_1, l_2)$ and $g_3 = g_3(l'_1, l'_2, l_2, l_3)$.*

*Proof.* For $j \in [1, q]$ and $\rho^1$, $\rho^2 \in I_3^+ = I_3 \backslash \{0\}$, we define the following events.

$$\begin{aligned} \mathcal{C}^2(j; \rho^1, \rho^2) \Leftrightarrow & \mathcal{A} \text{ sets } (x^{j^1_1}, y^{j^1_1}; x^{j^1_2}, y^{j^1_2}; x^{j^1_3}, y^{j^1_3}) \vdash w \text{ and } (x^{j^2_1}, y^{j^2_1}; x^{j^2_2}, y^{j^2_2}; x^{j^2_3}, y^{j^2_3}) \vdash w, \\ & \text{where } w \in \mathbb{F}_{2^n},\ (j^1_1, j^1_2, j^1_3) \neq (j^2_1, j^2_2, j^2_3) \in [1, j]^3, \text{ and} \\ & j^s_i = j \text{ if and only if } \rho^s_i = 1 \text{ for } i = 1, 2, 3 \text{ and } s = 1, 2. \end{aligned} \tag{80}$$

The occurrence of $\mathcal{C}^2(j; \rho^1, \rho^2)$ means that the *single* $j$-th query determines a collision for $\mathsf{lp}^A_{231}$. Here, $\rho^1$ and $\rho^2$ specify the positions where the $j$-th query-response pair contributes within the two-way collision. Let

$$\mathcal{C}^1 = \bigcup_{\substack{1 \le j_1 < j_2 \le q \\ w \in \mathbb{F}_{2^n}}} \left(\mathcal{P}(w, j_1) \cap \mathcal{P}(w, j_2)\right) \quad \text{and} \quad \mathcal{C}^2 = \bigcup_{\substack{1 \le j \le q \\ \rho^1, \rho^2 \in I_3^+}} \mathcal{C}^2(j; \rho^1, \rho^2). \tag{81}$$

Then it follows that

$$\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{lp}^A}(\mathcal{A}) = \mathbf{Pr}\left[\mathcal{C}^1 \cup \mathcal{C}^2\right] \le \mathbf{Pr}\left[\mathcal{C}^1\right] + \mathbf{Pr}\left[\mathcal{C}^2\right]. \tag{82}$$

**Estimation of $\mathbf{Pr}\left[\mathcal{C}^1\right]$.** If events $\mathcal{P}$ are defined as (66), then

$$\mathbf{Pr}\left[\mathcal{C}^1\right] \le \mathbf{Pr}\left[\bigcup_{\substack{1 \le j_1 < j_2 \le q \\ w \in \mathbb{F}_{2^n}}} \left(\mathcal{P}(w, j_1) \cap \mathcal{P}(w, j_2) \cap \overline{\mathcal{G}_{ex}(l'_1, l'_2)}\right)\right] + \mathbf{Pr}\left[\mathcal{G}_{ex}(l'_1, l'_2)\right]. \tag{83}$$

With a similar argument as the analysis of preimage resistance, we obtain

$$\mathbf{Pr}\left[\mathcal{P}(\hat{w}, \hat{j}_1) \cap \mathcal{P}(\hat{w}, \hat{j}_2) \cap \overline{\mathcal{G}_{ex}(l'_1, l'_2)}\right] \le \left(\frac{3l'_1 + 3l'_2 + 1}{2^{n-1}}\right)^2, \tag{84}$$

for fixed $\hat{w} \in \mathbb{F}_{2^n}$ and $1 \le \hat{j}_1 < \hat{j}_2 \le q$. Therefore, we have

$$\mathbf{Pr}\left[\bigcup_{\substack{1 \le j_1 < j_2 \le q \\ w \in \mathbb{F}_{2^n}}} \left(\mathcal{P}(w, j_1) \cap \mathcal{P}(w, j_2) \cap \overline{\mathcal{G}_{ex}(l'_1, l'_2)}\right)\right] \le 2^n q^2 \left(\frac{3l'_1 + 3l'_2 + 1}{2^{n-1}}\right)^2. \tag{85}$$

**Estimation of $\mathbf{Pr}\left[\mathcal{C}^2\right]$.** Let

$$\begin{aligned}\mathcal{C}_{ex} &= \mathcal{F}^2\left(A_2, B_2, A_3, B_3; 1\right) \cup \mathcal{F}^2\left(A_1, B_1, A_3, B_3; 1\right) \cup \mathcal{F}^2\left(A_1, B_1, A_2, B_2; 1\right) \\ &\cup \mathcal{E}^3_{\neq}\left(\bar{A}^* A_1, \bar{A}^* B_1, \bar{A}^* A_2, \bar{A}^* B_2, \bar{A}^* A_3, \bar{A}^* B_3; l'_3\right) \\ &\cup \mathcal{E}^3_{\neq}\left(\bar{B}^* A_1, \bar{B}^* B_1, \bar{B}^* A_2, \bar{B}^* B_2, \bar{B}^* A_3, \bar{B}^* B_3; l'_3\right) \\ &\cup \bigcup_{1\le i\le 4} \mathcal{F}^3\left(D^i; l_3\right) \cup \mathcal{E}^2\left(B_3^* A_1, B_3^* B_1, B_3^* A_2, B_3^* B_2; l'_2\right). \end{aligned} \tag{86}$$

By Corollary 1 and 2, we obtain

$$\begin{aligned}\mathbf{Pr}\left[\mathcal{C}_{ex}\right] &\le 3\left(\frac{\left(4q^2+2q\right) l'_2}{2^n} + 6f_2 + 12f_1\right) + 2(f_3 + 3f_2 + 9f_1) \\ &\quad + 4(g_3 + 3g_2 + 6f_2 + 30f_1) + (f_2 + 2f_1) \\ &= \frac{\left(12q^2+6q\right) l'_2}{2^n} + 4g_3 + 12g_2 + 2f_3 + 31f_2 + 176f_1. \end{aligned} \tag{87}$$

Since

$$\mathbf{Pr}\left[\mathcal{C}^2\right] \le \sum_{\substack{1\le j\le q \\ \rho^1,\rho^2\in I_3^+}} \mathbf{Pr}\left[\mathcal{C}^2(j;\rho^1,\rho^2) \cap \overline{\mathcal{C}_{ex}}\right] + \mathbf{Pr}\left[\mathcal{C}_{ex}\right], \tag{88}$$

we now focus on the estimation of $\mathbf{Pr}\left[\mathcal{C}^2\left(j;\rho^1,\rho^2\right) \cap \overline{\mathcal{C}_{ex}}\right]$ for each $(\rho^1,\rho^2) \in (I_3^+)^2$.

*Case 1:* We estimate the probability $\mathbf{Pr}\left[\mathcal{C}^2\left(j;\rho^1,\rho^2\right) \cap \overline{\mathcal{C}_{ex}}\right]$ for $\rho^1$ and $\rho^2$ such that $\rho^1 \cap \rho^2 \neq \emptyset$. Suppose that $\rho^1 = \rho^2 = (1,0,0)$. If the event $\mathcal{C}^2(j;(1,0,0),(1,0,0))$ occurs, then it holds that

$$A_1 x^j + B_1 y^j + A_2 x^{j_2^1} + B_2 y^{j_2^1} + A_3 x^{j_3^1} + B_3 y^{j_3^1} = Cw, \tag{89}$$

$$A_1 x^j + B_1 y^j + A_2 x^{j_2^2} + B_2 y^{j_2^2} + A_3 x^{j_3^2} + B_3 y^{j_3^2} = Cw, \tag{90}$$

for some $j_2^1$, $j_3^1$, $j_2^2$, $j_3^2 < j$ and $w \in \mathbb{F}_{2^n}$. The equations (89) and (90) imply that

$$A_2 x^{j_2^1} + B_2 y^{j_2^1} + A_3 x^{j_3^1} + B_3 y^{j_3^1} = A_2 x^{j_2^2} + B_2 y^{j_2^2} + A_3 x^{j_3^2} + B_3 y^{j_3^2}. \tag{91}$$

Therefore, it follows that

$$\mathcal{C}^2\left(j;(1,0,0),(1,0,0)\right) \subset \mathcal{F}^2\left(A_2, B_2, A_3, B_3; 1\right) \subset \mathcal{C}_{ex}, \tag{92}$$

and hence,

$$\mathbf{Pr}\left[\mathcal{C}^2\left(j;(1,0,0),(1,0,0)\right) \cap \overline{\mathcal{C}_{ex}}\right] = 0. \tag{93}$$

The same argument applies to any event $\mathcal{C}^2\left(j;\rho^1,\rho^2\right)$ such that $\rho^1 \cap \rho^2 \neq \emptyset$.

*Case 2:* We estimate the probability $\mathbf{Pr}\left[\mathcal{C}^2\left(j;\rho^1,\rho^2\right) \cap \overline{\mathcal{C}_{ex}}\right]$ for $\rho^1$ and $\rho^2$ such that $\rho^1 \cap \rho^2 = \emptyset$, $wt(\rho^1) = 2$ and $wt(\rho^2) = 1$. (Here $wt(\rho)$ denotes the number of 1's in $\rho$.) Say $\rho^1 = (1,1,0)$ and $\rho^2 = (0,0,1)$. Suppose that $\mathcal{A}$ makes the $j$-th query $\pi(\hat{x})$. There are $(2^n - (j-1))$ possible responses for $y = \pi(\hat{x})$. We now need to upper-bound the number of $y = \pi(\hat{x})$ satisfying

$$\left(A_1 + A_2\right)\hat{x} + \left(B_1 + B_2\right) y + A_3 x^{j_3^1} + B_3 y^{j_3^1} = Cw, \tag{94}$$

$$A_1 x^{j_1^2} + B_1 y^{j_1^2} + A_2 x^{j_2^2} + B_2 y^{j_2^2} + A_3 \hat{x} + B_3 y = Cw, \tag{95}$$

for some $j_3^1$, $j_1^2$, $j_2^2 < j$ and $w \in \mathbb{F}_{2^n}$. Adding (94) and (95), we obtain

$$\bar{A}\hat{x} + \bar{B}y + A_1 x^{j_1^2} + B_1 y^{j_1^2} + A_2 x^{j_2^2} + B_2 y^{j_2^2} + A_3 x^{j_3^1} + B_3 y^{j_3^1} = 0, \tag{96}$$

which implies the following equation.

$$\bar{B}^* A_1 x^{j_1^2} + \bar{B}^* B_1 y^{j_1^2} + \bar{B}^* A_2 x^{j_2^2} + \bar{B}^* B_2 y^{j_2^2} + \bar{B}^* A_3 x^{j_3^1} + \bar{B}^* B_3 y^{j_3^1} = \bar{B}^* \bar{A}\hat{x}. \tag{97}$$

The number of solutions $(j_3^1, j_1^2, j_2^2)$ to (97) is at most $l_3' + q$ without the occurrence of $\mathcal{C}_{ex}$. (The number of solutions $(j_3^1, j_1^2, j_2^2)$ to (97) such that $j_3^1 = j_1^2 = j_2^2$ is at most $q$.) With the same argument for events $\mathcal{C}^2\left(j; (0,1,1), (1,0,0)\right)$ and $\mathcal{C}^2\left(j; (1,0,1), (0,1,0)\right)$, we have

$$\mathbf{Pr}\left[\mathcal{C}^2\left(j; \rho^1, \rho^2\right) \cap \overline{\mathcal{C}_{ex}}\right] \leq \frac{l_3' + q}{2^n - (j-1)} \leq \frac{l_3' + q}{2^{n-1}}. \tag{98}$$

*Case 3:* We estimate the probability $\mathbf{Pr}\left[\mathcal{C}^2\left(j; \rho^1, \rho^2\right) \cap \overline{\mathcal{C}_{ex}}\right]$ for $\rho^1$ and $\rho^2$ such that $\rho^1 \cap \rho^2 = \emptyset$ and $wt(\rho^1) = wt(\rho^2) = 1$. Say $\rho^1 = (1,0,0)$ and $\rho^2 = (0,1,0)$. Suppose that $\mathcal{A}$ makes the $j$-th query $\pi(\hat{x})$. There are $(2^n - (j-1))$ possible responses for $y = \pi(\hat{x})$. We now need to upper-bound the number of $y = \pi(\hat{x})$ satisfying

$$A_1\hat{x} + B_1 y + A_2 x^{j_2^1} + B_2 y^{j_2^1} + A_3 x^{j_3^1} + B_3 y^{j_3^1} = Cw, \tag{99}$$

$$A_1 x^{j_1^2} + B_1 y^{j_1^2} + A_2\hat{x} + B_2 y + A_3 x^{j_3^2} + B_3 y^{j_3^2} = Cw, \tag{100}$$

for some $j_2^1$, $j_3^1$, $j_1^2$, $j_3^2 < j$ and $w \in \mathbb{F}_{2^n}$. Removing variables $y$ and $w$ from this system of equations, we obtain the following equation.

$$\begin{aligned}[B_1, C]^{-1} A_2 x^{j_2^1} + [B_1, C]^{-1} B_2 y^{j_2^1} + [B_1, C]^{-1} A_3 x^{j_3^1} + [B_1, C]^{-1} B_3 y^{j_3^1} \\ + [B_2, C]^{-1} A_1 x^{j_1^2} + [B_2, C]^{-1} B_1 y^{j_1^2} + \left([B_2, C]^{-1} A_3 x^{j_3^2} + [B_2, C]^{-1} B_3 y^{j_3^2}\right) \\ = \left([B_1, C]^{-1} A_1 + [B_2, C]^{-1} A_2\right)\hat{x}.\end{aligned} \tag{101}$$

For each $j_3^2$, the number of solutions $(j_2^1, j_3^1, j_1^2)$ to (101) is at most $l_3$ without the occurrence of $\mathcal{F}^3\left(D^4; l_3\right)$. Therefore, the number of solutions $(j_2^1, j_3^1, j_1^2, j_3^2)$ to (101) is at most $ql_3$.

One special case is when $\rho^1$ or $\rho^2$ is $(0,0,1)$ and $\mathcal{A}$ makes a forward query $y = \pi(\hat{x})$. Say $\rho^1 = (0,0,1)$. Then the response $y = \pi(\hat{x})$ should satisfy

$$A_1 x^{j_1^1} + B_1 y^{j_1^1} + A_2 x^{j_2^1} + B_2 y^{j_2^1} + A_3\hat{x} + B_3 y = Cw, \tag{102}$$

for some $j_1^1$, $j_2^1$ and $w \in \mathbb{F}_{2^n}$. By multiplying $B_3^*$ on both sides of (102), we observe that each $y$ satisfying (102) is associated with a solution $(j_1^1, j_2^1)$ to the following equation.

$$B_3^* A_1 x^{j_1^1} + B_3^* B_1 y^{j_1^1} + B_3^* A_2 x^{j_2^1} + B_3^* B_2 y^{j_2^1} = B_3^* A_3\hat{x}. \tag{103}$$

Here we note that $B_3^* C = 0$. The number of solutions $(j_1^1, j_2^1)$ to (103) is at most $l_2'$ without the occurrence of $\mathcal{E}^2\left(B_3^* A_1, B_3^* B_1, B_3^* A_2, B_3^* B_2; l_2'\right)$. Therefore, we have

$$\mathbf{Pr}\left[\mathcal{C}^2\left(j; \rho^1, \rho^2\right) \cap \overline{\mathcal{C}_{ex}}\right] \leq \frac{\max(ql_3, l_2')}{2^n - (j-1)} \leq \frac{\max(ql_3, l_2')}{2^{n-1}}. \tag{104}$$

To summarize the analysis for the three cases, we conclude that

$$\sum_{\substack{1\le j\le q\\ \rho^1,\rho^2\in I_3^+}} \mathbf{Pr}\left[\mathcal{C}^2(j;\rho^1,\rho^2)\cap\overline{\mathcal{C}_{ex}}\right] \le \frac{3q(l_3'+q)+3q\max(ql_3,l_2')}{2^{n-1}}. \tag{105}$$

Now the proof is complete from (64), (82), (83), (85), (87), (88) and (105). □

**Corollary 5.** *Let $A=(a_{ij})$ be a matrix in $\mathcal{M}_{\mathbb{F}_{2^n}}(2,3,1)$ such that $a_{11}a_{22}+a_{12}a_{21}\neq 0$ and $a_{45}\neq 0$. If $M(A)$ satisfies the conditions described in Theorem 5, then*

$$\lim_{n\to\infty}\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{lp}^A}\left(2^{\frac{n}{2}}/n^{1+\epsilon}\right)=0, \tag{106}$$

*for $\epsilon>0$.*

*Proof.* Let $q=2^{\frac{n}{2}}/n^{1+\epsilon}$, $(l_1',l_2',l_3')=(1,3n-1,(9+1/n)2^{n/2})$ and $(l_2,l_3)=(11,147)$. Then it is easy to check that

$$\begin{aligned}\lim_{n\to 0}\left(2^nq^2\left(\frac{3l_1'+3l_2'+1}{2^{n-1}}\right)^2\right) &= \lim_{n\to 0}\frac{3q(l_3'+q)+3q\max(ql_3,l_2')}{2^{n-1}}\\ &= \lim_{n\to 0}\frac{\left(12q^2+6q\right)l_2'}{2^n}=0.\end{aligned} \tag{107}$$

Since

$$\lim_{n\to 0}f_1(l_1')=\lim_{n\to 0}f_2(l_1',l_2')=\lim_{n\to 0}f_3(l_1',l_2',l_3')=\lim_{n\to 0}g_2(l_1',l_2)=\lim_{n\to 0}g_3(l_1',l_2',l_2,l_3)=0, \tag{108}$$

Theorem 5 completes the proof. □

*Example 1.* Let $n=128$ and let $\mathbb{F}_{2^{128}}=\mathbb{F}[\zeta]/(\zeta^{128}+\zeta^7+\zeta^2+\zeta+1)$ be a finite field of order $2^n$, where $f(\zeta)=\zeta^{128}+\zeta^7+\zeta^2+\zeta+1$ is an irreducible polynomial over $\mathbb{F}_2$. For simplicity of computation, assume that $a_{23}=0$, $a_{45}=1$, and

$$\begin{bmatrix}a_{11}\ a_{12}\\ a_{21}\ a_{22}\end{bmatrix}=\begin{bmatrix}1\ 0\\ 0\ 1\end{bmatrix}.$$

Then we have

$$M(A)=\begin{bmatrix}a_{31}\ a_{33}\ a_{32}\ a_{34}\ 1\ 0\\ a_{41}\ a_{43}\ a_{42}\ a_{44}\ 0\ 1\end{bmatrix}\qquad\text{and}\qquad C(A)=\begin{bmatrix}0\\1\end{bmatrix}.$$

If we set $a_{31}=a_{44}=\zeta$, $a_{33}=a_{42}=\zeta^3$, $a_{32}=a_{43}=\zeta^2+\zeta$, and $a_{34}=a_{41}=1$, then

$$A=\begin{bmatrix}1 & 0 & 0 & 0\ 0\\ 0 & 1 & 0 & 0\ 0\\ \zeta & \zeta^2+\zeta & \zeta^3 & 1\ 0\\ 1 & \zeta^3 & \zeta^2+\zeta & \zeta\ 1\end{bmatrix},$$

and the corresponding matrices $M(A)$ and $C(A)$ satisfy all the conditions described in Theorem 5.

## References


1. P. S. L. M. Barreto and V. Rijmen. The Whirlpool hashing function. Primitve submitted to NESSIE, September 2000, revised on May 2003.
2. G. Bertoni, J. Daemen, M. Peeters and G. Van Assche. On the indifferentiability of the Sponge construction. Eurocrypt 2008, LNCS 4965, pp. 181–197, Springer-Verlag, 2008.
3. J. Black, M. Cochran and T. Shrimpton. On the impossibility of highly-efficient blockcipher-based hash functions. Eurocrypt 2005, LNCS 3494, pp. 526–541, Springer-Verlag, 2005.
4. J. Black, P. Rogaway and T. Shrimpton. Black-box analysis of the block-cipher-based hash-function construction from PGV. Crypto 2002, LNCS 2442, pp. 320–325, Springer-Verlag, 2002.
5. Y. Dodis, T. Ristenpart and T. Shrimpton. Salvaging Merkle-Damgård for practical applications. Eurocrypt 2009, To appear. Available at http://www.cs.nyu/ dodis.
6. S. Hirose. Provably secure double-block-length hash functions in a black-box model. ICISC 2004, LNCS 3506, pp. 330–342, Springer-Verlag, 2005.
7. S. Hirose. Some plausible construction of double-block-length hash functions. FSE 2006, LNCS 4047, pp. 210–225, Springer-Verlag, 2006.
8. J. Lee and J. H. Park. Adaptive Preimage Resistance and Permutation-based Hash Functions. Available at http://eprint.iacr.org/2009/066.
9. S. Matyas, S. Meyer and J. Oseas. Generating strong one-way functions with cryptographic algorithm. IBM Technical Disclosure Bulletin 27, 10a, pp. 5658–5659, 1985.
10. B. Preneel, R. Govaerts and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. Crypto 1993, LNCS 773, pp. 368–378, Springer-Verlag, 1994.
11. T. Ristenpart and T. Shrimpton. How to build a hash function from any collision-resistant function. Asiacrypt 2007, LNCS 4833, pp. 147–163, Springer-Verlag, 2007.
12. P. Rogaway and J. Steinberger. Constructing cryptographic hash functions from fixed-key blockciphers. Crypto 2008, LNCS 5157, pp. 433–450, Springer-Verlag, 2008.
13. P. Rogaway and J. Steinberger. Security/efficiency tradeoffs fro permuation-based hashing. Eurocrypt 2008, LNCS 4965, pp. 220–236, Springer-Verlag, 2008.
14. T. Shrimpton and M. Stam. Building a collision-resistant function from non-compressing primitives. ICALP 2008, LNCS 5126, pp. 643–654, Springer-Verlag, 2008.
15. M. Stam. Beyond uniformity: Better security/efficiency tradeoffs for compression functions. Crypto 2008, LNCS 5157, pp. 397–412, Springer-Verlag, 2008.
16. J. Steinberger. The collision intractability of MDC-2 in the ideal-cipher model. Eurocrypt 2007, LNCS 4515, pp. 34–51, Springer-Verlag, 2008.
17. R. Winternitz. A secure one-way hash function built from DES. IEEE Symposium on Information Security and Privacy, pp. 88–90, IEEE Press, 1984.