Hash Functions Based on Three Permutations: A Generic Security Analysis

Bart Mennink and Bart Preneel

Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and IBBT, Belgium
bart.mennink@esat.kuleuven.be, bart.preneel@esat.kuleuven.be

Abstract. We consider the family of $2n$-to-n-bit compression functions that are solely based on at most three permutation executions and on XOR-operators, and analyze its collision and preimage security. Despite their elegance and simplicity, these designs are not covered by the results of Rogaway and Steinberger (CRYPTO 2008). By defining a carefully chosen equivalence relation on this family of compression functions, we obtain the following results. In the setting where the three permutations π_1, π_2, π_3 are selected independently and uniformly at random, there exist at most four equivalence classes that achieve optimal $2^{n/2}$ collision resistance. Under a certain extremal graph theory based conjecture, these classes are then proven optimally collision secure. Three of these classes allow for finding preimages in $2^{n/2}$ queries, and only one achieves optimal $2^{2n/3}$ preimage resistance (with respect to the bounds of Rogaway and Steinberger, EUROCRYPT 2008). Consequently, a compression function is optimally collision and preimage secure if and only if it is equivalent to $\mathsf{F}(x_1, x_2) = x_1 \oplus \pi_1(x_1) \oplus \pi_2(x_2) \oplus \pi_3(x_1 \oplus x_2 \oplus \pi_1(x_1))$. For compression functions that make three calls to the same permutation we obtain a surprising negative result, namely the impossibility of optimal $2^{n/2}$ collision security: for any scheme, collisions can be found with $2^{2n/5}$ queries. This result casts some doubt over the existence of any (larger) secure permutation-based compression function built only on XOR-operators and (multiple invocations of) a single permutation.

Keywords. Hash function, Permutation-based, Collision resistance, Preimage resistance.

1 Introduction

The traditional recipe for the design of a cryptographic hash function is to base it on one or more block ciphers. Since the late 70s, this methodology developed itself to become the dominating approach in the area of hash function design and plenty of hash functions have been constructed accordingly (either explicitly or implicitly) [3, 4, 6, 7]. These designs are, however, characterized by the fact that the key input to the cipher depends on the input values; this implies that the key schedule has to be strong and that it needs to be executed for every encryption (or for every second encryption), which entails a substantial computational cost. An alternative approach is to fix one or more keys, and restrict the hash function design to use the block cipher for these keys only. The usage of fixed-key block ciphers, or alternatively *permutations*, additionally causes gain that one does not need to implement an entire block cipher but only a limited number of instantiations of it.

Black, Cochran and Shrimpton [1] were the first to formally study this approach, demonstrating that a $2n$-to-n-bit compression function F using one n-bit permutation π cannot be secure. This result has been generalized by Rogaway and Steinberger [10], and refined by Stam [12] and Steinberger [13]. Consider any mn-to-rn-bit compression function using k n-bit permutations: if $2^{n(2m-2r-k+1)/(k+1)} \geq 17$, collisions can be found in at most $(2^n)^{1-(m-r+1)/(k+1)}$ queries to the underlying primitives, a bound proven by Steinberger in [13] but commonly known as "Stam's bound." Collisions and preimages can even be found in at most $(2^n)^{1-(m-r/2)/k}$ and $(2^n)^{1-(m-r)/k}$ queries respectively, provided the compression function satisfies the "uniformity assumption" [10]. Due to Stam's bound, a $2n$-to-n-bit compression function, which is the simplest case after all, achieves optimal $2^{n/2}$ collision resistance *only if* it employs at least three permutations. Yet, it cannot achieve optimal

preimage resistance if it fulfills the uniformity assumption. These observations apply to the "multi-permutation setting", where each of the permutations is generated independently, as well as the "single-permutation setting" where the permutations are the same.

The construction of $2n$-to-n-bit compression functions (based on three permutations) that provably attain optimal collision security, has turned out to be a very challenging exercise. In [9], Rogaway and Steinberger formally proved a broad class of $2n$-to-n-bit compression functions using three distinct permutations and finite field scalar multiplications optimally collision and preimage secure (w.r.t. the bounds of [10]), provided the compression function satisfies a so-called "independence criterion" (a similar result for the single-permutation setting has been obtained by Lee and Kwon [5]). Unfortunately, this technical criterion rules out the most intuitive and elegant type of designs, namely compression functions that are (apart from the three permutations) solely based on XOR-operators. As the proof of [9] extensively relies on its independence criterion, the proof cannot be generalized to compression functions of this type. In [11], Shrimpton and Stam derived a XOR-based compression function, using three one-way functions rather than permutations: $\mathsf{F}(x_1, x_2) = f_1(x_1) \oplus f_3(f_1(x_1) \oplus f_2(x_2))$. This function is proven collision resistant up to $2^{n/2}$ queries (asymptotically), but preimages can be found with high probability after $2^{n/2}$ queries [11]. It has been demonstrated by an automated analysis of Rogaway and Steinberger [9] that the same results hold if f_1, f_2, f_3 are Davies-Meyer-like compression functions using permutations π_1, π_2, π_3, i.e. $f_i(x) = x \oplus \pi_i(x)$, but a formal security analysis has never been given. Since these works, a synthetic formal collision and preimage security analysis of XOR-based compression functions has remained an interesting and important theoretical open problem, because of their elegance and simplicity (the functions only employ XOR-operators) as well as their slight efficiency improvement (XOR-operators are slightly cheaper than finite field multiplications).

Our Contributions. We focus on the entire family of $2n$-to-n-bit compression functions constructed only of three isolated permutations and of XOR-operators, and analyze the security of these functions against information-theoretic adversaries. For each of the functions, we either provide a proof of optimal collision resistance or a collision attack faster than the birthday bound. We also analyze the preimage resistance of the schemes that have optimal collision security.

The approach followed in this work is based on defining an equivalence class on the set of compression functions, and is of independent interest: informally, two compression functions are equivalent if there exists a tight bi-directional preimage and collision security reduction (cf. Def. 3). Consequently, security results of one compression function hold for the entire class, and it suffices to analyze the security of one function per class. In this work we restrict to equivalence reductions that are easy to verify, such as interchanging the inputs to the compression function.

For the *multi-permutation* setting, where the three permutations π_1, π_2, π_3 are assumed to be selected independently and uniformly at random, the results are as follows. A compression function F is optimally collision secure (asymptotically) *if and only if* it is equivalent to one of the four compression functions $\mathsf{F}_1, \ldots, \mathsf{F}_4$:

$$\begin{aligned}
\mathsf{F}_1(x_1, x_2) &= x_2 \oplus \pi_2(x_2) \oplus \pi_3(x_1 \oplus x_2 \oplus \pi_1(x_1))\,, \\
\mathsf{F}_2(x_1, x_2) &= x_1 \oplus \pi_1(x_1) \oplus \pi_2(x_2) \oplus \pi_3(x_1 \oplus x_2 \oplus \pi_1(x_1))\,, \\
\mathsf{F}_3(x_1, x_2) &= x_1 \oplus \pi_1(x_1) \oplus \pi_3(x_1 \oplus x_2 \oplus \pi_1(x_1) \oplus \pi_2(x_2))\,, \\
\mathsf{F}_4(x_1, x_2) &= x_1 \oplus x_2 \oplus \pi_1(x_1) \oplus \pi_3(x_1 \oplus x_2 \oplus \pi_1(x_1) \oplus \pi_2(x_2))\,.
\end{aligned} \tag{1}$$

These compression functions are depicted in Fig. 1. Not surprisingly, the permutation-based variant of the Shrimpton-Stam compression function [11] is included, it equals F_3. For compression functions non-equivalent to any of $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{F}_4$, collisions can be found faster than

the birthday bound, namely in at most $2^{2n/5}$ queries. Compression functions equivalent to F_2 are proven optimally preimage secure up to $2^{2n/3}$ queries, and compression functions equivalent to $\mathsf{F}_1, \mathsf{F}_3$ or F_4 are additionally shown to achieve tight $2^{n/2}$ preimage security. Therefore, a compression function achieves optimal collision and preimage resistance (w.r.t. the bounds of [10]) if and only if it is equivalent to F_2. Particularly, this class of functions beats the Shrimpton-Stam compression function [11] with respect to preimage resistance. These results are summarized in Table 1.

A minor part of the results in the multi-permutation setting, more concretely the collision resistance of $\mathsf{F}_1, \mathsf{F}_2$ and F_4 and the preimage resistance of F_2, are based on an extremal graph theory based conjecture. Informally, this conjecture bounds the number of solutions $(x_1, x_2, x_3) \in X_1 \times X_2 \times X_3$ such that $x_2 \oplus x_3 = x_1 \oplus \pi_1(x_1)$, where X_1, X_2, X_3 are three sets of q elements. This conjecture is similar to (but more complex than) a problem posed by Zarankiewicz in 1951 (cf. [2, Ch. 6.2]), and is of independent interest. In App. D, we analyze our conjecture in more detail, provide it with a heuristic argument, and compare it with the conjecture of Zarankiewicz.

Table 1. The security results of this work for the multi-permutation setting. The functions $\mathsf{F}_1, \ldots, \mathsf{F}_4$ are given in (1) and Fig. 1. The equivalence relation is defined in Def. 3. For F_2, the obtained security results are optimal with respect to the bounds of Rogaway and Steinberger [10]. The proofs of the results with appended "[c]" fall back on Conjecture 1.

	collision		preimage	
F equivalent to:	security	attack	security	attack
$\mathsf{F}_1, \mathsf{F}_4$	$2^{n/2}$ [c]	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
F_2	$2^{n/2}$ [c]	$2^{n/2}$	$2^{2n/3}$ [c]	$2^{2n/3}$
F_3	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
none of these	?	$2^{2n/5}$	?	?

In the *single-permutation* setting, where the compression function makes three calls to the same random permutation π, *there does not exist any* compression function that achieves optimal collision resistance. In particular, for any possible function, collisions can be found in at most $2^{2n/5}$ queries, beating the desired birthday bound. This negative result is surprising, given the fair amount of secure functions we have found in the multi-permutation setting. The attacks mainly rely on the fact that the adversary can misuse the single-permutation property by introducing dependencies between the two input values x_1 and x_2. For instance, the function F_2 of (1) satisfies $\mathsf{F}_2(x_1, x_2) = \mathsf{F}_2(x_1, x_2 \oplus x_1 \oplus \pi(x_1))$ in the single-permutation set-

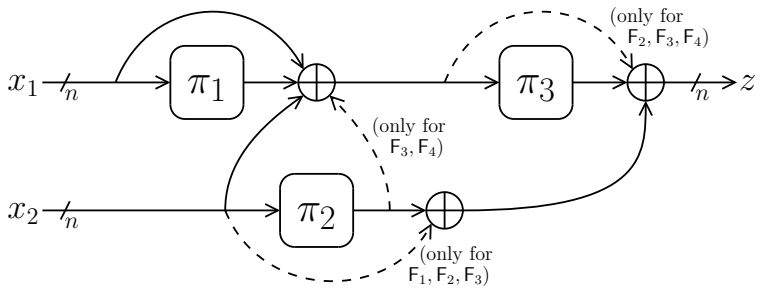

Fig. 1. A graphical representation of the compression functions $\mathsf{F}_1, \ldots, \mathsf{F}_4$ of (1).

ting. This result raises the interesting question whether (larger) compression functions exist based only on XOR-operators and (more than three invocations of) one single permutation.

Outline. In Sect. 2, we present some background information, and formally describe the set of permutation-based compression functions we have analyzed. In Sect. 3, the equivalence relation on the set of compression functions is formally defined. The main results are given in Sect. 4 for the multi-permutation setting and in Sect. 5 for the single-permutation setting. We conclude the paper in Sect. 6.

2 Preliminaries

For an integer $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set of bit strings of length n. For two bit strings x, y, we denote by $x\|y$ their concatenation and by $x \oplus y$ their bitwise XOR. If $\mathcal{X}$ is a set, by $x \xleftarrow{\$} \mathcal{X}$ we denote the uniformly random sampling of an element from $\mathcal{X}$. For two integers $m, n \in \mathbb{N}$, we denote by $\langle m \rangle_n$ the encoding of m as an n-bit string. By log we denote the logarithm function with respect to base 2. By P_n we denote the set of all permutations operating on n bits. Vectors are denoted as $\mathbf{x}$, and by $\|\mathbf{x}\| = \sum_i |x_i|$ we denote the 1-norm of $\mathbf{x}$. For a matrix A, by $a_{i,j}$ we denote its coefficient at the i^{th} row and j^{th} column. By $\mathbf{a}_{i,*}$ we denote the i^{th} row of A, and by $\mathbf{a}_{*,j}$ its j^{th} column.

2.1 Permutation Based Compression Functions

We consider the following type of $2n$-to-n-bit compression functions. Let $\pi_1, \pi_2, \pi_3 \in P_n$ be three permutations. For a binary 4×5 matrix A of the form

$$\mathrm{A} = \left(\begin{array}{cc|ccc} a_{11} & a_{12} & 0 & 0 & 0 \\ a_{21} & a_{22} & a_{23} & 0 & 0 \\ a_{31} & a_{32} & a_{33} & a_{34} & 0 \\ \hline a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \end{array}\right), \tag{2}$$

the compression function $\mathsf{F}_\mathrm{A} : \{0,1\}^{2n} \to \{0,1\}^n$ is defined as follows:

$$\begin{aligned} \mathsf{F}_\mathrm{A}(x_1, x_2) = z\,, \text{ where } \; & y_1 \leftarrow \pi_1(a_{11}x_1 \oplus a_{12}x_2)\,, \\ & y_2 \leftarrow \pi_2(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}y_1)\,, \\ & y_3 \leftarrow \pi_3(a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}y_1 \oplus a_{34}y_2)\,, \\ & z \leftarrow a_{41}x_1 \oplus a_{42}x_2 \oplus a_{43}y_1 \oplus a_{44}y_2 \oplus a_{45}y_3\,. \end{aligned} \tag{3}$$

The function F_A is depicted in Fig. 2. If the three permutations are all different, we refer to it as the *multi-permutation* setting. If π_1, π_2, π_3 are equal to one permutation π, we are in the *single-permutation* setting. In total, we thus analyze $2 \cdot 2^{14}$ compression functions. Many of these, however, are trivially weak (cf. Sect. 2.3).

For the single-permutation setting, it is of interest to also consider the case where n-bit constants are added to the inputs to the permutations (e.g. $y_1 \leftarrow \pi_1(a_{11}x_1 \oplus a_{12}x_2 \oplus b_1)$ for $b_1 \in \{0,1\}^n$). This results in many more schemes, but requires a more complex analysis. Therefore, we present our main results on F_A of (3), and in App. C we generalize our findings on the single-permutation setting to cover any F_A where additional affine transformations on the permutation inputs are taken into account.

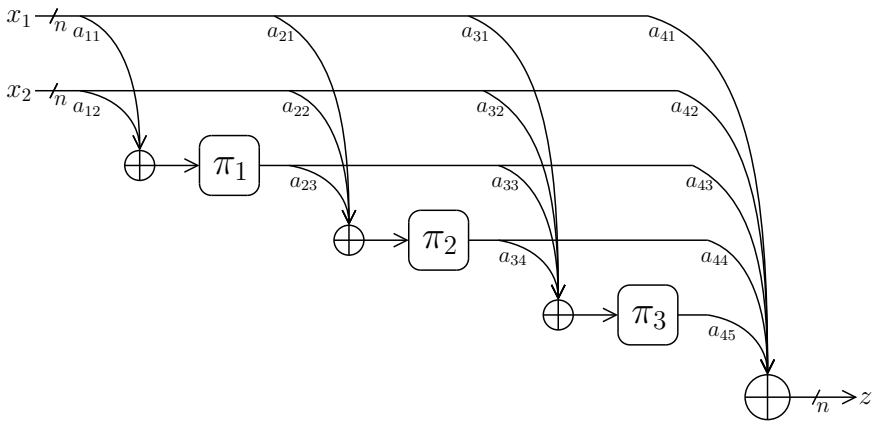

Fig. 2. The permutation-based compression function F_A of (3).

2.2 Security Notions

An adversary is a probabilistic algorithm with oracle access to the underlying permutations π_1, π_2, π_3. He can make forward and inverse queries to its oracles, and the queries are stored in a query history $\mathcal{Q}$. By $(x_k, y_k) \in \mathcal{Q}$, for $k \in \{1, 2, 3\}$, we denote that $y_k = \pi_k(x_k)$; the adversary either made a forward query x_k to obtain y_k or an inverse query y_k to obtain x_k. In the remainder, we assume that $\mathcal{Q}$ always contains the queries required for the attack, and we assume that the adversary does not make trivial queries, i.e. queries to which the adversary already knows the answer in advance. In this work we consider information-theoretic adversaries only. This type of adversary has unbounded computational power, and its complexity is measured by the number of queries made to its oracles.

Definition 1. *Let $\mathsf{F}_\mathrm{A} : \{0,1\}^{2n} \to \{0,1\}^n$ be a compression function defined by a matrix* A *of the form (2). Let $\mathcal{A}$ be a collision finding adversary for this compression function. The advantage of $\mathcal{A}$ is defined as*

$$\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_\mathrm{A}}(\mathcal{A}) = \mathbf{Pr}\left(\pi_1, \pi_2, \pi_3 \xleftarrow{\$} P_n,\ x, x' \leftarrow \mathcal{A}^{\pi_i, \pi_i^{-1}} \ :\ x \neq x',\ \mathsf{F}^{\pi_i}_\mathrm{A}(x) = \mathsf{F}^{\pi_i}_\mathrm{A}(x')\right).$$

By $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_\mathrm{A}}(q)$ we denote the maximum advantage, taken over all adversaries making q queries to each of their oracles.

Several definitions for preimage resistance are known, but we opt for everywhere preimage resistance [8], which intuitively guarantees preimage security for every range point.

Definition 2. *Let $\mathsf{F}_\mathrm{A} : \{0,1\}^{2n} \to \{0,1\}^n$ be a compression function defined by a matrix* A *of the form (2). Let $\mathcal{A}$ be an everywhere preimage finding adversary for this compression function. The advantage of $\mathcal{A}$ is defined as*

$$\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_\mathrm{A}}(\mathcal{A}) = \max_{z \in \{0,1\}^n} \mathbf{Pr}\left(\pi_1, \pi_2, \pi_3 \xleftarrow{\$} P_n,\ x \leftarrow \mathcal{A}^{\pi_i, \pi_i^{-1}}(z) \ :\ z = \mathsf{F}^{\pi_i}_\mathrm{A}(x)\right).$$

By $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_\mathrm{A}}(q)$ we denote the maximum advantage, taken over all adversaries making q queries to each of their oracles.

The security definitions for the single-permutation setting, where the compression function is built on one permutation π, are analogous.

2.3 Invalid Matrices

We will classify the set of optimally collision secure compression functions F_{A} of the form described in Sect. 2.1, but for some matrices A the induced compression function will clearly not fulfill the desired security requirements. For instance, if a compression function does not use one or more permutations, attacks faster than the birthday bound can easily be constructed. We introduce the notion of "valid" matrices, in order to rule out compression functions that trivially fail to achieve optimal collision resistance. A matrix A is called "valid" if it satisfies the following properties:

(1) For the j^{th} column ($j = 1, 2$), we have $a_{1j} + a_{2j} + a_{3j} \geq 1$. This requirement ensures that input x_j is used in the computation of at least one permutation. If this would not be the case, collisions can easily be constructed;
(2) For the j^{th} column ($j = 3, 4, 5$), we have $\|\mathbf{a}_{*,j}\| \geq 1$, and for the i^{th} row ($i = 1, 2, 3$), we have $\|\mathbf{a}_{i,*}\| \geq 1$. Notice that if the i^{th} row (resp. j^{th} column) would consist of zeroes only, it means that permutation π_i (resp. π_{j-2}) is not used in the computation, and collisions can be found in at most $2^{n/3}$ queries by Stam's bound [12, 13].

In the remainder, we will consider valid matrices A only. By an extensive computation one can show that $2796 < 2^{12}$ out of 2^{14} matrices are valid (for both the single- and multi-permutation setting).

3 Equivalence Classes of Permutation Based Compression Functions

We define an equivalence relation on the set of compression functions F_{A}. This equivalence relation intuitively describes classes of "equally secure" compression functions, and can be used to reduce the number of compression functions to be analyzed. Indeed, security properties of one compression function naturally convey to all compression functions in the same equivalence class. The equivalence relation is defined in Def. 3, and in Props. 1-4 we describe the four equivalence reductions that will be used in this work.

Definition 3. *Two compression functions* F_{A} *and* $\mathsf{F}_{\mathrm{A}'}$ *are* equivalent *if for both collision and preimage security there exists a tight reduction from* F_{A} *to* $\mathsf{F}_{\mathrm{A}'}$*, and vice versa.*

Proposition 1 (x-reduction). *Consider two matrices* $\mathrm{A} = \big(\mathbf{a}_{*,1}\ ;\ \mathbf{a}_{*,2}\ ;\ \mathbf{a}_{*,3}\ ;\ \mathbf{a}_{*,4}\ ;\ \mathbf{a}_{*,5}\big)$ *and* $\mathrm{A}' = \big(\mathbf{a}_{*,2}\ ;\ \mathbf{a}_{*,1}\ ;\ \mathbf{a}_{*,3}\ ;\ \mathbf{a}_{*,4}\ ;\ \mathbf{a}_{*,5}\big)$*. Then, the compression functions* F_{A} *and* $\mathsf{F}_{\mathrm{A}'}$ *are equivalent. Intuitively, this reduction corresponds to swapping* x_1 *and* x_2*.*

Proposition 2 (XOR-reduction). *Consider a matrix* $\mathrm{A} = \big(\mathbf{a}_{*,1}\ ;\ \mathbf{a}_{*,2}\ ;\ \mathbf{a}_{*,3}\ ;\ \mathbf{a}_{*,4}\ ;\ \mathbf{a}_{*,5}\big)$*, and let* $k = \min\{\ i \mid a_{i,2} \neq 0\ \}$ *(notice that* $k \in \{1, 2, 3\}$ *as* A *is valid). Let* $c_0, \ldots, c_2 \in \{0, 1\}$*. Consider the matrix* $\mathrm{A}' = \mathrm{A} \oplus \big(c_0\mathbf{a}_{*,2}\,;\,\mathbf{0}\,;\,[k \geq 2]c_1\mathbf{a}_{*,2}\,;\,[k \geq 3]c_2\mathbf{a}_{*,2}\,;\,\mathbf{0}\big)$*, where* $[X] = 1$ *if* X *holds and* 0 *otherwise. Then, the compression functions* F_{A} *and* $\mathsf{F}_{\mathrm{A}'}$ *are equivalent. Intuitively,* π_k *is the first permutation that incorporates* x_2*, and this reduction represents replacing* x_2 *by* $x_2 \oplus c_0 x_1 \oplus \sum_{i=1}^{k-1} c_i y_i$*, where* y_i *is the outcome of the* i^{th} *permutation. Using Prop. 1, the same reduction holds for* x_1*.*

Proposition 3 (π-swap-reduction). *Let* $i \in \{1, 2\}$*, and consider a matrix* A *with* $a_{i+1,i+2} = 0$*. Consider the matrix* A' *obtained from* A *by swapping rows* $\mathbf{a}_{i,*}$ *and* $\mathbf{a}_{i+1,*}$ *and consequently swapping columns* $\mathbf{a}_{*,i+2}$ *and* $\mathbf{a}_{*,i+3}$*. Then, the compression functions* F_{A} *and* $\mathsf{F}_{\mathrm{A}'}$ *are equivalent. Intuitively, this reduction corresponds to swapping* π_i *and* π_{i+1}*, which is only possible if the outcome of* π_i *is not used as input of* π_{i+1} *(i.e. if* $a_{i+1,i+2} = 0$*).*

Proposition 4 (π-inverse-reduction). *Consider a matrix* A *with* $(a_{11}, a_{12}) = (1, 0)$. *Consider the matrix* A' *obtained from* A *by swapping* (a_{21}, a_{31}, a_{41}) *and* (a_{23}, a_{33}, a_{43}). *Then, the compression functions* F_{A} *and* $\mathsf{F}_{\mathrm{A}'}$ *are equivalent. Intuitively, this reduction corresponds to replacing* π_1 *by* π_1^{-1}. *Using Prop. 1 and Prop. 3 on* $i = 1$, *the same reduction holds for* π_2.

Proof (Proof of Props. 1-4). Let F_{A} and $\mathsf{F}_{\mathrm{A}'}$ be two compression functions defined as in either of the propositions. For simplicity, in case of Prop. 2 we only consider $k = 2$ (so $a_{12} = 0$, $a_{22} = 1$ and $c_2 = 0$), for Prop. 3 we only consider $i = 1$ (so $a_{23} = 0$). By construction, the compression functions F_{A} and $\mathsf{F}_{\mathrm{A}'}$ satisfy the following properties:

$$\mathsf{F}_{\mathrm{A}}^{\pi_1,\pi_2,\pi_3}(x_1, x_2) = \begin{cases} \mathsf{F}_{\mathrm{A}'}^{\pi_1,\pi_2,\pi_3}(x_2, x_1) & \text{for Prop. 1,} \\ \mathsf{F}_{\mathrm{A}'}^{\pi_1,\pi_2,\pi_3}(x_1, x_2 \oplus c_0 x_1 \oplus c_1 \pi_1(a_{11} x_1)) & \text{for Prop. 2,} \\ \mathsf{F}_{\mathrm{A}'}^{\pi_2,\pi_1,\pi_3}(x_1, x_2) & \text{for Prop. 3,} \\ \mathsf{F}_{\mathrm{A}'}^{\pi_1^{-1},\pi_2,\pi_3}(\pi_1(x_1), x_2) & \text{for Prop. 4.} \end{cases} \tag{4}$$

We need to provide a bi-directional collision and preimage security reduction. For conciseness, we will provide only the collision security reduction; the case of preimage resistance is similar and is therefore omitted. Let $\mathcal{A}$ be a collision finding adversary for the compression function F_{A}, that on input of $\pi_1, \pi_2, \pi_3 \xleftarrow{\$} P_n$, outputs two tuples (x_1, x_2), (x_1', x_2') such that $\mathsf{F}_{\mathrm{A}}^{\pi_i}(x_1, x_2) = \mathsf{F}_{\mathrm{A}}^{\pi_i}(x_1', x_2')$. We construct a collision finding adversary $\mathcal{A}'$ for $\mathsf{F}_{\mathrm{A}'}$ that uses $\mathcal{A}$ as a subroutine and on input of $\pi_1', \pi_2', \pi_3' \xleftarrow{\$} P_n$ outputs a collision for $\mathsf{F}_{\mathrm{A}'}^{\pi_i'}$. Adversary $\mathcal{A}'$ operates as follows:

1. In Props. 1 and 2, the adversary $\mathcal{A}'$ sends $(\pi_1, \pi_2, \pi_3) \leftarrow (\pi_1', \pi_2', \pi_3')$ to $\mathcal{A}$. In Prop. 3, the adversary $\mathcal{A}'$ sends $(\pi_1, \pi_2, \pi_3) \leftarrow (\pi_2', \pi_1', \pi_3')$ to $\mathcal{A}$. In Prop. 4, the adversary $\mathcal{A}'$ sends $(\pi_1, \pi_2, \pi_3) \leftarrow ((\pi_1')^{-1}, \pi_2', \pi_3')$ to $\mathcal{A}$;
2. $\mathcal{A}$ outputs two tuples (x_1, x_2), (x_1', x_2') such that $\mathsf{F}_{\mathrm{A}}^{\pi_i}(x_1, x_2) = \mathsf{F}_{\mathrm{A}}^{\pi_i}(x_1', x_2')$;
3. In Prop. 1, $\mathcal{A}'$ outputs collision (x_2, x_1) and (x_2', x_1'). In Prop. 2, $\mathcal{A}'$ outputs $(x_1, x_2 \oplus c_0 x_1 \oplus c_1 \pi_1(a_{11} x_1))$ and $(x_1', x_2' \oplus c_0 x_1' \oplus c_1 \pi_1(a_{11} x_1'))$. In Prop. 3, $\mathcal{A}'$ outputs (x_1, x_2) and (x_1', x_2'). In Prop. 4, $\mathcal{A}'$ outputs $((\pi_1')^{-1}(x_1), x_2)$ and $((\pi_1')^{-1}(x_1'), x_2')$.

Notice that in step one, the permutations (π_1, π_2, π_3) are clearly randomly and independently distributed as (π_1', π_2', π_3') are, and therefore $\mathcal{A}$ can output (x_1, x_2), (x_1', x_2') such that $\mathsf{F}_{\mathrm{A}}^{\pi_1,\pi_2,\pi_3}(x_1, x_2) = \mathsf{F}_{\mathrm{A}}^{\pi_1,\pi_2,\pi_3}(x_1', x_2')$ with probability $\mathbf{Adv}_{\mathsf{F}_{\mathrm{A}}}^{\mathsf{col}}(\mathcal{A})$. For $\mathsf{F}_{\mathrm{A}'}$ of Prop. 3, these tuples indeed render a collision as given in step 3:

$$\begin{aligned} \mathsf{F}_{\mathrm{A}'}^{\pi_1',\pi_2',\pi_3'}(x_1, x_2) &= \mathsf{F}_{\mathrm{A}}^{\pi_2',\pi_1',\pi_3'}(x_1, x_2) && \text{by (4),} \\ &= \mathsf{F}_{\mathrm{A}}^{\pi_2',\pi_1',\pi_3'}(x_1', x_2') && \text{by collision for } \mathsf{F}_{\mathrm{A}}, \\ &= \mathsf{F}_{\mathrm{A}'}^{\pi_1',\pi_2',\pi_3'}(x_1', x_2') && \text{by (4).} \end{aligned}$$

The same argument applies to the other propositions. In any case, $\mathcal{A}'$ needs at most four queries more than $\mathcal{A}$, and thus we obtain $\mathbf{Adv}_{\mathsf{F}_{\mathrm{A}}}^{\mathsf{col}}(q) \leq \mathbf{Adv}_{\mathsf{F}_{\mathrm{A}'}}^{\mathsf{col}}(q+4)$. The reductions in the other direction (from $\mathsf{F}_{\mathrm{A}'}$ to F_{A}) are identical due to symmetry. □

Except for Prop. 4, the reductions also hold in the single-permutation setting. We remark that these reductions are not only restricted to binary matrices, but apply to general matrices A. In particular, the independence criterion of [9] can be derived using the given reductions. Also, we note that the reductions can easily be represented by linear matrix operations.

4 Main Result for Multi-Permutation Setting

We classify the set of permutation-based compression functions of the form (3) that achieve optimal collision resistance. Theorem 1 shows that the set of (asymptotically) secure functions is fully covered by four equivalence classes; for any other compression function collisions can be found faster than the birthday bound. One of these four classes – defined by $\mathsf{F}_{\mathrm{A}_2}$ below – provides optimal (asymptotic) $2^{2n/3}$ preimage security, for the other three classes preimages can be found significantly faster.

Theorem 1. *Consider the multi-permutation setting. Let* F_{A} *be any compression function defined by a binary matrix* A *of the form (2). Let* $\mathsf{F}_{\mathrm{A}_k}$ *for* $k = 1, 2, 3, 4$ *be the compression functions defined by matrices*

$$\mathrm{A}_1 = \left(\begin{array}{c|c|c} 1\,0 & 0\,0\,0 \\ 0\,1 & 0\,0\,0 \\ \hline 1\,1 & 1\,0\,0 \\ \hline 0\,1\,0\,1\,1 \end{array}\right), \quad \mathrm{A}_2 = \left(\begin{array}{c|c|c} 1\,0 & 0\,0\,0 \\ 0\,1 & 0\,0\,0 \\ \hline 1\,1 & 1\,0\,0 \\ \hline 1\,0\,1\,1\,1 \end{array}\right), \quad \mathrm{A}_3 = \left(\begin{array}{c|c|c} 1\,0 & 0\,0\,0 \\ 0\,1 & 0\,0\,0 \\ \hline 1\,1 & 1\,1\,0 \\ \hline 1\,0\,1\,0\,1 \end{array}\right), \quad \mathrm{A}_4 = \left(\begin{array}{c|c|c} 1\,0 & 0\,0\,0 \\ 0\,1 & 0\,0\,0 \\ \hline 1\,1 & 1\,1\,0 \\ \hline 1\,1\,1\,0\,1 \end{array}\right). \quad (5)$$

Let $\varepsilon > 0$.

(i) If F_{A} *is equivalent to* $\mathsf{F}_{\mathrm{A}_k}$ *for* $k \in \{1, 2, 3, 4\}$*, it satisfies* $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(2^{n/2(1-\varepsilon)}) = 0$. *Otherwise, it satisfies* $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Omega(q^5/2^{2n})$*;*

(ii) If F_{A} *is equivalent to* $\mathsf{F}_{\mathrm{A}_2}$*, it satisfies* $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}}}(2^{2n/3(1-\varepsilon)}) = 0$*;*

(iii) If F_{A} *is equivalent to* $\mathsf{F}_{\mathrm{A}_k}$ *for* $k \in \{1, 3, 4\}$*, it satisfies* $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Theta(q^2/2^n)$.

In other words, a compression function offers optimal collision resistance *if and only if* it is equivalent to either of $\mathsf{F}_{\mathrm{A}_1}, \mathsf{F}_{\mathrm{A}_2}, \mathsf{F}_{\mathrm{A}_3}, \mathsf{F}_{\mathrm{A}_4}$, and additionally achieves optimal preimage resistance (with respect to the bounds of [10]) *if and only if* it is equivalent to $\mathsf{F}_{\mathrm{A}_2}$.

In order to prove Thm. 1, more specifically part (i) for $k = 1, 2, 4$ and part (ii), we pose the following conjecture. This conjecture relates to the area of extremal graph theory and is of independent interest. In particular, it can be shown to be similar to (but more complex than) a longstanding problem of Zarankiewicz from 1951 [2, Ch. 6.2].

Conjecture 1. Let $q \leq 2^n$, and let Z be a set of q elements taken uniformly at random from $\{0,1\}^n$. Let β denote the maximum number of tuples $(x_1, x_2, z) \in X_1 \times X_2 \times Z$ such that $x_1 \oplus x_2 = z$, where X_1, X_2 are any two subsets of $\{0,1\}^n$ of size q. Formally:

$$\beta := \max_{\substack{X_1, X_2 \subseteq \{0,1\}^n \\ |X_1| = |X_2| = q}} \left| \{(x_1, x_2, z) \in X_1 \times X_2 \times Z \;\mid\; x_1 \oplus x_2 = z\} \right|. \quad (6)$$

There exists a constant d_1 such that $\mathbf{Pr}\left(\beta > d_1 q \log q\right) \to 0$ for $n \to \infty$ and $q < 2^{n/2}$. Similarly, there exists a constant d_2 such that $\mathbf{Pr}\left(\beta > d_2 q^{3/2}\right) \to 0$ for $n \to \infty$ and $q < 2^{2n/3}$.

The first bound is used in the proof Thm. 1(i) for $k = 1, 2, 4$, and the second bound in the proof Thm. 1(ii). A detailed heuristic for Conj. 1 is given in App. D, together with a comparison with Zarankiewicz's conjecture, but we leave a full proof of Conj. 1 as an open problem.

4.1 Proof of Theorem 1

The proof of Thm. 1 is structured as follows. Firstly, in Lem. 1 we show that any compression function F_{A} can be reduced either to an invalid compression function or to a compression function $\mathsf{F}_{\mathrm{A}'}$ defined by a matrix A' with first two rows $10000, 01000$. By construction (see

Sect. 3), the security properties of one compression function are valid for the whole equivalence class. Secondly, in Lem. 2 several collision attacks are described that invalidate the security of each of the remaining compression functions, except for the classes defined by $\mathsf{F}_{\mathrm{A}_k}$ ($k \in \{1,2,3,4\}$) for A_k as in (5). Thirdly, the collision and preimage resistance of the remaining four compression functions are analyzed in Lem. 3, which completes the proof of Thm. 1.

Lemma 1. *Any compression function* F_{A}*, for valid* A*, is equivalent to a compression function* $\mathsf{F}_{\mathrm{A}'}$*, where either* A′ *is invalid or the first two rows of* A′ *equal* $10000, 01000$*.*

Proof. The proof is constructive. Several reductions are used, but for ease of notation apostrophes are omitted. Let F_{A} be a compression function defined by some valid matrix A. As A is valid, we have $a_{11} + a_{12} \geq 1$. If $a_{11} + a_{12} = 2$, we can apply Prop. 2 on $c_0 = 1$ to obtain $a_{11} + a_{12} = 1$. Now, by Prop. 1 we can assume that $(a_{11}, a_{12}) = (1, 0)$.

Considering the second row of A, we distinguish between $a_{22} = 1$ and $a_{22} = 0$. In the former case, a XOR-reduction (Prop. 2) on $(c_0, c_1) = (a_{21}, a_{23})$ reduces the scheme to the required form. In the latter case, where $a_{22} = 0$, we proceed as follows. If $a_{32} = 0$, A is equivalent to an invalid matrix. Otherwise, by applying Prop. 2 with $(c_0, c_1, c_2) = (a_{31}, a_{33}, a_{34})$ we obtain that F_{A} is equivalent to a compression function $\mathsf{F}_{\mathrm{A}'}$, for some matrix A′ with rows $(10000, a'_{21}0a'_{23}00, 01000, a'_{41}a'_{42}a'_{43}a'_{44}a'_{45})$. The result is now obtained by swapping π_2 and π_3 (Prop. 3 for $i = 2$). □

As a direct consequence of Lem. 1, it suffices to consider compression functions F_{A}, where

$$\mathrm{A} = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & a_{34} & 0 \\ \hline a_{41} & a_{42} & a_{43} & a_{44} & 1 \end{array}\right) \tag{7}$$

for some binary values $a_{31}, \ldots, a_{44}$. Notice that $a_{45} = 1$ because of the validity of the matrix. We describe a couple of collision attacks that apply to compression functions of this form. We note that similar results also hold for preimage resistance.

Lemma 2. *Let* F_{A} *be a compression function defined by a valid matrix* A *of the form (7).*

(i) If A *satisfies* $(a_{31} + a_{33})(a_{32} + a_{34}) = 0$*, then* $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Omega(q^4/2^n)$*;*
(ii) If A *satisfies* $\bigvee_{j=1}^{4} a_{3j} = a_{4j} = 0$*, then* $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Omega(q^3/2^n)$*;*
(iii) If A *satisfies* $\bigwedge_{j=1}^{2} a_{3j}a_{4,j+2} \neq a_{3,j+2}a_{4j}$*, then* $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Omega(q^3/2^n)$*;*
(iv) If A *satisfies* $a_{41} + a_{42} + a_{43} + a_{44} = 1$*, then* $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Omega(q^5/2^{2n})$*.*

For clarity, the proofs of results (i), (ii), (iii) and (iv) will be given separately.

Proof (Proof of Lem. 2(i)). Without loss of generality, we assume $a_{32} + a_{34} = 0$, i.e. $a_{32} = a_{34} = 0$. Hence, we consider matrices A with $\left(\begin{smallmatrix} a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{smallmatrix}\right) = \left(\begin{smallmatrix} a_{31} & 0 & a_{33} & 0 \\ a_{41} & a_{42} & a_{43} & 1 \end{smallmatrix}\right)$, where $a_{31} + a_{33} \geq 1$, by validity of A. This matrix defines the compression function:

$$\mathsf{F}_{\mathrm{A}}(x_1, x_2) = a_{41}x_1 \oplus a_{42}x_2 \oplus a_{43}\pi_1(x_1) \oplus \pi_2(x_2) \oplus \pi_3(a_{31}x_1 \oplus a_{33}\pi_1(x_1))\,.$$

Define the functions $f_1(x) = a_{41}x \oplus a_{43}\pi_1(x) \oplus \pi_3(a_{31}x \oplus a_{33}\pi_1(x))$ and $f_2(x) = a_{42}x \oplus \pi_2(x)$. Notice that $\mathsf{F}_{\mathrm{A}}(x_1, x_2) = f_1(x_1) \oplus f_2(x_2)$. A collision-finding adversary $\mathcal{A}$ for F_{A} proceeds as follows. He sets up two lists of q random elements $X_1 := \{x_1^{(1)}, \ldots, x_1^{(q)}\}$ and $X_2 := \{x_2^{(1)}, \ldots, x_2^{(q)}\}$, and computes the corresponding values $f_1(x_1^{(k)})$ and $f_2(x_2^{(k)})$ (for $k = 1, \ldots, q$). Thus, in total $\mathcal{A}$ makes q queries to each of his random oracles. Given one of the $\binom{q}{2}^2$ combinations $x_1, x'_1 \in X_1$, $x_2, x'_2 \in X_2$, this combination yields a collision for F_{A} with probability $\Theta(2^{-n})$. Concluding, $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) = \Omega(q^4/2^n)$. □

Proof (Proof of Lem. 2(ii)). For the cases $j \in \{3,4\}$ as explained in Sect. 2.3 (these cases are in fact redundant due to the validity of A), collisions can be found in at most $2^{n/3}$ queries due to Stam's bound [12, 13]. We consider a matrix A with $a_{32} = a_{42} = 0$ (the case $j = 2$), a similar analysis holds for $j = 1$. Note that F_A satisfies $\mathsf{F}_\mathrm{A}(x_1, x_2) = \mathsf{F}_{\mathrm{A}'}(x_1, \pi_2(x_2))$, where A' has third and fourth rows $(a_{31}a_{34}a_{33}00, a_{41}a_{44}a_{43}01)$. The compression function $\mathsf{F}_{\mathrm{A}'}$ satisfies the condition of this lemma for $j = 4$, and invertibility of π_2 guarantees a collision for F_A in the same amount of queries plus 2. We note that the result also follows from Prop. 4, but as we will use Lem. 2(ii) in the single-permutation setting as well, we here consider a more robust reduction. □

Proof (Proof of Lem. 2(iii)). The idea of the attack is to focus on collisions $(x_1, x_2) \neq (x'_1, x'_2)$ for which the input to the third permutation π_3 is the same. We first consider the case of matrices A with $\left(\begin{smallmatrix} a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ a_{41} & a_{42} & 1 & 1 \end{smallmatrix}\right)$, the general case is discussed afterwards. The matrix defines compression function

$$\mathsf{F}_\mathrm{A}(x_1, x_2) = a_{41}x_1 \oplus a_{42}x_2 \oplus \pi_1(x_1) \oplus \pi_2(x_2) \oplus \pi_3(x_1 \oplus x_2)\,.$$

We construct an adversary $\mathcal{A}$ that aims at finding a collision $(x_1, x_2) \neq (x'_1, x'_2)$ such that

$$x_1 \oplus x_2 = x'_1 \oplus x'_2\,, \tag{8a}$$

$$a_{41}x_1 \oplus a_{42}x_2 \oplus \pi_1(x_1) \oplus \pi_2(x_2) = a_{41}x'_1 \oplus a_{42}x'_2 \oplus \pi_1(x'_1) \oplus \pi_2(x'_2)\,. \tag{8b}$$

The adversary sets up two lists of $q = 2^\alpha$ elements $X_1 := \{x_1^{(1)}, \ldots, x_1^{(q)}\}$ and $X_2 := \{x_2^{(1)}, \ldots, x_2^{(q)}\}$, where $x_1^{(k)} = x_2^{(k)} = 0^{n-\alpha} \| \langle k-1 \rangle_\alpha$ for $k = 1, \ldots, q$. He computes the corresponding values $\pi_1(x_1^{(k)})$ and $\pi_2(x_2^{(k)})$ (for $k = 1, \ldots, q$). Fix any x_1, x_2, x'_1 such that $x_1 \neq x'_1$. Then, there is exactly one x'_2 such that (8a) is satisfied. For any of these $q\binom{q}{2}$ options, (8b) is satisfied with probability $\Theta(2^{-n})$. For any of such succeeding tuples, the adversary additionally queries $\pi_3(x_1 \oplus x_2) = \pi_3(x'_1 \oplus x'_2)$ in order to get a collision. Concluding, $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_\mathrm{A}}(q) = \Omega(q^3/2^n)$.

The described attack relies on the key property that the set of equations

$$\begin{pmatrix} a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} (x_1 \oplus x'_1,\ x_2 \oplus x'_2,\ \pi_1(x_1) \oplus \pi_1(x'_1),\ \pi_2(x_2) \oplus \pi_2(x'_2))^\top = 0$$

contains an equation in which x_1, x_2, x'_1, x'_2 occur exactly once. By the requirement of A, $\left(\begin{smallmatrix} a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{smallmatrix}\right)$ contains at least two zeroes. If two zeroes are located in the same row, this key property is satisfied and the attack succeeds. On the other hand, if both rows contain exactly one zero, one can XOR the first equation to the second one to return to the first case. □

Proof (Proof of Lem. 2(iv)). Without loss of generality, we assume $a_{41} = 1$. By Lem. 2(ii), we can consider $a_{32} = a_{33} = a_{34} = 1$. The matrix defines compression function

$$\mathsf{F}_\mathrm{A}(x_1, x_2) = x_1 \oplus \pi_3(a_{31}x_1 \oplus x_2 \oplus \pi_1(x_1) \oplus \pi_2(x_2))\,.$$

We construct a collision adversary $\mathcal{A}$ for F_A. The adversary sets up a list of $q = 2^\alpha$ random elements $X_2 := \{x_2^{(1)}, \ldots, x_2^{(q)}\}$, and computes the corresponding values $y_2^{(k)} = \pi_2(x_2^{(k)})$ (for $k = 1, \ldots, q$). Additionally, the adversary sets up two lists $X_1 := \{x_1^{(1)}, \ldots, x_1^{(q)}\}$ and $Y_3 := \{y_3^{(1)}, \ldots, y_3^{(q)}\}$, where $x_1^{(k)} = y_3^{(k)} = 0^{n-\alpha} \| \langle k-1 \rangle_\alpha$ for $k = 1, \ldots, q$. He computes the corresponding values $y_1^{(k)} = \pi_1(x_1^{(k)})$ and $x_3^{(k)} = \pi_3^{-1}(y_3^{(k)})$ (for $k = 1, \ldots, q$). Fix any x_1, y_3, x'_1 such that $x_1 \neq x'_1$. Then, there is exactly one y'_3 such that $x_1 \oplus y_3 = x'_1 \oplus y'_3$. The adversary

obtains a collision for F_A if X_2 contains two elements x_2, x_2' such that $x_2 \oplus y_2 = a_{31}x_1 \oplus y_1 \oplus x_3$ and $x_2' \oplus y_2' = a_{31}x_1' \oplus y_1' \oplus x_3'$. Two such x_2, x_2' exist with probability $\Omega(\binom{q}{2}/2^{2n})$. As the adversary needs to succeed for only one of the $q\binom{q}{2}$ choices of x_1, y_3, x_1', he finds a collision for F_A with probability $\Omega(q^5/2^{2n})$. □

Next, the compression functions evolved from Lem. 1 are analyzed with respect to the attacks of Lem. 2. Before proceeding, we remark that for the multi-permutation setting, the following reductions apply to the compression function classes evolved from Lem. 1. We refer to these reductions as the "M- and N-reduction".

M-reduction: Applying Prop. 1, and Prop. 3 on $i = 1$ corresponds to mutually swapping $\binom{a_{31}}{a_{41}} \leftrightarrow \binom{a_{32}}{a_{42}}$ and $\binom{a_{33}}{a_{43}} \leftrightarrow \binom{a_{34}}{a_{44}}$;

N-reduction: Prop. 4 reduces to swapping $\binom{a_{3j}}{a_{4j}} \leftrightarrow \binom{a_{3,j+2}}{a_{4,j+2}}$ for $j \in \{1, 2\}$.

We now continue evaluating the matrices A of the form (7), and consider the different values of $\|\mathbf{a}_{3,*}\|$.

$\|\mathbf{a}_{3,*}\| = 0$. The matrix is invalid and excluded by definition;

$\|\mathbf{a}_{3,*}\| = 1$. The matrix is vulnerable to the attack of Lem. 2(i);

$\|\mathbf{a}_{3,*}\| = 2$. The matrix contradicts either one of the requirements of Lem. 2. Technically, if $(a_{31} + a_{33})(a_{32} + a_{34}) = 0$ it violates Lem. 2(i), and otherwise the values $a_{41}, \ldots, a_{44}$ will violate either the requirement of Lem. 2(ii) or of Lem. 2(iii);

$\|\mathbf{a}_{3,*}\| = 3$. Due to M- and N-reductions, it suffices to consider $a_{31}a_{32}a_{33}a_{34} = 1110$, and consequently $a_{44} = 1$ by Lem. 2(ii). Lemma 2(iii) now states that we require $a_{41} = a_{43}$, which gives the following four options for $a_{41}a_{42}a_{43}$: 000, 010, 101 and 111. The first one is vulnerable to the attack of Lem. 2(iv), and the fourth matrix is equivalent to the second (by consequently applying Prop. 2 on $(c_0, c_1) = (1, 1)$, and Prop. 3 for $i = 2$). We are left with A_1 and A_2 of (5):

$$\mathrm{A}_1 = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 & 1 \end{array}\right), \qquad \mathrm{A}_2 = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 1 & 1 \end{array}\right);$$

$\|\mathbf{a}_{3,*}\| = 4$. Due to M- and N-reductions, it suffices to consider $a_{41}a_{42}a_{43}a_{44} \in \{0000, 1000, 1010, 1100, 1110, 1111\}$. The cases 1000 and 1100 are vulnerable to the attacks of Lems. 2(iv) and 2(iii), respectively. For the cases 0000 and 1111, finding collisions is as hard as finding collisions for $\mathsf{F}(x_1, x_2) = x_1 \oplus x_2 \oplus \pi_1(x_1) \oplus \pi_2(x_2)$ (for which collisions are found in at most $2^{n/3}$ queries, due to Stam's bound [12, 13]). We are left with A_3 and A_4 of (5):

$$\mathrm{A}_3 = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 \end{array}\right), \qquad \mathrm{A}_4 = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 & 1 \end{array}\right).$$

It remains to analyze collision and preimage security of the four compression functions defined by the matrices of (5), which is done in the following lemma. Particularly, Lem. 3 completes the proof of Thm. 1.

Lemma 3. *Let $\varepsilon > 0$. Then:*

(i) $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_k}}(2^{n/2(1-\varepsilon)}) = 0$ *for* $k = 1, 2, 3, 4$*;*

(ii) $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_2}}(2^{2n/3(1-\varepsilon)}) = 0$*, and* $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_k}}(q) = \Theta(q^2/2^n)$ *for* $k = 1, 3, 4$.

Proof. Part (i) is proven in App. A, part (ii) in App. B. □

5 Main Result for Single-Permutation Setting

In a similar fashion as in Sect. 4, we analyze the security of compression functions based on three calls to the same permutations, the single-permutation setting. It turns out that *there does not exist any* compression function of the form (3) that achieves optimal collision resistance. We note that this result does not rely on Conj. 1. In App. C we show how the results of this section can be generalized to cover any single-permutation compression function where additional affine transformations on the permutation inputs are taken into account.

Theorem 2. *Consider the single-permutation setting, where* $\pi_1 = \pi_2 = \pi_3 =: \pi$*. Any compression function* F_A *defined by a binary matrix* A *of the form (2) satisfies* $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_\mathrm{A}}(q) = \Omega(q^5/2^{2n})$.

Proof. The proof of Thm. 2 is similar to the proof of Thm. 1, and we highlight the differences. Lemmas 1 and 2 still apply, and additionally the M-reduction also holds in the single-permutation setting. Notice that the N-reduction *does not hold* as it incorporates Prop. 4. Similar to before, we will evaluate the matrices A of the form (7). The case $\|\mathbf{a}_{3,*}\| \leq 2$ is the same as before.

$\|\mathbf{a}_{3,*}\| = 3$. Due to M-reductions, it suffices to consider $a_{31}a_{32}a_{33}a_{34} \in \{1110, 0111\}$.
- $a_{31}a_{32}a_{33}a_{34} = 1110$. The same analysis as in Sect. 4.1 applies, leaving the matrices A_1 and A_2 of (5). In the single-permutation setting, the two corresponding compression functions satisfy $\mathsf{F}_{\mathrm{A}_1}(x_1, \pi(x_1)) = \pi^2(x_1)$ and $\mathsf{F}_{\mathrm{A}_2}(x_1, x_2) = \mathsf{F}_{\mathrm{A}_2}(x_1, x_1 \oplus x_2 \oplus \pi(x_1))$ for any x_1, x_2. Collisions can thus be trivially found;
- $a_{31}a_{32}a_{33}a_{34} = 0111$. By Lem. 2(ii), we have $a_{41} = 1$. Lemma 2(iii) now states that we require $a_{42} = a_{44}$, which gives the following four options for $a_{42}a_{43}a_{44}$: 000, 010, 101 and 111. The first one is vulnerable to the attack of Lem. 2(iv), the second, third and fourth matrix satisfy $\mathsf{F}_\mathrm{A}(x_1, x_1) = x_1$, $\mathsf{F}_\mathrm{A}(x_1, x_1) = 0$ and $\mathsf{F}_\mathrm{A}(x_1, x_1) = \pi(x_1)$, respectively, for any x_1. Collisions can thus be trivially found;

$\|\mathbf{a}_{3,*}\| = 4$. Except for $a_{41}a_{42}a_{43}a_{44} \in \{1010, 1001, 0110, 0101\}$, all induced compression functions satisfy $\mathsf{F}_\mathrm{A}(x_1, x_1) \oplus \pi(0) \in \{0, x_1, \pi(x_1)\}$ for any x_1, for which collisions can be trivially found. The cases $1001, 0110$ are vulnerable to Lem. 2(iii). The remaining two cases, which are equivalent by M-reduction, allow for trivial collisions as well: the compression function induced by $(a_{41}a_{42}a_{43}a_{44}) = (1010)$ satisfies $\mathsf{F}_\mathrm{A}(x_1, \pi^{-1}(x_1 \oplus \pi(x_1))) = 0$ for any x_1 (cf. [9]).

Hence, the analyzed compression functions either allow for trivial collision or are vulnerable to Lem. 2, therewith allowing for collisions in at most $2^{2n/5}$ queries. □

Concluding, for any compression function F_A of the form (3), where the three permutations are equal to one single permutation π, collisions can be found in at most $2^{2n/5}$ queries, hence considerably faster than in $2^{n/2}$ queries.

6 Conclusions

We provided a full security classification of $2n$-to-n-bit compression functions that are solely built of XOR-operators and of three permutations. Therewith, we have analyzed compression functions that are not included in the analysis of Rogaway and Steinberger [9], but yet are interesting because of their elegance (they only employ XOR-operators) and efficiency (XOR-operators are slightly cheaper than finite field multiplications by constants). For any of the 2^{15} compression functions of the described form, we either provide a formal collision and preimage security proof or a collision attack more efficient than the birthday bound.

For the multi-permutation setting, where the three permutations are different, there are exactly four equivalence classes of functions that allow for optimal collision resistance, one class of which the compression functions achieve optimal preimage resistance w.r.t. the bounds of [10]. A summary of these results is given in Table 1. Regarding the absolute number of collision/preimage secure compression functions, by ways of an extensive computation one finds 96 functions equivalent to $\mathsf{F}_{\mathrm{A}_1}$ (including the $\mathsf{F}_{\mathrm{A}_1}$ itself), 48 functions in each of the classes defined by $\mathsf{F}_{\mathrm{A}_2}$ and $\mathsf{F}_{\mathrm{A}_4}$, and 24 functions equivalent to $\mathsf{F}_{\mathrm{A}_3}$. In total, we have thus proven 216 compression functions optimally collision secure, 48 of which we have proven optimally preimage secure. A small part of the results for the multi-permutation setting relies on an extremal graph theory based conjecture, Conj. 1, which we supported by an extensive and detailed heuristic. We leave the full analysis of Conj. 1 as an open problem.

For the single-permutation setting, where the three permutations are the same, we show that it is not possible to construct a $2n$-to-n-bit compression function that achieves optimal collision resistance. In light of the amount of optimally secure compression functions we have found in the multi-permutation setting, this observation is not as expected. This negative result casts doubts over the existence of any (larger) permutation-based XOR-based compression function built on (multiple invocations of) one single permutation. We leave this question as an open problem.

The results in this work are derived in the permutation setting. Different results may be obtained if we consider three underlying primitives to be one-way functions: in particular, the π-inverse-reduction (Prop. 4) and Lem. 2 rely on the invertibility of these primitives. Further research questions include the applicability of the approach followed in this work to different classes of compression functions, for instance with larger domain and range, with more permutations or random functions instead, or defined over different fields.

Acknowledgments. This work has been funded in part by the IAP Program P6/26 BCRYPT of the Belgian State (Belgian Science Policy), in part by the European Commission through the ICT program under contract ICT-2007-216676 ECRYPT II, and in part by the Research Council K.U.Leuven: GOA TENSE. The first author is supported by a Ph.D. Fellowship from the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

References

[1] Black, J., Cochran, M., Shrimpton, T.: On the impossibility of highly-efficient blockcipher-based hash functions. In: Advances in Cryptology - EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494, pp. 526–541. Springer-Verlag, Berlin (2005)

[2] Bollobás, B.: Extremal Graph Theory. Academic Press (1978)

[3] Hirose, S.: Some plausible constructions of double-block-length hash functions. In: Fast Software Encryption '06. Lecture Notes in Computer Science, vol. 4047, pp. 210–225. Springer-Verlag, Berlin (2006)

[4] Lai, X., Massey, J.: Hash function based on block ciphers. In: Advances in Cryptology - EUROCRYPT '92. Lecture Notes in Computer Science, vol. 658, pp. 55–70. Springer-Verlag, Berlin (1992)

[5] Lee, J., Kwon, D.: Security of single-permutation-based compression functions. Cryptology ePrint Archive, Report 2009/145 (2009)

[6] Preneel, B., Govaerts, R., Vandewalle, J.: Hash functions based on block ciphers: A synthetic approach. In: Advances in Cryptology - CRYPTO '93. Lecture Notes in Computer Science, vol. 773, pp. 368–378. Springer-Verlag, Berlin (1993)

[7] Rabin, M.: Digitalized signatures. In: Foundations of Secure Computation '78. pp. 155–166. Academic Press, New York (1978)

[8] Rogaway, P., Shrimpton, T.: Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In: Fast Software Encryption 2004. Lecture Notes in Computer Science, vol. 3017, pp. 371–388. Springer-Verlag, Berlin (2004)

[9] Rogaway, P., Steinberger, J.: Constructing cryptographic hash functions from fixed-key blockciphers. In: Advances in Cryptology - CRYPTO 2008. Lecture Notes in Computer Science, vol. 5157, pp. 433–450. Springer-Verlag, Berlin (2008)
[10] Rogaway, P., Steinberger, J.: Security/efficiency tradeoffs for permutation-based hashing. In: Advances in Cryptology - EUROCRYPT 2008. Lecture Notes in Computer Science, vol. 4965, pp. 220–236. Springer-Verlag, Berlin (2008)
[11] Shrimpton, T., Stam, M.: Building a collision-resistant compression function from non-compressing primitives. In: International Colloquium on Automata, Languages and Programming - ICALP (2) 2008. Lecture Notes in Computer Science, vol. 5126, pp. 643–654. Springer-Verlag, Berlin (2008)
[12] Stam, M.: Beyond uniformity: Better security/efficiency tradeoffs for compression functions. In: Advances in Cryptology - CRYPTO 2008. Lecture Notes in Computer Science, vol. 5157, pp. 397–412. Springer-Verlag, Berlin (2008)
[13] Steinberger, J.: Stam's collision resistance conjecture. In: Advances in Cryptology - EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 597–615. Springer-Verlag, Berlin (2010)

A Proof of Lemma 3(i)

For $\mathsf{F}_{\mathrm{A}_k}$ $(k = 1, \ldots, 4)$, where the matrices A_k are given in (5), the goal is to prove that $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_k}}(2^{n/2(1-\varepsilon)}) = 0$ for any $\varepsilon > 0$, demonstrating the asymptotic collision security of $\mathsf{F}_{\mathrm{A}_k}$. In the remainder of this section, π_1, π_2, π_3 are assumed to be three permutations taken uniformly at random from P_n.

The approach followed in this proof is as follows: finding a collision for a function F_{A}, with A of the form (7), corresponds to obtaining query pairs $(x_1, y_1), (x'_1, y'_1)$ for π_1, $(x_2, y_2), (x'_2, y'_2)$ for π_2, and $(x_3, y_3), (x'_3, y'_3)$ for π_3 in the query history, such that:

$$(x_1, x_2) \neq (x'_1, x'_2)\,, \tag{9a}$$
$$a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}y_1 \oplus a_{34}y_2 = x_3\,, \tag{9b}$$
$$a_{31}x'_1 \oplus a_{32}x'_2 \oplus a_{33}y'_1 \oplus a_{34}y'_2 = x'_3\,, \tag{9c}$$
$$a_{41}x_1 \oplus a_{42}x_2 \oplus a_{43}y_1 \oplus a_{44}y_2 \oplus y_3 = a_{41}x'_1 \oplus a_{42}x'_2 \oplus a_{43}y'_1 \oplus a_{44}y'_2 \oplus y'_3 \tag{9d}$$

(recall that the adversary is required to make the correct queries in order to form the collision). We will analyze the maximum probability of any adversary, making at most q queries to his oracles, in breaking (9), which equals $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q)$ by definition. Denote by $\mathcal{Q}_i$ for $i = 1, \ldots, q$ the first i queries of the query history $\mathcal{Q}_q$. To bound $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q)$, we distinguish among the possibilities that $x_j = x'_j$ (for $j = 1, 2, 3$). Formally, we obtain

$$\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}}}(q) \leq \sum_{c_1,c_2,c_3\in\{0,1\}} \mathbf{Pr}\Big(\text{ solution for (9) } \bigwedge x_j = x'_j \Longleftrightarrow c_j = 1\ (j = 1, 2, 3)\Big)\,. \tag{10}$$

Returning to the four compression functions $\mathsf{F}_{\mathrm{A}_k}$ $(k \in \{1, 2, 3, 4\})$, this leaves 32 cases to be evaluated, but for some choices of $c_1c_2c_3$ the probability on the right hand side of (10) equals 0. Starting with $\mathsf{F}_{\mathrm{A}_1}$, the cases $c_1c_2c_3 \in \{110, 111\}$ violate (9a), the case 010 would give contradiction for (9d), and 101 would give a contradiction in lines (9b-9c). On the other side, the case $c_1c_2c_3 = 000$ corresponds to $\mathsf{E}_1(\mathcal{Q}_q)$ of Fig. 3, and similarly the cases $001, 011$, and 100 correspond to events $\mathsf{E}_5(\mathcal{Q}_q), \mathsf{E}_9(\mathcal{Q}_q), \mathsf{E}_{10}(\mathcal{Q}_q)$ of Fig. 3, respectively. A similar analysis can be applied to $\mathsf{F}_{\mathrm{A}_2}, \mathsf{F}_{\mathrm{A}_3}, \mathsf{F}_{\mathrm{A}_4}$ to obtain the results of Table 2. In general, the following holds for $\mathsf{F}_{\mathrm{A}_k}$, where $k \in \{1, 2, 3, 4\}$:

$$\text{collision for } \mathsf{F}_{\mathrm{A}_1} \Longrightarrow \mathsf{E}_1(\mathcal{Q}_q) \vee \mathsf{E}_5(\mathcal{Q}_q) \vee \mathsf{E}_9(\mathcal{Q}_q) \vee \mathsf{E}_{10}(\mathcal{Q}_q)\,, \tag{11a}$$
$$\text{collision for } \mathsf{F}_{\mathrm{A}_2} \Longrightarrow \mathsf{E}_2(\mathcal{Q}_q) \vee \mathsf{E}_5(\mathcal{Q}_q) \vee \mathsf{E}_7(\mathcal{Q}_q) \vee \mathsf{E}_9(\mathcal{Q}_q) \vee \mathsf{E}_{11}(\mathcal{Q}_q)\,, \tag{11b}$$
$$\text{collision for } \mathsf{F}_{\mathrm{A}_3} \Longrightarrow \mathsf{E}_3(\mathcal{Q}_q) \vee \mathsf{E}_6(\mathcal{Q}_q) \vee \mathsf{E}_8(\mathcal{Q}_q) \vee \mathsf{E}_9(\mathcal{Q}_q) \vee \mathsf{E}_{13}(\mathcal{Q}_q)\,, \tag{11c}$$
$$\text{collision for } \mathsf{F}_{\mathrm{A}_4} \Longrightarrow \mathsf{E}_4(\mathcal{Q}_q) \vee \mathsf{E}_8(\mathcal{Q}_q) \vee \mathsf{E}_9(\mathcal{Q}_q) \vee \mathsf{E}_{12}(\mathcal{Q}_q)\,. \tag{11d}$$

Table 2. A case distinction for the analysis of (10) for $\mathsf{F}_{\mathrm{A}_k}$ ($k \in \{1,2,3,4\}$), where each column corresponds to a particular choice of $c_1c_2c_3$. In case of ✗, the choice $c_1c_2c_3$ renders violation of one or more equations of (9), otherwise the case corresponds to event $\mathsf{E}_l(\mathcal{Q}_q)$ ($l \in \{1,\ldots,13\}$) given in Fig. 3.

$c_1c_2c_3$	000	001	010	011	100	101	110	111
$\mathsf{F}_{\mathrm{A}_1}$	$\mathsf{E}_1(\mathcal{Q}_q)$	$\mathsf{E}_5(\mathcal{Q}_q)$	✗ (9d)	$\mathsf{E}_9(\mathcal{Q}_q)$	$\mathsf{E}_{10}(\mathcal{Q}_q)$	✗ (9b-9c)	✗ (9a)	✗ (9a)
$\mathsf{F}_{\mathrm{A}_2}$	$\mathsf{E}_2(\mathcal{Q}_q)$	$\mathsf{E}_5(\mathcal{Q}_q)$	$\mathsf{E}_7(\mathcal{Q}_q)$	$\mathsf{E}_9(\mathcal{Q}_q)$	$\mathsf{E}_{11}(\mathcal{Q}_q)$	✗ (9b-9c)	✗ (9a)	✗ (9a)
$\mathsf{F}_{\mathrm{A}_3}$	$\mathsf{E}_3(\mathcal{Q}_q)$	$\mathsf{E}_6(\mathcal{Q}_q)$	$\mathsf{E}_8(\mathcal{Q}_q)$	$\mathsf{E}_9(\mathcal{Q}_q)$	✗ (9d)	$\mathsf{E}_{13}(\mathcal{Q}_q)$	✗ (9a)	✗ (9a)
$\mathsf{F}_{\mathrm{A}_4}$	$\mathsf{E}_4(\mathcal{Q}_q)$	✗ (9b-9d)	$\mathsf{E}_8(\mathcal{Q}_q)$	$\mathsf{E}_9(\mathcal{Q}_q)$	$\mathsf{E}_{12}(\mathcal{Q}_q)$	✗ (9d)	✗ (9a)	✗ (9a)

Here, the events $\mathsf{E}_l(\mathcal{Q}_q)$ ($l \in \{1,\ldots,13\}$) are given in Fig. 3. Thus, it remains to analyze the probabilities of the events $\mathsf{E}_l(\mathcal{Q}_q)$ to occur, but we will analyze these under the condition that the previous query did not result in success, and some additional condition $\mathsf{C}(\mathcal{Q}_q) = \mathsf{C}_{1\vee\ldots\vee 4}(\mathcal{Q}_q)$, where the claims $\mathsf{C}_1(\mathcal{Q}_q),\ldots,\mathsf{C}_4(\mathcal{Q}_q)$ are given in Fig. 4:

$$\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q)\right) \le \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q) \mid \neg\mathsf{E}_l(\mathcal{Q}_{q-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_q)\right) + \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_{q-1}) \vee \mathsf{C}(\mathcal{Q}_q)\right).$$

Similarly, the second probability of this bound can be split up further:

$$\begin{aligned}\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_{q-1}) \vee \mathsf{C}(\mathcal{Q}_q)\right) \le\ & \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_{q-1}) \mid \neg\mathsf{E}_l(\mathcal{Q}_{q-2}) \wedge \neg\mathsf{C}(\mathcal{Q}_{q-1})\right) + \\ & \mathbf{Pr}\left(\mathsf{C}(\mathcal{Q}_q) \wedge \neg\mathsf{C}(\mathcal{Q}_{q-1})\right) + \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_{q-2}) \vee \mathsf{C}(\mathcal{Q}_{q-1})\right).\end{aligned}$$

Applying this trick q times eventually gives the following probability bound on $\mathsf{E}_l(\mathcal{Q}_q)$:

$$\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q)\right) \le \sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_i) \mid \neg\mathsf{E}_l(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) + \sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{C}(\mathcal{Q}_i) \wedge \neg\mathsf{C}(\mathcal{Q}_{i-1})\right). \quad (12)$$

The remainder of the section is now divided as follows. In App. A.1, we will bound the conditioned events $\mathsf{E}_l(\mathcal{Q}_q)$ to occur for $l \in \{1,\ldots,13\}$ (first sum of (12)). Then, in App. A.2, a bound on the occurrence of $\mathsf{C}(\mathcal{Q}_q)$ is computed (second sum of (12)). The results are assembled in App. A.3, to prove Lem. 3(i).

A.1 Bounding Occurrence of Conditioned $\mathsf{E}_l(\mathcal{Q}_q)$, $l = 1,\ldots,13$

In this section, we bound the conditioned events $\mathsf{E}_l(\mathcal{Q}_q)$ (for $l = 1,\ldots,13$) to occur, more specifically the first sum of (12). The cases $l = 1,2,3,4$ are found in Lems. 4-7, respectively. The cases $l = 10,11,12$ are found in Lem. 8, and the remaining cases in Lem. 9.

Let d_1 be the constant defined in Conj. 1. On input of parameters (q,n), we define $\varepsilon_{\mathsf{c}}(q,n) = \mathbf{Pr}\left(\beta > d_1 q \log q\right)$ of Conj. 1. This quantity tends to 0 for $n \to \infty$ and for $q < 2^{n/2}$. In the remainder of this work, we define $q_1 = d_1 q \log q$. We will also consider Conj. 1 on inputs (q_1,n) and $(K_2 q,n)$, where K_2 is a parameter used in Fig. 4.

Lemma 4. $\displaystyle\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_1(\mathcal{Q}_i) \mid \neg\mathsf{E}_1(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) \le \frac{K_2 q_1^2 \log q_1}{2^n - q} + 2\varepsilon_{\mathsf{c}}(q,n) + \varepsilon_{\mathsf{c}}(q_1,n).$

Proof. We write $\mathsf{E}_1\mathsf{a}, \mathsf{E}_1\mathsf{b}$ and $\mathsf{E}_1\mathsf{c}$ for the three equations of $\mathsf{E}_1(\mathcal{Q})$ (Fig. 3). We first bound the success probability of the i^{th} query ($i = 1,\ldots,q$), and then we sum over all values of i.

Assume first the adversary makes a query $x_3^{(i)} \to y_3^{(i)} = \pi_3(x_3^{(i)})$ for $i = 1,\ldots,q$ (the same treatment holds for queries $x_3' \to y_3'$, $x_2 \to y_2$ or $x_2' \to y_2'$). By Conj. 1, there exist at most q_1 tuples $(x_1',y_1'),(x_2',y_2'),(x_3',y_3')$ such that $\mathsf{E}_1\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q,n)$. Denote

$\mathsf{E}_1(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_2 \neq x'_2, x_3 \neq x'_3,$
$x_1 \oplus y_1 \oplus x_2 = x_3,$
$x'_1 \oplus y'_1 \oplus x'_2 = x'_3,$
$x_2 \oplus y_2 \oplus y_3 = x'_2 \oplus y'_2 \oplus y'_3.$

$\mathsf{E}_2(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_2 \neq x'_2, x_3 \neq x'_3,$
$x_1 \oplus y_1 \oplus x_2 = x_3,$
$x'_1 \oplus y'_1 \oplus x'_2 = x'_3,$
$x_1 \oplus y_1 \oplus y_2 \oplus y_3 = x'_1 \oplus y'_1 \oplus y'_2 \oplus y'_3.$

$\mathsf{E}_3(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_2 \neq x'_2, x_3 \neq x'_3,$
$x_1 \oplus y_1 \oplus x_2 \oplus y_2 = x_3,$
$x'_1 \oplus y'_1 \oplus x'_2 \oplus y'_2 = x'_3,$
$x_1 \oplus y_1 \oplus y_3 = x'_1 \oplus y'_1 \oplus y'_3.$

$\mathsf{E}_4(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_2 \neq x'_2, x_3 \neq x'_3,$
$x_1 \oplus y_1 \oplus x_2 \oplus y_2 = x_3,$
$x'_1 \oplus y'_1 \oplus x'_2 \oplus y'_2 = x'_3,$
$x_1 \oplus y_1 \oplus x_2 \oplus y_3 = x'_1 \oplus y'_1 \oplus x'_2 \oplus y'_3.$

$\mathsf{E}_5(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),(x'_2,y'_2) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_2 \neq x'_2,$
$x_1 \oplus y_1 \oplus x_2 = x'_1 \oplus y'_1 \oplus x'_2,$
$x_2 \oplus y_2 = x'_2 \oplus y'_2.$

$\mathsf{E}_6(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),(x'_2,y'_2) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_2 \neq x'_2,$
$x_1 \oplus y_1 = x'_1 \oplus y'_1,$
$x_2 \oplus y_2 = x'_2 \oplus y'_2.$

$\mathsf{E}_7(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_3 \neq x'_3,$
$x_1 \oplus y_1 \oplus x_3 = x'_1 \oplus y'_1 \oplus x'_3,$
$x_3 \oplus y_3 = x'_3 \oplus y'_3.$

$\mathsf{E}_8(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1),(x_2,y_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1, x_3 \neq x'_3,$
$x_1 \oplus y_1 \oplus x_3 = x'_1 \oplus y'_1 \oplus x'_3 = x_2 \oplus y_2,$
$x_3 \oplus y_3 = x'_3 \oplus y'_3.$

$\mathsf{E}_9(\mathcal{Q})$: $(x_1,y_1),(x'_1,y'_1) \in \mathcal{Q}$ **s.t.**
$x_1 \neq x'_1,$
$x_1 \oplus y_1 = x'_1 \oplus y'_1.$

$\mathsf{E}_{10}(\mathcal{Q})$: $(x_1,y_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_2 \neq x'_2, x_3 \neq x'_3,$
$x_2 \oplus x_3 = x'_2 \oplus x'_3 = x_1 \oplus y_1,$
$x_2 \oplus y_2 \oplus y_3 = x'_2 \oplus y'_2 \oplus y'_3.$

$\mathsf{E}_{11}(\mathcal{Q})$: $(x_1,y_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_2 \neq x'_2, x_3 \neq x'_3,$
$x_2 \oplus x_3 = x'_2 \oplus x'_3 = x_1 \oplus y_1,$
$y_2 \oplus y_3 = y'_2 \oplus y'_3.$

$\mathsf{E}_{12}(\mathcal{Q})$: $(x_1,y_1),(x_2,y_2),(x'_2,y'_2),$
$(x_3,y_3),(x'_3,y'_3) \in \mathcal{Q}$ **s.t.**
$x_2 \neq x'_2, x_3 \neq x'_3,$
$x_2 \oplus y_2 \oplus x_3 = x'_2 \oplus y'_2 \oplus x'_3 = x_1 \oplus y_1,$
$x_2 \oplus y_3 = x'_2 \oplus y'_3.$

$\mathsf{E}_{13}(\mathcal{Q})$: $(x_2,y_2),(x'_2,y'_2) \in \mathcal{Q}$ **s.t.**
$x_2 \neq x'_2,$
$x_2 \oplus y_2 = x'_2 \oplus y'_2.$

Fig. 3. The events $\mathsf{E}_l(\mathcal{Q})$ ($l \in \{1,\ldots,13\}$) employed in the proof of Lem. 3(i) (App. A). $\mathcal{Q}$ is a query history.

L_i to be the number of tuples $(x_1,y_1),(x_2,y_2)$ that make equation $\mathsf{E}_1\mathsf{a}$ satisfied for $x_3^{(i)}$. For any of the tuples satisfying $\mathsf{E}_1\mathsf{b}$, and any of the tuples satisfying $\mathsf{E}_1\mathsf{a}$, equation $\mathsf{E}_1\mathsf{c}$ is satisfied with probability at most $1/(2^n-q)$. Considering all queries $x_3 \rightarrow y_3$, the adversary succeeds in breaking $\mathsf{E}_1(\mathcal{Q}_q)$ with probability at most $\sum_{i=1}^{q} \frac{L_i q_1}{2^n-q} + \varepsilon_{\mathsf{c}}(q,n)$. Notice that by Conj. 1, $\sum_{i=1}^{q} L_i \leq q_1$, except w.p. at most $\varepsilon_{\mathsf{c}}(q,n)$. We thus obtain upper bound $\frac{q_1^2}{2^n-q} + 2\varepsilon_{\mathsf{c}}(q,n)$.

Assume the adversary makes a query $y_2^{(i)} \rightarrow x_2^{(i)} = \pi_2^{-1}(y_2^{(i)})$ for $i = 1,\ldots,q$ (the same treatment holds for query $y'_2 \rightarrow x'_2$). By Conj. 1, there exist at most q_1 tuples $(x'_1,y'_1),(x'_2,y'_2)$, (x'_3,y'_3) such that $\mathsf{E}_1\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q,n)$. This consequently leads to at most q_1 possible values of $y_2^{(i)} \oplus x'_2 \oplus y'_2 \oplus y'_3$. For any of these values, by $\neg\mathsf{C}_2(\mathcal{Q}_i)$ there exist at most K_2 combinations of queries $(x_1,y_1),(x_3,y_3)$ such that $y_2^{(i)} \oplus x'_2 \oplus y'_2 \oplus y'_3 = x_1 \oplus y_1 \oplus x_3 \oplus y_3$. For any of these $K_2 q_1$ choices, the adversary breaks $\mathsf{E}_1(\mathcal{Q}_i)$ if $x_2^{(i)}$ hits

$\mathsf{C}_1(\mathcal{Q})$: **for some** c **there exist more than** K_1 **solutions in** $\mathcal{Q}$ **to one of the** 3 **equations:**

$$x_1 \oplus y_1 = c \qquad x_2 \oplus y_2 = c \qquad x_3 \oplus y_3 = c.$$

$\mathsf{C}_2(\mathcal{Q})$: **for some** c **there exist more than** K_2 **solutions in** $\mathcal{Q}$ **to one of the** 3 **equations:**

$$x_1 \oplus y_1 \oplus x_2 \oplus y_2 = c \qquad x_1 \oplus y_1 \oplus x_3 \oplus y_3 = c \qquad x_2 \oplus y_2 \oplus x_3 \oplus y_3 = c.$$

$\mathsf{C}_3(\mathcal{Q})$: **there exist more than** $K_2 q$ **solutions in** $\mathcal{Q}$ **to one of the** 3 **equations:**

$$x_1 \oplus y_1 \oplus x_2 \oplus y_2 = x_3 \qquad x_1 \oplus y_1 \oplus x_3 \oplus y_3 = x_2 \qquad x_2 \oplus y_2 \oplus x_3 \oplus y_3 = x_1.$$

$\mathsf{C}_4(\mathcal{Q})$: **there exist more than** $q-1$ **solutions in** $\mathcal{Q}$ **to one of the** 3 **equations:**

$x_2 \neq x_2',\ x_3 \neq x_3'$**, and** $x_2 \oplus x_3 = x_2' \oplus x_3'$**, and** $y_2 \oplus y_3 = y_2' \oplus y_3'$

$x_2 \neq x_2',\ x_3 \neq x_3'$**, and** $x_2 \oplus x_3 = x_2' \oplus x_3'$**, and** $x_2 \oplus y_2 \oplus y_3 = x_2' \oplus y_2' \oplus y_3'$

$x_2 \neq x_2',\ x_3 \neq x_3'$**, and** $x_2 \oplus y_3 = x_2' \oplus y_3'$**, and** $x_2 \oplus y_2 \oplus x_3 = x_2' \oplus y_2' \oplus x_3'$.

Fig. 4. The claims $\mathsf{C}_1(\mathcal{Q}), \ldots, \mathsf{C}_4(\mathcal{Q})$ employed in the proof of Lem. 3(i) (App. A). We denote $\mathsf{C}(\mathcal{Q}) = \mathsf{C}_{1 \vee \ldots \vee 4}(\mathcal{Q})$. The parameters $K_1 \geq 1$, $K_2 > 1$ are any fixed constants. $\mathcal{Q}$ is a query history.

$y_2^{(i)} \oplus y_3 \oplus x_2' \oplus y_2' \oplus y_3' = x_1 \oplus y_1 \oplus x_3$, hence with probability at most $1/(2^n - q)$. Considering all queries $y_2 \to x_2$, the adversary succeeds with probability at most $\frac{K_2 q q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$.

Assume the adversary makes a query $y_3^{(i)} \to x_3^{(i)} = \pi_3^{-1}(y_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for query $y_3' \to x_3'$). By Conj. 1, there exist at most q_1 tuples $(x_1', y_1'), (x_2', y_2'), (x_3', y_3')$ such that $\mathsf{E}_1\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. This consequently leads to at most q_1 possible values of $x_2' \oplus y_2' \oplus y_3'$. Denote L_i to be the number of choices $(x_2, y_2), x_2' \oplus y_2' \oplus y_3'$ that make equation $\mathsf{E}_1\mathsf{c}$ satisfied for $y_3^{(i)}$. For any of these L_i tuples, equation $\mathsf{E}_1\mathsf{a}$ is satisfied with probability at most $q/(2^n - q)$. Considering all queries $y_3 \to x_3$, the adversary succeeds in breaking $\mathsf{E}_1(\mathcal{Q}_q)$ with probability at most $\sum_{i=1}^{q} \frac{L_i q}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$. Notice that by Conj. 1, $\sum_{i=1}^{q} L_i \leq d_1 q_1 \log q_1$, except w.p. at most $\varepsilon_{\mathsf{c}}(q_1, n)$.[1] We thus obtain upper bound $\frac{d_1 q q_1 \log q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n) + \varepsilon_{\mathsf{c}}(q_1, n)$.

Assume the adversary makes a query $x_1^{(i)} \to y_1^{(i)} = \pi_1(x_1^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_1 \to x_1$, $x_1' \to y_1'$ or $y_1' \to x_1'$). By Conj. 1, there exist at most q_1 tuples $(x_1', y_1'), (x_2', y_2'), (x_3', y_3')$ such that $\mathsf{E}_1\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. This consequently leads to at most q_1 possible values of $x_2' \oplus y_2' \oplus y_3'$. Again by Conj. 1, there exist at most $d_1 q_1 \log q_1$ combinations of queries $(x_1', y_1'), (x_2', y_2'), (x_3', y_3'), (x_2, y_2), (x_3, y_3)$ such that $\mathsf{E}_1\mathsf{c}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q_1, n)$. For any of these combinations, the adversary breaks $\mathsf{E}_1(\mathcal{Q}_q)$ if $y_1^{(i)}$ hits $x_1^{(i)} \oplus x_2 \oplus x_3$, hence with probability at most $1/(2^n - q)$. Considering all queries $x_1 \to y_1$, the adversary succeeds with probability at most $\frac{d_1 q q_1 \log q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n) + \varepsilon_{\mathsf{c}}(q_1, n)$.

In any case, the success probability is at most $\frac{K_2 q_1^2 \log q_1}{2^n - q} + 2\varepsilon_{\mathsf{c}}(q, n) + \varepsilon_{\mathsf{c}}(q_1, n)$. □

Lemma 5. $\displaystyle\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_2(\mathcal{Q}_i) \mid \neg\mathsf{E}_2(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) \leq \frac{K_2 q_1^2 \log q_1}{2^n - q} + 2\varepsilon_{\mathsf{c}}(q, n) + \varepsilon_{\mathsf{c}}(q_1, n).$

Proof. We write $\mathsf{E}_2\mathsf{a}, \mathsf{E}_2\mathsf{b}$ and $\mathsf{E}_2\mathsf{c}$ for the three equations of $\mathsf{E}_2(\mathcal{Q})$ (Fig. 3). The approach is similar as before.

Assume first the adversary makes a query $x_3^{(i)} \to y_3^{(i)} = \pi_3(x_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $x_3' \to y_3'$, $x_2 \to y_2$ or $x_2' \to y_2'$). By Conj. 1, there exist at most q_1

[1] Here, Z (the values $x_2 \oplus y_2$) is a set of q random elements, and the adversary is challenged to find two sets, one of size q (the values x_3) and one of size at most q_1 (the values $x_2' \oplus y_2' \oplus y_3'$), to maximize the number of matches. The success probability for this is upper bounded by the success probability in breaking this problem if all sets are of size q_1. Then, we can apply Conj. 1 on (q_1, n).

tuples $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3)$ such that $\mathsf{E}_2\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. Denote L_i to be the number of tuples $(x_1, y_1), (x_2, y_2)$ that make equation $\mathsf{E}_2\mathsf{a}$ satisfied for $x_3^{(i)}$. For any of the tuples satisfying $\mathsf{E}_2\mathsf{b}$, and any of the tuples satisfying $\mathsf{E}_2\mathsf{a}$, equation $\mathsf{E}_2\mathsf{c}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_3 \to y_3$, the adversary succeeds in breaking $\mathsf{E}_2(\mathcal{Q}_q)$ with probability at most $\sum_{i=1}^{q} \frac{L_i q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$. Notice that by Conj. 1, $\sum_{i=1}^{q} L_i \leq q_1$, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. We thus obtain upper bound $\frac{q_1^2}{2^n - q} + 2\varepsilon_{\mathsf{c}}(q, n)$.

Assume the adversary makes a query $y_3^{(i)} \to x_3^{(i)} = \pi_3^{-1}(y_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for query $y'_3 \to x'_3$, $y_2 \to x_2$ or $y'_2 \to x'_2$). By Conj. 1, there exist at most q_1 tuples $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3)$ such that $\mathsf{E}_2\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. This consequently leads to at most q_1 possible values of $y_3^{(i)} \oplus x'_1 \oplus y'_1 \oplus y'_2 \oplus y'_3$. Again by Conj. 1, there exist at most $d_1 q_1 \log q_1$ combinations of queries $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3), (x_1, y_1)$, (x_2, y_2) such that $\mathsf{E}_2\mathsf{c}$ is satisfied for $y_3^{(i)}$, except w.p. at most $\varepsilon_{\mathsf{c}}(q_1, n)$. For any of these combinations, the adversary breaks $\mathsf{E}_2(\mathcal{Q}_q)$ if $x_3^{(i)}$ hits $x_1 \oplus y_1 \oplus x_2$, hence with probability at most $1/(2^n - q)$. Considering all queries $y_3 \to x_3$, the adversary succeeds with probability at most $\frac{d_1 q q_1 \log q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n) + \varepsilon_{\mathsf{c}}(q_1, n)$.

Assume the adversary makes a query $x_1^{(i)} \to y_1^{(i)} = \pi_1(x_1^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_1 \to x_1$, $x'_1 \to y'_1$ or $y'_1 \to x'_1$). By Conj. 1, there exist at most q_1 tuples $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3)$ such that $\mathsf{E}_2\mathsf{b}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. This consequently leads to at most q_1 possible values of $x'_1 \oplus y'_1 \oplus y'_2 \oplus y'_3$. For any of these values, by $\neg\mathsf{C}_2(\mathcal{Q}_i)$ there exist at most K_2 combinations of queries $(x_2, y_2), (x_3, y_3)$ such that $x_2 \oplus y_2 \oplus x_3 \oplus y_3 = x'_1 \oplus y'_1 \oplus y'_2 \oplus y'_3$. For any of these $K_2 q_1$ choices, the adversary breaks $\mathsf{E}_2(\mathcal{Q}_i)$ if $y_1^{(i)}$ hits $x_1^{(i)} \oplus x_2 \oplus x_3$, hence with probability at most $1/(2^n - q)$. Considering all queries $x_1 \to y_1$, the adversary succeeds with probability at most $\frac{K_2 q q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$.

In any case, the success probability is at most $\frac{K_2 q_1^2 \log q_1}{2^n - q} + 2\varepsilon_{\mathsf{c}}(q, n) + \varepsilon_{\mathsf{c}}(q_1, n)$. □

Lemma 6. $\displaystyle\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_3(\mathcal{Q}_i) \mid \neg\mathsf{E}_3(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) \leq \frac{K_2^2 q^2}{2^n - q}.$

Proof. The case of $\mathsf{E}_3(\mathcal{Q}_q)$ is fairly similar to the case of $\mathsf{E}_2(\mathcal{Q}_q)$ (see Lem. 5), with the difference that the usage of Conj. 1 is replaced with $\neg\mathsf{C}_3(\mathcal{Q}_i)$. We write $\mathsf{E}_3\mathsf{a}, \mathsf{E}_3\mathsf{b}$ and $\mathsf{E}_3\mathsf{c}$ for the three equations of $\mathsf{E}_3(\mathcal{Q})$ (Fig. 3). The cases of queries $x_1, x'_1, y_1, y'_1, x_3$ and x'_3 are the same as before (notice that $\mathsf{E}_3\mathsf{a}$ and $\mathsf{E}_3\mathsf{b}$ can be substituted in $\mathsf{E}_3\mathsf{c}$), resulting in a success probability upper bounded by $\frac{K_2^2 q^2}{2^n - q}$.

Assume the adversary makes a query $x_2^{(i)} \to y_2^{(i)} = \pi_2(x_2^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_2 \to x_2$, $x'_2 \to y'_2$ or $y'_2 \to x'_2$). As $\neg\mathsf{C}_3(\mathcal{Q}_i)$, there exist at most $K_2 q$ tuples $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3)$ such that $\mathsf{E}_3\mathsf{b}$ is satisfied, and this consequently leads to at most $K_2 q$ possible values of $x'_2 \oplus y'_2 \oplus x'_3 \oplus y'_3$, which behave random. By a slight variant of $\neg\mathsf{C}_3(\mathcal{Q}_i)$ (as the previously mentioned values behave random), there exist at most $K_2^2 q$ combinations of queries $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3), (x_1, y_1), (x_3, y_3)$ such that $x_1 \oplus y_1 \oplus y_3 = x'_2 \oplus y'_2 \oplus x'_3 \oplus y'_3$. For any of these combinations, the adversary breaks $\mathsf{E}_3(\mathcal{Q}_q)$ if $y_2^{(i)}$ hits $x_1 \oplus y_1 \oplus x_2^{(i)} \oplus x_3$, hence with probability at most $1/(2^n - q)$. Considering all queries $x_2 \to y_2$, the adversary succeeds with probability at most $\frac{K_2^2 q^2}{2^n - q}$.

Assume the adversary makes a query $y_3^{(i)} \to x_3^{(i)} = \pi_3^{-1}(y_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for query $y'_3 \to x'_3$). As $\neg\mathsf{C}_3(\mathcal{Q}_i)$, there exist at most $K_2 q$ tuples $(x'_1, y'_1), (x'_2, y'_2), (x'_3, y'_3)$ such that $\mathsf{E}_3\mathsf{b}$ is satisfied, and this consequently leads to at most $K_2 q$ possible values of $x'_2 \oplus y'_2 \oplus x'_3 \oplus y'_3$. Denote L_i to be the number of choices $(x_1, y_1), x'_1 \oplus y'_1 \oplus y'_3$ that make equation $\mathsf{E}_3\mathsf{c}$ satisfied for $y_3^{(i)}$. For any of these tuples, equation $\mathsf{E}_3\mathsf{a}$ is satisfied

with probability at most $q/(2^n-q)$. Considering all queries $y_3 \to x_3$, the adversary succeeds in breaking $\mathsf{E}_3(\mathcal{Q}_q)$ with probability at most $\sum_{i=1}^{q} \frac{L_i q}{2^n-q}$. Notice that by a slight variant of $\neg\mathsf{C}_3(\mathcal{Q}_i)$, $\sum_{i=1}^{q} L_i \leq K_2^2 q$. We thus obtain upper bound $\frac{K_2^2 q^2}{2^n-q}$.

In any case, the success probability is at most $\frac{K_2^2 q^2}{2^n-q}$. □

The slight variant of $\mathsf{C}_3(\mathcal{Q}_i)$ employed in the proof of Lem. 6 embraces the case the adversary has i different tuples (x_1, y_1) and i different tuples (x_3, y_3), but (at most) $K_2 i$ different random values $z_2 = x_2' \oplus y_2' \oplus x_3' \oplus y_3'$, and aims at finding combinations such that $x_1 \oplus y_1 \oplus z_2 = x_3$ (or similar variants). Rather than introducing a separate claim for this, it suffices to condition for $\mathsf{E}_3(\mathcal{Q})$ on claim $\mathsf{C}(\mathcal{Q})$ where $K_2 q$ queries are allowed. This observation is used in Sect. A.3, where the results are assembled.

Lemma 7. $\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_4(\mathcal{Q}_i) \mid \neg\mathsf{E}_4(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) \leq \frac{d_1 K_2^2 q^2 \log(K_2 q)}{2^n - q} + \varepsilon_{\mathsf{c}}(K_2 q, n).$

Proof. The case of $\mathsf{E}_4(\mathcal{Q}_q)$ is fairly similar to the case of $\mathsf{E}_1(\mathcal{Q}_q)$ (see Lem. 4), with the difference that most of the usages of Conj. 1 are replaced with $\neg\mathsf{C}_3(\mathcal{Q}_i)$. We write $\mathsf{E}_4\mathsf{a}, \mathsf{E}_4\mathsf{b}$ and $\mathsf{E}_4\mathsf{c}$ for the three equations of $\mathsf{E}_4(\mathcal{Q})$ (Fig. 3). Note that equation $\mathsf{E}_4\mathsf{c}$ reduces to $y_2 \oplus x_3 \oplus y_3 = y_2' \oplus x_3' \oplus y_3'$ by substituting equations $\mathsf{E}_4\mathsf{a}, \mathsf{E}_4\mathsf{b}$. The cases of queries $x_1, x_1', y_1, y_1', x_3$ and x_3' are the same as before. For queries x_2, x_2', y_3 and y_3', one follows the same reasoning as for queries $y_2 \to x_2$ in the analysis of $\mathsf{E}_1(\mathcal{Q}_q)$, and for queries y_2, y_2' one follows the same reasoning as for $y_3 \to x_3$ in the analysis of $\mathsf{E}_1(\mathcal{Q}_q)$. Concretely, the success probability is at most $\frac{d_1 K_2^2 q^2 \log(K_2 q)}{2^n - q} + \varepsilon_{\mathsf{c}}(K_2 q, n)$. □

Lemma 8.

$$\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_i) \mid \neg\mathsf{E}_l(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) \leq \begin{cases} \frac{K_1 q q_1 + q^2}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n) \text{ for } l = 10, \\ \frac{q q_1 + q^2}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n) \text{ for } l = 11, \\ \frac{K_1 K_2 q^2 + q^2}{2^n - q} \text{ for } l = 12. \end{cases}$$

Proof. We start with $\mathsf{E}_{11}(\mathcal{Q}_q)$, and write $\mathsf{E}_{11}\mathsf{a}, \mathsf{E}_{11}\mathsf{b}$ for the two equations of $\mathsf{E}_{11}(\mathcal{Q})$ (Fig. 3). The approach is similar as before.

Assume first the adversary makes a query $x_3^{(i)} \to y_3^{(i)} = \pi_3(x_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $x_3' \to y_3'$, $x_2 \to y_2$ or $x_2' \to y_2'$). By Conj. 1, there exist at most q_1 tuples $(x_2', y_2'), (x_3', y_3'), (x_1, y_1)$ such that the second equality of $\mathsf{E}_{11}\mathsf{a}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. For any such choice, as $x_3^{(i)}$ is fixed there exists at most one (x_2, y_2) such that equation $\mathsf{E}_{11}\mathsf{a}$ is satisfied. For any of the combinations, $\mathsf{E}_{11}\mathsf{b}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_3 \to y_3$, the adversary succeeds in breaking $\mathsf{E}_{11}(\mathcal{Q}_q)$ with probability at most $\frac{q q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$.

Assume the adversary makes a query $y_3^{(i)} \to x_3^{(i)} = \pi_3^{-1}(y_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_3' \to x_3'$, $y_2 \to x_2$ or $y_2' \to x_2'$). By Conj. 1, there exist at most q_1 tuples $(x_2', y_2'), (x_3', y_3'), (x_1, y_1)$ such that the second equality of $\mathsf{E}_{11}\mathsf{a}$ is satisfied, except w.p. at most $\varepsilon_{\mathsf{c}}(q, n)$. For any such choice, as $y_3^{(i)}$ is fixed there exists at most one (x_2, y_2) such that equation $\mathsf{E}_{11}\mathsf{b}$ is satisfied. For any of the combinations, $\mathsf{E}_{11}\mathsf{a}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $y_3 \to x_3$, the adversary succeeds in breaking $\mathsf{E}_{11}(\mathcal{Q}_q)$ with probability at most $\frac{q q_1}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$.

Assume the adversary makes a query $x_1^{(i)} \to y_1^{(i)} = \pi_1(x_1^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_1 \to x_1$). By $\neg\mathsf{C}_4(\mathcal{Q}_i)$, there exist at most $q - 1$ tuples (x_2, y_2),

$(x_3, y_3), (x'_2, y'_2), (x'_3, y'_3)$ such that $x_2 \oplus x_3 = x'_2 \oplus x'_3$ and $y_2 \oplus y_3 = y'_2 \oplus y'_3$. For any such tuple, the adversary succeeds with probability at most $1/(2^n - q)$. Considering all queries $x_1 \to y_1$, the adversary succeeds in breaking $\mathsf{E}_{11}(\mathcal{Q}_q)$ with probability at most $\frac{q^2}{2^n - q}$.

In any case, the success probability is at most $\frac{qq_1+q^2}{2^n-q} + \varepsilon_{\mathsf{c}}(q, n)$. The cases of $\mathsf{E}_{10}(\mathcal{Q}_q)$, $\mathsf{E}_{12}(\mathcal{Q}_q)$ are fairly similar, with the major difference that one needs to take into account that by $\neg\mathsf{C}_1(\mathcal{Q}_i)$ the query history contains at most K_1 collisions $x_2 \oplus y_2 = c$, for any c, and similar for x_3. Additionally, for $\mathsf{E}_{12}(\mathcal{Q}_q)$ the usage of Conj. 1 is replaced with $\neg\mathsf{C}_3(\mathcal{Q}_i)$. Concretely, the success probabilities are upper bounded by $\frac{K_1 q q_1 + q^2}{2^n - q} + \varepsilon_{\mathsf{c}}(q, n)$ for $\mathsf{E}_{10}(\mathcal{Q}_q)$ and $\frac{K_1 K_2 q^2 + q^2}{2^n - q}$ for $\mathsf{E}_{12}(\mathcal{Q}_q)$. □

Lemma 9. $\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_i) \mid \neg\mathsf{E}_l(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}(\mathcal{Q}_i)\right) = 0$ *for* $l = 5, \ldots, 9, 13$*, provided* $K_1 = 1$.

Proof. Starting with $\mathsf{E}_5(\mathcal{Q}_q)$, for the i^{th} query $x_2^{(i)} \leftrightarrow y_2^{(i)}$ for $i = 1, \ldots, q$. As $\neg\mathsf{C}_1(\mathcal{Q}_i)$ for $K_1 = 1$ there does not exist any other query (x'_2, y'_2) such that $x_2^{(i)} \oplus y_2^{(i)} = x'_2 \oplus y'_2$. The same reasoning applies to the other events. □

A.2 Bounding Occurrence of $\mathsf{C}(\mathcal{Q}_q)$

In this section, we bound the event $\mathsf{C}(\mathcal{Q}_q)$ to occur, more specifically the second sum of (12). Notice that this sum by probability theory equals $\mathbf{Pr}\left(\mathsf{C}(\mathcal{Q}_q)\right)$. However, we can split up the probability as follows:

$$\mathbf{Pr}\left(\mathsf{C}_{1\vee\ldots\vee 4}\right) \leq \mathbf{Pr}\left(\mathsf{C}_1\right) + \mathbf{Pr}\left(\mathsf{C}_2 \mid \neg\mathsf{C}_1\right) + \mathbf{Pr}\left(\mathsf{C}_3 \mid \neg\mathsf{C}_{1\vee 2}\right) + \mathbf{Pr}\left(\mathsf{C}_4\right). \tag{13}$$

The probability bounds on $\mathsf{C}_1(\mathcal{Q}_q), \ldots, \mathsf{C}_4(\mathcal{Q}_q)$ (the four quantities of (13)) are obtained in Lems. 10-13. The proofs rely on the following bound, which holds due to Stirling's approximation ($b! \geq (b/e)^b$ for any b):

$$\binom{a}{b} \leq \frac{a^b}{b!} \leq \left(\frac{ae}{b}\right)^b.$$

Lemma 10. $\mathbf{Pr}\left(\mathsf{C}_1(\mathcal{Q}_q)\right) \leq 3 \cdot 2^n \left(\frac{qe}{(K_1+1)(2^n-q)}\right)^{K_1+1}$.

Proof. We start with the first equation of $\mathsf{C}_1(\mathcal{Q}_q)$. Fix any c. For any (x_1, y_1), the equation is satisfied with probability at most $1/(2^n - q)$. More than K_1 such tuples give a collision with probability at most

$$\binom{q}{K_1+1}\left(\frac{1}{2^n-q}\right)^{K_1+1} \leq \left(\frac{qe}{(K_1+1)(2^n-q)}\right)^{K_1+1}.$$

Now, the result follows by quantifying over the number of choices for c and the number of equations of $\mathsf{C}_1(\mathcal{Q}_q)$. □

Lemma 11. $\mathbf{Pr}\left(\mathsf{C}_2(\mathcal{Q}_q) \mid \neg\mathsf{C}_1(\mathcal{Q}_q)\right) \leq 3 \cdot 2^n \left(\frac{K_1 2q^2 e}{(K_2+1)(2^n-q)}\right)^{(K_2+1)/K_1}$.

Proof. We start with the first equation of $\mathsf{C}_2(\mathcal{Q}_q)$. Fix any c. Assume the adversary makes a query $x_1^{(i)} \to y_1^{(i)}$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_1 \to x_1$, $x_2 \to y_2$ or $y_2 \to x_2$). For any tuple (x_2, y_2), the equation is satisfied with probability at most $1/(2^n - q)$. Thus, the query results in a solution with probability at most $q/(2^n - q)$. The adversary

makes $2q$ queries, and as $\neg\mathsf{C}_1(\mathcal{Q}_q)$, each "hit" adds at most K_1 solutions. Therefore, the adversary needs at least $(K_2+1)/K_1$ out of at most $2q$ hits. Consequently, $\mathcal{Q}_q$ contains more than K_2 solutions to the first equation of $\mathsf{C}_2(\mathcal{Q}_q)$ with probability at most

$$\binom{2q}{(K_2+1)/K_1}\left(\frac{q}{2^n-q}\right)^{(K_2+1)/K_1} \leq \left(\frac{K_1 2q^2 e}{(K_2+1)(2^n-q)}\right)^{(K_2+1)/K_1}.$$

Now, the result follows by quantifying over the number of choices for c and the number of equations of $\mathsf{C}_2(\mathcal{Q}_q)$. □

Lemma 12. $\mathbf{Pr}\left(\mathsf{C}_3(\mathcal{Q}_q) \mid \neg\mathsf{C}_{1\vee 2}(\mathcal{Q}_q)\right) = 0.$

Proof. We start with the first equation of $\mathsf{C}_3(\mathcal{Q}_q)$, a similar reasoning applies to the other equations. As $\neg\mathsf{C}_2(\mathcal{Q}_q)$, for any (x_3, y_3) there are at most K_2 solutions to $x_1 \oplus y_1 \oplus x_2 \oplus y_2 = x_3$. As $\mathcal{Q}_q$ contains q tuples (x_3, y_3), it contains at most $K_2 q$ solutions to the first equation of $\mathsf{C}_3(\mathcal{Q}_q)$. □

Lemma 13. $\mathbf{Pr}\left(\mathsf{C}_4(\mathcal{Q}_q)\right) \leq 3\left(\frac{q^2 e}{2^n-q}\right)^q.$

Proof. We start with the first equation of $\mathsf{C}_4(\mathcal{Q}_q)$. By construction, there are at most q^3 tuples of queries that satisfy $x_2 \oplus x_3 = x_2' \oplus x_3'$, and the adversary can achieve this number if he makes forward queries only, and we will assume henceforth. For any of these tuples, the second equation is satisfied with probability at most $1/(2^n-q)$. More than $q-1$ such tuples give a collision with probability at most

$$\binom{q^3}{q}\left(\frac{1}{2^n-q}\right)^q \leq \left(\frac{q^3 e}{q(2^n-q)}\right)^q.$$

Now, the result follows by quantifying over the number of equations of $\mathsf{C}_4(\mathcal{Q}_q)$. □

A.3 Assembling the Results

Denote by $\mathsf{bndE}_l(q)$ the bound obtained for conditional events $\mathsf{E}_l(\mathcal{Q}_q)$ ($l = 1, \ldots, 13$, Lems. 4-9), and by $\mathsf{bndC}_l(q)$ the bound obtained for claim $\mathsf{C}_l(\mathcal{Q}_q)$ ($l = 1, \ldots, 4$, Lems. 10-13). Recall that $q_1 = d_1 q \log q$. Using slight variants of (11-13), one gets

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_1}}(q) &\leq \sum_{l\in\{1,5,9,10\}} \mathsf{bndE}_l(q) + \sum_{l\in\{1,\ldots,4\}} \mathsf{bndC}_l(q)\,,\\
\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_2}}(q) &\leq \sum_{l\in\{2,5,7,9,11\}} \mathsf{bndE}_l(q) + \sum_{l\in\{1,\ldots,4\}} \mathsf{bndC}_l(q)\,,\\
\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_3}}(q) &\leq \sum_{l\in\{3,6,8,9,13\}} \mathsf{bndE}_l(q) + \sum_{l\in\{1,2,3\}} \mathsf{bndC}_l(q) + \sum_{l\in\{1,2,3\}} \mathsf{bndC}_l(K_2 q)\,,\\
\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_4}}(q) &\leq \sum_{l\in\{4,8,9,12\}} \mathsf{bndE}_l(q) + \sum_{l\in\{1,\ldots,4\}} \mathsf{bndC}_l(q)\,.
\end{aligned}$$

Note that the bound for $\mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_3}}(q)$ includes a third sum, the cause of which is explained after Lem. 6. Let $\varepsilon > 0$. In order to prove $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{col}}_{\mathsf{F}_{\mathrm{A}_k}}(2^{n/2(1-\varepsilon)}) = 0$ (for $k = 1, 2, 3, 4$), it suffices to prove that the separate bounds tend to zero for $n \to \infty$. The results of Sects. A.1 and A.2 hold provided $K_1 = 1$, but still hold for any choice of K_2. Set $K_2 = n - 1$. Note that the ε_{c}-parts in the bounds $\mathsf{bndE}_l(q)$ all approach 0 for $q = 2^{n/2(1-\varepsilon)}$: in particular, for large enough n we have $d_1 q \log q < 2^{n/2}$ and $K_2 q < 2^{n/2}$, and Conj. 1 applies. Therefore, we

omit the ε_{c}-parts for simplicity. The evaluations are now fairly the same and mostly rely on the fact that for large enough n the bounds behave like $\frac{\alpha n^\beta}{2^{n\varepsilon}}$ for some constants α, β. This function clearly tends to 0 for $n \to \infty$. We discuss $\mathsf{bndE}_1(q)$ and $\mathsf{bndC}_2(q)$ in detail. As we consider the asymptotic behavior, without loss of generality we assume n is large enough to obtain $\frac{1}{2^n - K_2 q} \leq \frac{2}{2^n}$ and $\frac{1}{2^n - q} \leq \frac{2}{2^n}$ for $q < 2^{n/2}$. By elementary mathematics,

$$\mathsf{bndE}_1(q) = \frac{(n-1)(d_1 q \log q)^2 \log(d_1 q \log q)}{2^n - q} \leq \frac{d_1^2 n^4 q^2}{2^n}\,.$$

Consequently, $\mathsf{bndE}_1(2^{n/2(1-\varepsilon)}) \leq \frac{d_1^2 n^4}{2^{n\varepsilon}}$, approaching 0 for $n \to \infty$. Similarly, for bndC_2:

$$\mathsf{bndC}_2'(q) := \mathsf{bndC}_2(K_2 q) = 3 \cdot 2^n \left(\frac{2(K_2 q)^2 e}{n(2^n - K_2 q)}\right)^n \leq 3 \cdot 2^n \left(\frac{4enq^2}{2^n}\right)^n,$$

which implies $\mathsf{bndC}_2'(2^{n/2(1-\varepsilon)}) \leq 3\left(\frac{8en}{2^{n\varepsilon}}\right)^n$, approaching 0 for $n \to \infty$.

B Proof of Lemma 3(ii)

For $\mathsf{F}_{\mathrm{A}_k}$ $(k = 1, 2, 3, 4)$, where the matrices A_k are given in (5), the goal is to prove that $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_k}}(q) = \Theta(q^2/2^n)$ for $k = 1, 3, 4$, and to prove $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_2}}(2^{2n/3(1-\varepsilon)}) = 0$ for any $\varepsilon > 0$, demonstrating the asymptotic preimages security of $\mathsf{F}_{\mathrm{A}_2}$. In the remainder of this section, π_1, π_2, π_3 are assumed to be three permutations taken uniformly at random from P_n, and z denotes any challenge. We will analyze the maximum probability of any adversary $\mathcal{A}$, making at most q queries to his oracles, in finding preimage for $\mathsf{F}_{\mathrm{A}_k}$, denoted as $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_k}}(q)$ by definition. Denote by $\mathcal{Q}_i$ for $i = 1, \ldots, q$ the first i queries of the query history $\mathcal{Q}_q$. By construction, we have $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_1}}(q) = \mathbf{Pr}\left(\mathsf{E}_{14}(\mathcal{Q}_q)\right)$, $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_2}}(q) = \mathbf{Pr}\left(\mathsf{E}_{15}(\mathcal{Q}_q)\right)$, $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_3}}(q) = \mathbf{Pr}\left(\mathsf{E}_{16}(\mathcal{Q}_q)\right)$, and $\mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_4}}(q) = \mathbf{Pr}\left(\mathsf{E}_{17}(\mathcal{Q}_q)\right)$, where the events $\mathsf{E}_l(\mathcal{Q}_q)$ $(l \in \{14, \ldots, 17\})$ are given in Fig. 5.

$\mathsf{E}_{14}(\mathcal{Q})$: $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathcal{Q}$ **s.t.**
$x_1 \oplus y_1 \oplus x_2 = x_3$,
$x_2 \oplus y_2 \oplus y_3 = z$.

$\mathsf{E}_{15}(\mathcal{Q})$: $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathcal{Q}$ **s.t.**
$x_1 \oplus y_1 \oplus x_2 = x_3$,
$x_1 \oplus y_1 \oplus y_2 \oplus y_3 = z$.

$\mathsf{E}_{16}(\mathcal{Q})$: $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathcal{Q}$ **s.t.**
$x_1 \oplus y_1 \oplus x_2 \oplus y_2 = x_3$,
$x_1 \oplus y_1 \oplus y_3 = z$.

$\mathsf{E}_{17}(\mathcal{Q})$: $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathcal{Q}$ **s.t.**
$x_1 \oplus y_1 \oplus x_2 \oplus y_2 = x_3$,
$y_2 \oplus x_3 \oplus y_3 = z$.

Fig. 5. The events $\mathsf{E}_l(\mathcal{Q})$ $(l \in \{14, \ldots, 17\})$ employed in the proof of Lem. 3(ii) (App. B). $\mathcal{Q}$ is a query history.

In App. B.1, we will upper bound $\mathbf{Pr}\left(\mathsf{E}_{15}(\mathcal{Q}_q)\right)$. In App. B.2, we provide a tight bound for $\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q)\right)$ for $l = 14, 16, 17$.

B.1 Bounding Occurrence of $\mathsf{E}_{15}(\mathcal{Q}_q)$

In order to bound $\mathbf{Pr}\left(\mathsf{E}_{15}(\mathcal{Q}_q)\right)$, we define a new claim $\mathsf{C}_{2'}(\mathcal{Q})$. This claim equals $\mathsf{C}_2(\mathcal{Q})$ of Fig. 4 restricted to the third equation and for fixed c instead of for any c. In a similar fashion as in (12)-(13), we obtain:

$$\begin{aligned}\mathbf{Pr}\left(\mathsf{E}_{15}(\mathcal{Q}_q)\right) \leq \sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_{15}(\mathcal{Q}_i) \mid \neg\mathsf{E}_{15}(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}_{1\vee 2'}(\mathcal{Q}_i)\right) + \\ \mathbf{Pr}\left(\mathsf{C}_1(\mathcal{Q}_q)\right) + \mathbf{Pr}\left(\mathsf{C}_{2'}(\mathcal{Q}_q) \mid \neg\mathsf{C}_1(\mathcal{Q}_q)\right).\end{aligned} \tag{14}$$

In Lem. 14 we bound the conditioned occurrence of $\mathsf{E}_{15}(\mathcal{Q}_q)$ (the first part (14)), and in Lem. 15 we compute probability on $\mathsf{C}_{2'}(\mathcal{Q}_q)$ (the third part of (14)). A bound on $\mathsf{C}_1(\mathcal{Q}_q)$ is given in Lem. 10. The results are then assembled to prove $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_2}}(2^{2n/3(1-\varepsilon)}) = 0$ for any $\varepsilon > 0$.

Let d_2 be the constant defined in Conj. 1. On input of parameters (q, n), we define $\varepsilon'_{\mathsf{c}}(q, n) = \mathbf{Pr}\left(\beta > d_2 q^{3/2}\right)$ of Conj. 1. This quantity tends to 0 for $n \to \infty$ and for $q < 2^{2n/3}$.

Lemma 14. $\displaystyle\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_{15}(\mathcal{Q}_i) \mid \neg\mathsf{E}_{15}(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}_{1\vee 2'}(\mathcal{Q}_i)\right) \leq \frac{d_2 q^{3/2} + K_2 q}{2^n - q} + \varepsilon'_{\mathsf{c}}(q, n).$

Proof. We write $\mathsf{E}_{15}\mathsf{a}$ and $\mathsf{E}_{15}\mathsf{b}$ for the two equations of $\mathsf{E}_{15}(\mathcal{Q})$ (Fig. 5). The approach is similar as before.

Assume first the adversary makes a query $x_3^{(i)} \to y_3^{(i)} = \pi_3(x_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_3 \to x_3$, $x_2 \to y_2$ and $y_2 \to x_2$). Denote L_i to be the number of tuples $(x_1, y_1), (x_2, y_2)$ that make equation $\mathsf{E}_{15}\mathsf{a}$ satisfied for $x_3^{(i)}$. For any of these tuples, equation $\mathsf{E}_{15}\mathsf{b}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_3 \to y_3$, the adversary succeeds in breaking $\mathsf{E}_{15}(\mathcal{Q}_q)$ with probability at most $\sum_{i=1}^{q} \frac{L_i}{2^n - q}$. Notice that by Conj. 1, $\sum_{i=1}^{q} L_i \leq d_2 q^{3/2}$, except w.p. at most $\varepsilon'_{\mathsf{c}}(q, n)$. We thus obtain upper bound $\frac{d_2 q^{3/2}}{2^n - q} + \varepsilon'_{\mathsf{c}}(q, n)$.

Assume the adversary makes a query $x_1^{(i)} \to y_1^{(i)} = \pi_1(x_1^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_1 \to x_1$). As $\neg\mathsf{C}_{2'}(\mathcal{Q}_i)$, there exist at most K_2 tuples (x_2, y_2), (x_3, y_3) such that $x_2 \oplus y_2 \oplus x_3 \oplus y_3 = z$ is satisfied. For any of these tuples, equation $\mathsf{E}_{15}\mathsf{a}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_1 \to y_1$, the adversary succeeds in breaking $\mathsf{E}_{15}(\mathcal{Q}_q)$ with probability at most $\frac{K_2 q}{2^n - q}$.

In any case, the success probability is at most $\frac{d_2 q^{3/2} + K_2 q}{2^n - q} + \varepsilon'_{\mathsf{c}}(q, n)$. □

Lemma 15. $\displaystyle\mathbf{Pr}\left(\mathsf{C}_{2'}(\mathcal{Q}_q) \mid \neg\mathsf{C}_1(\mathcal{Q}_q)\right) \leq \left(\frac{K_1 2q^2 e}{(K_2+1)(2^n - q)}\right)^{(K_2+1)/K_1}.$

Proof. The proof is identical to the proof of the bound for $\mathsf{C}_2(\mathcal{Q}_q)$ (Lem. 11). Note that $\mathsf{C}_{2'}(\mathcal{Q}_q)$ consists of one equation, and one choice for c only. □

Let $\varepsilon > 0$. Similar to App. A.3, in order to prove $\lim_{n\to\infty} \mathbf{Adv}^{\mathsf{epre}}_{\mathsf{F}_{\mathrm{A}_2}}(2^{2n/3(1-\varepsilon)}) = 0$, it suffices to prove that the separate bounds tend to zero for $n \to \infty$. Put $K_1 = 2$ and $K_2 = 2^{n/3} - 1$. The evaluations are now fairly the same, and we only discuss the bound $\mathsf{bnd}\mathsf{E}_{15}(q)$ on $\mathsf{E}_{15}(\mathcal{Q}_q)$. Again, by Conj. 1 the $\varepsilon'_{\mathsf{c}}$-part goes to 0 for $q = 2^{2n/3(1-\varepsilon)}$, and we omit it for simplicity. Notice that $\frac{1}{2^n - q} \leq \frac{2}{2^n}$ for $q \leq 2^{n-1}$. We obtain:

$$\mathsf{bnd}\mathsf{E}_{15}(q) = \frac{d_2 q^{3/2} + (2^{n/3} - 1)q}{2^n - q} \leq 2\frac{d_2 q^{3/2} + 2^{n/3} q}{2^n}.$$

Consequently, $\mathsf{bnd}\mathsf{E}_{15}(2^{2n/3(1-\varepsilon)}) \leq \dfrac{2d_2}{2^{n\varepsilon}} + \dfrac{2}{2^{2n/3\varepsilon}}$, which approaches 0 for $n \to \infty$.

B.2 Bounding Occurrence of $\mathsf{E}_l(\mathcal{Q}_q)$, $l = 14, 16, 17$

In this section, we prove $\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q)\right) = \Theta(q^2/2^n)$ $(l = 14, 16, 17)$ by providing a lower bound in Lem. 16, and an upper bound in Lem. 17.

Lemma 16. $\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q)\right) = \Omega(q^2/2^n)$ *for* $l = 14, 16, 17$.

Proof. We consider $\mathsf{E}_{14}(\mathcal{Q}_q)$, the analysis for the other compression functions is analogous[2].

We construct an adversary $\mathcal{A}$ whose goal is to find tuples $(x_1, y_1) \in \pi_1, (x_2, y_2) \in \pi_2$, and $(x_3, y_3) \in \pi_3$ such that $\mathsf{E}_{14}(\mathcal{Q}_q)$ is satisfied. The adversary proceeds as follows. He sets up two lists of q random elements $X_1 := \{x_1^{(1)}, \ldots, x_1^{(q)}\}$ and $X_2 := \{x_2^{(1)}, \ldots, x_2^{(q)}\}$, and computes the corresponding values $y_1^{(k)} = \pi_1(x_1^{(k)})$ and $y_2^{(k)} = \pi_2(x_2^{(k)})$ (for $k = 1, \ldots, q$). Additionally, for each $k = 1, \ldots, q$, the adversary sets $y_3^{(k)} = x_2^{(k)} \oplus y_2^{(k)} \oplus z$ and computes the corresponding value $x_3^{(k)} = \pi_3^{-1}(y_3^{(k)})$. Fix any $k \in \{1, \ldots, q\}$, then $x_2^{(k)} \oplus y_2^{(k)} \oplus y_3^{(k)} = z$ by construction. The adversary obtains a solution for $\mathsf{E}_{14}(\mathcal{Q}_q)$ if X_1 contains an element x_1 such that $x_1 \oplus y_1 = x_2 \oplus x_3$. By basic probability theory, such x_1 exists with probability $\Omega(q/2^n)$. As the adversary needs to succeed for only one of the q choices of k, he finds a solution for $\mathsf{E}_{14}(\mathcal{Q}_q)$ with probability $\Omega(q^2/2^n)$. □

Lemma 17. $\mathbf{Pr}\left(\mathsf{E}_l(\mathcal{Q}_q)\right) = O(q^2/2^n)$ *for* $l = 14, 16, 17$.

Proof. We consider $\mathsf{E}_{14}(\mathcal{Q}_q)$, the analysis for the other compression functions is analogous. We write $\mathsf{E}_{14}\mathsf{a}, \mathsf{E}_{14}\mathsf{b}$ for the two equations of $\mathsf{E}_{14}(\mathcal{Q}_q)$. The approach is similar to before. By basic probability theory,

$$\mathbf{Pr}\left(\mathsf{E}_{14}(\mathcal{Q}_q)\right) \leq \sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_{14}(\mathcal{Q}_i) \mid \neg\mathsf{E}_{14}(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}_1(\mathcal{Q}_i)\right) + \mathbf{Pr}\left(\mathsf{C}_1(\mathcal{Q}_q)\right). \tag{15}$$

We start with the first probability and consider $K_1 = 1$.

Assume first the adversary makes a query $x_3^{(i)} \to y_3^{(i)} = \pi_3(x_3^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $x_2 \to y_2$). For each of the $\leq q$ tuples (x_1, y_1), by $\neg\mathsf{C}_1(\mathcal{Q}_i)$ the values $x_1 \oplus y_1$ are distinct, and there exists at most one (x_2, y_2) such that equation $\mathsf{E}_{14}\mathsf{a}$ is satisfied. For any of the combinations, $\mathsf{E}_{14}\mathsf{b}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_3 \to y_3$, the adversary succeeds in breaking $\mathsf{E}_{14}(\mathcal{Q}_q)$ with probability at most $\frac{q^2}{2^n - q}$.

Assume the adversary makes a query $y_3^{(i)} \to x_3^{(i)} = \pi_3^{-1}(x_3^{(i)})$ for $i = 1, \ldots, q$. By $\neg\mathsf{C}_1(\mathcal{Q}_i)$, there exists at most one tuple (x_2, y_2) such that equation $\mathsf{E}_{14}\mathsf{b}$ is satisfied. For this tuple, $\mathsf{E}_{14}\mathsf{a}$ is satisfied with probability at most $q/(2^n - q)$. Considering all queries $x_3 \to y_3$, the adversary succeeds in breaking $\mathsf{E}_{14}(\mathcal{Q}_q)$ with probability at most $\frac{q^2}{2^n - q}$.

Assume the adversary makes a query $y_2^{(i)} \to x_2^{(i)} = \pi_2^{-1}(x_2^{(i)})$ for $i = 1, \ldots, q$. For each of the $\leq q$ tuples (x_1, y_1), by $\neg\mathsf{C}_1(\mathcal{Q}_i)$ the values $x_1 \oplus y_1$ are distinct, and there exists at most one (x_3, y_3) such that $x_1 \oplus y_1 \oplus y_2 \oplus x_3 \oplus y_3 = z$. For any of the combinations, $\mathsf{E}_{14}\mathsf{a}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_2 \to y_2$, the adversary succeeds in breaking $\mathsf{E}_{14}(\mathcal{Q}_q)$ with probability at most $\frac{q^2}{2^n - q}$.

Assume the adversary makes a query $x_1^{(i)} \to y_1^{(i)} = \pi_1(x_1^{(i)})$ for $i = 1, \ldots, q$ (the same treatment holds for queries $y_1 \to x_1$). For each of the $\leq q$ tuples (x_3, y_3), by $\neg\mathsf{C}_1(\mathcal{Q}_i)$ there exists at most one (x_2, y_2) such that equation $\mathsf{E}_{14}\mathsf{b}$ is satisfied. For any of the combinations, $\mathsf{E}_{14}\mathsf{a}$ is satisfied with probability at most $1/(2^n - q)$. Considering all queries $x_1 \to y_1$, the adversary succeeds in breaking $\mathsf{E}_{14}(\mathcal{Q}_q)$ with probability at most $\frac{q^2}{2^n - q}$.

In any case, we obtain $\sum_{i=1}^{q} \mathbf{Pr}\left(\mathsf{E}_{14}(\mathcal{Q}_i) \mid \neg\mathsf{E}_{14}(\mathcal{Q}_{i-1}) \wedge \neg\mathsf{C}_1(\mathcal{Q}_i)\right) \leq \dfrac{q^2}{2^n - q}$. The claim now immediately follows from (15), Lem. 10, and the fact that $q \leq 2^{n-1}$. □

[2] The attack defining the lower bound for $\mathsf{E}_{16}(\mathcal{Q}_q)$ corresponds to an attack by Joux described in [11].

C Generalization of Theorem 2

We generalize our findings on the single-permutation setting to cover *any* function, where affine transformations on the inputs to the permutations are taken into account. This generalization is straightforward, but technical and more elaborate. For a matrix $\mathrm{B} = (b_1, b_2, b_3, b_4)^\top$ with elements in $\{0,1\}^n$, we define the compression function F_{AB} as follows:

$$\begin{aligned} \mathsf{F}_{\mathrm{AB}}(x_1, x_2) = z\,, \text{ where } \; & y_1 \leftarrow \pi_1(a_{11}x_1 \oplus a_{12}x_2 \oplus b_1)\,, \\ & y_2 \leftarrow \pi_2(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}y_1 \oplus b_2)\,, \\ & y_3 \leftarrow \pi_3(a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}y_1 \oplus a_{34}y_2 \oplus b_3)\,, \\ & z \leftarrow a_{41}x_1 \oplus a_{42}x_2 \oplus a_{43}y_1 \oplus a_{44}y_2 \oplus a_{45}y_3 \oplus b_4\,. \end{aligned} \tag{16}$$

where A is as in Sect. 2.1. We note that for the multi-permutation setting, this generalization is of no added value, as the permutations are independently distributed anyway. Adding constants is, however, a customary approach to obtain "different" permutations from a single one (e.g. $\pi_i(x) = \pi(b_i \oplus x)$ for $i = 1, 2, 3$), but as we will show, the findings of Thm. 2 also apply to this extended setting.

We reformulate Props. 1-3 to the case of F_{AB} (recall that Prop. 4 did not apply to the single-permutation setting in the first place). Propositions 1 and 2 apply to any F_{AB} and $\mathsf{F}_{\mathrm{A'B'}}$ with $\mathrm{B} = \mathrm{B'}$ and Prop. 3 holds for any B and B′ with $(b'_i, b'_{i+1}) = (b_{i+1}, b_i)$. Given this, the proof of Thm. 2 almost carries over. Lemmas 1 and 2 apply with straightforward generalization. It remains to evaluate the matrices A of the form (7) *for any* $\mathrm{B} \in (\{0,1\}^n)^{4\times 1}$. The case $\|\mathbf{a}_{3,*}\| \leq 2$ is the same as in the proof of Thm. 2.

$\|\mathbf{a}_{3,*}\| = 3$. Due to M-reductions, it suffices to consider $a_{31}a_{32}a_{33}a_{34} \in \{1110, 0111\}$.

- $a_{31}a_{32}a_{33}a_{34} = 1110$. The same analysis as in Sect. 4.1 applies, leaving the matrices A_1 and A_2 of (5). In the extended single-permutation setting, the two corresponding compression functions satisfy $\mathsf{F}_{\mathrm{A}_1\mathrm{B}}(x_1 \oplus b_1, \pi(x_1) \oplus b_1 \oplus b_3) = \pi(\pi(x_1) \oplus b_1 \oplus b_2 \oplus b_3) \oplus b_1 \oplus b_3 \oplus b_4$ and $\mathsf{F}_{\mathrm{A}_2\mathrm{B}}(x_1, x_2) = \mathsf{F}_{\mathrm{A}_2\mathrm{B}}(x_1, x_1 \oplus x_2 \oplus \pi(x_1 \oplus b_1) \oplus b_2 \oplus b_3)$ for any x_1, x_2. Collisions can thus be trivially found;
- $a_{31}a_{32}a_{33}a_{34} = 0111$. By Lem. 2(ii), we have $a_{41} = 1$. Lemma 2(iii) now states that we require $a_{42} = a_{44}$, which gives the following four options for $a_{42}a_{43}a_{44}$: 000, 010, 101 and 111. The first one is vulnerable to the attack of Lem. 2(iv), the second, third and fourth matrix satisfy $\mathsf{F}_{\mathrm{AB}}(x_1, \pi^{-1}(\pi(x_1 \oplus b_1) \oplus b_2 \oplus b_3) \oplus b_2) = x_1 \oplus b_2 \oplus b_3 \oplus b_4$, $\mathsf{F}_{\mathrm{AB}}(x_1 \oplus b_1, x_1 \oplus b_2) = \mathsf{F}_{\mathrm{AB}}(x_1 \oplus b_1 \oplus b_2 \oplus b_3, x_1 \oplus b_3)$ and $\mathsf{F}_{\mathrm{AB}}(x_1 \oplus b_1, x_1 \oplus b_2) = \pi(x_1 \oplus b_2 \oplus b_3) \oplus b_1 \oplus b_2 \oplus b_4$, respectively, for any x_1. Collisions can thus be trivially found;

$\|\mathbf{a}_{3,*}\| = 4$. Except for $a_{41}a_{42}a_{43}a_{44} \in \{1010, 1001, 0110, 0101\}$, all induced compression functions satisfy $\mathsf{F}_{\mathrm{AB}}(x_1 \oplus b_1, x_1 \oplus b_2) \oplus \pi(b_1 \oplus b_2 \oplus b_3) \oplus a_{41}b_1 \oplus a_{42}b_2 \oplus b_4 \in \{0, x_1, \pi(x_1)\}$ for any x_1, for which collisions can be trivially found. The cases 1001, 0110 are vulnerable to Lem. 2(iii). The remaining two cases, which are equivalent by M-reduction, allow for trivial collisions as well: the compression function induced by $(a_{41}a_{42}a_{43}a_{44}) = (1010)$ satisfies $\mathsf{F}_{\mathrm{AB}}(x_1, \pi^{-1}(x_1 \oplus \pi(x_1 \oplus b_1) \oplus b_2 \oplus b_3) \oplus b_2) = b_2 \oplus b_3 \oplus b_4$ for any x_1.

Hence, any of the analyzed compression functions either allows for trivial collision or is vulnerable to Lem. 2, therewith allowing for collisions in at most $2^{2n/5}$ queries.

Concluding, for any compression function F_{AB} of the generalized form (16), collisions can be found in at most $2^{2n/5}$ queries, hence considerably faster than in $2^{n/2}$ queries.

D Heuristic Argument for Conjecture 1

In this section, we provide a heuristic argument for the first part of Conj. 1, a similar argument applies to part two. Throughout the argument it becomes clear why the conjecture is similar to but more complex than Zarankiewicz problem [2, Ch. 6.2], as claimed in Sect. 4.

In more detail, we will show that the conjecture should hold for $d_1 = 10$ for large enough n. Let Z be a given set of $q < 2^{n/2}$ random elements. Denote by $\mathbf{Pr}(\mathsf{succ}(Z))$ the probability that there exist two sets X_1, X_2 such that the number of solutions $(x_1, x_2, z) \in X_1 \times X_2 \times Z$ with $x_1 \oplus x_2 = z$ is larger than $10q \log q$. In this heuristic argument we will provide a bound on $\mathbf{Pr}(\mathsf{succ}(Z))$. In fact, we will first consider $q = 2^\alpha$ and show that the number of solutions is with high probability upper bounded by $2q \log q + q$. If q is no power of two, the number of solutions is then clearly upper bounded by the amount of solutions for $q' = 2^{\lceil \log q \rceil}$, hence upper bounded by $8q \log q + 2q \leq 10q \log q$ (provided $q \geq 2$).

Before proceeding, we pose the following claim on Z:

$$\mathsf{D}_1(Z) : \textbf{there exist } z_1, z_2 \in Z \textbf{ such that } z_1 = z_2.$$

Clearly, $\mathbf{Pr}(\mathsf{D}_1(Z)) \leq q^2/2^n$, and by probability theory we have

$$\mathbf{Pr}(\mathsf{succ}(Z)) \leq \mathbf{Pr}(\mathsf{succ}(Z) \mid \neg\mathsf{D}_1(Z)) + \mathbf{Pr}(\mathsf{D}_1(Z)) \leq \mathbf{Pr}(\mathsf{succ}(Z) \mid \neg\mathsf{D}_1(Z)) + \frac{q^2}{2^n}. \quad (17)$$

Therefore, it suffices to analyze $\mathsf{succ}(Z)$ given that Z contains no collisions. The goal for an adversary now is to come up with two sets $X_1 = \{x_1^{(1)}, \ldots, x_1^{(q)}\}$ and $X_2 = \{x_2^{(1)}, \ldots, x_2^{(q)}\}$ such that $\left|\{(x_1, x_2, z) \in X_1 \times X_2 \times Z \mid x_1 \oplus x_2 = z\}\right|$ is maximized.

Consider a $q \times q$ matrix X with rows corresponding to $x_1^{(i)}$ and columns to $x_2^{(j)}$, and the coefficient x_{ij} of X equals $z \in Z$ if $x_1^{(i)} \oplus x_2^{(j)} = z$, and is empty if $x_1^{(i)} \oplus x_2^{(j)} \notin Z$. Now, the goal of the adversary is to maximize the number of filled coefficients of X, by smartly choosing $x_1^{(i)}, x_2^{(j)}$. Denote by $s(\mathrm{X})$ the maximum number of elements in the matrix X. Some restrictions apply to the choices for $x_1^{(i)}, x_2^{(j)}$.

(i) An element $z \in Z$ does not occur twice in one row or column (it would imply a collision in X_1 or X_2);
(ii) Let $i, i', j, j' \in \{1, \ldots, q\}$ and $z_1, z_2 \in Z$. If $x_{ij} = x_{i'j'} = z_1$ and $x_{ij'} = z_2$, then $x_{i'j} = z_2$ (obtained by XORing the first three equations);
(iii) Let $i, i', j, j' \in \{1, \ldots, q\}$ and $z_1, \ldots, z_4 \in Z$ satisfying $z_1 \oplus z_2 \oplus z_3 \oplus z_4 = 0$. If $x_{ij} = z_1$, $x_{ij'} = z_2$ and $x_{i'j} = z_3$, then $x_{i'j'} = z_4$ (obtained by XORing the first three equations).

The problem now reduces to smartly positioning in X as many elements from Z as possible.

Let K be maximal such that there exists a set of values $z_1, \ldots, z_{2K} \in Z$ satisfying $z_1 \oplus z_2 = \ldots = z_{2K-1} \oplus z_{2K}$. We call this set of values a K-way collision, and two consecutive elements z_{2i-1}, z_{2i} are called a twin. Using properties (ii,iii), the adversary can obtain a 4×4 submatrix of X filled with four values z_1, z_2, z_3, z_4 each occurring four times[3], but as we will argue this is essentially the best the adversary can get. Notice that this also demonstrates that the best approach followed by the adversary is to exploit the K-way collision.

In Fig. 6, we introduce four claims $\mathsf{D}_2(Z), \ldots, \mathsf{D}_5(Z)$ to further analyze event $\mathsf{succ}(Z)$, and we bound the occurrence of these events provided $\neg\mathsf{D}_1(Z)$.

– $\left[\mathbf{Pr}(\mathsf{D}_2(Z) \mid \neg\mathsf{D}_1(Z)) \leq 2^n \left(\frac{2q^2 e}{(K_2+1)2^n}\right)^{(K_2+1)}\right]$ The proof is similar to the proof of Lem. 11, with the difference that now q random values are generated (being Z) that piece for piece may result in a solution;
– $\left[\mathbf{Pr}(\mathsf{D}_3(Z) \mid \neg\mathsf{D}_{1\vee 2}(Z)) \leq 2^n \left(\frac{K_2^3 q}{2^n}\right)^2\right]$ Fix any c. By $\neg\mathsf{D}_2(Z)$, there are at most $2^3\binom{K_2}{3}$ possible choices for z_1, z_3, z_5 (the choices for z_2, z_4, z_6 follow directly), any of which satisfies

[3] The adversary chooses $x_1^{(1)}$, sets $x_2^{(j)} = z_j \oplus x_1^{(1)}$ for $j = 1, 2, 3, 4$, and $x_1^{(i)} = z_i \oplus x_2^{(1)}$ for $i = 2, 3, 4$. By properties (ii,iii), the remaining coefficients are filled.

$\mathsf{D}_2(Z)$: **for some** c **there exist more than** K_2 **solutions in** Z **to:**

$z_1 \neq z_2$**, and**
$z_1 \oplus z_2 = c$.

$\mathsf{D}_3(Z)$: **for some** c **there exist more than one solution in** Z **to (with different** z_7 **for each solution):**

$z_1, \ldots, z_7$ **distinct, and**
$z_{2i-1} \oplus z_{2i} = c$ **(for** $i = 1, 2, 3$**), and**
$z_1 \oplus z_3 \oplus z_5 \oplus z_7 = 0$.

$\mathsf{D}_4(Z)$: **for some** c **there exist a solution in** Z **to:**

$z_1, \ldots, z_{12}$ **distinct, and**
$z_{2i-1} \oplus z_{2i} = c$ **(for** $i = 1, \ldots, 5$**), and**
$z_1 \oplus z_3 \oplus z_5 \oplus z_{11} = 0$**, and**
$z_7 \oplus z_9 \oplus z_{11} \oplus z_{12} = 0$.

$\mathsf{D}_5(Z)$: **let** $d \geq 4$**, for some** c **there exists a solution in** $\mathcal{Q}$ **to:**

$z_1, \ldots, z_{2d}$ **distinct, and**
$z_{2i-1} \oplus z_{2i} = c$ **(for** $i = 1, \ldots, d$**), and**
$z_1 \oplus z_3 \oplus \cdots \oplus z_{2d-1} = 0$.

Fig. 6. The claims $\mathsf{D}_2(Z), \ldots, \mathsf{D}_5(Z)$ employed in the heuristic argument for Conj. 1 (App. D). The parameter $K_2 > 1$ is any fixed constant.

the second equation with probability at most $q/2^n$. As we require more than one *different* value z_7 to be hit, and Z contains q *different* possibilities for $z_3^{(7)}$ by $\neg\mathsf{D}_1(Z)$, Z contains more than one solution to $\mathsf{D}_3(Z)$ with probability at most

$$\binom{2^3\binom{K_2}{3}}{2}\left(\frac{q}{2^n}\right)^2 \leq \left(\frac{K_2^3 q}{2^n}\right)^2.$$

Now, the result follows by quantifying over the number of choices for c;

– $\left[\mathbf{Pr}\left(\mathsf{D}_4(Z) \mid \neg\mathsf{D}_{1\vee 2}(Z)\right) \leq 2^n\left(\frac{K_2^3 q}{2^n}\right)^2\right]$ Fix any c. By $\neg\mathsf{D}_2(Z)$, there are at most $2^5\binom{K_2}{5}$ possible choices for $z_1, z_3, \ldots, z_9$ (the choices for $z_2, z_4, \ldots, z_{10}$ follow directly). For any choice, the second and third equation are both satisfied with probability at most $q/2^n$. Therefore, Z contains a solution to $\mathsf{D}_4(Z)$ with probability at most

$$2^5\binom{K_2}{5}\left(\frac{q}{2^n}\right)^2 \leq \left(\frac{K_2^3 q}{2^n}\right)^2.$$

Now, the result follows by quantifying over the number of choices for c;

– $\left[\mathbf{Pr}\left(\mathsf{D}_5(Z) \mid \neg\mathsf{D}_1(Z)\right) \leq 2^n \sum_{d=4}^{\infty} \frac{q^{2d}}{(2^n)^{d+1}}\right]$ Fix any c, d. Without loss of generality we can consider the values of Z to be generated piece for piece. Consider the generation of z_i for $i = 1, \ldots, q$. For any other value z, the first equation is satisfied with probability at most $1/2^n$. Thus, the query results in a solution with probability at most $q/2^n$. In total q values are generated, and as $\neg\mathsf{D}_1(Z)$, each "hit" adds at most 1 solution. Therefore, we need d out of at most q hits. Given that d pairs are found, the second equation of $\mathsf{D}_5(Z)$ is then satisfied with probability at most $1/2^n$, as the values $z_3^{(i)}$ are different by $\neg\mathsf{D}_1(Z)$. Consequently, Z contains a solution to $\mathsf{D}_5(Z)$ with probability at most

$$\binom{q}{d}\left(\frac{q}{2^n}\right)^d \cdot \frac{1}{2^n} \leq \frac{q^{2d}}{(2^n)^{d+1}}.$$

Now, the result follows by quantifying over the number of choices for c and d (in fact, we are using $\mathsf{D}_5(Z)$ for $d = 4, 6$ only but we generalize its usage for simplicity).

We obtain for (17):

$$\begin{aligned}\mathbf{Pr}\left(\mathsf{succ}(Z) \mid \neg\mathsf{D}_1\right) \leq \mathbf{Pr}\left(\mathsf{succ}(Z) \mid \neg\mathsf{D}_{1\vee\ldots\vee 5}\right) + \mathbf{Pr}\left(\mathsf{D}_2 \mid \neg\mathsf{D}_1\right) + \mathbf{Pr}\left(\mathsf{D}_3 \mid \neg\mathsf{D}_{1\vee 2}\right) \\ + \mathbf{Pr}\left(\mathsf{D}_4 \mid \neg\mathsf{D}_{1\vee 2}\right) + \mathbf{Pr}\left(\mathsf{D}_5 \mid \neg\mathsf{D}_1\right).\end{aligned} \tag{18}$$

Similar to before (e.g., Sect. A.3), one can show that for $K_2 = n - 1$ the second part of (18) approaches 0 for $q = 2^{n/2(1-\varepsilon)}$ and $n \to \infty$. In what remains, we heuristically argue that $\mathbf{Pr}\left(\mathsf{succ}(Z) \mid \neg\mathsf{D}_{1\vee\ldots\vee 5}(Z)\right)$ is expected to equal 0 for $d_1 = 10$.

Naturally, the maximal number of solutions is achieved when the adversary includes in the matrix X as many boxes $\left(\begin{smallmatrix} z_a & z_b \\ z_b & z_a \end{smallmatrix}\right)$ as possible, where z_a, z_b denotes any twin of the maximal K-way collision. However, it may be the case that three values z_1, z_2, z_3 coming from *different* twins form a collision with a value $z \in Z$ no member of the K-way collision, therewith resulting in more solutions due to property (iii) described above. However, by $\neg\mathsf{D}_3(Z)$, there is only one such possible value z, and XORed with any other values from different twins it does not collide with another element from Z (by $\neg\mathsf{D}_4(Z)$). Thus, the value z appears in X at most q times, and no other value can occur. We just scrap this value out of the matrix, continue with the matrix built of the K-way collision only, and add q to the finally obtained number of elements in the matrix. Concluding, the best approach is to consider the matrix X consisting of 2×2 submatrices that satisfy the following property: each block is either entirely filled by a twin of the K-way collision, or empty. Additionally, any two rows of 2×2 submatrices share at most 2 "positions" (by $\neg\mathsf{D}_3(Z)$). Now, we can constrict rows $2i-1$ and $2i$ (for $i = 1, \ldots, q/2$) and columns $2j-1$ and $2j$ (for $j = 1, \ldots, q/2$) to obtain a matrix $\mathrm{X}^{[q/2]}$. Here we replace every 2×2 submatrix by the first element of the twin. Matrix $\mathrm{X}^{[q/2]}$ still satisfies properties (i,ii), and moreover it satisfies the next properties:

(iv) The matrix does not contain a full 2×3 (or 3×2) submatrix (by $\neg\mathsf{D}_3(Z)$);
(v) For any $d \geq 4$, the matrix does not contain d different values that XOR up to 0 (by $\neg\mathsf{D}_5(Z)$).

Now, the number of coefficients filled in X satisfies $s(\mathrm{X}) \leq 4s(\mathrm{X}^{[q/2]}) + q$, and hence we bound the maximum number of elements in any matrix $\mathrm{X}^{[q/2]}$ satisfying (i,ii,iv,v).

Before proceeding, we point out the relation of our conjecture with Zarankiewicz conjecture[4]. Let $G_n = (V_1 \cup V_2, E)$ be a bipartite graph on color classes V_1, V_2 of equal size n. Zarankiewicz problem regards the case of determining the maximal graph G_n that does not contain any complete bipartite subgraph on $3 + 3$ vertices. With respect to our problem, we can consider $\mathrm{X}^{[q/2]}$ to represent an incidence matrix of a bipartite graph, where the rows correspond to one side of the bipartition, and the columns to the other side. An element $x_{ij} \in \mathrm{X}^{[q/2]}$ is non-empty if and only if $x_1^{(i)} \oplus x_2^{(j)} = z \in Z$, and the corresponding edge is labeled by z. By virtue of (i,ii,iv,v) several restrictions apply to this graph: for instance, it does not contain a complete bipartite subgraph on $2 + 3$ vertices (property (iv)), and it does not contain a complete bipartite subgraph on $2 + 2$ vertices where the four edges have different labels (property (v)). Various other restrictions to this matrix can be extracted from the randomness of Z, but for our heuristic argument the restrictions put forward suffice.

We proceed with the heuristic argument. Consider a matrix $\mathrm{X}^{[q/2]}$ that achieves the maximum number of solutions. $\mathrm{X}^{[q/2]}$ is likely to have two elements $z_1, z_2 \in Z$ occurring $q/2$ times, which can be seen as follows. Consider a first element z_1. Suppose z_1 occurs $q/2 - 1$ times, w.l.o.g. (by graph isomorphism) at the first $q/2 - 1$ diagonal elements of $\mathrm{X}^{[q/2]}$. This means that $x_{q/2,q/2} \neq z_1$. Without loss of generality, $\left|\{i \mid x_{i,q/2} \in Z\}\right| \leq \left|\{j \mid x_{q/2,j} \in Z\}\right|$. We construct the matrix $\overline{\mathrm{X}}^{[q/2]}$, with the first $q/2 - 1$ columns identical to the ones of $\mathrm{X}^{[q/2]}$, but with $\overline{x}_{q/2,q/2} = z_1$. By property (ii) and the fact that all diagonal elements of $\overline{\mathrm{X}}^{[q/2]}$ equal z_1, we obtain $\overline{x}_{i,q/2} = \overline{x}_{q/2,i} = x_{q/2,i}$ for $i = 1, \ldots, q/2 - 1$. It is easy to check that $\overline{\mathrm{X}}^{[q/2]}$ satisfies (i,ii,iv,v) if $\mathrm{X}^{[q/2]}$ does. In particular, it does not violate property (i) (similar argument applies to other properties): it would violate (i) if $\overline{x}_{i,q/2} = \overline{x}_{ij} = x_{ij}$ for some $i, j \in \{1, \ldots, q/2 - 1\}$, which for the original matrix $\mathrm{X}^{[q/2]}$ would imply that $x_{q/2,i} = x_{ij}$,

[4] Generalizations of Zarankiewicz problem exist, but this problem is the most well-known among them.

and thus (by property (ii) for $\mathrm{X}^{[q/2]}$) $x_{q/2,j} = x_{ii} = z_1$, impossible by construction. Thus, we obtained a matrix $\overline{\mathrm{X}}^{[q/2]}$ with z_1 occurring $q/2$ times and with at least as many solutions as $\mathrm{X}^{[q/2]}$. A second element is likely to occur $q/2$ times for similar reasons.

$\mathrm{X}^{[q/2]}$ can thus be considered to be of the following form:

$$\mathrm{X}^{[q/2]} = \left(\begin{array}{c|c|c|c} \begin{matrix} z_1 & z_2 \\ z_2 & z_1 \end{matrix} & \mathrm{X}_{12} & \cdots & \mathrm{X}_{1,\frac{q}{4}} \\ \hline \mathrm{X}_{21} & \begin{matrix} z_1 & z_2 \\ z_2 & z_1 \end{matrix} & \cdots & \mathrm{X}_{2,\frac{q}{4}} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathrm{X}_{\frac{q}{4},1} & \mathrm{X}_{\frac{q}{4},2} & \cdots & \begin{matrix} z_1 & z_2 \\ z_2 & z_1 \end{matrix} \end{array}\right),$$

for some 2×2 submatrices X_{ij}. Now, by property (ii) we have $\mathrm{X}_{ij} = \mathrm{X}_{ji}$ for all i, j. Additionally, as no two rows share three columns (and vice versa), each block is either empty or an (anti-)diagonal matrix where the two (anti-)diagonal elements are equal by property (ii). Consequently, we can constrict rows $2i - 1$ and $2i$ (for $i = 1, \ldots, q/4$) and columns $2j - 1$ and $2j$ (for $j = 1, \ldots, q/4$) to obtain a matrix $\mathrm{X}^{[q/4]}$. Here each 2×2 block on the diagonal of $\mathrm{X}^{[q/2]}$ is constricted to z_1, and each other block to its only element. Now, the number of coefficients in $\mathrm{X}^{[q']}$ (with $q' = q/2$) satisfies $s(\mathrm{X}^{[q']}) \leq 2 \cdot (q'/2) + 2s(\mathrm{X}^{[q'/2]})$: the second part counts each element in $\mathrm{X}^{[q'/2]}$ as two original elements, and we add two remaining from the original diagonal blocks. The matrix $\mathrm{X}^{[q/4]}$ satisfies (i,ii,iv,v) if $\mathrm{X}^{[q/2]}$ does. For (i,ii,v) this is clear, and we briefly consider property (iv). Notice that a diagonal element of $\mathrm{X}^{[q/4]}$ corresponds to a full 2×2 submatrix of $\mathrm{X}^{[q/2]}$ but a non-empty non-diagonal element corresponds to a diagonal or anti-diagonal 2×2 submatrix with one and the same element. Suppose $\mathrm{X}^{[q/4]}$ contains a full 2×3 submatrix $\mathrm{X}^{[2\times 3]}$. If $\mathrm{X}^{[2\times 3]}$ involves two diagonal elements, it implies $z_3 \oplus z_4 = 0$ for some $z_3, z_4 \in Z$ (impossible by $\neg\mathsf{D}_1(Z)$). If $\mathrm{X}^{[2\times 3]}$ involves one diagonal element, it implies $z_1 \oplus z_2 \oplus z_3 \oplus z_4 = 0$ for some $z_3, z_4 \in Z$ (impossible by (v)). If $\mathrm{X}^{[2\times 3]}$ involves zero diagonal elements, it implies $z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 = 0$ for some $z_3, z_4, z_5, z_6 \in Z$ (impossible by (v)). The last property comes from selecting 6 coefficients of $\mathrm{X}^{[q/2]}$ such that in any row/column either two or zero coefficients are selected. By the form of $\mathrm{X}^{[2\times 3]}$ and the properties (i,ii), this turns out to be possible for the matrix $\mathrm{X}^{[q/2]}$.

We reduced the problem to a smaller dimension $q/4$, but with the same properties. This analysis can be applied recursively, until we are left with a 2×2 matrix $\mathrm{X}^{[2]}$. By induction to the size of q, we can now show that for matrices satisfying properties (i,ii,iv,v) the number of elements is upper bounded by $q \log(2q)$. For $q = 2$, we have $s(\mathrm{X}^{[2]}) = 4 = q \log(2q)$, so the claim holds. Suppose $s(\mathrm{X}^{[k/2]}) \leq k/2 \log k$. Then,

$$s(\mathrm{X}^{[k]}) \leq 2 \cdot (k/2) + 2s(\mathrm{X}^{[k/2]}) \leq k(1 + \log k) = k \log(2k)\,.$$

Thus, $s(\mathrm{X}^{[q/2]}) \leq q/2 \log q$. For the original matrix X, we now obtain $s(\mathrm{X}) \leq 4s(X^{[q/2]}) + q \leq 2q \log q + q$, which completes the argument for q a power of two. As explained in the beginning of this appendix, this result implies $s(\mathrm{X}) \leq 10q \log q$ for any q.