Tweakable Block Ciphers Secure Beyond the Birthday Bound in the Ideal Cipher Model

ByeongHak Lee and Jooyoung Lee*

KAIST, Korea
{lbh0307,hicalf}@kaist.ac.kr

Abstract. We propose a new construction of tweakable block ciphers from standard block ciphers. Our construction, dubbed XHX2, is the cascade of two independent XHX block ciphers, so it makes two calls to the underlying block cipher using tweak-dependent keys. We prove the security of XHX2 up to $\min\{2^{2(n+m)/3}, 2^{n+m/2}\}$ queries (ignoring logarithmic factors) in the ideal cipher model, when the block cipher operates on n-bit blocks using m-bit keys. The XHX2 tweakable block cipher is the first construction that achieves beyond-birthday-bound security with respect to the input size of the underlying block cipher in the ideal cipher model.

Keywords: tweakable block cipher, beyond-birthday-bound security, ideal cipher model

1 Introduction

Tweakable block ciphers, first introduced in [9], are a generalization of standard block ciphers that accept extra inputs called *tweaks*. The tweak, providing inherent variability to the block cipher, makes it easy to design various higher level cryptographic schemes such as message authentication codes and modes of operation.

Tweakable block ciphers can either be designed from scratch [4, 5, 17], or be built upon off-the-shelf cryptographic primitives such as block ciphers and (public) permutations [3, 8, 11, 14]. In this work, we will specifically focus on block cipher-based constructions; one of the advantages of such constructions is that the trust in extensively-studied block ciphers can be transferred to the tweakable block ciphers via security reductions. In this line of research, it has been suggested that changing tweaks should be cheaper than changing keys. Following this principle, early proposals including LRW1 and LRW2 [8, 9], and their cascades used their underlying block ciphers with fixed keys, namely *tweak independent keys*. So changing tweaks does not require rekeying the underlying block cipher. The security of tweakable block ciphers without tweak-rekeying

* Jooyoung Lee was supported by a National Research Foundation of Korea (NRF) grant funded by the Korean government (Ministry of Science and ICT), No. NRF-2017R1E1A1A03070248.

has typically been analyzed in the standard model, where the block cipher with a secret random key is replaced by a secret random permutation.

Recently, a unified vision for the tweak and key inputs has been proposed within the TWEAKEY framework [6]. From this point of view, tweakable block ciphers using *tweak dependent keys* have been studied [10, 18]. By using tweak dependent keys, one might expect a higher level of security (than using fixed keys), whereas the security of such constructions is typically analyzed in the ideal cipher model.

Our Results. Suppose that a κ-bit key tweakable block cipher TBC has been built on an m-bit key n-bit block cipher E (modeled as an ideal cipher). Typically, each evaluation of TBC would need a fixed number of calls to the underlying block cipher E, and hence $O(2^\kappa)$ block cipher queries will be sufficient to mount an exhaustive key search on TBC. However, if $n+m < \kappa$, then one would be able to find its secret key (in an information theoretic sense) by making all possible 2^{n+m} block cipher queries. Therefore, TBC will not be provably secure beyond $2^{\min\{\kappa,n+m\}}$ queries in the ideal cipher model. In this line of research, recent work has been aimed at achieving security beyond $2^{n/2}$ (precisely, 2^n) assuming $\kappa = m = n$ [10, 18]. This level of security is optimal, but still it is only the birthday bound with respect to the input size of the ideal cipher, namely $n + m$. If a tweakable block cipher accepts sufficiently large keys (for example, if $\kappa > n = m$), then one might expect security beyond 2^n. The problem that we tackle in this paper is to construct a tweakable block cipher secure beyond the birthday bound with respect to the input size of the underlying block cipher in the ideal cipher model (as the counterpart of $\mathsf{LRW2}$[2] in the standard model), assuming $\kappa > n + m$. [1]

We begin with XHX proposed by Jha et al. [7]. Let $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be an m-bit key n-bit block cipher, let $\mathcal{T}$ be a tweak space, and let $\mathcal{G}$ and $\mathcal{H}$ be families of functions $g : \mathcal{T} \to \{0,1\}^n$ and $h : \mathcal{T} \to \{0,1\}^m$, respectively. Then the XHX tweakable block cipher accepts a key $(g, h) \in \mathcal{G} \times \mathcal{H}$ and a tweak $t \in \mathcal{T}$, and encrypts a plaintext $x \in \{0,1\}^n$ by computing

$$E_{h(t)}(x \oplus g(t)) \oplus g(t).$$

If $\mathcal{G}$ is δ-almost uniform and δ-almost XOR-universal, and if $\mathcal{H}$ is δ'-almost uniform and δ'-almost universal with $\delta \approx 1/2^n$ and $\delta' \approx 1/2^m$, then XHX is proved to be secure up to $2^{(n+m)/2}$ queries in the ideal cipher model.

Our main contribution is to prove the security of the cascade of two independent XHX constructions (see Figure 1), dubbed $\mathsf{XHX2}$, up to

$$\min\{2^{\frac{2(n+m)}{3}}, 2^{n+\frac{m}{2}-\log_2 n}\}$$

queries. To the best of our knowledge, this is the first construction of a tweakable block cipher that achieves beyond-birthday-bound security with respect to the input size of the underlying block cipher.

[1] This assumption is similar to the study of key length extension, where the key size of the entire scheme is sometimes larger than the input size of the underlying block cipher.

Table 1: Comparison of XHX2 with existing tweakable block ciphers.

Construction	Key size	Security ($\log_2$)	Efficiency			References
			E	$\otimes/\mathcal{H}$	TDK	
LRW1	n	$n/2$	2	0	✗	[9]
LRW2, XEX	$2n$	$n/2$	1	1		[9, 16]
LRW2[2]	$4n$	$2n/3$	2	2		[3]
LRW2[s]	$2sn$	$sn/(s+2)$	s	s		[3]
Min	n	$\max\{n/2, n-\|t\|\}$	2	0	✓	[12]
$\widetilde{F}[1]$	n	$2n/3$	1	1		[10]
$\widetilde{F}[2]$	n	n	2	0		[10, 18]
$\widetilde{E1}, \ldots, \widetilde{E32}$	$n(2n)$	n	2(1)	0		[18]
XHX	$n+m$	$(n+m)/2$	1	2		[7]
XHX2	$2n+2m$	$\min\{2(n+m)/3, n+m/2\}$	2	4		This work

For simplicity, we will prove the security of XHX2 under the assumption that the first and the second block cipher calls are made to independent block ciphers. However, in the ideal cipher model, a single key bit will be sufficient to separate a single block cipher into two independent ones with negligible security loss.

We believe that our results are not only of theoretical interest, but also practically relevant in certain environments, in particular where stronger security is required with block ciphers operating on (relatively) small blocks (e.g., CAST-128 [1], KATAN, KTANTAN [2], Simeck [19]). For example, CAST-128 (used in GPG and PGP) operates on 64-bit blocks using 128-bit keys. Based on this block cipher, the resulting XHX2 provides 128-bit security (ignoring log factors and constants), while this level of security would not be achieved with any other existing construction. On the other hand, the key schedule of the underlying block cipher should not be too simple (being secure against related-key and known-/chosen-key distinguishing attacks) since every block cipher key is supposed to define an independent permutation in our security model.

Comparison. A comparison of XHX2 with the existing tweakable block ciphers is given in Table 1. In this table, security is evaluated by the threshold number of queries in $\log_2$. In Min, $|t|$ denotes the fixed tweak length. All the constructions with tweak-rekeying are analyzed in the ideal cipher model, while the constructions without tweak-rekeying are in the standard model. Efficiency is evaluated by the number of block cipher calls, the number of multiplications or universal hashes, and the use of tweak dependent keys (represented by TDK).

Discussion. It is notable that our result for XHX2 implies beyond-birthday-bound security for the cascade of two independent XTX [13] constructions (for the first time).

In typical TBC-based modes of operation (such as TBC, TAE [9] and SCT [15]), nonces and counters are placed into the tweak; when the tweak size is limited to the key size of the underlying block cipher, the hash computation can be defined as a single multiplication, namely $t \cdot k$ for a hash key k and a tweak t. In this case,

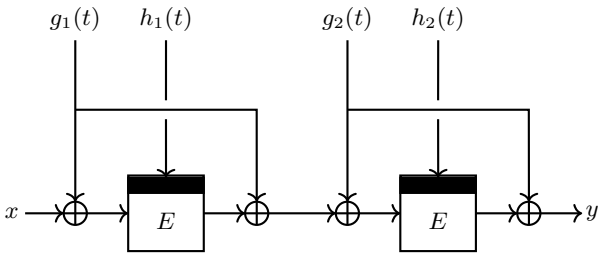
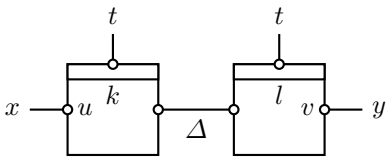


Fig. 1: Tweakable block cipher XHX2.

different tweaks map to different block cipher keys, removing the possibility of (C-14), and hence the term $2^{n+m/2}$ from the security bound.

Overview of the Proof. Our security proof is based on the standard H-coefficient technique. We begin by defining a set of bad transcripts. The badness will be determined solely by the choice of hash keys g_1, g_2, h_1 and h_2. Once the hash keys are fixed, we can associate each construction query (t, x, y) with a 5-tuple $(h_1(t), h_2(t), x \oplus g_1(t), y \oplus g_2(t), g_1(t) \oplus g_2(t))$, which will be called a "reduced query". As long as the hash keys are not bad, the reduced queries will be all distinct. Let $k = h_1(t)$, $l = h_2(t)$, $u = x \oplus g_1(t)$, $v = y \oplus g_2(t)$ and $\Delta = g_1(t) \oplus g_2(t)$. The relation between a reduced query (k, l, u, v, Δ) and its original query (t, x, y) can be pictorially represented as follows.



The core of the proof is to show that the probabilities to obtain any good transcript are close in the real and in the ideal world, or particularly, to tightly lower bound the probability of obtaining a good transcript in the real world. In the real world, randomness comes only from the underlying ideal ciphers E_1 and E_2. For example, suppose that $E_1(k, u)$ has been determined by a block cipher query (i.e., query history $\mathcal{Q}_E$). Then the probability that E_1 and E_2 complete the reduced query (k, l, u, v, Δ) becomes the probability that E_2 maps $E_1(k, u) \oplus \Delta$ to v with key l, where we can assume that $E_2(l, E_1(k, u) \oplus \Delta)$ and $E_2^{-1}(l, v)$ have not been fixed excluding bad keys (of (C-9) and (C-10)). Fixing $E_2(l, E_1(k, u) \oplus \Delta) = v$ might affect the freedom of other construction queries, making the analysis complicated. The notion of a reduced query helps systematically dealing with this problem; we will carefully classify the reduced queries into five classes, and compute the (conditional) probability of completing each class of queries one by one. This classification will be defined in detail at Section 3.3.

2 Preliminaries

Basic Notation. In all the following, we fix positive integers m and n, and denote $N = 2^n$. Given a non-empty set $\mathcal{X}$, $x \leftarrow_{\$} \mathcal{X}$ denotes that x is chosen uniformly at random from $\mathcal{X}$. For a set $\mathcal{X}$ and an integer $b \geq 1$, we write $x_1, \ldots, x_b \in^{\neq} \mathcal{X}$ to mean that $x_1, \ldots, x_b$ are pairwise distinct elements of $\mathcal{X}$. The set of all sequences that consist of b pairwise distinct elements of $\mathcal{X}$ is denoted $\mathcal{X}^{*b}$. For integers $1 \leq b \leq a$, we will write $(a)_b = a(a-1)\cdots(a-b+1)$ and $(a)_0 = 1$ by convention. If $|\mathcal{X}| = a$, then $(a)_b$ becomes the size of $|\mathcal{X}^{*b}|$. When two sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint, we denote $\mathcal{X} \sqcup \mathcal{Y}$ their (disjoint) union.

Useful Lemma. The following lemma, viewed as a generalization of Lemma 5 in [3], will be used in the security proof of XHX2.

Lemma 1. *Let N, a, b, c, d be positive integers such that $a+b \leq N/2$, $a+c \leq N/2$, $d \leq b$ and $d \leq c$. Then*

$$\frac{(N-d)_a(N-b-c+d)_a}{(N-b)_a(N-c)_a} \geq 1 - \frac{4a(b-d)(c-d)}{N^2}.$$

Due to the space limit, the proof of this lemma will be given in the full version.

Uniform, Universal and XOR-Universal Hash Functions. We will need the following definitions of almost uniform, almost universal (AU) and almost XOR-universal (AXU) hash functions.

Definition 1. *Let $\delta > 0$, and let $\mathcal{H}$ be a family of functions $h : \mathcal{T} \to \mathcal{Y}$ for non-empty sets $\mathcal{T}$ and $\mathcal{Y}$.*

1. *$\mathcal{H}$ is said to be* δ-almost uniform *if for any $x \in \mathcal{T}$ and any $y \in \mathcal{Y}$,*

$$\Pr[h \leftarrow_{\$} \mathcal{H} : h(x) = y] \leq \delta.$$

2. *$\mathcal{H}$ is said to be* δ-almost universal (δ-AU) *if for any distinct x and $x' \in \mathcal{T}$,*

$$\Pr[h \leftarrow_{\$} \mathcal{H} : h(x) = h(x')] \leq \delta.$$

3. *When $\mathcal{Y} = \{0,1\}^n$, $\mathcal{H}$ is said to be* δ-almost XOR-universal (δ-AXU) *if for any distinct $x, x' \in \mathcal{T}$ and any $y \in \mathcal{Y}$,*

$$\Pr[h \leftarrow_{\$} \mathcal{H} : h(x) \oplus h(x') = y] \leq \delta.$$

Remark 1. Hash functions in $\mathcal{H}$ are typically indexed by keys in a certain key space, written as $\mathcal{H} : \mathcal{K} \times \mathcal{T} \to \mathcal{Y}$ for a key space $\mathcal{K}$. For example, let $\mathcal{K} = \mathcal{Y} = \{0,1\}^n$ and let $\mathcal{T} = \{0,1\}^{dn} \setminus \{(0,\ldots,0)\}$ for a positive integer d. Identifying $\{0,1\}^n$ with a finite field $\mathbf{GF}(2^n)$ with 2^n elements and representing an element $t \in \mathcal{T}$ as a concatenation of n-bit elements $t_d, \ldots, t_1$, define

$$\begin{aligned} \mathcal{H} \ : \ \mathcal{K} \times \mathcal{T} &\longrightarrow \{0,1\}^n \\ (k, t_d || \ldots || t_1) &\longmapsto t_d \cdot k^d + \cdots + t_1 \cdot k. \end{aligned}$$

Then it is not hard to show that $\mathcal{H}$ is $\frac{d}{2^n}$-almost uniform and $\frac{d}{2^n}$-almost XOR-universal. As seen in this example, for any n, one can define a δ-almost uniform and δ-almost XOR-universal family of functions with n-bit key, n-bit output, and $\delta \approx 1/2^n$ (ignoring d).

The Ideal Cipher Model. A block cipher with key space $\mathcal{K}$ and message space $\mathcal{X}$ is a mapping $E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ such that, for any key $k \in \mathcal{K}$, $x \mapsto E(k, x)$ is a permutation of $\mathcal{X}$. Throughout this paper, we will fix $\mathcal{K} = \{0,1\}^m$ and $\mathcal{X} = \{0,1\}^n$, and write $\mathsf{BC}(m, n)$ to mean the set of all such block ciphers.

In the ideal cipher model, a block cipher E is chosen from $\mathsf{BC}(m, n)$ uniformly at random. It allows for two types of oracle queries $E(k, x)$ and $E^{-1}(k, y)$ for $x, y \in \{0,1\}^n$ and $k \in \{0,1\}^m$. The response to an inverse query $E^{-1}(k, y)$ is $x \in \{0,1\}^n$ such that $E(k, x) = y$.

Tweakable Block Ciphers. A tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $\widetilde{P} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that, for any tweak $t \in \mathcal{T}$, $x \mapsto \widetilde{P}(t, x)$ is a permutation of $\mathcal{X}$. Throughout the paper, we will fix $\mathcal{X} = \{0,1\}^n$, and write $\mathsf{Perm}(\mathcal{T}, n)$ to mean the set of all tweakable permutations with tweak space $\mathcal{T}$ and message space $\{0,1\}^n$.

A tweakable block cipher TBC with key space $\mathcal{K}$, tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $\mathsf{TBC} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that for any key $\mathbf{k} \in \mathcal{K}$, $(t, x) \mapsto \mathsf{TBC}(\mathbf{k}, t, x)$ is a tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$.

Indistinguishability. For $s \geq 1$, we will consider a tweakable block cipher TBC based on a set of block ciphers

$$\mathcal{E} = (E_1, \ldots, E_s) \in \mathsf{BC}(m, n)^s.$$

So each key $\mathbf{k} \in \mathcal{K}$ and a set of block ciphers $\mathcal{E} = (E_1, \ldots, E_s) \in \mathsf{BC}(m, n)^s$ define a tweakable permutation, denoted $\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}]$, with tweak space $\mathcal{T}$ and message space $\mathcal{X}$. Specifically, we have $s = 1$ for XHX and $s = 2$ for $\mathsf{XHX2}$, and $\mathcal{X} = \{0,1\}^n$ for both constructions.

In the *real* world, a secret key $\mathbf{k} \in \mathcal{K}$ is chosen uniformly at random. A set of s block ciphers $E_1, \ldots, E_s$ are also chosen independently at random from $\mathsf{BC}(m, n)$. A distinguisher $\mathcal{D}$ is given oracle access to $\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}]$ as well as $\mathcal{E} = (E_1, \ldots, E_s)$. In the *ideal* world, $\mathcal{D}$ is given a random tweakable permutation $\widetilde{P} \in \mathsf{Perm}(\mathcal{T}, n)$ instead of $\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}]$. However, oracle access to $\mathcal{E} = (E_1, \ldots, E_s)$ is still allowed in this world.

The adversarial goal is to tell apart the two worlds $(\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}], \mathcal{E})$ and $(\widetilde{P}, \mathcal{E})$ by adaptively making forward and backward queries to the construction and each of the block ciphers. Formally, $\mathcal{D}$'s distinguishing advantage is defined by

$$\begin{aligned}\mathbf{Adv}_{\mathsf{TBC}}(\mathcal{D}) = &\Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}(\mathcal{T}, n), \mathcal{E} \leftarrow_{\$} \mathsf{BC}(m, n)^s : 1 \leftarrow \mathcal{D}^{\mathcal{E}, \widetilde{P}}\right] \\ &- \Pr\left[\mathbf{k} \leftarrow_{\$} \mathcal{K}, \mathcal{E} \leftarrow_{\$} \mathsf{BC}(m, n)^s : 1 \leftarrow \mathcal{D}^{\mathcal{E}, \mathsf{TBC}_{\mathbf{k}}[\mathcal{E}]}\right].\end{aligned}$$

For p, $q > 0$, we define

$$\mathbf{Adv}_{\mathsf{TBC}}(p, q) = \max_{\mathcal{D}} \mathbf{Adv}_{\mathsf{TBC}}(\mathcal{D})$$

where the maximum is taken over all adversaries $\mathcal{D}$ making at most p queries to each of the block ciphers and at most q queries to the outer tweakable permutation.

H-coefficient Technique. Suppose that a distinguisher $\mathcal{D}$ makes p queries to each of the block ciphers, and q queries to the construction oracle. The queries made to the construction oracle are recorded in a query history

$$\mathcal{Q}_C = (t_i, x_i, y_i)_{1 \le i \le q}.$$

So according to the instantiation, it would imply either $\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}](t_i, x_i) = y_i$ or $\widetilde{P}(t_i, x_i) = y_i$. For $j = 1, \ldots, s$, the queries made to E_j are recorded in a query history

$$\mathcal{Q}_{E_j} = (j, k_{j,i}, u_{j,i}, v_{j,i})_{1 \le i \le p},$$

where $(j, u_{j,i}, v_{j,i})$ represents the evaluation $E_j(k_{j,i}, u_{j,i}) = v_{j,i}$ obtained by the i-th query to E_j. We will often omit the index j when it is clear from context. Let

$$\mathcal{Q}_E = \mathcal{Q}_{E_1} \cup \cdots \cup \mathcal{Q}_{E_s}.$$

Then the pair of query histories $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$ will be called the *transcript* of the attack: it contains all the information that $\mathcal{D}$ has obtained at the end of the attack. In this work, we will only consider information theoretic distinguishers. Therefore we can assume that a distinguisher is deterministic without making any redundant query, and hence the output of $\mathcal{D}$ can be regarded as a function of τ, denoted $\mathcal{D}(\tau)$ or $\mathcal{D}(\mathcal{Q}_C, \mathcal{Q}_E)$.

Fix a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, a key $\mathbf{k} \in \mathcal{K}$, a tweakable permutation $\widetilde{P} \in \mathsf{Perm}(\mathcal{T}, n)$, a tuple of block ciphers $\mathcal{E} = (E_1, \ldots, E_s) \in \mathsf{BC}(m, n)^s$ and $j \in \{1, \ldots, s\}$: if $\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}](t_i, x_i) = y_i$ (resp. $\widetilde{P}(t_i, x_i) = y_i$) for every $i = 1, \ldots, q$, then we will write $\mathsf{TBC}_{\mathbf{k}}[\mathcal{E}] \vdash \mathcal{Q}_C$ (resp. $\widetilde{P} \vdash \mathcal{Q}_C$). Similarly, if $E_j(k_{j,i}, u_{j,i}) = v_{j,i}$ for every $i = 1, \ldots, p$, then we will write $E_j \vdash \mathcal{Q}_{E_j}$. We will write $\mathcal{E} \vdash \mathcal{Q}_E$ if $E_j \vdash \mathcal{Q}_{E_j}$ for every $j = 1, \ldots, s$.

If there exist $\widetilde{P} \in \mathsf{Perm}(\mathcal{T}, n)$ and $\mathcal{E} \in \mathsf{BC}(m, n)^s$ that outputs τ at the end of the interaction with $\mathcal{D}$, then we will call the transcript τ *attainable*. So for any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, there exist $\widetilde{P} \in \mathsf{Perm}(\mathcal{T}, n)$ and $\mathcal{E} \in \mathsf{BC}(m, n)^s$ such that $\widetilde{P} \vdash \mathcal{Q}_C$ and $\mathcal{E} \vdash \mathcal{Q}_E$. For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$ and a key $\mathbf{k} \in \mathcal{K}$, let

$$\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C | \mathcal{Q}_E) = \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}(\mathcal{T}, n), \mathcal{E} \leftarrow_{\$} \mathsf{BC}(m, n)^s : \widetilde{P} \vdash \mathcal{Q}_C \middle| \mathcal{E} \vdash \mathcal{Q}_E\right],$$

$$\mathsf{p}_{\mathsf{re}}(\mathcal{Q}_C | \mathcal{Q}_E) = \Pr\left[\mathbf{k} \leftarrow_{\$} \mathcal{K}, \mathcal{E} \leftarrow_{\$} \mathsf{BC}(m, n)^s : \mathsf{TBC}_{\mathbf{k}}[\mathcal{E}] \vdash \mathcal{Q}_C \middle| \mathcal{E} \vdash \mathcal{Q}_E\right],$$

$$\mathsf{p}^{\mathbf{k}}_{\mathsf{re}}(\mathcal{Q}_C | \mathcal{Q}_E) = \Pr\left[\mathcal{E} \leftarrow_{\$} \mathsf{BC}(m, n)^s : \mathsf{TBC}_{\mathbf{k}}[\mathcal{E}] \vdash \mathcal{Q}_C \middle| \mathcal{E} \vdash \mathcal{Q}_E\right].$$

With respect to an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, we will define a set of "bad" keys, denoted $\mathcal{K}_{\mathsf{bad}}$, such that the probability of a uniform random key being bad is small, while the ratio $\mathsf{p}^{\mathbf{k}}_{\mathsf{re}}(\mathcal{Q}_C|\mathcal{Q}_E)/\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C|\mathcal{Q}_E)$ is close to 1 for any "good" key $\mathbf{k} \in \mathcal{K} \setminus \mathcal{K}_{\mathsf{bad}}$. With these definitions, the following lemma, the core of the H-coefficients technique, will be also used in our security proof.

Lemma 2. *Let $\varepsilon_1, \varepsilon_2 > 0$. Suppose that for any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, there exists $\mathcal{K}_{\mathsf{bad}} \subset \mathcal{K}$ such that $|\mathcal{K}_{\mathsf{bad}}|/|\mathcal{K}| \leq \varepsilon_1$ and for any $\mathbf{k} \in \mathcal{K} \setminus \mathcal{K}_{\mathsf{bad}}$*

$$\mathsf{p}^{\mathbf{k}}_{\mathsf{re}}(\mathcal{Q}_C|\mathcal{Q}_E) \geq (1-\varepsilon_2)\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C|\mathcal{Q}_E).$$

Then one has

$$\mathbf{Adv}_{\mathsf{TBC}}(\mathcal{D}) \leq \varepsilon_1 + \varepsilon_2.$$

3 Security Proof for XHX2

Let $E_1, E_2 : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be m-bit key n-bit block ciphers, let $\mathcal{T}$ be a tweak space, and let $\mathcal{G}$ and $\mathcal{H}$ be families of hash functions $g : \mathcal{T} \to \{0,1\}^n$ and $h : \mathcal{T} \to \{0,1\}^m$, respectively. The XHX2 tweakable block cipher accepts a key $\mathbf{k} = (g_1, h_1, g_2, h_2) \in \mathcal{K} =^{\text{def}} \mathcal{G} \times \mathcal{H} \times \mathcal{G} \times \mathcal{H}$ and a tweak $t \in \mathcal{T}$, and encrypts a plaintext $x \in \{0,1\}^n$ by computing

$$E_2\left(h_2(t), E_1(h_1(t), x \oplus g_1(t)) \oplus g_1(t) \oplus g_2(t)\right) \oplus g_2(t).$$

Theorem 1. *Let $\delta, \delta' > 0$, let $\mathcal{G}$ be a δ-almost uniform and universal family of hash functions from $\mathcal{T}$ to $\{0,1\}^n$ and let $\mathcal{H}$ be a δ'-almost uniform and XOR-universal family of hash functions from $\mathcal{T}$ to $\{0,1\}^m$. Then for any integers p and q, one has*

$$\mathbf{Adv}_{\mathsf{XHX2}}(p,q) \leq 64p^{\frac{2}{3}}q^{\frac{2}{3}}\delta\delta' + \frac{256(8q^3+2pq^2)^{\frac{1}{2}}\delta^{\frac{1}{2}}\delta'}{N^{\frac{1}{2}}} + \frac{160(16q^3+8pq^2+p^2q)^{\frac{1}{2}}\delta'}{N}$$
$$+ 256(16q^3+8pq^2+2q^2+3p^2q)\delta^2(\delta')^2 + \frac{131072n^2q^2\delta'}{N^2}.$$

3.1 Giving Free Queries to the Distinguisher

For the security proof of XHX2, we will make an additional assumption on the attack model; a distinguisher $\mathcal{D}$ will be given free queries at the end of the attack by the following rule.

1. If $\mathcal{D}$ has made $N/4$ or more block cipher queries to E_1 (resp. E_2) for a fixed key $k \in \{0,1\}^m$, then $\mathcal{D}$ will be given $E_1(k,u)$ (resp. $E_2(k,u)$) for all unqueried u (if any).
2. If $\mathcal{D}$ has made $N/16$ or more queries to the construction oracle C for a fixed tweak $t \in \mathcal{T}$, then $\mathcal{D}$ will be given $C(t,x)$ for all unqueried x (if any).

This modification would not degrade the adversarial distinguishing advantage since $\mathcal{D}$ is free to ignore the additional information. Suppose that $\mathcal{D}$ makes at most p queries to each of the block ciphers and at most q queries to the outer tweakable permutation. Then the number of free queries given to $\mathcal{D}$ is upper bounded by $3p$ for each block cipher, and by $15q$ for the tweakable permutation. So this assumption can be viewed as transforming $\mathcal{D}$ into a new distinguisher $\mathcal{D}'$ that

(i) makes at most $4p$ queries to each of the block ciphers and at most $16q$ queries to the outer tweakable permutation;

(ii) makes either all N queries or less than $N/4$ queries for each key and each of the block ciphers;

(iii) makes either all N queries or less than $N/16$ construction queries for each tweak.

Let

$$\mathbf{Adv}^{*}_{\mathsf{TBC}}(p,q) = \max_{\mathcal{D}'} \mathbf{Adv}_{\mathsf{TBC}}(\mathcal{D}')$$

where the maximum is taken over all adversaries $\mathcal{D}'$ that make at most p queries to each of the block ciphers and at most q queries to the outer tweakable permutation *satisfying conditions (ii) and (iii)*. Then we have

$$\mathbf{Adv}_{\mathsf{XHX2}}(p,q) \leq \mathbf{Adv}^{*}_{\mathsf{XHX2}}(4p, 16q). \tag{1}$$

Henceforth, we will assume that a modified adversary $\mathcal{D}'$ makes p primitive queries to each of the block ciphers and q construction queries.

For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, we will use the following notations: for r, $s \in \{0,1\}^m$, and $w \in \mathcal{T}$,

$$\begin{aligned}
\mathcal{Q}_{E_1}(r) &= \{(k,u,v) \in \mathcal{Q}_{E_1} : k = r\},\\
\mathcal{Q}_{E_2}(s) &= \{(l,u,v) \in \mathcal{Q}_{E_2} : l = s\},\\
\mathcal{Q}_{C}(w) &= \{(t,x,y) \in \mathcal{Q}_{C} : t = w\}.
\end{aligned}$$

Note that either $|\mathcal{Q}_{E_i}(r)| < N/4$ or $|\mathcal{Q}_{E_i}(r)| = N$ for any $r \in \{0,1\}^m$ and $i = 1, 2$. Similarly, we have either $|\mathcal{Q}_C(w)| < N/16$ or $|\mathcal{Q}_C(w)| = N$ for any $w \in \mathcal{T}$. In particular, we will write

$$\mathcal{T}^{*} = \{t \in \mathcal{T} : |\mathcal{Q}_C(t)| = N\}, \qquad \mathcal{Q}^{*}_{C} = \bigsqcup_{t \in \mathcal{T}^{*}} \mathcal{Q}_C(t).$$

3.2 Bad Keys

Fix an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, and positive integers M_1, M_2, M_3 (that will be optimized later). Let

$$\mathcal{A}_1 = \{((t,x,y),(k,u,v)) \in \mathcal{Q}_C \times \mathcal{Q}_{E_1} : (h_1(t), x \oplus g_1(t)) = (k,u)\},$$
$$\mathcal{A}_2 = \{((t,x,y),(k,u,v)) \in \mathcal{Q}_C \times \mathcal{Q}_{E_2} : (h_2(t), y \oplus g_2(t)) = (k,v)\},$$
$$\mathcal{B}_1 = \{((t,x,y),(t',x',y')) \in \mathcal{Q}_C^{*2} : \exists (t'',x'',y'') \neq (t,x,y),(t',x',y') \text{ such that } x \oplus g_1(t) = x'' \oplus g_1(t''),\ h_1(t) = h_1(t''),\ h_2(t) = h_2(t')\},$$
$$\mathcal{B}_2 = \{((t,x,y),(t',x',y')) \in \mathcal{Q}_C^{*2} : \exists (t'',x'',y'') \neq (t,x,y),(t',x',y') \text{ such that } y \oplus g_2(t) = y'' \oplus g_2(t''),\ h_2(t) = h_2(t''),\ h_1(t) = h_1(t')\},$$
$$\mathcal{B}_3 = \{((t,x,y),(k,u,v)) \in \mathcal{Q}_C \times \mathcal{Q}_{E_1} : \exists (t',x',y') \neq (t,x,y) \text{ such that } y \oplus g_2(t) = y' \oplus g_2(t'),\ h_2(t) = h_2(t'),\ h_1(t) = k\},$$
$$\mathcal{B}_4 = \{((t,x,y),(k,u,v)) \in \mathcal{Q}_C \times \mathcal{Q}_{E_2} : \exists (t',x',y') \neq (t,x,y) \text{ such that } x \oplus g_1(t) = x' \oplus g_1(t'),\ h_1(t) = h_1(t'),\ h_2(t) = k\},$$
$$\mathcal{C}_1 = \{((t,x,y),(t',x',y'),(t'',x'',y'')) \in \mathcal{Q}_C^3 : t \neq t',\ t \neq t'',\ h_1(t) = h_1(t'),\ h_2(t) = h_2(t'')\},$$
$$\mathcal{C}_2 = \{((t,x,y),(t',x',y'),(k,u,v)) \in \mathcal{Q}_C^2 \times \mathcal{Q}_{E_1} : t \neq t',\ h_2(t) = h_2(t'),\ h_1(t) = k\},$$
$$\mathcal{C}_3 = \{((t,x,y),(t',x',y'),(k,u,v)) \in \mathcal{Q}_C^2 \times \mathcal{Q}_{E_2} : t \neq t',\ h_1(t) = h_1(t'),\ h_2(t) = k\},$$
$$\mathcal{C}_4 = \{((t,x,y),(k,u,v),(k',u',v')) \in \mathcal{Q}_C \times \mathcal{Q}_{E_1} \times \mathcal{Q}_{E_2} : h_1(t) = k, h_2(t) = k'\}.$$

A key $\mathbf{k} = (g_1, h_1, g_2, h_2) \in \mathcal{K}$ is defined to be *bad* if one of the following conditions is fulfilled:

(C-1) $|\mathcal{A}_i| \geq M_1$ for some $i = 1, 2$;

(C-2) there exist $(t,x,y),(t',x',y') \stackrel{\neq}{\in} \mathcal{Q}_C$ and $(k,u,v),(k',u',v') \in \mathcal{Q}_{E_1}$ such that

$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (k,u),\\ (h_1(t'), x' \oplus g_1(t')) &= (k',u'),\\ (h_2(t), v \oplus g_1(t) \oplus g_2(t)) &= (h_2(t'), v' \oplus g_1(t') \oplus g_2(t'));\end{aligned}$$

(C-3) there exist $(t,x,y),(t',x',y') \stackrel{\neq}{\in} \mathcal{Q}_C$ and $(k,u,v),(k',u',v') \in \mathcal{Q}_{E_2}$ such that

$$\begin{aligned}(h_2(t), y \oplus g_2(t)) &= (k,v),\\ (h_2(t'), y' \oplus g_2(t')) &= (k',v'),\\ (h_1(t), u \oplus g_1(t) \oplus g_2(t)) &= (h_1(t'), u' \oplus g_1(t') \oplus g_2(t'));\end{aligned}$$

(C-4) $|\mathcal{B}_i| \geq M_2$ for some $i = 1, 2, 3, 4$;

(C-5) $|\mathcal{C}_i| \geq M_3$ for some $i = 1, 2, 3, 4$;

(C-6) there exist $(t, x, y), (t', x', y'), (t'', x'', y'') \in \mathcal{Q}_C$ such that $(t, x, y) \neq (t', x', y')$, $(t, x, y) \neq (t'', x'', y'')$ and

$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (h_1(t'), x' \oplus g_1(t')),\\ (h_2(t), y \oplus g_2(t)) &= (h_2(t''), y'' \oplus g_2(t''));\end{aligned}$$

(C-7) there exist $(t, x, y), (t', x', y') \in^{\neq} \mathcal{Q}_C$ such that

$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (h_1(t'), x' \oplus g_1(t')),\\ (h_2(t), g_1(t) \oplus g_2(t)) &= (h_2(t'), g_1(t') \oplus g_2(t'));\end{aligned}$$

(C-8) there exist $(t, x, y), (t', x', y') \in^{\neq} \mathcal{Q}_C$ such that

$$\begin{aligned}(h_1(t), g_1(t) \oplus g_2(t)) &= (h_1(t'), g_1(t') \oplus g_2(t')),\\ (h_2(t), y \oplus g_2(t)) &= (h_2(t'), y' \oplus g_2(t'));\end{aligned}$$

(C-9) there exist $(t, x, y) \in \mathcal{Q}_C$, $(k, u, v) \in \mathcal{Q}_{E_1}$ and $(k', u', v') \in \mathcal{Q}_{E_2}$ such that

$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (k, u),\\ (h_2(t), y \oplus g_2(t)) &= (k', v');\end{aligned}$$

(C-10) there exist $(t, x, y) \in \mathcal{Q}_C$, $(k, u, v) \in \mathcal{Q}_{E_1}$ and $(k', u', v') \in \mathcal{Q}_{E_2}$ such that

$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (k, u),\\ (h_2(t), v \oplus g_1(t) \oplus g_2(t)) &= (k', u');\end{aligned}$$

(C-11) there exist $(t, x, y) \in \mathcal{Q}_C$, $(k, u, v) \in \mathcal{Q}_{E_1}$ and $(k', u', v') \in \mathcal{Q}_{E_2}$ such that

$$\begin{aligned}(h_1(t), u' \oplus g_1(t) \oplus g_2(t)) &= (k, v),\\ (h_2(t), y \oplus g_2(t)) &= (k', v');\end{aligned}$$

(C-12) there exist $(t, x, y), (t', x', y') \in^{\neq} \mathcal{Q}_C$ and $(k, u, v) \in \mathcal{Q}_{E_1}$ such that

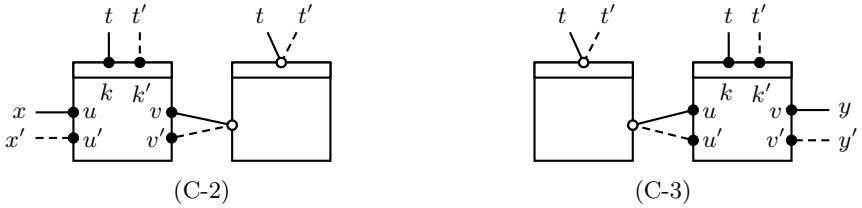
$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (k, u),\\ (h_2(t), y \oplus g_2(t)) &= (h_2(t'), y' \oplus g_2(t'));\end{aligned}$$

(C-13) there exist $(t, x, y), (t', x', y') \in^{\neq} \mathcal{Q}_C$ and $(k, u, v) \in \mathcal{Q}_{E_2}$ such that

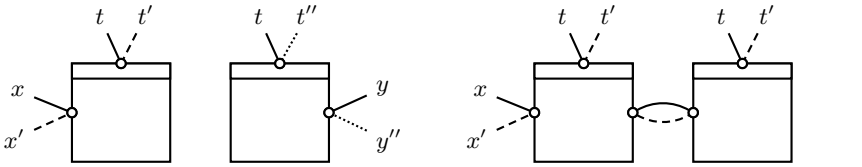
$$\begin{aligned}(h_1(t), x \oplus g_1(t)) &= (h_1(t'), x' \oplus g_1(t')),\\ (h_2(t), y \oplus g_2(t)) &= (k, v);\end{aligned}$$

(C-14) there exist $k \in \{0, 1\}^m$ and $h \in \{h_1, h_2\}$ such that

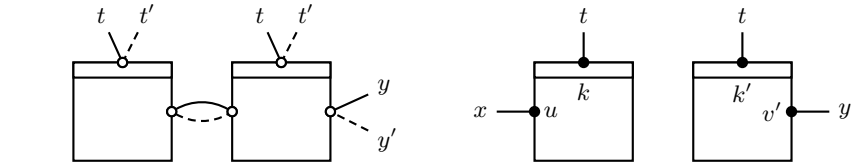
$$\frac{N}{4} \leq |\{(t, x, y) \in \mathcal{Q}_C \setminus \mathcal{Q}_C^* : h(t) = k\}|.$$



(C-2) (C-3)

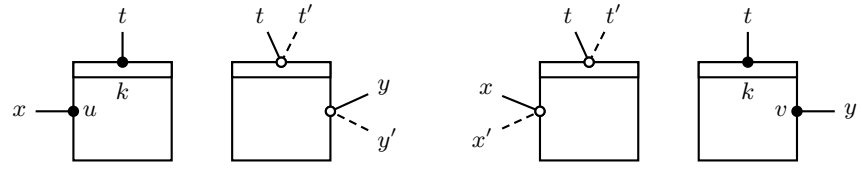


(C-6) (C-7)



(C-8) (C-9)

(C-10) (C-11)



(C-12) (C-13)

Fig. 2: Reduced queries that make bad conditions (C-2), (C-3) and (C-6) to (C-13). Black dots (resp. white dots) represent values fixed by $\mathcal{Q}_{E_1}$ and $\mathcal{Q}_{E_2}$ (resp. free values).

Fig. 2 pictorially represents bad conditions (C-2), (C-3) and (C-6) to (C-13) in terms of reduced queries (as defined in Section 3.3). The probability of having bad keys in the ideal world is upper bounded as follows.

Lemma 3. *For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$, let $\mathcal{K}_{\mathsf{bad}}$ be the set of bad keys defined as above. Then we have*

$$\frac{|\mathcal{K}_{\mathsf{bad}}|}{|\mathcal{K}|} \le \frac{2pq\delta\delta'}{M_1} + 2M_1^2\delta\delta' + \frac{(2q^3+2pq^2)\delta(\delta')^2}{M_2} + \frac{(q^3+2pq^2+p^2q)(\delta')^2}{M_3} + (q^3+2pq^2+2q^2+3p^2q)\delta^2(\delta')^2 + \frac{512n^2q^2\delta'}{N^2}.$$

For $i = 1, \ldots, 14$, let E_i denote the event that a uniform random key $\mathbf{k} \in \mathcal{K}$ satisfies condition (C-i). Then we have

$$\frac{|\mathcal{K}_{\mathsf{bad}}|}{|\mathcal{K}|} \le \Pr[\mathsf{E}_1 \vee \mathsf{E}_2 \vee \mathsf{E}_3] + \sum_{i=4}^{14} \Pr[\mathsf{E}_i]. \tag{2}$$

Here we only upper bound $\Pr[\mathsf{E}_{14}]$; the analysis of the other events are rather straightforward. Due to the space limit, the complete proof will be given in the full version.

Upper Bounding $\Pr[\mathsf{E}_{14}]$. Let

$$\mathcal{T}^i = \{w \in \mathcal{T} : 2^{i-1} \le |\mathcal{Q}_C(w)| < 2^i\},$$
$$\mathcal{Q}_C^i = \{(t,x,y) \in \mathcal{Q}_C(w) : w \in \mathcal{T}^i\},$$

for $i = 1, \ldots, n-4$. Then we have

$$\mathcal{T} \setminus \mathcal{T}^* = \bigsqcup_{i=1}^{n-4} \mathcal{T}^i, \qquad \mathcal{Q}_C \setminus \mathcal{Q}_C^* = \bigsqcup_{i=1}^{n-4} \mathcal{Q}_C^i.$$

For each $h \in \{h_1, h_2\}$ and $i \in \{1, \ldots, n-4\}$, we define two random variables

$$X_i = |\{(t,t') \in (\mathcal{T}^i)^{*2} : h(t) = h(t')\}|,$$
$$Y_i = \max_{\substack{\exists t_1,\ldots,t_\ell \in^{\neq} \mathcal{T}^i \text{ s.t.} \\ h(t_1)=\cdots=h(t_\ell)}} \ell.$$

Since $|\mathcal{T}^i| \le \frac{q}{2^{i-1}}$ and by the δ'-almost uniformity of $\mathcal{H}$, we have

$$\mathbf{E}[X_i] \le |\mathcal{T}^i|(|\mathcal{T}^i|-1)\delta' \le \left(\frac{q}{2^{i-1}}\right)^2 \delta'$$

for $i = 1, \ldots, n-4$. Since $Y_i(Y_i-1) \le X_i$ and by Markov's inequality, we have

$$\Pr\left[Y_i \ge \frac{q\sqrt{C\delta'}}{2^{i-1}} + 1\right] \le \Pr\left[Y_i(Y_i-1) \ge \left(\frac{q\sqrt{C\delta'}}{2^{i-1}}\right)^2\right] \le \Pr\left[X_i \ge C\left(\frac{q}{2^{i-1}}\right)^2 \delta'\right] \le \frac{1}{C}$$

for any $C > 0$. Therefore, for each $k \in \{0,1\}^m$ and $h \in \{h_1, h_2\}$, we have

$$|\{(t,x,y) \in \mathcal{Q}_C \setminus \mathcal{Q}_C^* : h(t) = k\}| < \sum_{i=1}^{n-4} Y_i 2^i < \sum_{i=1}^{n-4} \left(\frac{q\sqrt{C\delta'}}{2^{i-1}} + 1 \right) 2^i$$
$$< 2nq\sqrt{C\delta'} + \frac{N}{8}$$

except with probability at most n/C. By letting $C = \left(\frac{N}{16nq}\right)^2 \frac{1}{\delta'}$ (satisfying $2nq\sqrt{C\delta'} = N/8$), we have

$$\Pr[\mathsf{E}_{14}] \leq \frac{512n^2q^2\delta'}{N^2}. \tag{3}$$

3.3 Lower Bounding $\mathsf{p}^{\mathbf{k}}_{\mathsf{re}}(\mathcal{Q}_C|\mathcal{Q}_E)/\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C|\mathcal{Q}_E)$ For a Good Key

This section will be devoted to the proof of the following lemma.

Lemma 4. *For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_E)$ and a good key $\mathbf{k} = (g_1, h_1, g_2, h_2) \in \mathcal{K}$, one has*

$$\frac{\mathsf{p}^{\mathbf{k}}_{\mathsf{re}}(\mathcal{Q}_C|\mathcal{Q}_E)}{\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C|\mathcal{Q}_E)} \geq 1 - \left(\frac{16M_2}{N} + \frac{16M_3}{N^2} \right).$$

3.3.1 Useful Definitions and Properties

Let

$$\overline{\mathcal{Q}_C} = \{(h_1(t), h_2(t), x \oplus g_1(t), y \oplus g_2(t), g_1(t) \oplus g_2(t)) : (t,x,y) \in \mathcal{Q}_C\}.$$

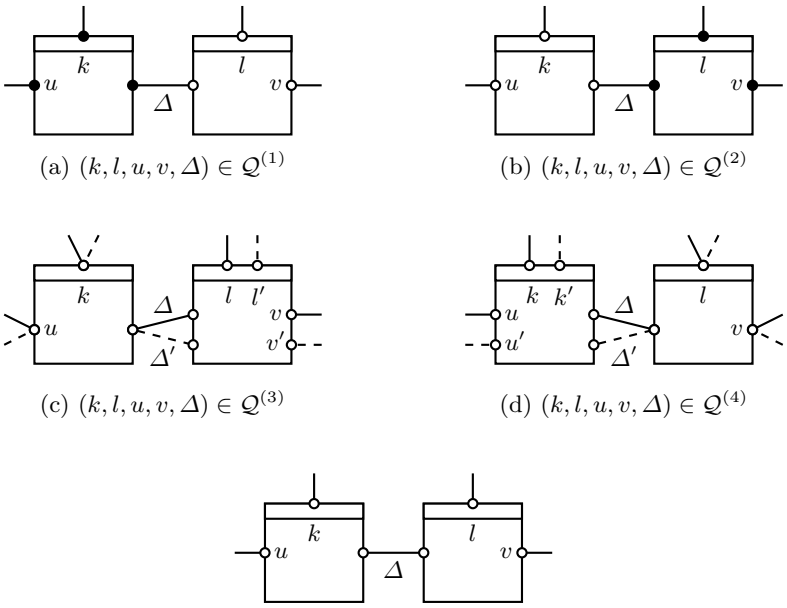
The elements of $\overline{\mathcal{Q}_C}$ will be called *reduced queries* (or simply queries). The reduced queries of $\overline{\mathcal{Q}_C}$ are all distinct, namely, if $(t,x,y) \neq (t',x',y')$, then

$$(h_1(t), h_2(t), x \oplus g_1(t), y \oplus g_2(t), g_1(t) \oplus g_2(t))$$
$$\neq (h_1(t'), h_2(t'), x \oplus g_1(t'), y \oplus g_2(t'), g_1(t') \oplus g_2(t'))$$

since $\mathbf{k}$ does not satisfy condition (C-6). Let

$$\mathcal{Q}^{(1)} = \{(k,l,u,v,\Delta) \in \overline{\mathcal{Q}_C} : (k,u,*) \in \mathcal{Q}_{E_1} \text{ for some } * \in \{0,1\}^n\},$$
$$\mathcal{Q}^{(2)} = \{(k,l,u,v,\Delta) \in \overline{\mathcal{Q}_C} : (l,*,v) \in \mathcal{Q}_{E_2} \text{ for some } * \in \{0,1\}^n\},$$
$$\mathcal{Q}^{(3)} = \{(k,l,u,v,\Delta) \in \overline{\mathcal{Q}_C} : \exists (k',l',u',v',\Delta') \in \overline{\mathcal{Q}_C} \text{ such that}$$
$$(k',l',u',v',\Delta') \neq (k,l,u,v,\Delta),\ (k',u') = (k,u)\} \setminus \mathcal{Q}^{(1)},$$
$$\mathcal{Q}^{(4)} = \{(k,l,u,v,\Delta) \in \overline{\mathcal{Q}_C} : \exists (k',l',u',v',\Delta') \in \overline{\mathcal{Q}_C} \text{ such that}$$
$$(k',l',u',v',\Delta') \neq (k,l,u,v,\Delta),\ (l',v') = (l,v)\} \setminus \mathcal{Q}^{(2)},$$
$$\mathcal{Q}^{(5)} = \overline{\mathcal{Q}_C} \setminus \left(\bigcup_{i=1}^{4} \mathcal{Q}^{(i)} \right).$$

Each class of queries are pictorially represented in Fig. 3.



(a) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(1)}$

(b) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(2)}$

(c) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(3)}$

(d) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(4)}$

(e) $(k, l, u, v, \Delta) \in \mathcal{Q}^{(5)}$

Fig. 3: Reduced queries in $\mathcal{Q}^{(i)}$, $i = 1, 2, 3, 4, 5$. Black dots represent values fixed by $\mathcal{Q}_{E_1}$ and $\mathcal{Q}_{E_2}$, while white dots are "free". Two distinct dots on each side do not necessarily correspond to distinct values.

Property 1. Sets $\mathcal{Q}^{(i)}$, $i = 1, 2, 3, 4, 5$, partition $\overline{\mathcal{Q}_C}$, namely,

$$\overline{\mathcal{Q}_C} = \bigsqcup_{i=1}^{5} \mathcal{Q}^{(i)}.$$

Proof. The union of $\mathcal{Q}^{(i)}$, $i = 1, 2, 3, 4, 5$, is $\overline{\mathcal{Q}_C}$ by the definition of $\mathcal{Q}^{(5)}$. Furthermore, they are pairwise disjoint; in particular,

1. $\mathcal{Q}^{(1)} \cap \mathcal{Q}^{(2)} = \emptyset$ by excluding bad keys satisfying (C-9);
2. $\mathcal{Q}^{(1)} \cap \mathcal{Q}^{(4)} = \emptyset$ by excluding bad keys satisfying (C-12);
3. $\mathcal{Q}^{(2)} \cap \mathcal{Q}^{(3)} = \emptyset$ by excluding bad keys satisfying (C-13);
4. $\mathcal{Q}^{(3)} \cap \mathcal{Q}^{(4)} = \emptyset$ by excluding bad keys satisfying (C-6). □

We will further classify the queries and count each class using the following notations.

1. For $r, s \in \{0,1\}^m$, $d \in \{0,1\}^n$ and $i \in \{1, 2, 3, 4, 5\}$, let

$$\mathcal{Q}^{(i)}_{r,s,d} = \{(k, l, u, v, \Delta) \in \mathcal{Q}^{(i)} : (k, l, \Delta) = (r, s, d)\},$$

and let

$$\mathcal{Q}^{(i)}_{r,s} = \bigsqcup_{d\in\{0,1\}^n} \mathcal{Q}^{(i)}_{r,s,d}, \quad \mathcal{Q}^{(i)}_{r,*} = \bigsqcup_{l\in\{0,1\}^m} \mathcal{Q}^{(i)}_{r,l}, \quad \mathcal{Q}^{(i)}_{*,s} = \bigsqcup_{k\in\{0,1\}^m} \mathcal{Q}^{(i)}_{k,s}.$$

2. For $w \in \mathcal{T}$, $r, s \in \{0,1\}^m$, $d \in \{0,1\}^n$ and $i \in \{1,2,3,4,5\}$, let

$$\begin{aligned} q_w &= |\mathcal{Q}_C(w)|, & p_{r,*} &= |\mathcal{Q}_{E_1}(r)|, & p_{*,s} &= |\mathcal{Q}_{E_2}(s)|, \\ q^{(i)}_{r,s,d} &= |\mathcal{Q}^{(i)}_{r,s,d}|, & q^{(i)}_{r,s} &= |\mathcal{Q}^{(i)}_{r,s}|, \\ q^{(i)}_{r,*} &= |\mathcal{Q}^{(i)}_{r,*}|, & q^{(i)}_{*,s} &= |\mathcal{Q}^{(i)}_{*,s}|. \end{aligned}$$

Given the partition of the queries, we can also define the following sets.

1. For $r, s \in \{0,1\}^m$, let

$$\begin{aligned} U_1(r) &= \{u \in \{0,1\}^n : \exists v \in \{0,1\}^n \text{ such that } (u,v) \in \mathcal{Q}_{E_1}(r)\}, \\ V_1(r) &= \{v \in \{0,1\}^n : \exists u \in \{0,1\}^n \text{ such that } (u,v) \in \mathcal{Q}_{E_1}(r)\}, \\ U_2(s) &= \{u \in \{0,1\}^n : \exists v \in \{0,1\}^n \text{ such that } (u,v) \in \mathcal{Q}_{E_2}(s)\}, \\ V_2(s) &= \{v \in \{0,1\}^n : \exists u \in \{0,1\}^n \text{ such that } (u,v) \in \mathcal{Q}_{E_2}(s)\}. \end{aligned}$$

2. For $r, s \in \{0,1\}^m$ and $i \in \{1,2,3,4,5\}$, let

$$\begin{aligned} U^{(i)}_1(r) &= \{u \in \{0,1\}^n : \exists s, v, \Delta \text{ such that } (r,s,u,v,\Delta) \in \mathcal{Q}^{(i)}\}, \\ V^{(i)}_2(s) &= \{v \in \{0,1\}^n : \exists r, u, \Delta \text{ such that } (r,s,u,v,\Delta) \in \mathcal{Q}^{(i)}\}. \end{aligned}$$

Sets $U^{(i)}_1(r)$ and $V^{(i)}_2(s)$, $i = 1,2,3,4,5$, are pictorially represented in Fig. 4. We have the following properties on these sets.

Property 2. For $r, s \in \{0,1\}^m$, one has

1. $U^{(1)}_1(r) \subset U_1(r)$;
2. $U_1(r)$ and $U^{(i)}_1(r)$, $i = 2,3,4,5$, are pairwise disjoint;
3. $V^{(1)}_2(s) \subset V_2(s)$;
4. $V_2(s)$ and $V^{(i)}_2(s)$, $i = 1,3,4,5$, are pairwise disjoint.

Proof. By definition, $U^{(1)}_1(r) \subset U_1(r)$. $U_1(r)$ and $U^{(2)}_1(r)$ are disjoint by excluding bad keys of (C-9); $U_1(r)$ and $U^{(3)}_1(r)$ are disjoint since $\mathcal{Q}^{(1)}$ and $\mathcal{Q}^{(3)}$ are disjoint; $U_1(r)$ and $U^{(4)}_1(r)$ are disjoint by excluding bad keys of (C-12); $U^{(2)}_1(r)$ and $U^{(3)}_1(r)$ are disjoint by excluding bad keys of (C-13); $U^{(2)}_1(r)$ and $U^{(4)}_1(r)$ are disjoint by excluding bad keys of (C-13) and since $\mathcal{Q}^{(2)}$ and $\mathcal{Q}^{(4)}$ are disjoint; $U^{(3)}_1(r)$ and $U^{(4)}_1(r)$ are disjoint by excluding bad keys of (C-6). Since $\mathcal{Q}^{(1)} \cup \mathcal{Q}^{(2)} \cup \mathcal{Q}^{(3)} \cup \mathcal{Q}^{(4)}$ and $\mathcal{Q}^{(5)}$ are disjoint, $U^{(1)}_1(r) \cup U^{(2)}_1(r) \cup U^{(3)}_1(r) \cup U^{(4)}_1(r)$ and $U^{(5)}_1(r)$ are also disjoint. The remaining properties are proved similarly. □

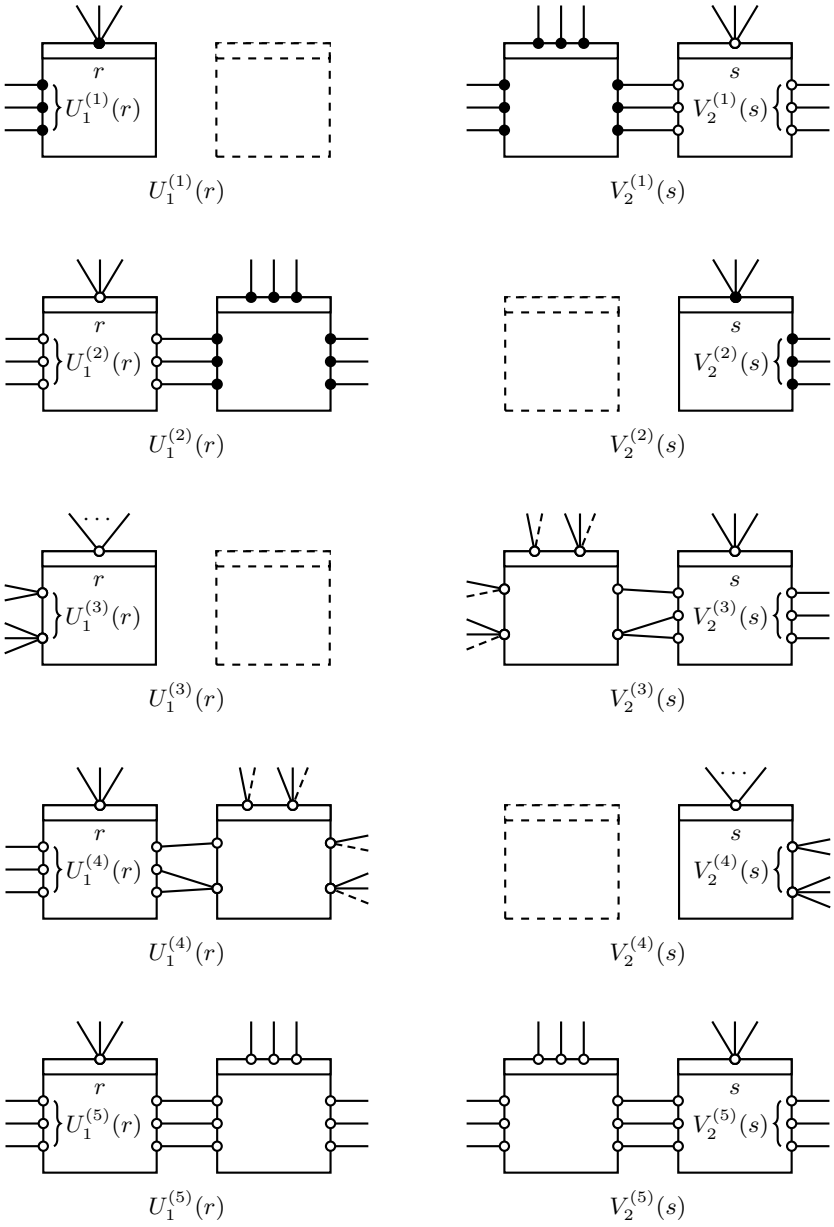


Fig. 4: Sets $U_1^{(i)}(r)$ and $V_2^{(i)}(s)$, $i = 1, 2, 3, 4, 5$. As in Fig. 3, black dots (resp. white dots) represent values fixed by $\mathcal{Q}_{E_1}$ and $\mathcal{Q}_{E_2}$ (resp. free values). Distinct dots on each side do not necessarily correspond to distinct values.

Property 3. For $r, s \in \{0,1\}^m$, one has

1. $|U_1(r)| = |V_1(r)| = p_{r,*}$;
2. $|U_2(s)| = |V_2(s)| = p_{*,s}$;
3. $|U_1^{(i)}(r)| = q_{r,*}^{(i)}$ for $i = 2, 4, 5$;
4. $|V_2^{(i)}(s)| = q_{*,s}^{(i)}$ for $i = 1, 3, 5$.

Proof. It is straightforward to prove the first two properties. Every $(k, l, u, v, \Delta) \in \mathcal{Q}_{r,*}^{(2)}$ (resp. $\mathcal{Q}_{r,*}^{(4)}$) contains a distinct u since otherwise we would find queries satisfying (C-13) (resp. (C-6)), which implies $|U_1^{(2)}(r)| = q_{r,*}^{(2)}$ (resp. $|U_1^{(4)}(r)| = q_{r,*}^{(4)}$). We also have $|U_1^{(5)}(r)| = q_{r,*}^{(5)}$ since $\mathcal{Q}^{(5)}$ and $\mathcal{Q}^{(3)}$ are disjoint. The last property is proved similarly. □

We define $a_{r,*}^{(3)} = |U_1^{(3)}(r)|$ and $a_{*,s}^{(4)} = |V_2^{(4)}(s)|$.

Property 4. For $r, s \in \{0,1\}^m$ and $d \in \{0,1\}^n$, one has

1. $p_{r,*} \geq q_{r,s,d}^{(1)}$;
2. $p_{*,s} \geq q_{r,s,d}^{(2)}$;
3. $a_{r,*}^{(3)} \geq q_{r,s,d}^{(3)}$;
4. $a_{*,s}^{(4)} \geq q_{r,s,d}^{(4)}$.

Proof. Every $(k, l, u, v, \Delta) \in \mathcal{Q}_{r,s,d}^{(1)}$ contains a distinct u since otherwise we would find queries satisfying (C-7). Therefore we have $p_{r,*} = |U_1(r)| \geq q_{r,s,d}^{(1)}$. The other properties are proved similarly. □

For a subset $\mathcal{Q} \subset \overline{\mathcal{Q}_C}$, we will write $(E_1, E_2) \vdash \mathcal{Q}$ if

$$E_2(l, E_1(k, u) \oplus \Delta) = v$$

for every $(k, l, u, v, \Delta) \in \mathcal{Q}$. With this notation, let

$$\mathsf{p}_1 = \Pr\left[(E_1, E_2) \vdash \mathcal{Q}^{(1)} \cup \mathcal{Q}^{(2)} \middle| E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2}\right],$$
$$\mathsf{p}_2 = \Pr\left[(E_1, E_2) \vdash \mathcal{Q}^{(3)} \cup \mathcal{Q}^{(4)} \middle| E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2} \wedge (E_1, E_2) \vdash \mathcal{Q}^{(1)} \cup \mathcal{Q}^{(2)}\right],$$
$$\mathsf{p}_3 = \Pr\left[(E_1, E_2) \vdash \mathcal{Q}^{(5)} \middle| E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2} \wedge (E_1, E_2) \vdash \bigcup_{i=1}^{4} \mathcal{Q}^{(i)}\right].$$

Then we have

$$\mathsf{p}_{\mathsf{re}}^{\mathbf{k}}(\mathcal{Q}_C | \mathcal{Q}_E) = \Pr\left[(E_1, E_2) \vdash \overline{\mathcal{Q}_C} | E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2}\right] = \mathsf{p}_1 \cdot \mathsf{p}_2 \cdot \mathsf{p}_3. \quad (4)$$

3.3.2 Computing p_1

Suppose that $(k, l, u, v, \Delta) \in \mathcal{Q}^{(1)}$. It means that $E_1(k, u)$ has been already determined by $\mathcal{Q}_{E_1}$. In order for (E_1, E_2) to complete this query, E_2 should map $E_1(k, u) \oplus \Delta$ to v with key l. In this situation, the following properties are noteworthy.

1. Not either $E_2^{-1}(l, v)$ or $E_2(l, E_1(k, u) \oplus \Delta)$ has been determined by $\mathcal{Q}_{E_2}$ since $\mathbf{k}$ does not satisfy either (C-9) or (C-10).
2. There is no collision on the input to E_2 by the queries of $\mathcal{Q}^{(1)}$; precisely, for any (k, l, u, v, Δ), $(k', l', u', v', \Delta') \in^{\neq} \mathcal{Q}^{(1)}$ such that $l = l'$, we have $E_1(k, u) \oplus \Delta \neq E_1(k', u') \oplus \Delta'$ since $\mathbf{k}$ does not satisfy (C-2).
3. There is no collision on the output from E_2 by any other query of $\overline{\mathcal{Q}_C}$; precisely, for any distinct queries $(k, l, u, v, \Delta) \in \mathcal{Q}^{(1)}$ and $(k', l', u', v', \Delta') \in \overline{\mathcal{Q}_C}$ such that $l = l'$, we have $v \neq v'$ since $\mathbf{k}$ does not satisfy (C-12).

For a fixed $s \in \{0,1\}^m$, $\mathcal{Q}_{E_2}$ determines $p_{*,s}$ evaluations of $E_2(s, \cdot)$. On the other hand, the number of queries $(k, l, u, v, \Delta) \in \mathcal{Q}^{(1)}$ such that $l = s$ is $q^{(1)}_{*,s}$ (by definition). Such queries determine all different inputs and outputs of $E_2(s, \cdot)$, so $E_2(s, \cdot)$ would complete the queries with probability $1/(N - p_{*,s})_{q^{(1)}_{*,s}}$. Therefore we have

$$\Pr\left[(E_1, E_2) \vdash \mathcal{Q}^{(1)} \middle| E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2}\right] = \prod_{s \in \{0,1\}^m} \frac{1}{(N - p_{*,s})_{q^{(1)}_{*,s}}}.$$

Applying a similar argument to $\mathcal{Q}^{(2)}$ (excluding bad key satisfying (C-3), (C-9), (C-11) or (C-13)), we have

$$\mathsf{p}_1 = \prod_{r \in \{0,1\}^m} \frac{1}{(N - p_{r,*})_{q^{(2)}_{r,*}}} \cdot \prod_{s \in \{0,1\}^m} \frac{1}{(N - p_{*,s})_{q^{(1)}_{*,s}}}. \tag{5}$$

3.3.3 Computing p_2

Subject to

$$E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2} \wedge (E_1, E_2) \vdash \mathcal{Q}^{(1)} \cup \mathcal{Q}^{(2)},$$

we will lower bound the probability of completing the reduced queries of $\mathcal{Q}^{(3)} \cup \mathcal{Q}^{(4)}$ when extending the evaluations of E_1 and E_2. For $r, s \in \{0,1\}^m$, we can fix

$$V_1^{(2)}(r) \stackrel{\text{def}}{=} \{E_1(r, u) : u \in U_1^{(2)}(r)\},$$
$$U_2^{(1)}(s) \stackrel{\text{def}}{=} \{E_2^{-1}(s, v) : v \in V_2^{(1)}(s)\}.$$

Property 5. For any $r \in \{0,1\}^m$ such that $U_1^{(3)}(r) \neq \emptyset$, $|V_1(r) \cup V_1^{(2)}(r)| < N/2$.

Proof. We distinguish two cases.

Case 1) There exists no tweak $w \in \mathcal{T}^*$ such that $h_1(w) = r$. In this case,
- i) $|V_1(r)| < N/4$ since we have modified the adversary so that the number of block cipher queries is either N or less than $N/4$ (for any fixed key), and $U_1^{(3)}(r)$ being nonempty implies that the number of block cipher queries cannot be N, and
- ii) $|V_1^{(2)}(r)| < N/4$ since we are excluding bad keys of (C-14) (with no tweak w in $\mathcal{T}^*$ such that $h_1(w) = r$).

Therefore we have

$$|V_1(r) \cup V_1^{(2)}(r)| \le |V_1(r)| + |V_1^{(2)}(r)| < \frac{N}{4} + \frac{N}{4} = \frac{N}{2}.$$

Case 2) There exists $w \in \mathcal{T}^*$ such that $h_1(w) = r$; we again distinguish three cases. Let $s = h_2(w)$.
- i) $|\mathcal{Q}_{E_1}(r)| = N$; we have $U_1(r) = \{0,1\}^n$, and hence $U_1^{(3)}(r) = \emptyset$.
- ii) $|\mathcal{Q}_{E_2}(s)| = N$; since $w \in \mathcal{T}^*$, all possible N construction queries are made with tweak w, and they are all contained in $\mathcal{Q}^{(2)}$ since $|\mathcal{Q}_{E_2}(s)| = N$ for $s = h_2(w)$. This means that $U_1^{(2)}(r) = \{0,1\}^n$. Since $U_1^{(2)}(r)$ and $U_1^{(3)}(r)$ are disjoint by Property 2, we have $U_1^{(3)}(r) = \emptyset$.
- iii) $|\mathcal{Q}_{E_1}(r)|, |\mathcal{Q}_{E_2}(s)| < N/4$; there is no query $(k,l,u,v,\Delta) \in \mathcal{Q}^{(2)}$ such that $k = r$ and $l \neq s$ since otherwise we will see queries satisfying (C-13). Therefore $|V_1^{(2)}(r)|$ counts the number of queries $(k,l,u,v,\Delta) \in \mathcal{Q}^{(2)}$ such that $k = r$ and $l = s$. Such queries correspond to queries in $\mathcal{Q}_{E_2}(s)$, where $|\mathcal{Q}_{E_2}(s)| < N/4$. Since $|V_1(r)| \le |\mathcal{Q}_{E_1}(r)| < N/4$, we have $|V_1(r) \cup V_1^{(2)}(r)| < N/2$. □

Similarly, we can prove the following property.

Property 6. For any $s \in \{0,1\}^m$ such that $V_2^{(4)}(s) \neq \emptyset$, $|U_2(s) \cup U_2^{(1)}(s)| < N/2$.

In order to estimate the probability that E_1 and E_2 complete $\mathcal{Q}^{(3)} \cup \mathcal{Q}^{(4)}$, we will choose an (ordered) set of $a_{r,*}^{(3)} (= |U_1^{(3)}(r)|)$ elements, denoted $V_1^{(3)}(r)$, from $\{0,1\}^n \setminus (V_1(r) \cup V_1^{(2)}(r))$ for each $r \in \{0,1\}^m$. Once $V_1^{(3)}(r)$ is chosen, we will compute the probability that the queries of $\mathcal{Q}^{(3)}$ are completed satisfying $E_1(r, U_1^{(3)}(r)) = V_1^{(3)}(r)$.[2] Similarly, for each $s \in \{0,1\}^m$, we will choose a set of $a_{*,s}^{(4)}$ elements, denoted $U_2^{(4)}(s)$, from $\{0,1\}^n \setminus (U_2(s) \cup U_2^{(1)}(s))$, and compute the probability that the queries of $\mathcal{Q}^{(4)}$ are completed via the elements of $U_2^{(4)}(s)$ (as $E_2^{-1}(l,v)$).

Without any restriction, the number of ways of choosing $V_1^{(3)}(r)$ and $U_2^{(4)}(s)$ (over all the keys r, $s \in \{0,1\}^m$) would be

$$\prod_{r \in \{0,1\}^m} (N - p_{r,*} - q_{r,*}^{(2)})_{a_{r,*}^{(3)}} \cdot \prod_{s \in \{0,1\}^m} (N - p_{*,s} - q_{*,s}^{(1)})_{a_{*,s}^{(4)}}.$$

[2] $U_1^{(3)}(r)$ and $V_1^{(3)}(r)$ are viewed as ordered sets, and $E_1(r, U_1^{(3)}(r)) = V_1^{(3)}(r)$ means that each element of $U_1^{(3)}(r)$ is mapped to the corresponding element of $V_1^{(3)}(r)$ (with respect to the ordering) under $E_1(r, \cdot)$.

However, in order to make the analysis simpler, we will avoid certain bad conditions when choosing $V_1^{(3)}(r)$ and $U_2^{(4)}(s)$; suppose that y has been chosen as $E_1(r,u)$ from $\{0,1\}^n \setminus (V_1(r) \cup V_1^{(2)}(r))$ for a query $(r,s,u,v,\Delta) \in \mathcal{Q}^{(3)}$. In order for E_2 complete this query, one should have $E_2(s, y \oplus \Delta) = v$. Here we would like the element $y \oplus \Delta$ to be "free", namely to lie outside $U_2(s) \cup U_2^{(1)}(s) \cup U_2^{(4)}(s)$. We would also like the elements $y \oplus \Delta$ to be all distinct for each key of E_2. Similarly, for each element x that has been chosen as $E_2^{-1}(s,v)$ for a query $(r,s,u,v,\Delta) \in \mathcal{Q}^{(4)}$, we would like $x \oplus \Delta$ to be outside $V_1(r) \cup V_1^{(2)}(r) \cup V_1^{(3)}(r)$. For each key of E_1, there should be no collision between $x \oplus \Delta$. More precisely, the undesirable "colliding" events can be classified as follows.[3]

$\mathsf{Col}_1 \Leftrightarrow$ there exist $(k,l,u,v,\Delta) \in \mathcal{Q}^{(3)}$ and $(l',u',v') \in \mathcal{Q}_{E_2}$ such that
$l = l'$ and $E_1(k,u) \oplus \Delta = u'$.

$\mathsf{Col}_2 \Leftrightarrow$ there exist $(k,l,u,v,\Delta) \in \mathcal{Q}^{(3)}$ and $(k',l',u',v',\Delta') \in \mathcal{Q}^{(1)}$ such that
$l = l'$ and $E_1(k,u) \oplus \Delta = E_2^{-1}(l',v')$.

$\mathsf{Col}_3 \Leftrightarrow$ there exist (k,l,u,v,Δ), $(k',l',u',v',\Delta') \in^{\neq} \mathcal{Q}^{(3)}$ such that
$l = l'$ and $E_1(k,u) \oplus \Delta = E_1(k',u') \oplus \Delta'$.

$\mathsf{Col}_4 \Leftrightarrow$ there exist $(k,l,u,v,\Delta) \in \mathcal{Q}^{(3)}$ and $(k',l',u',v',\Delta') \in \mathcal{Q}^{(4)}$ such that
$l = l'$ and $E_1(k,u) \oplus \Delta = E_2^{-1}(l',v')$.

$\mathsf{Col}_5 \Leftrightarrow$ there exist $(k,l,u,v,\Delta) \in \mathcal{Q}^{(4)}$ and $(k',u',v') \in \mathcal{Q}_{E_1}$ such that
$k = k'$ and $E_2^{-1}(l,v) \oplus \Delta = v'$.

$\mathsf{Col}_6 \Leftrightarrow$ there exist $(k,l,u,v,\Delta) \in \mathcal{Q}^{(4)}$ and $(k',l',u',v',\Delta') \in \mathcal{Q}^{(2)}$ such that
$k = k'$ and $E_2^{-1}(l,v) \oplus \Delta = E_1(k',u')$.

$\mathsf{Col}_7 \Leftrightarrow$ there exist $(k,l,u,v,\Delta) \in \mathcal{Q}^{(4)}$ and $(k',l',u',v',\Delta') \in \mathcal{Q}^{(3)}$ such that
$k = k'$ and $E_2^{-1}(l,v) \oplus \Delta = E_1(k',u')$.

$\mathsf{Col}_8 \Leftrightarrow$ there exist (k,l,u,v,Δ), $(k',l',u',v',\Delta') \in^{\neq} \mathcal{Q}^{(4)}$ such that
$k = k'$ and $E_2^{-1}(l,v) \oplus \Delta = E_2^{-1}(l',v') \oplus \Delta'$.

Property 7. The probabilities of Col_i, $i = 1, \ldots, 8$, (over random choices of $V_1^{(3)}(r)$ and $U_2^{(4)}(s)$) are all upper bounded by $2M_2/N$.

Proof. To estimate the probability of Col_3, consider pairs of distinct queries (k,l,u,v,Δ), $(k',l',u',v',\Delta') \in \mathcal{Q}^{(3)}$ such that $l = l'$. The set of such pairs can be partitioned into the following two types;

1. there exists a query $(k'',l'',u'',v'',\Delta'')$ such that $(k'',u'') = (k,u)$ and
$$(k'',l'',u'',v'',\Delta'') \notin \{(k,l,u,v,\Delta),(k',l',u',v',\Delta')\};$$

[3] For $(k,l,u,v,\Delta) \in \mathcal{Q}^{(3)} \cup \mathcal{Q}^{(4)}$, we will write $E_1(k,u)$ and $E_2^{-1}(l,v)$ to denote the elements determined by the choice of $V_1^{(3)}(k)$ and $U_2^{(4)}(l)$, respectively.

2. there exists no query $(k'', l'', u'', v'', \Delta'')$ such that $(k'', u'') = (k, u)$ and

$$(k'', l'', u'', v'', \Delta'') \notin \{(k, l, u, v, \Delta), (k', l', u', v', \Delta')\}.$$

Since $(k, l, u, v, \Delta) \in \mathcal{Q}^{(3)}$, one always has a query $(k^*, l^*, u^*, v^*, \Delta^*)$ such that $(k^*, u^*) = (k, u)$ and $(k^*, l^*, u^*, v^*, \Delta^*) \neq (k, l, u, v, \Delta)$, so if a pair of queries falls into the second type, then it means that $(k^*, l^*, u^*, v^*, \Delta^*) = (k', l', u', v', \Delta')$, and hence $(k, l, u) = (k', l', u')$. Then by excluding bad keys of (C-7), we have $\Delta \neq \Delta'$. So for any pair of queries of the second type, it cannot be the case that $E_1(k, u) \oplus \Delta = E_1(k', u') \oplus \Delta'$. On the other hand, the number of the pairs of the first type is upper bounded by $|\mathcal{B}_1|$, which is smaller than M_2 by excluding bad keys of (C-4). For each pair, the probability that $E_1(k, u) \oplus \Delta = E_1(k', u') \oplus \Delta'$ is upper bounded by $2/N$ (since $|\{0,1\}^n \setminus (V_1(r) \cup V_1^{(2)}(r))| > N/2$ by Property 5). Therefore, we have

$$\Pr\left[\mathsf{Col}_3\right] \leq \frac{2M_2}{N}.$$

The other bounds are proved similarly. □

The number of ways of choosing $V_1^{(3)}(r)$ and $U_2^{(4)}(s)$ over all $r, s \in \{0,1\}^m$, without fulfilling any of the bad conditions Col_i, $i = 1, \ldots, 8$, is lower bounded by

$$\prod_{r \in \{0,1\}^m} (N - p_{r,*} - q_{r,*}^{(2)})_{a_{r,*}^{(3)}} \cdot \prod_{s \in \{0,1\}^m} (N - p_{*,s} - q_{*,s}^{(1)})_{a_{*,s}^{(4)}} \cdot \left(1 - \sum_{i=1}^{8} \Pr\left[\mathsf{Col}_i\right]\right). \quad (6)$$

For each of "good" choices for $V_1^{(3)}(r)$ and $U_2^{(4)}(s)$, (E_1, E_2) complete the queries of $\mathcal{Q}^{(3)}$ and $\mathcal{Q}^{(4)}$ (via $V_1^{(3)}(r)$ and $U_2^{(4)}(s)$, respectively) with probability

$$\frac{1}{\prod_{r \in \{0,1\}^m} (N - p_{r,*} - q_{r,*}^{(2)})_{a_{r,*}^{(3)} + q_{r,*}^{(4)}} \cdot \prod_{s \in \{0,1\}^m} (N - p_{*,s} - q_{*,s}^{(1)})_{a_{*,s}^{(4)} + q_{*,s}^{(3)}}}. \quad (7)$$

By (6), (7) and Property 7, we have

$$\begin{aligned}
\mathsf{p}_2 &\geq \frac{\prod_{r \in \{0,1\}^m} (N - p_{r,*} - q_{r,*}^{(2)})_{a_{r,*}^{(3)}} \cdot \prod_{s \in \{0,1\}^m} (N - p_{*,s} - q_{*,s}^{(1)})_{a_{*,s}^{(4)}} \cdot \left(1 - \sum_{i=1}^{8} \Pr\left[\mathsf{Col}_i\right]\right)}{\prod_{r \in \{0,1\}^m} (N - p_{r,*} - q_{r,*}^{(2)})_{a_{r,*}^{(3)} + q_{r,*}^{(4)}} \cdot \prod_{s \in \{0,1\}^m} (N - p_{*,s} - q_{*,s}^{(1)})_{a_{*,s}^{(4)} + q_{*,s}^{(3)}}} \\
&\geq \frac{1}{\prod_{r \in \{0,1\}^m} (N - p_{r,*} - q_{r,*}^{(2)} - a_{r,*}^{(3)})_{q_{r,*}^{(4)}} \cdot \prod_{s \in \{0,1\}^m} (N - p_{*,s} - q_{*,s}^{(1)} - a_{*,s}^{(4)})_{q_{*,s}^{(3)}}} \\
&\quad \times \left(1 - \frac{16M_2}{N}\right). \quad (8)
\end{aligned}$$

3.3.4 Computing $\mathbf{p_3}$

Subject to

$$E_1 \vdash \mathcal{Q}_{E_1} \wedge E_2 \vdash \mathcal{Q}_{E_2} \wedge (E_1, E_2) \vdash \bigcup_{i=1}^{4} \mathcal{Q}^{(i)}, \tag{9}$$

we can fix

$$b_r \stackrel{\text{def}}{=} p_{r,*} + q^{(2)}_{r,*} + a^{(3)}_{r,*} + q^{(4)}_{r,*} \tag{10}$$

evaluations of $E_1(r, \cdot)$ and

$$c_s \stackrel{\text{def}}{=} p_{*,s} + q^{(1)}_{*,s} + q^{(3)}_{*,s} + a^{(4)}_{*,s} \tag{11}$$

evaluations of $E_2(s, \cdot)$ for each $(r, s) \in \{0,1\}^m \times \{0,1\}^m$. Let

$$\mathcal{Q}^{(5)}_1 = \{(r, s, u, v, \Delta) \in \mathcal{Q}^{(5)} : r = h_1(t) \text{ and } s = h_2(t) \text{ for some } t \in \mathcal{T}^*\},$$
$$\mathcal{Q}^{(5)}_2 = \{(r, s, u, v, \Delta) \in \mathcal{Q}^{(5)} : r \neq h_1(t) \text{ and } s \neq h_2(t) \text{ for every } t \in \mathcal{T}^*\}.$$

Let

$$\mathcal{R} = \{r \in \{0,1\}^m : r = h_1(t) \text{ for some } t \in \mathcal{T}^*\},$$
$$\mathcal{S} = \{s \in \{0,1\}^m : s = h_2(t) \text{ for some } t \in \mathcal{T}^*\},$$

and let $\mathcal{R}' = \{0,1\}^m \setminus \mathcal{R}$ and $\mathcal{S}' = \{0,1\}^m \setminus \mathcal{S}$.

Property 8. With the above definitions, the following hold:

1. $\mathcal{Q}^{(5)}$ is partitioned into $\mathcal{Q}^{(5)}_1$ and $\mathcal{Q}^{(5)}_2$, namely, $\mathcal{Q}^{(5)} = \mathcal{Q}^{(5)}_1 \sqcup \mathcal{Q}^{(5)}_2$;
2. $\mathcal{Q}^{(5)}_1 = \bigsqcup_{(r,s) \in \mathcal{R} \times \mathcal{S}} \mathcal{Q}^{(5)}_{r,s}$;
3. $\mathcal{Q}^{(5)}_2 = \bigsqcup_{(r,s) \in \mathcal{R}' \times \mathcal{S}'} \mathcal{Q}^{(5)}_{r,s}$;
4. $\mathcal{Q}^{(5)}_{r,s} = \emptyset$ for $(r, s) \notin (\mathcal{R} \times \mathcal{S}) \cup (\mathcal{R}' \times \mathcal{S}')$.

Proof. By definition, we have

$$\mathcal{Q}^{(5)}_1 \subset \bigsqcup_{(r,s) \in \mathcal{R} \times \mathcal{S}} \mathcal{Q}^{(5)}_{r,s}, \qquad \mathcal{Q}^{(5)}_2 \subset \bigsqcup_{(r,s) \in \mathcal{R}' \times \mathcal{S}'} \mathcal{Q}^{(5)}_{r,s},$$
$$\mathcal{Q}^{(5)}_1 \cup \mathcal{Q}^{(5)}_2 \subset \mathcal{Q}^{(5)} = \bigsqcup_{(r,s) \in (\mathcal{R} \cup \mathcal{R}') \times (\mathcal{S} \cup \mathcal{S}')} \mathcal{Q}^{(5)}_{r,s}. \tag{12}$$

Therefore it is obvious that $\mathcal{Q}^{(5)}_1$ and $\mathcal{Q}^{(5)}_2$ are disjoint. If $(r, s, u, v, \Delta) \in \mathcal{Q}^{(5)} \setminus \mathcal{Q}^{(5)}_2$, then it should be the case that either $r = h_1(t)$ or $s = h_2(t)$ for some $t \in \mathcal{T}^*$; if $r = h_1(t)$ for some $t \in \mathcal{T}^*$, then we would have a query $(r', s', u', v', \Delta') \in \overline{\mathcal{Q}_C}$ such that $u' = u$, $r' = h_1(t) = r$ and $s' = h_2(t)$. Since $\mathcal{Q}^{(5)}$ is disjoint from $\mathcal{Q}^{(3)}$, it must be the case that $(r', s', u', v', \Delta') = (r, s, u, v, \Delta)$. Since $r = r' = h_1(t)$ and $s = s' = h_2(t)$, we have $(r, s, u, v, \Delta) \in \mathcal{Q}^{(5)}_1$. With a similar argument for the case that $s = h_2(t)$ for some $t \in \mathcal{T}^*$, we have $\mathcal{Q}^{(5)} = \mathcal{Q}^{(5)}_1 \sqcup \mathcal{Q}^{(5)}_2$. The remaining properties are immediate from the first one (combined with the observation (12)). □

Let

$$\mathsf{p}'_3 = \Pr\left[(E_1(r,\cdot), E_2(s,\cdot)) \vdash \mathcal{Q}^{(5)}_{r,s} \text{ for every } (r,s) \in \mathcal{R} \times \mathcal{S}\right],$$
$$\mathsf{p}''_3 = \Pr\left[(E_1(r,\cdot), E_2(s,\cdot)) \vdash \mathcal{Q}^{(5)}_{r,s} \text{ for every } (r,s) \in \mathcal{R}' \times \mathcal{S}'\right], \tag{13}$$

where both probabilities are conditioned on (9). Then by Property 8, we have

$$\mathsf{p}_3 = \mathsf{p}'_3 \cdot \mathsf{p}''_3. \tag{14}$$

COMPUTING p'_3. We begin with the following property.

Property 9. For $(r,s) \in \mathcal{R} \times \mathcal{S}$, one has

1. $q^{(1)}_{r,*} = q^{(1)}_{*,s} = q^{(1)}_{r,s} = p_{r,*}$;
2. $q^{(2)}_{r,*} = q^{(2)}_{*,s} = q^{(2)}_{r,s} = p_{*,s}$;
3. $q^{(3)}_{*,s} = a^{(3)}_{r,*} = q^{(3)}_{r,s}$;
4. $q^{(4)}_{r,*} = a^{(4)}_{*,s} = q^{(4)}_{r,s}$;
5. $q^{(1)}_{r,s} + q^{(2)}_{r,s} + q^{(3)}_{r,s} + q^{(4)}_{r,s} + q^{(5)}_{r,s} = N$;
6. $b_r = c_s = N - q^{(5)}_{r,s}$.

Proof. Define a function

$$\phi : \mathcal{Q}^{(1)}_{r,s} \longrightarrow U_1(r)$$
$$(k,l,u,v,\Delta) \longmapsto u.$$

Since $r = h_1(t)$ for some $t \in \mathcal{T}^*$, ϕ is surjective. Suppose that $(k,l,u,v,\Delta) \neq (k',l',u',v',\Delta') \in \mathcal{Q}^{(1)}_{r,s}$ with $(k,l) = (k',l') = (r,s)$ and $u = u'$. If their original queries contain an identical tweak in $\mathcal{T}$, then we have $\Delta = \Delta'$, which is a contradiction since we are excluding bad keys of (C-7). If their original queries contain different tweaks in $\mathcal{T}$, then we would be able to find queries satisfying (C-6). So ϕ is injective. This implies that $q^{(1)}_{r,s} = p_{r,*}$. Since $U^{(1)}_1(r) = U_1(r)$, we also have $q^{(1)}_{r,*} = p_{r,*}$. Furthermore, for any $r' \in \{0,1\}^m$ such that $r' \neq r$, we have $q^{(1)}_{r',s} = 0$ since otherwise we could find queries satisfying (C-12). So we have $q^{(1)}_{*,s} = q^{(1)}_{r,s}$. The second property is proved similarly.

Define a function

$$\psi : \mathcal{Q}^{(3)}_{r,s} \longrightarrow U^{(3)}_1(r)$$
$$(k,l,u,v,\Delta) \longmapsto u.$$

Since $s = h_2(t)$ for some $t \in \mathcal{T}^*$, ψ is surjective. Suppose that $(k,l,u,v,\Delta) \neq (k',l',u',v',\Delta') \in \mathcal{Q}^{(3)}_{r,s}$ with $(k,l) = (k',l') = (r,s)$ and $u = u'$. If their original queries contain an identical tweak in $\mathcal{T}$, then we have $\Delta = \Delta'$, which is a contradiction since we are excluding bad keys of (C-7). If their original queries

contain different tweaks in $\mathcal{T}$, then we would be able to find queries satisfying (C-6). So ϕ is injective. This implies that $q^{(3)}_{*,s} = a^{(3)}_{r,*}$. Furthermore, for any $r' \in \{0,1\}^m$ such that $r' \neq r$, we have $q^{(3)}_{r',s} = 0$ since otherwise we could find queries satisfying (C-12). So we have $q^{(3)}_{*,s} = q^{(3)}_{r,s}$. The remaining properties are proved similarly. □

Fix $(r,s) \in \mathcal{R} \times \mathcal{S}$. If $q^{(5)}_{r,s} = 0$, then we have $N - b_r = 0$. If $q^{(5)}_{r,s} > 0$, then there would exist $w \in \mathcal{T}^*$ such that $r = h_1(w)$ and $s = h_2(w)$, and $E_1(r,\cdot)$ and $E_2(s,\cdot)$ might complete the queries in $\mathcal{Q}^{(5)}_{r,s}$ that contain w (in their original forms). In this case, it cannot be the case that either $r \neq h_1(w')$ or $s \neq h_2(w')$ for any $w' \in \mathcal{T}^*$ such that $w' \neq w$ since the existence of such a tweak would imply $\mathcal{Q}^{(5)}_{r,s} = \emptyset$. Note that

$$V_2(s) \cup \bigcup_{i=1,3,4} V_2^{(i)}(s) = \left\{ E_2(s, E_1(r,u) \oplus \Delta) : u \in U_1(r) \cup \bigcup_{i=2,3,4} U_1^{(i)}(r) \right\},$$

where $\Delta = g_1(w) \oplus g_2(w)$, and $q^{(5)}_{r,s} = N - b_r = N - c_s$. So the probability that $E_1(r,\cdot)$ and $E_2(s,\cdot)$ complete all the queries of $\mathcal{Q}^{(5)}_{r,s}$ is $1/(N-b_r)!$, and hence

$$\mathsf{p}'_3 = \prod_{(r,s) \in \mathcal{R} \times \mathcal{S}} \frac{1}{(N-b_r)!}. \tag{15}$$

Computing p''_3. We first fix a lexicographical order on $\mathcal{R}' \times \mathcal{S}' \times \{0,1\}^n$; $(r,s,d) < (r',s',d')$ if and only if $r < r'$ or ($r = r'$ and $s < s'$) or ($r = r'$, $s = s'$ and $d < d'$).

Next, we fix $(r,s,d) \in \mathcal{R}' \times \mathcal{S}' \times \{0,1\}^n$, and suppose that E_1 and E_2 have completed all the queries of $\mathcal{Q}^{(5)}_{r',s',d'}$ for $(r',s',d') < (r,s,d)$. Subject to this event, let

$$B_{r,s,d} = V_1(r) \cup \left\{ E_1(k,u) : (k,l,u,v,\Delta) \in \bigcup_{i=2,3,4} \mathcal{Q}^{(i)}_{r,*} \cup \bigcup_{\substack{(r',s',d')<(r,s,d) \\ r'=r}} \mathcal{Q}^{(5)}_{r',s',d'} \right\},$$

$$C_{r,s,d} = \{x \oplus d : x \in U_2(s)\} \cup \left\{ E_2^{-1}(l,v) \oplus d : (k,l,u,v,\Delta) \in \bigcup_{i=1,3,4} \mathcal{Q}^{(i)}_{*,s} \cup \bigcup_{\substack{(r',s',d')<(r,s,d) \\ s'=s}} \mathcal{Q}^{(5)}_{r',s',d'} \right\},$$

be the set of all elements y for which $E_1^{-1}(r,y)$ have been determined, and the set of all elements y for which $E_2(s, y \oplus d)$ have been determined, respectively. We will choose an (ordered) set of $q^{(5)}_{r,s,d}$ elements, denoted Y, from $\{0,1\}^n \backslash (B_{r,s,d} \cup C_{r,s,d})$ and consider the probability that each $(r,s,u,v,d) \in \mathcal{Q}^{(5)}_{r,s,d}$ is completed with $E_1(r,u) = y$ and $E_2(s, y \oplus d) = v$ for a distinct $y \in Y$.

Let $b_{r,s,d} = |B_{r,s,d}|$ and $c_{r,s,d} = |C_{r,s,d}|$. Then we have

$$b_{r,s,d} = b_r + \sum_{i<s} q^{(5)}_{r,i} + \sum_{j<d} q^{(5)}_{r,s,j},$$
$$c_{r,s,d} = c_s + \sum_{i<r} q^{(5)}_{i,s} + \sum_{j<d} q^{(5)}_{r,s,j}.$$

Define a function

$$\phi : \bigsqcup_{i=1}^{4} \mathcal{Q}^{(i)}_{r,s,d} \longrightarrow B_{r,s,d} \cap C_{r,s,d}$$
$$(k, l, u, v, \Delta) \longmapsto E_1(k, u),$$

where $E_1(k, u)$ has already been determined. Suppose that (k, l, u, v, Δ) and $(k', l', u', v', \Delta')$ are mapped to the same $E_1(k, u) = E_1(k', u')$. Since both queries are contained in $\bigsqcup_{i=1}^{4} \mathcal{Q}^{(i)}_{r,s,d}$, we have $(k, l, \Delta) = (k', l', \Delta') = (r, s, d)$. It implies that $u = u'$ and $v = E_2(l, E_1(k, u) \oplus \Delta) = E_2(l', E_1(k', u') \oplus \Delta') = v'$, and hence $(k, l, u, v, \Delta) = (k', l', u', v', \Delta')$. So we see that ϕ is injective. Therefore we have

$$\begin{aligned} |B_{r,s,d} \cup C_{r,s,d}| &= |B_{r,s,d}| + |C_{r,s,d}| - |B_{r,s,d} \cap C_{r,s,d}| \\ &\leq b_{r,s,d} + c_{r,s,d} - e_{r,s,d}, \end{aligned}$$

where

$$e_{r,s,d} \stackrel{\text{def}}{=} \left| \bigsqcup_{i=1}^{4} \mathcal{Q}^{(i)}_{r,s,d} \right| = q^{(1)}_{r,s,d} + q^{(2)}_{r,s,d} + q^{(3)}_{r,s,d} + q^{(4)}_{r,s,d}.$$

Overall, the number of ways of choosing Y so that $E_1^{-1}(r, y)$ and $E_2(s, y \oplus d)$ have not been determined for any $y \in Y$ is at least

$$(N - b_{r,s,d} - c_{r,s,d} + e_{r,s,d})_{q^{(5)}_{r,s,d}}.$$

Property 10. For $(r, s, d) \in \mathcal{R}' \times \mathcal{S}' \times \{0, 1\}^n$ such that $\mathcal{Q}^{(5)}_{r,s,d} \neq \emptyset$, one has

1. $q^{(5)}_{r,s,d} + b_{r,s,d} < N/2$;
2. $q^{(5)}_{r,s,d} + c_{r,s,d} < N/2$.

Proof. Note that

$$q^{(5)}_{r,s,d} + b_{r,s,d} = q^{(5)}_{r,s,d} + p_{r,*} + q^{(2)}_{r,*} + a^{(3)}_{r,*} + q^{(4)}_{r,*} + \sum_{i<s} q^{(5)}_{r,i} + \sum_{j<d} q^{(5)}_{r,s,j},$$

where $p_{r,*} < N/4$ (since $\mathcal{Q}^{(5)}_{r,s,d} \neq \emptyset$), and the sum of the remaining summands is upper bounded by the number of queries (k, l, u, v, Δ) such that $k = r$, which is smaller than $N/4$ since there is no tweak $t \in \mathcal{T}^*$ such that $r = h_1(t)$ and by excluding bad keys of (C-14). Therefore we have $q^{(5)}_{r,s,d} + b_{r,s,d} < N/2$. The second property is proved similarly. □

Thanks to Property 10, we can apply Lemma 1 to lower bound the probability that E_1 and E_2 complete the queries of $\mathcal{Q}^{(5)}_{r,s,d}$ by

$$\frac{(N-b_{r,s,d}-c_{r,s,d}+e_{r,s,d})_{q^{(5)}_{r,s,d}}}{(N-b_{r,s,d})_{q^{(5)}_{r,s,d}}(N-c_{r,s,d})_{q^{(5)}_{r,s,d}}} \geq \frac{1}{(N-e_{r,s,d})_{q^{(5)}_{r,s,d}}}\left(1-\frac{4q^{(5)}_{r,s,d}(b_{r,s,d}-e_{r,s,d})(c_{r,s,d}-e_{r,s,d})}{N^2}\right).$$

Therefore we have

$$\begin{aligned}
\mathsf{p}''_3 &\geq \prod_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} \frac{1}{(N-e_{r,s,d})_{q^{(5)}_{r,s,d}}}\left(1-\frac{4q^{(5)}_{r,s,d}(b_{r,s,d}-e_{r,s,d})(c_{r,s,d}-e_{r,s,d})}{N^2}\right)\\
&\geq \prod_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} \frac{1}{(N-e_{r,s,d})_{q^{(5)}_{r,s,d}}}\\
&\times\left(1-\frac{\sum\limits_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} 4q^{(5)}_{r,s,d}(b_{r,s,d}-e_{r,s,d})(c_{r,s,d}-e_{r,s,d})}{N^2}\right) \qquad (16)
\end{aligned}$$

By replacing $(b_{r,s,d}-e_{r,s,d})$ and $(c_{r,s,d}-e_{r,s,d})$ by $(p_{r,*}+(b_{r,s,d}-p_{r,*}-e_{r,s,d}))$ and $(p_{*,s}+(c_{r,s,d}-p_{*,s}-e_{r,s,d}))$, respectively, we have

$$\begin{aligned}
&\sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(b_{r,s,d}-e_{r,s,d})(c_{r,s,d}-e_{r,s,d})\\
&= \sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}p_{r,*}p_{*,s} + \sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(b_{r,s,d}-p_{r,*}-e_{r,s,d})p_{*,s}\\
&+ \sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(c_{r,s,d}-p_{*,s}-e_{r,s,d})p_{r,*}\\
&+ \sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(b_{r,s,d}-p_{r,*}-e_{r,s,d})(c_{r,s,d}-p_{*,s}-e_{r,s,d}). \qquad (17)
\end{aligned}$$

Each term of (17) is upper bounded as follows.

Property 11. One has the following upper bounds:

1. $\sum\limits_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}p_{r,*}p_{*,s} \leq M_3$;

2. $\sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(b_{r,s,d}-p_{r,*}-e_{r,s,d})p_{*,s}\le M_3$;
3. $\sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(c_{r,s,d}-p_{*,s}-e_{r,s,d})p_{r,*}\le M_3$;
4. $\sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(b_{r,s,d}-p_{r,*}-e_{r,s,d})(c_{r,s,d}-p_{*,s}-e_{r,s,d})\le M_3$.

Proof. We will prove the third upper bound; the other bounds are proved similarly.

Consider

$$\bigsqcup_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}}\left(\mathcal{Q}^{(5)}_{r,s,d}\times\left(\bigsqcup_{i=1,3,4}\mathcal{Q}^{(i)}_{*,s}\sqcup\bigsqcup_{i<r}\mathcal{Q}^{(5)}_{i,s}\sqcup\bigsqcup_{j<d}\mathcal{Q}^{(5)}_{r,s,j}\setminus\bigsqcup_{i=1,3,4}\mathcal{Q}^{(i)}_{r,s,d}\right)\times\mathcal{Q}_{E_1}(r)\right).$$

A triple of queries from this set corresponds to a triple

$$((t,x,y),(t',x',y'),(k,u,v))\in\mathcal{Q}_C^2\times\mathcal{Q}_{E_1}$$

(in their original forms) such that $t\neq t'$, $h_2(t)=h_2(t')$ and $h_1(t)=k$. (Note that if two queries (r,s,u,v,d) and (r',s',u',v',d') share a common tweak, then we would have $(r,s,d)=(r',s',d')$.) Since such a triple is contained in $\mathcal{C}_2$ and $|\mathcal{C}_2|\le M_3$ by excluding bad keys of (C-5), the size of this set is also upper bounded by M_3.

For $(r,s)\in\mathcal{R}'\times\mathcal{S}'$ and $d\in\{0,1\}^n$, we have

$$\begin{aligned}\left|\bigsqcup_{i=1,3,4}\mathcal{Q}^{(i)}_{*,s}\sqcup\bigsqcup_{i<r}\mathcal{Q}^{(5)}_{i,s}\sqcup\bigsqcup_{j<d}\mathcal{Q}^{(5)}_{r,s,j}\setminus\bigsqcup_{i=1,3,4}\mathcal{Q}^{(i)}_{r,s,d}\right|&\\ =(q^{(1)}_{*,s}-q^{(1)}_{r,s,d})+(q^{(3)}_{*,s}-q^{(3)}_{r,s,d})+(a^{(4)}_{*,s}-q^{(4)}_{r,s,d})+\sum_{i<r}q^{(5)}_{i,s}+\sum_{j<d}q^{(5)}_{r,s,j}&\\ \ge c_{r,s,d}-p_{*,s}-e_{r,s,d}.&\end{aligned}$$

Therefore we have

$$\sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(c_{r,s,d}-p_{*,s}-e_{r,s,d})p_{r,*}\le|\mathcal{C}_2|\le M_3.$$ □

By (17) and Property 11, we have

$$\sum_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}} q^{(5)}_{r,s,d}(b_{r,s,d}-e_{r,s,d})(c_{r,s,d}-e_{r,s,d})\le 4M_3,$$

and by plugging it into (16), we obtain

$$\mathsf{p}''_3\ge\left(1-\frac{16M_3}{N^2}\right)\cdot\prod_{\substack{(r,s)\in\mathcal{R}'\times\mathcal{S}'\\ d\in\{0,1\}^n}}\frac{1}{(N-e_{r,s,d})_{q^{(5)}_{r,s,d}}}.\tag{18}$$

3.3.5 Lower Bounding the Ratio

For each $(r, s, d) \in \{0,1\}^m \times \{0,1\}^m \times \{0,1\}^n$, let

$$\mathcal{T}(r, s, d) = \{w \in \mathcal{T} : (h_1(w), h_2(w), g_1(w) \oplus g_2(w)) = (r, s, d)\}.$$

Then we have a partition of $\mathcal{T}$, namely,

$$\mathcal{T} = \bigsqcup_{\substack{r,s\in\{0,1\}^m \\ d\in\{0,1\}^n}} \mathcal{T}(r, s, d).$$

Since $\sum_{w\in\mathcal{T}(r,s,d)} q_w = q^{(1)}_{r,s,d} + q^{(2)}_{r,s,d} + q^{(3)}_{r,s,d} + q^{(4)}_{r,s,d} + q^{(5)}_{r,s,d}$, we have

$$\begin{aligned}
\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C|\mathcal{Q}_E) = \prod_{w\in\mathcal{T}} \frac{1}{(N)_{q_w}} &\leq \prod_{\substack{r,s\in\{0,1\}^m \\ d\in\{0,1\}^n}} \frac{1}{(N)_{\sum_{w\in\mathcal{T}(r,s,d)} q_w}} \\
&= \prod_{\substack{r,s\in\{0,1\}^m \\ d\in\{0,1\}^n}} \frac{1}{(N)_{q^{(1)}_{r,s,d}+q^{(2)}_{r,s,d}+q^{(3)}_{r,s,d}+q^{(4)}_{r,s,d}+q^{(5)}_{r,s,d}}}. \quad (19)
\end{aligned}$$

By (4), (5), (8), (13), (14), (15), (18), (19), we can prove

$$\frac{\mathsf{p}^{\mathsf{k}}_{\mathsf{re}}(\mathcal{Q}_C|\mathcal{Q}_E)}{\mathsf{p}_{\mathsf{id}}(\mathcal{Q}_C|\mathcal{Q}_E)} \geq 1 - \left(\frac{16M_2}{N} + \frac{16M_3}{N^2}\right), \quad (20)$$

which completes the proof of Lemma 4. The detailed computation will be given in the full version of this paper.

3.4 Putting the Pieces Together

Theorem 1 follows from (1), Lemma 2, Lemma 3 and Lemma 4 with

$$\begin{aligned}
M_1 &= p^{\frac{1}{3}} q^{\frac{1}{3}}, \\
M_2 &= \frac{1}{4}(2q^3 + 2pq^2)^{\frac{1}{2}} N^{\frac{1}{2}} \delta^{\frac{1}{2}} \delta', \\
M_3 &= \frac{1}{2}(q^3 + 2pq^2 + p^2 q)^{\frac{1}{2}} N \delta'.
\end{aligned}$$

References

[1] Carlisle M. Adams. Constructing Symmetric Ciphers Using the CAST Design Procedure. *Designs, Codes and Cryptography*, 12(3):283–316, 1997.

[2] Christophe De Canniere, Orr Dunkelman, and Miroslav Knezevic. KATAN and KTANTAN-A Family of Small and Efficient Hardware-Oriented Block Ciphers. In *CHES 2009*, volume 5747 of *LNCS*, pages 272–288. Springer, 2009.

[3] Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking Even-Mansour Ciphers. In *Crypto 2015, Part I*, volume 9215 of *LNCS*, pages 189–208. Springer, 2015.

[4] Paul Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In *FSE 2000*, volume 1978 of *LNCS*, pages 49–63. Springer, 2000.

[5] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. *Submission to NIST (round 3)*, 7(7.5):3, 2010.

[6] Jérémy Jean, Ivica Nikolić, and Thomas Peyrin. Tweaks and Keys for Block Ciphers: the TWEAKEY Framework. In *Asiacrypt 2014, Part II*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.

[7] Ashwin Jha, Sweta Mishra, Eik List, Kazuhiko Minematsu, and Mridul Nandi. XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing. In *Latincrypt 2017*, To appear. Available at https://eprint.iacr.org/2017/1075.pdf.

[8] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In *Crypto 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.

[9] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In *Crypto 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

[10] Bart Mennink. Optimally Secure Tweakable Blockciphers. In *FSE 2015*, volume 9054 of *LNCS*, pages 428–448. Springer, 2015.

[11] Bart Mennink. XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees. In *Crypto 2016, Part I*, volume 9814 of *LNCS*, pages 64–94. Springer, 2016.

[12] Kazuhiko Minematsu. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In *FSE 2009*, volume 5665 of *LNCS*, pages 308–326. Springer, 2009.

[13] Kazuhiko Minematsu and Tetsu Iwata. Tweak-Length Extension for Tweakable Blockciphers. In *IMACC 2015*, volume 9496 of *LNCS*, pages 77–93. Springer, 2015.

[14] Yusuke Naito. Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security. *IACR Transactions on Symmetric Cryptology*, 2017(2):1–26, 2017.

[15] Thomas Peyrin and Yannick Seurin. Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. In *Crypto 2016, Part I*, volume 9814 of *LNCS*, pages 33–63. Springer, 2016.

[16] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In *Asiacrypt 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.

[17] Rich Schroeppel and Hilarie Orman. The Hasty Pudding Cipher. *AES candidate submitted to NIST*, page M1, 1998.

[18] Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu. How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers. In *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 455–483. Springer, 2016.

[19] Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong. The Simeck Family of Lightweight Block Ciphers. In *CHES 2015*, volume 9293 of *LNCS*, pages 307–329. Springer, 2015.