

ZLR: a fast online authenticated encryption scheme achieving full security

Wonseok Choi¹ · Seongha Hwang² · Byeonghak Lee³ · Jooyoung Lee²

Received: 4 December 2023 / Revised: 27 March 2024 / Accepted: 21 May 2024 © The Author(s) 2024

Abstract

Online authenticated encryption has been considered of practical relevance in light-weight environments due to low latency and constant memory usage. In this paper, we propose a new tweakable block cipher-based online authenticated encryption scheme, dubbed ZLR, and its domain separation variant, dubbed DS-ZLR. ZLR and DS-ZLR follow the Encrypt-Mix-Encrypt paradigm. However, in contrast to existing schemes using the same paradigm such as ELmE and CoLM, ZLR and DS-ZLR enjoy *n*-bit security by using larger internal states with an efficient ZHash-like hashing algorithm. In this way, 2n-bit blocks are processed with only a single primitive call for hashing and two primitive calls for encryption and decryption, when they are based on an *n*-bit tweakable block cipher using *n*-bit (resp. 2n-bit) tweaks for ZLR (resp. DS-ZLR). Furthermore, they support pipelined computation as well as online nonce-misuse resistance. To the best of our knowledge, ZLR and DS-ZLR are the first pipelineable tweakable block cipher-based online authenticated encryption schemes of rate-2/3 that provide *n*-bit security with online nonce-misuse resistance.

Keywords Online authenticated encryption · Nonce-misuse resistance · Tweakable block ciphers

Mathematics Subject Classification 94A60 · 68P25

Communicated by M. Eichlseder.

☑ Jooyoung Lee hicalf@kaist.ac.kr

> Wonseok Choi wonseok@purdue.edu

Seongha Hwang mathience98@kaist.ac.kr

Byeonghak Lee byghak.lee@samsung.com

- ¹ Computer Science Department, Purdue University, West Lafayette, IN 47907, USA
- ² Graduate School of Information Security, KAIST, 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
- ³ Samsung SDS, 125, Olympic-ro 35-gil, Songpa-gu, Seoul 05510, Republic of Korea

1 Introduction

1.1 Authenticated encryption

An authenticated encryption (AE) scheme is a symmetric encryption scheme that achieves both confidentiality and authenticity of data. Recent AE schemes accept associated data (AD) that should be authenticated but not encrypted, sometimes called AEAD schemes. Throughout a significant amount of research and standardization process (e.g., the CAESAR competition and NIST's lightweight cryptography competition), AE schemes have evolved in many ways. Although conventional AE standards (e.g., GCM [24] and CCM [29]) are built on top of block ciphers, recent AE schemes are based on not only a conventional block cipher but also various cryptographic primitives such as public permutations [1, 7, 11], tweakable block ciphers [5, 14, 19, 20, 23, 27], and fork ciphers [3, 4]. In addition, many analyses are being made on security requirements for special environments such as resource-constrained and quantum computing environments. We now have various AE security notions including nonce-misuse security, released unverified plaintext (RUP) security, and so on.

1.2 NAE, MRAE, and OAE

A nonce is an arbitrary value that should never be reused during cryptographic communication. Using a nonce in AE is a typical way of providing variability to the ciphertext and an AE scheme using nonces is called a *nonce-based* AE (NAE). On the other hand, only a single nonce repetition might completely break the security of NAE schemes. For example, GCM leaks its hash key as soon as a single nonce is used twice. Therefore, it is crucial to guarantee the uniqueness of nonces in NAE schemes. In order to avoid nonce repetition, NAE schemes either maintain an internal state to change the nonce for every encryption or choose a nonce as a random value using a sufficiently large amount of entropy. However, it is hard to find and reject all faulty implementations of NAE schemes. It might be challenging to maintain the uniqueness of nonces in a certain environment, for example, a stateless device where good quality randomness is not available.

To address this problem, Rogaway and Shrimpton [28] formalized the notion of *misuse-resistant* AE (MRAE). An MRAE scheme provides a reasonable level of security even if nonces are repeated. Later, the notion of nonce misuse resistance is refined by viewing the adversarial distinguishing advantage as a function of the maximum number of multi-collisions in nonce values or the number of queries with repeated nonces (amongst all encryption queries). There has been a considerable amount of research on the design of MRAE schemes including SIV [28], AEZ [17], and GCM-SIV [15]. However, using MRAE in practice has a fundamental problem in efficiency that such schemes can never be online; in order to achieve MRAE security, each bit of the ciphertext should be affected by every input bit, so one can start encryption only after accepting all the input blocks. The online property and the MRAE security are both highly desirable in resource-constrained environments, where it seems hard to achieve both of them at the same time.

As a compromise between security and efficiency, Fleischmann et al. [13] proposed a security notion that slots between NAE and MRAE, namely, *online* AE (OAE) security. In an OAE scheme, the *i*-th ciphertext block depends only on a key and the first *i* blocks of the plaintext. Then, if we use a nonce as the first input block, OAE security is exactly the same as NAE security in the nonce-respecting scenario. In the case where nonces are repeated, an

OAE scheme loses its privacy only up to the longest common prefix. On the other hand, OAE security guarantees data integrity even in the nonce-misuse setting.

Later, Hoang et al. [18] proposed an alternative security notion for online authenticated encryption, dubbed OAE2. They argued that the existing OAE security does not capture resistance to common-prefix-secret-suffix (CPSS) attacks, while OAE2 security guarantees better security by extending the unit of computation from blocks to segments. However, we believe that OAE2 security is not yet a perfect replacement for OAE since the proposed OAE2-secure constructions require large ciphertext expansions or achieve limited onlineness without providing full security against CPSS attacks. Therefore, in this paper, we focus on OAE-secure constructions.

1.3 Pipelineablility

Suppose that a message block $x \in X$ and a counter $i \in \mathcal{I}$ is processed by an algorithm $f: X \times \mathcal{I} \to Y$, where f is decomposed into $f_1: X \times \mathcal{I} \to Z$ and $f_2: Z \times \mathcal{I} \to Y$ such that $f(x, i) = f_2(f_1(x, i), i)$. If $f_1(x', i+1)$ can be computed without knowing f(x, i), then f is called *pipelineable*. Pipelineability is regarded as advantageous for hardware implementation. Most authenticated encryption schemes based on the Encrypt-Mix-Encrypt paradigm, such as ELmE [12] and CoLM [22], are pipelinable.

1.4 Tweakable block cipher based AE

Tweakable block ciphers (TBCs) are useful for constructing encryption modes since their additional input space gives variety to every encryption. SCT [27], Θ CB [21], Deoxys-I/II [20], LOTUS/LOCUS-AEAD [9] and LightOCB [10] are AE schemes using TBCs as their building primitives. All these schemes provide *n*-bit security for the block length *n* whereas most of (conventional) block cipher-based AE schemes provide only *n*/2-bit security, namely, the birthday bound security (with respect to the block size). TBC is also advantageous as a primitive for hashing modes because it allows for the use of both the tweak space and the message space as the input space, resulting in a reduced number of primitive calls per message block. As authenticated encryption can be considered a combination of encryption and hashing (for authentication), using tweakable block ciphers is one of the promising ways of building an authenticated encryption scheme that achieves both better efficiency and higher security at the same time. ZAE [19], DoveSIV [14], ZOCB and ZOTR [5] are examples of such TBC-based AEs.

1.5 Our contribution

The focus of this paper is put on the construction of tweakable block cipher-based online AE schemes with full *n*-bit OAE security and reasonable efficiency; we propose a new tweakable block cipher-based online authenticated encryption scheme, dubbed ZLR (ZHash–Luby–Rackoff) and its domain separation variant, dubbed DS-ZLR. ZLR follows the Encrypt-Mix-Encrypt paradigm with a novel mixing function that allows online computation. This approach has been already used in previous constructions such as ELmE and CoLM, but all of those are block cipher-based, birthday bound secure, and of rate 1/2, where the rate is defined by the number of input blocks processed per primitive call. ZLR is a tweakable block cipher-based AE scheme that adopts the structure of ZMAC to reduce primitive calls and

AEAD	Primitive	# bits p	ber call	Security	Туре	Pipelineability	Ref.
		AD	Msg				
GCM	BC	n	<i>n</i> /2	<i>n</i> /2	NAE	1	[24]
OCB3	BC	n	n	n/2	NAE	\checkmark	[21]
mGCM	BC	п	n/2	n	NAE	\checkmark	[8]
GCM-SIV	BC	n	<i>n</i> /2	n/2	MRAE	\checkmark	[15]
COPA	BC	п	<i>n</i> /2	n/2	OAE	X	[2]
CoLM	BC	n	<i>n</i> /2	n/2	OAE	\checkmark	[22]
ELmE	BC	п	<i>n</i> /2	n/2	OAE	\checkmark	[12]
LOCUS-AEAD	TBC^{\dagger}	п	<i>n</i> /2	n	NAE	\checkmark	[9]
LOTUS-AEAD	TBC^\dagger	п	<i>n</i> /2	n	NAE	\checkmark	[<mark>9</mark>]
Light-OCB	TBC^\dagger	п	n	n	NAE	\checkmark	[<mark>10</mark>]
ΘCΒ	TBC	п	n	n	NAE	\checkmark	[21]
SCT	TBC	n	n	$n \sim n/2^{\ddagger}$	MRAE	\checkmark	[27]
DoveSIV	TBC	n + t	n(n+t)/(2n+t)	$n \sim n/2^{\ddagger}$	MRAE	X	[14]
ZAE	TBC	n + t	n(n+t)/(2n+t)	n	MRAE	\checkmark	[19]
ZLR	TBC	2 <i>n</i>	2 <i>n</i> /3	n	OAE	\checkmark	This work
DS-ZLR	TBC	2n	2 <i>n</i> /3	n	OAE	✓	This work

 Table 1
 Comparison of ZLR and DS-ZLR with existing AE modes. n denotes the block size and t denote the tweak size

[†]Ideal tweakable block ciphers with small tweaks

^{\ddagger}The security of SCT and DoveSIV degrades from *n*-bit to *n*/2-bit depending on how much nonce is misused

uses a Luby–Rackoff-like structure to encrypt internal states into the ciphertext blocks. More precisely, for an associated data A and a message M, ZLR computes its tag T = ZMAC'(A, M)where ZMAC' is a variant of ZMAC with similar structure. While computing T, ZLR maintains the internal state S, and encrypts T and S by a 2n-bit pseudo-random permutation which is instantiated with two TBC calls in a Luby–Rackoff-like structure. In this way, ZLR processes 2n-bit blocks with only a single TBC call for hashing and two TBC calls for encryption and decryption, achieving rate 2/3, when it is based on an n-bit tweakable block cipher using n-bit tweaks. Furthermore, it supports pipelined computation as well as online nonce-misuse resistance.

We also propose a domain-separated variant of ZLR, dubbed DS-ZLR. The design principle of DS-ZLR is similar to ZLR, while the underlying tweakable block cipher uses a larger tweak space than ZLR, which allows an efficient initialization phase. We believe that ZLR and DS-ZLR will be useful in protocols where high security and efficiency are required simultaneously, especially in protocols where latency is critical and online properties are required (e.g., network protocols).

Table 1 compares ZLR and DS-ZLR to well-known AE schemes based on (tweakable) block ciphers. For simplicity of comparison, we assume that all the underlying tweakable block ciphers use tweaks larger than blocks (i.e., $t \ge n$), except DS-ZLR using 2*n*-bit tweaks. Compared to block cipher based AE schemes with online security such as COPA, CoLM and ELME, ZLR enjoys stronger security and higher rate, while it might suffer from performance loss by using TBCs and require larger memory for masks and internal states. There are a bunch of TBC based AE schemes that achieve full *n*-bit security and some of them also achieve higher rate by utilizing tweak spaces of TBCs, but still, none of them provide OAE security.

To the best of our knowledge, ZLR and DS-ZLR are the first pipelineable tweakable block cipher-based OAE schemes of rate 2/3 that provide *n*-bit security.

2 Preliminaries

2.1 Notation

Throughout this paper, we fix a positive integer *n* such that $n \ge 3$. We write **0** to denote 0^n (i.e., *n*-bit string of all zeros). Let $\lfloor n \rfloor$ is the largest integer *m* such that $m \le n$. Let $w_n = n - 2\lfloor \frac{n}{2} \rfloor$, which is 0 if *n* is even and 1 otherwise. The set $\{0, 1\}^n$ is sometimes regarded as a set of integers $\{0, 1, \ldots, 2^n - 1\}$ by converting an *n*-bit string $a_{n-1} \cdots a_1 a_0 \in \{0, 1\}^n$ to an integer $a_{n-1}2^{n-1} + \cdots + a_12 + a_0$. We also identify $\{0, 1\}^n$ with a finite field $\mathbf{GF}(2^n)$ with 2^n elements, assuming that 2 cyclically generates all the nonzero elements of $\mathbf{GF}(2^n)$. We write $\{0, 1\}^*$ to denote the set of all binary strings including the empty string. For $A, B \in \{0, 1\}^*, |A|$ denotes the length of A, and $A \parallel B$ denotes the concatenation of A and B. For a string $A \in \{0, 1\}^*$, $(A[1], A[2], \ldots, A[m]) \xleftarrow{n} A$ denotes that A is partitioned into strings $A[1], \ldots, A[m]$, where $|A[1]| = \cdots = |A[m-1]| = n$ and $|A[m]| \le n$. For $i = 1, \ldots, m$, let

$$A[:i] = A[1] \parallel \ldots \parallel A[i].$$

For positive integers p and q such that $p \le q$, we write $[q] = \{1, \ldots, q\}$ and $[p, q] = \{p, p + 1, \ldots, q\}$. For a non-empty set $\mathcal{X}, X \leftarrow_{\$} \mathcal{X}$ denotes that X is drawn uniformly at random from \mathcal{X} . The set of all sequences that consist of b pairwise distinct elements of \mathcal{X} is denoted \mathcal{X}^{*b} . For a > b, let $(a)_b = a(a-1) \dots (a-b+1)$, and $(a)_0 = 1$ by convention. If $|\mathcal{X}| = a$, then $(a)_b$ becomes the size of $|\mathcal{X}|^{*b}$

2.2 Security notions

2.2.1 TPRPs

A tweakable permutation with tweak space \mathcal{W} and message space \mathcal{X} is a mapping \tilde{P} : $\mathcal{W} \times \mathcal{M} \to \mathcal{M}$ such that, for any tweak $W \in \mathcal{W}, x \mapsto \tilde{P}(t, x)$ is a permutation of \mathcal{X} . Throughout this paper, we will fix $\mathcal{X} = \{0, 1\}^n$, and write $\operatorname{TP}(\mathcal{W}, n)$ to mean the set of all tweakable permutations with tweak space \mathcal{W} and message space $\{0, 1\}^n$. Let \tilde{E} : $\mathcal{K} \times \mathcal{W} \times \{0, 1\}^n \to \{0, 1\}^n$ be a keyed tweakable permutation with key space \mathcal{K} , where $\tilde{E}(K, W, \cdot)$ is a permutation for each $K \in \mathcal{K}$ and $W \in \mathcal{W}$. We will denote $\tilde{E}_K(W, X)$ for E(K, W, X). A (q, t)-distinguisher against \tilde{E} is an algorithm \mathcal{D} with oracle access to an *n*-bit tweakable permutation and its inverse, making at most *q* oracle queries, running in time at most *t*, and outputting a single bit. The advantage of \mathcal{D} in breaking the TPRP-security of \tilde{E} , i.e., in distinguishing \tilde{E} from a uniform random tweakable permutation $\tilde{\pi} \leftarrow_{\$} \operatorname{TP}(\mathcal{W}, n)$, is defined as

$$\mathsf{Adv}_{\tilde{E}}^{\mathsf{tprp}}(\mathcal{D}) = \left| \Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{\tilde{E}_{K}, \tilde{E}_{K}^{-1}} = 1 \right] - \Pr\left[\tilde{\pi} \leftarrow_{\$} \mathsf{TP}(\mathcal{W}, n) : \mathcal{D}^{\tilde{\pi}, \tilde{\pi}^{-1}} = 1 \right] \right|.$$

We define $\operatorname{Adv}_{\tilde{E}}^{\operatorname{tprp}}(q, t)$ as the maximum of $\operatorname{Adv}_{\tilde{E}}^{\operatorname{tprp}}(\mathcal{D})$ over all (q, t)-distinguishers against \tilde{E} , and when considering information theoretic security, we drop *t*.

2.2.2 OAEs

Given key space \mathcal{K} , associate data (AD) space \mathcal{A} , message space \mathcal{M} , ciphertext space \mathcal{C} , and tag space \mathcal{T} , a online authenticated encryption (OAE) scheme is defined by a tuple

$$\Pi = (\mathcal{K}, \mathcal{A}, \mathcal{M}, \mathcal{C}, \mathsf{Enc}, \mathsf{Dec}),$$

where Enc and Dec denote encryption and decryption schemes, respectively. More precisely,

Enc:
$$\mathcal{K} \times \mathcal{A} \times \mathcal{M} \longrightarrow \mathcal{C} \times \mathcal{T}$$
,
Dec: $\mathcal{K} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T} \longrightarrow \mathcal{M} \cup \{\bot\}$,

where for Enc(K, A, M) = (C, T), we require |C| = |M| and

$$\mathsf{Dec}(K, A, C, T') = \begin{cases} M & \text{if } T = T', \\ \bot & \text{otherwise.} \end{cases}$$

We will write $\text{Enc}_K(A, M)$ to denote Enc(K, A, M) and $\text{Dec}_K(A, C)$ to denote Dec(K, A, C). Throughout this paper, we will fix $\mathcal{A} = \mathcal{M} = \mathcal{C} = \{0, 1\}^*$ and $\mathcal{T} = \{0, 1\}^n$.

The goal of an adversary \mathcal{D} against the OAE security of Π is to distinguish the real world (Enc_K, Dec_K) (using a random key K, unknown to \mathcal{D}) and the ideal world. We assume that \mathcal{D} does not make a redundant query, including a decryption query that reuses any previous encryption query. Given an associated data $A \in \mathcal{A}$ and a message $M \in \mathcal{M}$, let \$ be a random function that outputs

$$_{2n}(A, M[1]) \parallel _{2n}(A, M[:2]) \parallel ... \parallel _{2n}(A, M) \parallel _{n}(A, M),$$

where $(M[1], \ldots, M[m]) \xleftarrow{2n} M$, and $\$_d$ denotes a random function from $\mathcal{A} \times \mathcal{M}$ to $\{0, 1\}^d$. Then, the ideal world oracles are (\$, Rej), where Rej always returns \bot for every decryption query.¹ The advantage of \mathcal{D} breaking the OAE-security of Π is defined as

$$\mathsf{Adv}_{\Pi}^{\mathsf{oae}}(\mathcal{D}) = \left| \Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{\mathsf{Enc}_{K}, \mathsf{Dec}_{K}} = 1 \right] - \Pr\left[\mathcal{D}^{\$, \mathsf{Rej}} = 1 \right] \right|.$$

A (q_e, q_d, σ, l, t) -adversary against the OAE security of Π is an algorithm that makes at most q_e encryption queries to its first oracle and at most q_d decryption queries to its second oracle, and running in time at most t, where the length of each encryption/decryption query is at most l blocks of 2n bits, and the total length of the encryption/decryption queries is at most σ blocks of 2n bits. We define $Adv_{\Pi}^{oae}(q_e, q_d, \sigma, l, t)$ as the maximum of $Adv_{\Pi}^{oae}(\mathcal{D})$ over all (q_e, q_d, σ, l, t) -adversaries \mathcal{D} against Π . When we consider information theoretic security, we will drop the parameter t.

2.3 Coefficient-H technique

We will use Patarin's coefficient-H technique [26]. The goal of this technique is to upper bound the adversarial distinguishing advantage between a real construction and its ideal counterpart. In the real and the ideal worlds, an information-theoretic adversary \mathcal{D} is allowed to make queries to certain oracles (with the same oracle interfaces), denoted \mathcal{O}_{real} and \mathcal{O}_{ideal} , respectively. The interaction between the adversary \mathcal{D} and the oracle determines a "transcript"; it contains all the information obtained by \mathcal{D} during the interaction. We call a transcript τ

¹ The ideal encryption oracle \$ does not accept decryption queries, while this definition is enough to prove security against adversaries without making redundant queries.

attainable if the probability of obtaining τ in the ideal world is non-zero. We also denote T_{id} (resp. T_{re}) the probability distribution of the transcript τ induced by the ideal world (resp. the real world). By extension, we use the same notation to denote a random variable distributed according to each distribution.

We partition the set of attainable transcripts Γ into a set of "good" transcripts Γ_{good} such that the probabilities to obtain some transcript $\tau \in \Gamma_{good}$ are close in the real world and the ideal world, and a set Γ_{bad} of "bad" transcripts such that the probability to obtain any $\tau \in \Gamma_{bad}$ is small in the ideal world. With this partition, the coefficient-H technique is summarized by the following lemma.

Lemma 1 Let $\Gamma = \Gamma_{good} \sqcup \Gamma_{bad}$ be a partition of the set of attainable transcripts, where there exists a non-negative real number ε_1 such that for any $\tau \in \Gamma_{good}$,

$$\frac{\Pr\left[\mathsf{T}_{re}=\tau\right]}{\Pr\left[\mathsf{T}_{id}=\tau\right]} \geq 1 - \varepsilon_1,$$

and there exists ε_2 such that $\Pr[\mathsf{T}_{id} \in \Gamma_{bad}] \leq \varepsilon_2$. Then for any distinguisher \mathcal{D} , one has

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}_{\mathsf{real}}}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_{\mathsf{ideal}}}=1\right]\right| \leq \varepsilon_1+\varepsilon_2$$

We refer to [16] for the proof of Lemma 1.

3 New authenticated encryption modes

In this section, we propose new online deterministic authenticated encryption modes, dubbed ZLR and DS-ZLR. Both ZLR and DS-ZLR are built on top of a tweakable block cipher

$$E: \mathcal{K} \times \mathcal{W} \times \mathcal{N} \to \mathcal{N},$$

and a linear function

$$\rho: \mathcal{S} \times \mathcal{N} \times \mathcal{N} \to \mathcal{S} \times \mathcal{N} \times \mathcal{N},$$

where $S = \{0, 1\}^{2n}$ is a internal state space, $W = \{0, 1\}^t$ and $N = \{0, 1\}^n$ are the tweak and message space for a given \tilde{E} , respectively. We also call ρ as a state update function. Additionally, for given $\rho(S, R, X) = (S', Y, Z)$, we assume that there is a special *inversion* function $\hat{\rho}^{-1}$ such that

$$\hat{\rho}^{-1}(S, Y, Z) = (S', R, X).$$

For given \widetilde{E} and ρ , we denote the mode as

$$\mathsf{ZLR}[E, \rho] = (\mathcal{K}, \mathcal{A}, \mathcal{M}, \mathsf{ZLR}.\mathsf{Enc}, \mathsf{ZLR}.\mathsf{Dec}),$$

and

$$\mathsf{DS}\text{-}\mathsf{ZLR}[E, \rho] = (\mathcal{K}, \mathcal{A}, \mathcal{M}, \mathsf{DS}\text{-}\mathsf{ZLR}\text{.}\mathsf{Enc}, \mathsf{DS}\text{-}\mathsf{ZLR}\text{.}\mathsf{Dec}),$$

where a key space \mathcal{K} , arbitrary associated data space and message space $\mathcal{A} = \mathcal{M} = \{0, 1\}^*$, encryption algorithm ZLR.Enc (and DS-ZLR.Enc), and decryption algorithm ZLR.Dec (and DS-ZLR.Dec), which are deterministic.

Given a key $K \in \mathcal{K}$, we assume that a length of a message $M \in \mathcal{M}$ is divided by 2n, and so does for an associated data $A \in \mathcal{A}$. For the general case, it is sufficient to use one-to-one padding algorithms; for example,

$$ozp(X) = X \parallel 1 \parallel 0^{2n-1+(|X| \mod 2n)}$$
.

By using ozp (or any other proper padding algorithm), one can make lengths of M and A multiples of 2n.

Now, let A = A[1] || A[2] || ... || A[a] and <math>M = M[1] || M[2] || ... || M[m] where $|A[\alpha]| = |B[\beta]| = 2n$ for $\alpha \in [a]$ and $\beta \in [b]$. We denote $A[\alpha] = A_L[\alpha] || A_R[\alpha]$ and $M[\beta] = M_L[\beta] || M_R[\beta]$ where $A_L[\alpha], A_R[\alpha], M_L[\beta], M_R[\beta] \in \{0, 1\}^n$. Figures 1, 2 and 3 show graphical representations and pseudocodes of ZLR.Enc and DS-ZLR.Enc. While ZLR needs additional masking computation compared to DS-ZLR, DS-ZLR needs the primitive with larger tweak space. Therefore, ZLR and DS-ZLR have trade-off in the computational cost and the primitive constraints.

3.1 ZLR

ZLR maintains and updates a 2n-bit state S by proceeding each associated data block or message block in the order. We also denote the *i*-th state as S[i] with the initial state $S[0] = \mathbf{0}$. For given tweakable block cipher \tilde{E} with a secret key $K \in \mathcal{K}$ and tweak space $\mathcal{W} = \{0, 1\}^n$, at first, ZLR pre-calculates masking values Δ_i for i = 1, ..., 6 that will be utilized for both encryption and decryption. To achieve the claimed security, at least two random variables are required for each system of equations in the collision. At the same time, we want to reduce the number of primitive calls needed to produce the maskings. Considering all of the above, ZLR generates masking values in the following way:

$$\Delta_1 = \widetilde{E}_K(\mathbf{0}, \mathbf{0}), \qquad \Delta_3 = \widetilde{E}_K(\mathbf{0}, \mathbf{2}), \qquad \Delta_5 = \Delta_1 \oplus \Delta_3,$$

$$\Delta_2 = \widetilde{E}_K(\mathbf{0}, \mathbf{1}), \qquad \Delta_4 = \widetilde{E}_K(\mathbf{0}, \mathbf{3}), \qquad \Delta_6 = \Delta_2 \oplus \Delta_4.$$

For given associated date $A = A[1] \parallel A[2] \parallel ... \parallel A[a]$, message $M = M[1] \parallel M[2] \parallel ... \parallel M[m]$ and $i \in [a + m]$, we define *i*-th state S[i] and intermediate values X[i], Y[i] and Z[i] as follows:

1. for an associated data block with given $\alpha \in [a]$,

$$X[\alpha] = \widetilde{E}_K(A_R[\alpha] \oplus 2^{\alpha-1}\Delta_2, A_L[\alpha] \oplus 2^{\alpha-1}\Delta_1),$$

(S[\alpha], Y'[\alpha], Z'[\alpha]) = \rho(S[\alpha - 1], X[\alpha], A_R[\alpha] \oplus 2^{\alpha-1}\Delta_2);

2. for a message block with given $\beta \in [m]$,

$$\begin{split} X[\beta+a] &= \widetilde{E}_K(M_R[\beta] \oplus 2^{\beta-1}\Delta_4, M_L[\beta] \oplus 2^{\beta-1}\Delta_3), \\ (S[\beta+a], Y[\beta], Z[\beta]) &= \rho(S[\beta+a-1], X[\beta+a], M_R[\beta] \oplus 2^{\beta-1}\Delta_4). \end{split}$$

Note that $Y'[\alpha]$ and $Z'[\alpha]$ have no usage and the construction uses $S[\alpha]$ only. Hence one may gain slightly better efficiency by implementing the encryption algorithm to calculate $S[\alpha]$ only for the case of associated data blocks. Using the above intermediate values, encryption/decryption process can be described as follows:

1. In the encryption algorithm of ZLR, let (A, M) be a queried data of ZLR.Enc. For $\beta \in [m]$, the β -th ciphertext block $C[\beta] = C_L[\beta] \parallel C_R[\beta]$ is obtained by following calculations:

$$C_R[\beta] = \widetilde{E}_K(Y[\beta], Z[\beta]) \oplus 2^{\beta-1}\Delta_6,$$

$$C_L[\beta] = \widetilde{E}_K(\widetilde{E}_K(Y[\beta], Z[\beta]), Y[\beta]) \oplus 2^{\beta-1}\Delta_5.$$

After the encryption phase, S[a + m] is the final internal state and denote $S[a + m] = U \parallel V$ for $U, V \in \{0, 1\}^n$. Using S[a + m], an *n*-bit authentication tag *T* is derived by $T = \widetilde{E}_K(V, U)$.



(a) Computing a next internal state $S' = S[\alpha]$ in ZLR.Enc (left) and DS-ZLR.Enc (right) by using the previous internal state $S = S[\alpha - 1]$ and α -th associated data block $A[\alpha] = A_L[\alpha] \parallel A_R[\alpha]$.



(b) Computing a next internal state $S' = S[\beta + a]$ and β -th ciphertext block $C[\beta] = C_L[\beta] \parallel C_R[\beta]$ in ZLR.Enc (left) and DS-ZLR.Enc (right) by using the previous internal state $S = S[\beta + a - 1]$ and β -th message block $M[\beta] = M_L[\beta] \parallel M_R[\beta]$.



(c) Computing a tag T in ZLR.Enc (left) and DS-ZLR.Enc (right) from the final state $S[a + m] = U \parallel V$ where l implies a length of a + m in binary manner.

Fig. 1 Algorithm ZLR.Enc (left) and DS-ZLR.Enc (right) based on \widetilde{E} with a key K

$$\begin{array}{c|c} \frac{\operatorname{ZLR}\operatorname{Enc}(A,M)}{1: \quad S \leftarrow \mathbf{0}} & \frac{\operatorname{ZLR}\operatorname{Dec}(A,C,T)}{1: \quad S \leftarrow \mathbf{0}} \\ \hline \\ 2: \quad \Delta_1 \leftarrow \widetilde{E}_K(\mathbf{0},\mathbf{0}), \Delta_2 \leftarrow \widetilde{E}_K(\mathbf{0},\mathbf{1}) \\ 3: \quad \Delta_3 \leftarrow \widetilde{E}_K(\mathbf{0},\mathbf{2}), \Delta_4 \leftarrow \widetilde{E}_K(\mathbf{0},\mathbf{3}) \\ 4: \quad \Delta_5 \leftarrow \Delta_1 \oplus \Delta_3, \Delta_6 \leftarrow \Delta_2 \oplus \Delta_4 \\ 5: \quad \mathbf{for} \ \alpha \in [a] & 3: \quad \Delta_3 \leftarrow \widetilde{E}_K(\mathbf{0},\mathbf{2}), \Delta_4 \leftarrow \widetilde{E}_K(\mathbf{0},\mathbf{3}) \\ 6: \quad A'_L \leftarrow A_L[\alpha] \oplus 2^{\alpha-1}\Delta_1 & 6: \quad A'_L \leftarrow A_L[\alpha] \oplus 2^{\alpha-1}\Delta_1 \\ 7: \quad A'_R \leftarrow A_R[\alpha] \oplus 2^{\alpha-1}\Delta_2 & 7: \quad A'_R \leftarrow A_R[\alpha] \oplus 2^{\alpha-1}\Delta_2 \\ 8: \quad X \leftarrow \widetilde{E}_K(A'_R,A'_L) & 8: \quad X \leftarrow \widetilde{E}_K(A'_R,A'_L) \\ 9: \quad (S,Y,Z) \leftarrow \rho(S,X,A'_R) & 9: \quad (S,Y,Z) \leftarrow \rho(S,X,A'_R) \\ 10: \quad \mathbf{endfor} & 10: \quad \mathbf{endfor} \\ 11: \quad \mathbf{for} \ \beta \in [m] & 11: \quad \mathbf{for} \ \beta \in [m] \\ 12: \quad M'_L \leftarrow M_L[\beta] \oplus 2^{\beta-1}\Delta_3 & 12: \quad C'_L \leftarrow C_L[\beta] \oplus 2^{\beta-1}\Delta_5 \\ 13: \quad M'_R \leftarrow M_R[\beta] \oplus 2^{\beta-1}\Delta_4 & 13: \quad C'_R \leftarrow C_R[\beta] \oplus 2^{\beta-1}\Delta_6 \\ 14: \quad X \leftarrow \widetilde{E}_K(M'_R,M'_L) & 14: \quad Y \leftarrow \widetilde{E}_K^{-1}(C'_R,C'_L) \\ 15: \quad (S,Y,Z) \leftarrow \rho(S,X,M'_R) & 15: \quad Z \leftarrow \widetilde{E}_K^{-1}(M'_R,X) \\ 16: \quad C'_R \leftarrow \widetilde{E}_K(Y,Z) & 16: \quad (S,X,M'_R) \leftarrow \rho^{-1}(S,Y,Z) \\ 17: \quad C'_L \leftarrow \widetilde{E}_K(C'_R,Y) & 17: \quad M'_L \leftarrow \widetilde{E}_K^{-1}(M'_R,X) \\ 18: \quad C_L[\beta] \leftarrow C'_L \oplus 2^{\beta-1}\Delta_5 & 18: \quad M_L[\beta] \leftarrow M'_L \oplus 2^{\beta-1}\Delta_3 \\ 19: \quad C_R[\beta] \leftarrow C'_R \oplus 2^{\beta-1}\Delta_6 & 19: \quad M_R[\beta] \leftarrow M'_R \oplus 2^{\beta-1}\Delta_4 \\ 20: \quad \mathbf{endfor} & 20: \quad \mathbf{endfor} \\ 21: \quad U \parallel V \leftarrow S & 21: \quad U \parallel V \leftarrow S \\ 22: \quad T \leftarrow \widetilde{E}_K(V,U) & 22: \quad T' \leftarrow \widetilde{E}_K(V,U) \\ 23: \quad \mathbf{return} (C,T) & 23: \quad \mathbf{if} \ T = T' \\ 24: & 24: \quad \mathbf{return} \ M \\ 25: \quad \mathbf{else} \\ 26: \quad \mathbf{return} \ \bot \\ 27: \quad \mathbf{endif} \end{array}$$

Fig. 2 ZLR algorithm

2. In the decryption algorithm of ZLR, the order of blocks to process ZLR.Dec is same to ZLR.Enc, however, the calculations for each block are processing in the reverse order. Let (A, C, T) be a queried data of ZLR.Dec. At first, obtain the *a*-th internal state S[a] by processing associated data blocks by the same way as ZLR.Enc. For $\beta \in [m]$, obtain the intermediate values $Y[\beta]$ and $Z[\beta]$ by using β -th ciphertext block $C[\beta] = C_L[\beta] ||C_R[\beta]$:

$$Y[\beta] = \widetilde{E}_K^{-1}(C_R[\beta] \oplus 2^{\beta-1}\Delta_6, C_L[\beta] \oplus 2^{\beta-1}\Delta_5),$$

$$Z[\beta] = \widetilde{E}_K^{-1}(Y[\beta], C_R[\beta] \oplus 2^{\beta-1}\Delta_6).$$

Note that the $(\beta + a - 1)$ -th internal state $S[\beta + a - 1]$ is calculated at the point that $(\beta + a - 1)$ -th ciphertext block has been decrypted. The other intermediate value $X[\beta + a]$ and the partial message block $M_R[\beta]$ are derived by using $Y[\beta]$, $Z[\beta]$, and $S[\beta + a - 1]$ with the inversion function $\hat{\rho}^{-1}$:

$$(X[\beta + a], M_R[\beta]) = \hat{\rho}^{-1}(S[\beta + a - 1], Y[\beta], Z[\beta]).$$

🖄 Springer

$DS ext{-}ZLR ext{.}Enc(A,M)$		DS-Z	ZLR.Dec(A,C,T)
1:	$S \leftarrow 0$	1:	$S \leftarrow 0$
2:	for $\alpha \in [a]$	2:	for $\alpha \in [a]$
3 :	$X \leftarrow \widetilde{E}_K^{0 \parallel \alpha}(A_R[\alpha], A_L[\alpha])$	3 :	$X \leftarrow \widetilde{E}_K^{0 \parallel \alpha}(A_R[\alpha], A_L[\alpha])$
4:	$(S, Y, Z) \leftarrow \rho(S, X, A_R[\alpha])$	4:	$(S, Y, Z) \leftarrow \rho(S, X, A_R[\alpha])$
5:	endfor	5:	endfor
6:	for $\beta \in [m]$	6 :	for $\beta \in [m]$
7:	$X \leftarrow \widetilde{E}_K^{1 \beta}(M_R[\beta], M_L[\beta])$	7:	$Y \leftarrow \widetilde{E}_K^{-1,3 \beta}(C_R[\beta], C_L[\beta])$
8:	$(S, Y, Z) \leftarrow \rho(S, X, M_R[\beta])$	8:	$Z \leftarrow \widetilde{E}_K^{-1,2 \parallel \beta}(Y, C_R[\beta])$
9 :	$C_R[\beta] \leftarrow \widetilde{E}_K^{2 \beta}(Y,Z)$	9 :	$(S, X, M_R[\beta]) \leftarrow \hat{\rho}^{-1}(S, Y, Z)$
10:	$C_L[\beta] \leftarrow \widetilde{E}_K^{3 \beta}(C_R[\beta], Y)$	10 :	$M_L[\beta] \leftarrow \widetilde{E}_K^{-1,1 \parallel \beta}(M_R[\beta], X)$
11:	endfor	11:	endfor
12:	$U \parallel V \leftarrow S$	12:	$U \parallel V \leftarrow S$
13:	$T \leftarrow \widetilde{E}_K^{4 \parallel 0^l}(V, U)$	13:	$T' \leftarrow \widetilde{E}_K^{4 \parallel 0^l}(V, U)$
14:	return (C,T)	14:	if $T = T'$
		15:	$\mathbf{return} \ M$
		16:	else
		17:	$\mathbf{return} \perp$
		18:	endif

Fig. 3 DS-ZLR Algorithm. We denote $\widetilde{E}_{K}^{t_{1}}(t_{2}, m) = \widetilde{E}_{K}(\mathsf{Pad}_{t}(t_{1} || t_{2}), m)$ and $\widetilde{E}_{K}^{-1, t_{1}}(t_{2}, c) = \widetilde{E}_{K}^{-1}(\mathsf{Pad}_{t}(t_{1} || t_{2}), c)$

Remark that, by the definition,

$$X[\beta + a] = \widetilde{E}_K(M_R[\beta] \oplus 2^{\beta - 1} \Delta_4, M_L[\beta] \oplus 2^{\beta - 1} \Delta_3),$$

and therefore,

$$M_{L}[\beta] = \widetilde{E}_{K}^{-1}(M_{R}[\beta] \oplus 2^{\beta-1}\Delta_{4}, X[\beta+a]) \oplus 2^{\beta-1}\Delta_{3}$$

After all ciphertext blocks are decrypted, the final internal state $S[a + b] = U \parallel V$ is given and the algorithm checks whether $T = \widetilde{E}_K(V, U)$ or not. If $T \neq \widetilde{E}_K(V, U)$, the algorithm only returns \perp , and otherwise, it returns the decrypted message $M = M[1] \parallel \ldots \parallel M[m]$.

3.2 DS-ZLR

DS-ZLR, similarly to ZLR, maintains and updates a 2*n*-bit state *S*, by denoting the *i*-th state as S[i] with the initial state S[0] = 0. We also define Pad_t is a padding algorithm to make a *t*-bit string. It can be anything but for simplicity, we define Pad_t as for $X \in \{0, 1\}^{t-d}$ with $0 \le d < t$, Pad_t(X) returns $X \parallel 0^d$. We write A as an element in \mathbb{Z} or in $\{0, 1\}^d$ for an arbitrary d interchangeably, so that $A \parallel B$ with $A \in \mathbb{Z}$ makes sense with an appropriate conversion into binary numbers. For given tweakable block cipher \tilde{E} with a secret key $K \in \mathcal{K}$ and *large enough* tweak space $\mathcal{W} = \{0, 1\}^t$, (i - 1)-th internal state S[i - 1], and *i*-th message (or associated data) block M[i] (A[i]), respectively, we define *i*-th state S[i], *i*-th intermediate values X[i], Y[i] and Z[i] as follows: 1. For an associated data block with given $\alpha \in [a]$,

$$X[\alpha] = \tilde{E}_K(\mathsf{Pad}_t(0 \parallel \alpha \parallel A_R[\alpha]), A_L[\alpha]),$$
$$(S[\alpha], Y'[\alpha], Z'[\alpha]) = \rho(S[\alpha - 1], X[\alpha], A_R[\alpha]),$$

2. For a message block with given $\beta \in [m]$,

$$X[\beta + a] = \overline{E}_K(\mathsf{Pad}_t(1 \parallel \beta \parallel M_R[\beta]), M_L[\beta]),$$
$$(S[\beta + a], Y[\beta], Z[\beta]) = \rho(S[\beta + a - 1], X[\beta + a], M_R[\beta]).$$

Similarly to ZLR, encryption/decryption process can be described as follows:

1. In the encryption algorithm of DS-ZLR, let (A, M) be a queried data of DS-ZLR.Enc. For $\beta \in [m]$, the β -th ciphertext block $C[\beta] = C_L[\beta] \parallel C_R[\beta]$ is obtained by following calculations:

$$C_R[\beta] = \widetilde{E}_K(\mathsf{Pad}_t(2 \parallel \beta \parallel Y[\beta]), Z[\beta]),$$

$$C_L[\beta] = \widetilde{E}_K(\mathsf{Pad}_t(3 \parallel \beta \parallel C_R[\beta]), Y[\beta]).$$

After the encryption phase, S[a+m] is the final internal state and denote S[a+m] = U || V for $U, V \in \{0, 1\}^n$. Using S[a+m], an *n*-bit authentication tag *T* is derived by a following calculation:

$$T = \widetilde{E}_K(\mathsf{Pad}_t(4 \parallel 0^l \parallel V), U),$$

where *l* implies a length of a + m in binary manner.

2. In the decryption algorithm of DS-ZLR, let (A, C, T) be a queried data of ZLR.Dec. At first, obtain the *a*-th internal state S[a] by processing associated data blocks by the same way as ZLR.Enc. For $\beta \in [m]$, obtain the intermediate values $Y[\beta]$ and $Z[\beta]$ by using β -th ciphertext block $C[\beta] = C_L[\beta] \parallel C_R[\beta]$:

$$Y[\beta] = \widetilde{E}_{K}^{-1}(\operatorname{Pad}_{t}(3 \parallel \beta \parallel C_{R}[\beta]), C_{L}[\beta]),$$

$$Z[\beta] = \widetilde{E}_{K}^{-1}(\operatorname{Pad}_{t}(2 \parallel \beta \parallel Y[\beta]), C_{R}[\beta]).$$

We also assume to know the $(\beta + a - 1)$ -th internal state $S[\beta + a - 1]$ when $(\beta + a - 1)$ th ciphertext block has been decrypted. The other intermediate value $X[\beta + a]$ and the partial message block $M_R[\beta]$ are derived by using $Y[\beta]$, $Z[\beta]$, and $S[\beta + a - 1]$ with the inversion function $\hat{\rho}^{-1}$:

$$(X[\beta + a], M_R[\beta]) = \hat{\rho}^{-1}(S[\beta + a - 1], Y[\beta], Z[\beta]).$$

Remark that, by the definition,

$$X[\beta + a] = \tilde{E}_K(\mathsf{Pad}_t(1 \parallel \beta \parallel M_R[\beta]), M_L[\beta]),$$

and therefore,

$$M_L[\beta] = \widetilde{E}_K^{-1}(\mathsf{Pad}_t(1 \parallel \beta \parallel M_R[\beta]), X[\beta + a]).$$

After all ciphertext blocks are decrypted, the final internal state $S[a + b] = U \parallel V$ is given and the algorithm checks whether $T = \widetilde{E}_K(\mathsf{Pad}_t(4 \parallel 0^l \parallel V), U)$ or not. If $T \neq \widetilde{E}_K(\mathsf{Pad}_t(4 \parallel 0^l \parallel V), U)$, the algorithm only returns \bot , and otherwise, it returns the decrypted message $M = M[1] \parallel \ldots \parallel M[m]$.

Note that to cover tweak inputs, we should have $t \ge n + \lceil \log_2(\max(a, m)) \rceil + 3$.



Fig. 4 Algorithm ZLR.Enc based on \widetilde{E} with a key K

3.3 State update function

Remark that the state update function $\rho : S \times N \times N \to S \times N \times N$ should be paired with the inversion function $\hat{\rho}^{-1} : S \times N \times N \to N \times N$ such that, for given $\rho(S, X, R) = (S', Y, Z)$, it always satisfies that $\hat{\rho}^{-1}(S, Y, Z) = (S', X, R)$. Also remark that $S = \{0, 1\}^{2n}$ and $N = \{0, 1\}^n$. For the efficiency of the algorithm, it is desirable that ρ is as simple as possible. On the other hand, if ρ is too simple that it cannot guarantee the security, the entire construction may be vulnerable to distinguishing attacks. In summary, the state update function should satisfy the following properties.

- 1. It must be invertible.
- 2. Every input bit must affect the next state, *Y* value and *Z* value.
- 3. Every output bit must affect the previous state, X value and R value (in inverse).

We need to define ρ (and $\hat{\rho}^{-1}$) to make a probability of bad events small enough and at the same time, we want ρ to be as simple as possible.

In this paper, we define ρ as follows: for S_L , S_R , X, $R \in \{0, 1\}^n$,

$$\rho(S_L \parallel S_R, X, R) = (S'_L \parallel S'_R, S_R \oplus X \oplus R, S_L, \oplus X), \tag{1}$$

where $S'_L = 2 \cdot (S_L \oplus X \oplus R)$ and $S'_R = S_R \oplus X$. For a such ρ and given S_L , S_R , Y, $Z \in \{0, 1\}^n$, it is easy to see that

$$\hat{\rho}^{-1}(S_L \parallel S_R, Y, Z) = (S'_L \parallel S'_R, X, R),$$

where $X = S_L \oplus Z$, $R = S_L \oplus S_R \oplus Y \oplus Z$, $S'_L = 2 \cdot (S_L \oplus X \oplus R)$ and $S'_R = S_R \oplus X$. With this construction, we can compute the internal variables in ZLR; for $\alpha \in [m]$, $Y[\alpha]$ and $Z[\alpha]$ can be formulated by following equations,

$$Y[\alpha] = M_R[\alpha] \oplus 2^{\alpha-1} \Delta_4 \oplus \bigoplus_{\beta=1}^{a+\alpha} X[\beta],$$
(2)
$$Z[\alpha] = X[a+\alpha] \oplus \bigoplus_{\beta=1}^{a} 2^{a+\alpha-\beta} \left(X[\beta] \oplus A_R[\beta] \oplus 2^{\beta-1} \Delta_2 \right)$$

$$\oplus \bigoplus_{\beta=1}^{\alpha-1} 2^{\alpha-\beta} \left(X[a+\beta] \oplus M_R[\beta] \oplus 2^{\beta-1} \Delta_4 \right).$$
(3)

Also, the final state $S = U \parallel V$ can be formulated by following equations,

$$U = \bigoplus_{\beta=1}^{a} 2^{a+m+1-\beta} \left(X[\beta] \oplus A_R[\beta] \oplus 2^{\beta-1} \Delta_2 \right)$$
$$\oplus \bigoplus_{\beta=1}^{m} 2^{m+1-\beta} \left(X[a+\beta] \oplus M_R[\beta] \oplus 2^{\beta-1} \Delta_4 \right), \tag{4}$$

$$V = \bigoplus_{\beta=1}^{a+m} X[\beta].$$
(5)

4 Security of DS-ZLR

We claim OAE-security bound for DS-ZLR by the following theorems.

Theorem 1 Let l, w are non-negative integers such that $w \ge n + \lceil \log_2(l) \rceil + 3$, let \tilde{E} : $\mathcal{K} \times \{0, 1\}^w \times \{0, 1\}^n \to \{0, 1\}^n$ be a tweakable block cipher and ρ be a state update function given in Sect. 3.3. Then for nonnegative integers q_e , q_d , σ , and t such that q_e , $\sigma < 2^{n-1}$, we have

$$\mathsf{Adv}^{\mathsf{oae}}_{\mathsf{DS-ZLR}[\tilde{E},\rho]}(q_e, q_d, \sigma, l, t) \leq \frac{2q_d}{2^n} + \frac{6q^2 + 8\sigma^2 + \sigma l}{2^{2n}} + \mathsf{Adv}^{\mathsf{tprp}}_{\tilde{E}}(3\sigma + q, t + t'),$$

where $q = q_e + q_d$ and t' is the time complexity necessary to compute \widetilde{E} for $3\sigma + q$ queries.

For a better understanding, we give a brief overview of the proof in this section. Since proving the security bound of DS-ZLR is easier, we will provide our proof of Theorem 1 first. The core idea of our proof is simple; we use the standard coefficient-H technique. We define bad events, namely bad_1 and bad_2 , to avoid any collision between two primitives. Additional information on the internal states will be freely given to an adversary at the end of the distinguishing game, but before deciding the final output. The probability of the bad events, which handle the collisions, can be computed using these internal states. In particular, upper bounding the probability of bad_2 needs some tedious computation, while all we need to do is simply dividing all possible cases and bounding each case. We obtain Theorem 1 from (10), Lemmas 2 and 3.

4.1 Proof setup

Fix a (q_e, q_d, σ, l, t) -adversary \mathcal{A} against DS-ZLR $[\tilde{E}, \rho]$. Up to the TPRP security of \tilde{E}, \tilde{E} can be replaced by random tweakable permutation $\tilde{\pi}$. Precisely, the cost of this replacement is upper bounded by

$$\operatorname{Adv}_{\tilde{E}}^{\operatorname{tprp}}(3\sigma + q, t + t'),$$

where t' is the time complexity necessary to compute \widetilde{E} for $3\sigma + q$ queries.

Let \$ denote the online random function defined as in Sect. 2.2. A has to distinguish (ZLR.Enc, ZLR.Dec) and (\$, Rej) using q_e encryption queries and q_d decryption queries. In

the real world, the adversary A interacts with DS-ZLR = (ZLR.Enc, ZLR.Dec). In the ideal world, A interacts with (\$, Rej).

In the *i*-th encryption query, A queries with the associated data A_i and the message M_i , and get the ciphertext C_i and the tag T_i . In the *j*-th decryption query, A queries with the associated data A'_i , the ciphertext C'_i , and the tag T'_i and get $b'_i = M'_i$ or \bot . Then let

$$\tau_e = (A_i, M_i, C_i, T_i)_{i \in [q_e]}, \tau_d = (A'_i, C'_j, T'_j, b'_j)_{j \in [q_d]},$$

denote the list of the encryption queries and the decryption queries, respectively. We can assume that the adversary queries all the decryption queries after all the encryption queries are done because of the following reason.

- Adversary A' assume that all the decryption queries would return \bot , and queries encryption queries with this assumption.
- If one of the decryption queries actually return M'_j for some $j \in [q_d]$, then \mathcal{A} and \mathcal{A}' has the same distinguishing advantage 1.
- If all the decryption queries return ⊥, then A and A' has the same distinguishing advantage since there is no change of the information.

Therefore, let $q = q_e + q_d$ and we can rearrange the queries and their answers as

$$\{(A_i, M_i, C_i, T_i)_{i \in [q_e]}, (A_j, C_j, T_j, b_j)_{j \in [q_e+1,q]}\}.$$

Recall that $|A_i| \mod 2n = |M_i| \mod 2n = |C_i| \mod 2n = 0$ for all $i \in [q]$. Now for $i \in [q]$, set:

$$(A_i[1], \dots, A_i[a_i]) \stackrel{2n}{\longleftarrow} A_i;$$
$$(C_i[1], \dots, C_i[m_i]) \stackrel{2n}{\longleftarrow} C_i.$$

Similarly, for $i \in [q_e]$, set:

$$(M_i[1],\ldots,M_i[m_i]) \stackrel{2n}{\longleftarrow} M_i.$$

Let $l_i = a_i + m_i$ for $i \in [q]$, then $\sigma = \sum_{i \in [q]} l_i$ and $l = \max \{l_i : i \in [q]\}$. We define some useful index set that

$$\mathcal{P}_A = \{(i, \alpha) : i \in [q], \alpha \in [a_i]\};$$
$$\mathcal{P}_M = \{(i, \alpha) : i \in [q_e], \alpha \in [m_i]\};$$
$$\mathcal{P}_C = \{(i, \alpha) : i \in [q], \alpha \in [m_i]\},$$

which denote the set of the indices of the associated data, the message, and the ciphertext, respectively. Now we reveal the actual internal states $X_i[\alpha]$, $Y_i[\alpha]$, and $Z_i[\alpha]$ variables in the real world. We set for the encryption queries:

- for $(i, \alpha) \in \mathcal{P}_A, X_i[\alpha] = \tilde{\pi}(\mathsf{Pad}_t(0 \parallel \alpha \parallel A_{i,R}[\alpha]), A_{i,L}[\alpha]);$
- for $(i, \alpha) \in \mathcal{P}_M, X_i[a_i + \alpha] = \tilde{\pi}(\mathsf{Pad}_t(1 \parallel \alpha \parallel M_{i,R}[\alpha]), M_{i,L}[\alpha]);$
- for $(i, \alpha) \in \mathcal{P}_C$, $Y_i[\alpha] = \tilde{\pi}^{-1}(\mathsf{Pad}_t(3 \parallel \alpha \parallel C_{i,R}[\alpha]), C_{i,L}[\alpha]);$
- for $(i, \alpha) \in \mathcal{P}_C$, $Z_i[\alpha] = \tilde{\pi}^{-1}(\mathsf{Pad}_t(2 \parallel \alpha \parallel Y_i[\alpha]), C_{i,R}[\alpha]).$

On the other hand, in the ideal world, for $i \in [q_e]$ and $\alpha \in [l_i]$, $X_i[\alpha]$ is chosen satisfying following rules. For $i \in [q_e]$,

• if $\alpha \in [a_i]$ and there exists j < i such that $A_i[\alpha] = A_j[\alpha]$, set $X_i[\alpha] = X_j[\alpha]$;

🖄 Springer

- if $\alpha \in [m_i]$ and there exists j < i such that $M_i[\alpha] = M_i[\alpha]$, set $X_i[a_i + \alpha] = X_i[a_i + \alpha]$;
- if $\alpha \in [a_i]$, sample $X_i[\alpha] \leftarrow \{0, 1\}^n$ different from $X_i[\alpha]$ for all $j \in [q_e]$ satisfying $a_i \geq \alpha, A_i[\alpha] \neq A_i[\alpha], \text{ and } A_{i,R}[\alpha] = A_{i,R}[\alpha];$
- if $\alpha \in [m_i]$, sample $X_i[a_i + \alpha] \leftarrow \{0, 1\}^n$ different from $X_j[a_i + \alpha]$ for all $j \in [q_e]$ satisfying $a_i < \alpha$, $M_i[\alpha] \neq M_j[\alpha]$, and $M_{i,R}[\alpha] = M_{j,R}[\alpha]$;
- otherwise, sample $X_i[\alpha] \leftarrow_{\$} \{0, 1\}^n$ uniformly at random.

Now $Y_i[\alpha]$ and $Z_i[\alpha]$ for $i \in [q_e]$ and $\alpha \in [m_i]$ can be given by (2) and (3), and those would be revealed. For $i \in [q_e + 1, q]$ and $\alpha \in [m_i]$, $Y_i[\alpha]$ and $Z_i[\alpha]$ are chosen satisfying following rules:

- if there exists j < i such that $C_i[\alpha] = C_i[\alpha]$, set $Y_i[\alpha] = Y_i[\alpha]$ and set $Z_i[\alpha] = Z_i[\alpha]$;
- if there exists j < i such that $C_i[\alpha] \neq C_i[\alpha]$ and $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, sample $Y_j[\alpha] \leftarrow_{\$}$ $\{0, 1\}^n$ different from $Y_k[\alpha]$;
- otherwise, sample $Y_i[\alpha] \leftarrow_{\$} \{0, 1\}^n$ and $Z_i[\alpha] \leftarrow_{\$} \{0, 1\}^n$ uniformly at random.

Finally, A attains the following transcript:

 $\tau = \left\{ (A_i, M_i, X_i, Y_i, Z_i, C_i, T_i)_{i \in [q_e]}, (A_i, X_i, Y_i, Z_i, C_i, T_i, b_i)_{i \in [q_e+1, q]} \right\}.$

4.2 Defining bad events

In this section, we define bad events. For $i \in [q]$, let U_i and V_i be the final state $S_i[l_i]$, which is defined in (4) and (5). To describe the bad cases, we will define some functions which take the indices as input. Let

- $\mathcal{I}_1 = \{(i, \alpha) \in \mathcal{P}_A : \forall j < i, A_i[\alpha] \neq A_j[\alpha]\};$
- $\mathcal{I}_2 = \{(i, \alpha) \in \mathcal{P}_M : \forall j < i, M_i[\alpha] \neq M_j[\alpha]\};$ $\mathcal{I}_3 = \mathcal{I}_4 = \{(i, \alpha) \in \mathcal{P}_C : \forall j < i, C_i[\alpha] \neq C_j[\alpha]\}.$

For $r \in [4]$, let $f_r, g_r : \mathcal{I}_r \to (\{0, 1\}^n)^2$ be functions where

$f_1(i,\alpha) = (A_{i,R}[\alpha], A_{i,L}[\alpha]),$	$g_1(i,\alpha) = (A_{i,R}[\alpha], X_i[\alpha]),$
$f_2(i,\alpha) = (M_{i,R}[\alpha], M_{i,L}[\alpha]),$	$g_2(i,\alpha) = (M_{i,R}[\alpha], X_i[a_i + \alpha]),$
$f_3(i,\alpha) = (Y_i[\alpha], Z_i[\alpha]),$	$g_3(i,\alpha) = (Y_i[\alpha], C_{i,R}[\alpha]),$
$f_4(i, \alpha) = (C_i R[\alpha], Y_i[\alpha]),$	$g_4(i, \alpha) = (C_i R[\alpha], C_i L[\alpha]).$

Note that f_r gives the pair of the tweak and the input of each tweakable block cipher call, and g_r gives the pair of the tweak and the output of each tweakable block cipher call. For $r \in [4]$, we define the following events.

- $\mathsf{IC}_r \Leftrightarrow \text{there exists } ((i, \alpha), (j, \alpha)) \in \mathcal{I}_r^{*2} \text{ such that } i \neq j \text{ and } f_r(i, \alpha) = f_r(j, \alpha);$
- $\mathsf{OC}_r \Leftrightarrow$ there exists $((i, \alpha), (j, \alpha)) \in \mathcal{I}_r^{*2}$ such that $i \neq j$ and $g_r(i, \alpha) = g_r(j, \alpha)$,

and let

- $\mathsf{IC}_5 \Leftrightarrow$ there exists distinct $i, j \in [q]$ such that $(V_i, U_i) = (V_i, U_i)$;
- OC₅ \Leftrightarrow there exists distinct $i, j \in [q_e]$ such that $(V_i, T_i) = (V_i, T_i)$.

A transcript τ is defined as *bad* if one of the following events occurs:

- 1. bad₁ \Leftrightarrow there exists $i, j \in [q_e]$ and $\alpha \in [\min\{m_i, m_i\}]$ such that $(A_i, M_i[:\alpha]) \neq i$ $(A_i, M_i[:\alpha])$ and $C_i[\alpha] = C_i[\alpha];$
- 2. bad₂ $\Leftrightarrow \bigvee_{1 \le r \le 5} (\mathsf{IC}_r \lor \mathsf{OC}_r).$

We denote Γ_{bad} as a set of all bad transcripts.

4.3 Analyzing good transcripts

In this section, we will prove the following lemma.

Lemma 2 For any $\tau \notin \Gamma_{\text{bad}}$,

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} \ge 1 - \frac{2q_d}{2^n}$$

Proof Fix $\tau \notin \Gamma_{bad}$. For the proof, we define following sets,

- $\mathcal{I}'_{3} = \{(i, \alpha) : i \in [q_{e} + q_{d}], \alpha \in [m_{i}], \forall j < i, (A_{i}, C_{i}[:\alpha]) \neq (A_{j}, C_{j}[:\alpha])\}.$
- $W_1[\alpha, v] = \{(i, \alpha) \in \mathcal{I}_1 : A_{i,R}[\alpha] = v\};$
- $W_2[\alpha, v] = \{(i, \alpha) \in \mathcal{I}_2 : M_{i,R}[\alpha] = v\};$
- $W_3[\alpha, v] = \{(i, \alpha) \in \mathcal{I}'_3 : C_{i,R}[\alpha] = v\};$ $W_4[\alpha, v] = \{(i, \alpha) \in \mathcal{I}'_3 : Y_i[\alpha] = v\},$

and following notations,

- $u_j[\alpha, v] = |W_j[\alpha, v]|$ for $j \in [4]$;
- $u_5[\alpha] = |\{(i, \alpha) \in \mathcal{I}'_3 : \forall j < i, C_i[\alpha] \neq C_j[\alpha]\}|;$ $u_6^e[v] = |\{i \in [q_e] : V_i = v\}|;$ $u_6^d[v] = |\{i \in [q_e + 1, q_e + q_d] : V_i = v\}|.$

For $j \in [4]$, let

$$W_j^e[\alpha, v] = \left\{ (i, \alpha) \in W_j[\alpha, v] : i \in [q_e] \right\},\$$

and

$$W_j^d[\alpha, v] = W_j[\alpha, v] \setminus W_j^e[\alpha, v].$$

We also denote $u_j^e[\alpha, v] = |W_j^e[\alpha, v]|$ and $u_j^d[\alpha, v] = |W_j^d[\alpha, v]|$, so we have $u_j[\alpha, v] =$ $u_i^e[\alpha, v] + u_i^d[\alpha, v].$

First, we consider the ideal world. The probability that ciphertext C_1, \ldots, C_{q_e} is given is $\frac{1}{2^{2n|\mathcal{B}|}} \text{ where } \mathcal{B} = \{(A_i, M_i[:\alpha]) : 1 \le i \le q_e, \alpha \in [m_i]\}, \text{ and one that tags } T_1, \ldots, T_{q_e} \text{ are } I_1 \le q_e, \alpha \in [m_i]\}, \text{ and one that tags } T_1, \ldots, T_{q_e} \text{ are } I_1 \le q_e, \alpha \in [m_i]\}, \beta \in [m_i]\}$ given is $\frac{1}{2^{nq_e}}$. Let **X**, **Y**, **Z** be the distribution of $(X_1, \ldots, X_{q_e+q_d}), (Y_{q_e+1}, \ldots, Y_{q_e+q_d})$, and $(Z_{q_e+1}, \ldots, Z_{q_e+q_d})$, respectively. First, $X_i[\alpha]$ and $X_j[\alpha]$ are given differently if $A_{i,R}[\alpha] =$ $A_{j,R}[\alpha]$ or $M_{i,R}[\alpha] = M_{j,R}[\alpha]$. Therefore, for each $v \in \{0, 1\}^n$ and $\alpha \in [a_i]$, the probability that $X_i[\alpha]$'s for $A_{i,R}[\alpha] = v$ are given according to associated data is $\frac{1}{(2^n)_{u_1[\alpha,v]}}$. Similarly, for each $v \in \{0, 1\}^n$ and $\alpha \in [m_i]$, one that corresponding $X_i[\alpha]$'s for $M_{i,R}[\alpha] = v$ are given according to message is $\frac{1}{(2^n)_{\mu_2}[\alpha,\nu]}$. Hence,

$$\Pr\left[\mathbf{X} = (X_1, \dots, X_{q_e+q_d})\right] = \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_1[\alpha,v]}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_2[\alpha,v]}}$$

Also, $Y_i[\alpha]$ and $Y_j[\alpha]$ are given differently if $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, while $\{Y_i\}_{1 \le i \le q_e}$ is determined from $(X_1, \ldots, X_{q_e+q_d})$. Therefore, for each $v \in \{0, 1\}^n$ and $\alpha \in [l]$, the probability that corresponding $Y_i[\alpha]$'s are given is $\frac{1}{(2^n - u_3^e[\alpha, v])_{u_i^d[\alpha, v]}}$. Hence similarly from the case above,

Springer
 Springer

$$\Pr\left[\mathbf{Y} = (Y_{q_e+1}, \dots, Y_{q_e+q_d}) | \mathbf{X}\right] = \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n - u_3^e[\alpha, v])_{u_3^d[\alpha, v]}}.$$

Now, since $Z_i[\alpha]$'s are given uniformly at random in decryption queries,

$$\Pr\left[\mathbf{Z} = (Z_{q_e+1}, \dots, Z_{q_e+q_d})\right] = \prod_{1 \le \alpha \le l} \frac{1}{(2^n)^{u_5[\alpha]}}.$$

Hence, we can conclude the following probability.

$$\Pr\left[\mathsf{T}_{\mathsf{id}} = \tau\right] = \frac{1}{2^{2n|\mathcal{B}|}} \times \frac{1}{2^{nq_e}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_1[\alpha,v]}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_2[\alpha,v]}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n - u_3^e[\alpha,v])_{u_3^d[\alpha,v]}} \times \left(\prod_{\substack{1 \le \alpha \le l}} \frac{1}{(2^n)^{u_5[\alpha]}}\right).$$
(6)

Now, we consider the real world. First, in decryption queries, the probability attaining \perp for every answer is bounded below by

$$\prod_{v \in \{0,1\}^n} \left(1 - \frac{1}{2^n - u_6^e[v]} \right)^{u_6^d[v]} \ge \left(1 - \frac{1}{2^n - q_e} \right)^{q_d} \ge 1 - \frac{q_d}{2^n - q_e}.$$

Since the case bad_2 does not exist in any good transcript, the number of tweakable block ciphers in all queries that has

- 1. $(0 \parallel \alpha) \parallel v$ as tweak is $u_1[\alpha, v]$;
- 2. $(1 \parallel \alpha) \parallel v$ as tweak is $u_2[\alpha, v]$;
- 3. $(2 \parallel \alpha) \parallel v$ as tweak is $u_3[\alpha, v]$;
- 4. $(3 \parallel \alpha) \parallel v$ as tweak is $u_4[\alpha, v]$;
- 5. $(4 \parallel 0) \parallel v$ as tweak is $u_6^e[v]$,

for fixed $v \in \{0, 1\}^n$. Therefore,

$$\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right] \ge \prod_{\substack{1 \le \alpha \le l \\ v \in \{0,1\}^n}} \frac{1}{(2^n)_{u_1[\alpha,v]}(2^n)_{u_2[\alpha,v]}(2^n)_{u_3[\alpha,v]}(2^n)_{u_4[\alpha,v]}} \times \prod_{v \in \{0,1\}^n} \frac{1}{(2^n)_{u_6^e[v]}}.$$
(7)

For simplicity, we use the following formula.

$$\prod_{v \in \{0,1\}^n} \frac{1}{(2^n)_{u_6^e[v]}} \ge \prod_{v \in \{0,1\}^n} \frac{1}{(2^n)^{u_6^e[v]}} = \frac{1}{(2^n)^{q_e}}.$$
(8)

Also,

$$\prod_{1 \le \alpha \le l} (2^n)^{u_5[\alpha]} \ge \prod_{1 \le \alpha \le l} (2^n)_{u_5[\alpha]} \ge \prod_{1 \le \alpha \le l} (2^n)_{u_4^d[\alpha]}.$$
(9)

Therefore by (6), (7), (8) and (9),

$$\begin{aligned} \frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} &\geq \frac{2^{2n|\mathcal{B}|}}{\prod_{\substack{v \in \{0,1\}^n \\ 1 \leq \alpha \leq l}} (2^n)_{\substack{u_3^e[\alpha,v] \\ 1 \leq \alpha \leq l}} \prod_{\substack{v \in \{0,1\}^n \\ 1 \leq \alpha \leq l}} (2^n)_{\substack{u_4^e[\alpha,v] \\ 1 \leq \alpha \leq l}} \times \left(1 - \frac{q_d}{2^n - q_e}\right) \\ &\geq 1 - \frac{q_d}{2^n - q_e} \geq 1 - \frac{2q_d}{2^n}. \end{aligned}$$

The last inequality follows that

$$|\mathcal{B}| \ge \sum_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} u_3^e[\alpha, v],$$

so

$$2^{n|\mathcal{B}|} \ge \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)^{u_3^e[\alpha,v]} \ge \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)_{u_3^e[\alpha,v]}$$

and similarly,

$$2^{n|\mathcal{B}|} \ge \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)_{u_4^e[\alpha,v]}.$$

It completes the proof.

4.4 Bounding the probability of bad events

In this section, we will now find the upper bound on the probability that each bad event will occur in the ideal world. Fix $i, j \in [q_e]$ and $\alpha \in [\min\{m_i, m_j\}]$ such that $(A_i, M_i[:\alpha]) \neq (A_j, M_j[:\alpha])$. Then, since $C_i[\alpha]$ and $C_j[\alpha]$ are chosen uniformly at random, one has

$$\Pr\left[\mathsf{bad}_1\right] \le \frac{\sigma l}{2^{2n}}.\tag{10}$$

We now claim the following lemma.

Lemma 3

$$\Pr\left[\mathsf{bad}_2 \land \neg \mathsf{bad}_1\right] \leq \frac{8\sigma^2 + 6q^2}{2^{2n}}.$$

Let

$$\mathsf{IC} = \bigvee_{1 \le i \le 5} \mathsf{IC}_i, \qquad \qquad \mathsf{OC} = \bigvee_{1 \le i \le 5} \mathsf{OC}_i.$$

Note that $bad_2 = IC \lor OC$. We can upper bound the probability of each collision event as follows.

Lemma 4

$$\Pr\left[\mathsf{IC}\right] \le \frac{4q^2 + 6\sigma^2}{2^{2n}}.$$

Deringer

Lemma 5

$$\Pr\left[\mathsf{OC}\right] \le \frac{2q_e^2 + 2\sigma^2}{2^{2n}}.$$

Then, Lemma 3 follows from Lemmas 4 and 5. Finally, by Lemmas 3, 2, and (10), we can conclude that Theorem 1 holds.

Before we start, we will use the following lemma through the whole proof.

Lemma 6 *Fix* $(i, \alpha) \in \mathcal{I}_1$ *. Then*

$$\Pr\left[X_i[\alpha]=Q\right] \le \frac{2}{2^n},$$

for any $Q \in \{0, 1\}^n$. Similarly, fix $(i, \alpha) \in \mathcal{I}_2$. Then

$$\Pr\left[X_i[a_i+\alpha]=Q\right] \le \frac{2}{2^n},$$

for any $Q \in \{0, 1\}^n$.

Proof Let J be the set of $j \in [q]$ such that If $A_{i,R}[\alpha] = A_{j,R}[\alpha]$ but $A_{i,L}[\alpha] \neq A_{j,L}[\alpha]$, then $X_i[\alpha]$ is sampled uniformly at random from $\{0, 1\}^n \setminus \{X_j[\alpha] : j \in J\}$. In this case,

$$\Pr[X_i[\alpha] = Q] \le \frac{1}{2^n - |J|} \le \frac{2}{2^n}.$$

We can apply the similar argument when $M_i[\alpha] \neq M_i[\alpha]$ for some α .

Proof of Lemma 4 We calculate each probability of IC_i for $1 \le i \le 5$.

1. Fix $((i, \alpha), (j, \alpha)) \in (\mathcal{I}_1)^{*2}$. Then one should have $A_i[\alpha] \neq A_j[\alpha]$ and $f_1(i, \alpha) \neq f_1(j, \alpha)$. Therefore, we get

 $\Pr\left[\mathsf{IC}_1\right] = 0.$

2. Fix $((i, \alpha), (j, \alpha)) \in \mathcal{I}_2^{*2}$. Then $M_i[\alpha] \neq M_j[\alpha]$ so $f_2(i, \alpha) \neq f_2(j, \alpha)$. Therefore, we get

$$\Pr[IC_2] = 0.$$

3. Fix $((i, \alpha), (j, \alpha)) \in (\mathcal{I}_3)^{*2}$ where $i \leq j$. First, assume that $j \in [q_e + 1, q_e + q_d]$. Then $f_3(i, \alpha) = f_3(j, \alpha)$ if and only if

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} Y_j[\alpha] \\ Z_j[\alpha] \end{pmatrix} = \begin{pmatrix} Y_i[\alpha] \\ Z_i[\alpha] \end{pmatrix}.$$

By the sampling process of Y and Z variables in the ideal world,

$$\Pr\left[Y_i[\alpha] = Y_j[\alpha] \land Z_i[\alpha] = Z_j[\alpha]\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

Therefore, we have

$$\Pr[f_3(i, \alpha) = f_3(j, \alpha)] \le \frac{4}{2^{2n}}$$

when $j \in [q_e + 1, q_e + q_d]$. Suppose $j \in [q_e]$. Then, by (2) and (3), $f_3(i, \alpha) = f_3(j, \alpha)$ if and only if

$$\begin{cases} \bigoplus_{\substack{\gamma=1\\\gamma=1}}^{a_i+\alpha} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\alpha} X_j[\gamma] = P; \\ \bigoplus_{\substack{\gamma=1\\\gamma=1}}^{a_i+\alpha} 2^{a_i+\alpha-\gamma} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\alpha} 2^{a_j+\alpha-\gamma} X_j[\gamma] = Q, \end{cases}$$
(11)

🖄 Springer

$$P = M_{i,R}[\alpha] \oplus M_{j,R}[\alpha],$$

$$Q = \bigoplus_{\gamma=1}^{a_i} 2^{a_i + \alpha - \gamma} A_{i,R}[\gamma] \oplus \bigoplus_{\gamma=1}^{\alpha - 1} 2^{\alpha - \gamma} M_{i,R}[\gamma]$$

$$\oplus \bigoplus_{\gamma=1}^{a_j} 2^{a_j + \alpha - \gamma} A_{j,R}[\gamma] \oplus \bigoplus_{\gamma=1}^{\alpha - 1} 2^{\alpha - \gamma} M_{j,R}[\gamma]$$

Let us take a look at each of the subcase below.

(a) If $a_i < a_j$, (11) can be rewritten as

$$\begin{cases} X_j[a_i] \oplus X_j[a_j] = P'; \\ 2^{a_j - a_i} X_j[a_i] \oplus X_j[a_j] = Q', \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} Y_j[\alpha] \\ Z_j[\alpha] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix}, \end{cases}$$

for some P' and Q' which are independent of $X_j[a_i]$ and $X_j[a_j]$. Then, when $j \in [q_e]$,

Pr
$$[f_3(i, \alpha) = f_3(j, \alpha)] = \frac{1}{2^{2n}},$$

by the sampling process of $X_i[a_i]$ and $X_i[a_i]$. Therefore, we have

$$\Pr\left[f_3(i,\alpha) = f_3(j,\alpha)\right] \le \frac{4}{2^{2n}}$$

(b) If there exists two different $\gamma_1, \gamma_2 \leq \alpha$ such that $A_i[\gamma_1] \neq A_j[\gamma_1]$ and $A_i[\gamma_2] \neq A_j[\gamma_2]$, (11) can be rewritten as

$$\begin{cases} X_j[\gamma_1] \oplus X_j[\gamma_2] = P'; \\ 2^{a_j + \alpha - \gamma_1} X_j[\gamma_1] \oplus 2^{a_j + \alpha - \gamma_2} X_j[\gamma_2] = Q', \end{cases}$$

for some P' and Q' which are independent of $X_i[\gamma_1]$ and $X_i[\gamma_2]$. Therefore, we get

$$\Pr[f_3(i, \alpha) = f_3(j, \alpha)] \le \frac{1}{2^{2n}}$$

by the sampling process of $X_j[\gamma_1]$ and $X_j[\gamma_2]$. We can apply the similar argument if $(A_i, M_i[: \alpha])$ and $(A_j, M_j[: \alpha])$ are differ in two or more blocks.

(c) Let $a_i = a_j$ and $M_i[\alpha] \neq M_j[\alpha]$ while $(A_i, M_i[\alpha - 1]) = (A_j, M_j[\alpha - 1])$, Then, (11) can be rewritten as

$$\begin{cases} X_i[a_i + \alpha] \oplus X_j[a_i + \alpha] = M_{i,R}[\alpha] \oplus M_{j,R}[\alpha]; \\ X_i[a_i + \alpha] \oplus X_j[a_i + \alpha] = 0, \end{cases}$$

so one should have $X_i[a_i + \alpha] = X_j[a_i + \alpha]$ and $M_{i,R}[\alpha] = M_{j,R}[\alpha]$ which contradicts the rules for choosing X variables. Therefore,

$$\Pr[f_3(i, \alpha) = f_3(j, \alpha)] = 0,$$

and one can apply the similar argument if there exists only one different block between $(A_i, M_i[: \alpha])$ and $(A_j, M_j[: \alpha])$.

All in all, we get

$$\Pr\left[\mathsf{IC}_3\right] \le \frac{4|\mathcal{I}_3|^2}{2^{2n}}.$$

- Fix ((i, α), (j, α)) ∈ I^{*2}₄. Without loss of generality, let i ≤ j. We distinguish some sub-cases as below.
 - (a) Let $i, j \in [q_e]$. Note that $C_i[\alpha] \neq C_j[\alpha]$ and $M_i[:\alpha] \neq M_j[:\alpha]$ since $((i, \alpha), (j, \alpha)) \in \mathcal{I}_4^{*2}$. Let $h \in [\alpha]$ the index such that $M_i[h] \neq M_j[h]$. Then $f_4(i, \alpha) = f_4(j, \alpha)$ if and only if

$$\begin{cases} C_{i,R}[\alpha] = C_{j,R}[\alpha];\\ X_i[h] = M_{i,R}[\alpha] \oplus M_{j,R}[\alpha] \oplus \bigoplus_{\gamma \neq a_i+h} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\alpha} X_j[\gamma]. \end{cases}$$

Since $C_{i,R}[\alpha]$ is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[h]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_4(i,\alpha) = f_4(j,\alpha)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

(b) Let $i \in [q_e]$, $j \in [q_e + 1, q]$. If $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, then $Y_i[\alpha] \neq Y_j[\alpha]$ by the sampling process. In this case, $\Pr[f_4(i, \alpha) = f_4(j, \alpha)] = 0$. If $C_{i,R}[\alpha] \neq C_{j,R}[\alpha]$, then similarly $\Pr[f_4(i, \alpha) = f_4(j, \alpha)] = 0$. Therefore,

$$\Pr [f_4(i, \alpha) = f_4(j, \alpha)] = 0.$$

(c) Let $i, j \in [q_e + 1, q]$. If $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, then $Y_i[\alpha] \neq Y_j[\alpha]$ by the sampling process, so the probability is zero. If $C_{i,R}[\alpha] \neq C_{j,R}[\alpha]$, then the probability is obviously zero.

To sum up, we have

$$\Pr\left[\mathsf{IC}_4\right] \le \frac{2\,|\mathcal{I}_4|^2}{2^{2n}}.$$

- 5. Fix $i, j \in [q]^{*2}$. Without loss of generality, let $i \leq j$. We restore X values and R values by the $\hat{\rho}^{-1}$. Then since there is no redundant query, $A_i \neq A_j$ or $M_i \neq M_j$. Let $A_i \neq A_j$. We can apply the similar argument when $M_i \neq M_j$. We can consider the following cases.
 - (a) If $a_i > a_j + 1$, then $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 2^{a_i+m_i-a_j} & 2^{a_i+m_i-a_j-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[a_j+1] \\ X_i[a_j+2] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

for some P' and Q' which are independent of $X_i[a_j + 1]$ and $X_i[a_j + 2]$. By the sampling process of $X_i[a_j+1]$ and $X_i[a_j+2]$, in this case $\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{22n}$. We can apply the similar argument when $a_j > a_i + 1$ and get the same result.

(b) Assume that $a_i = a_j + 1$ and $A_i[\beta] \neq A_j[\beta]$ for some $\beta \in [a_j]$. Then $(V_i, U_i) = (V_i, U_i)$ if and only if

$$\begin{pmatrix} 2^{m_i+a_i-\beta+1} & 2^{m_i+1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[\beta] \\ X_i[a_i] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

🖄 Springer

for some P' and Q' which are independent of $X_i[\beta]$ and $X_i[a_i]$. By Lemma 6, we can conclude

$$\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}.$$

(c) Assume that $a_i = a_j + 1$ and $A_i[: a_j] = A_j$. If $M_i[\beta] \neq M_j[\beta]$ or there exists $\beta \in [m_i]$, we can use the randomness of $X_i[a_i + \beta]$ and $X_i[a_i]$. More precisely, $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\binom{2^{m_i-\beta+1} \ 2^{m_i+1}}{1 \ 1} \binom{X_i[a_i+\beta]}{X_i[a_i]} = \binom{P'}{Q'}$$

for some P' and Q' which are independent of $X_i[a_i + \beta]$ and $X_i[a_i]$. If $M_i = M_j$, we have two cases, $X_i[a_i] = 0$ or $X_i[a_i] \neq 0$. $X_i[a_i] \neq 0$ implies $V_i \neq V_j$ (see (5).). Also, if $X_i[a_i] = 0$, then $U_i = U_j$ if and only if

$$\bigoplus_{\beta=1}^{m_i} 2^{m+1-\beta} (X_i[a_i+\beta] \oplus M_{i,R}[\beta]) \oplus 2^{m+1} A_{i,R}[a_i] = 0.$$

Therefore, $(V_i, U_i) = (V_i, U_i)$ if and only if

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X_i[a_i] \\ X_i[a_i + m_i] \end{pmatrix} = \begin{pmatrix} 0 \\ Q' \end{pmatrix},$$

where

$$Q' = \bigoplus_{\beta=1}^{m_i-1} 2^{m+1-\beta} (X_i[a_i + \beta] \oplus M_{i,R}[\beta]) \oplus M_{i,R}[m_i] \oplus 2^{m+1} A_{i,R}[a_i],$$

(see (4)) Therefore, by the sampling process of $X_i[a_i]$ and Lemma 6,

$$\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}.$$

We can apply the similar argument when $a_i = a_i + 1$ and $A_i[:a_i] = A_i$.

(d) Assume that $a_i = a_j$. If there exist $\alpha, \beta \in [a_i]$ such that $A_i[\alpha] \neq A_j[\alpha]$ and $A_i[\beta] \neq A_j[\beta], (V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 2^{a_i+m_i-\alpha+1} & 2^{a_i+m_i-\beta+1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[\alpha] \\ X_i[\beta] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

for some P' and Q' which are independent of $X_i[\alpha]$ and $X_i[\beta]$. Then by Lemma 6, $\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}$. If there exists only one $\alpha \in [a_i]$ such that $A_i[\alpha] \ne A_j[\alpha]$, then $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\binom{2^{a_i+m_i-\alpha+1} \ 2^{a_j+m_j-\alpha+1}}{1} \binom{X_i[\alpha]}{X_j[\alpha]} = \binom{P'}{Q'},$$

for some P' and Q' which are independent of $X_i[\alpha]$ and $X_j[\alpha]$. Therefore,

$$\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - 1)} \le \frac{4}{2^{2n}}.$$

By the above analysis, we have

$$\Pr\left[\mathsf{IC}_5\right] \le \frac{4q^2}{2^{2n}}.$$

All in all, we have

$$\Pr\left[\mathsf{IC}\right] \le \frac{4q^2 + 6\sigma^2}{2^{2n}}.$$

Proof of Lemma 5 We calculate each probability of OC_i for $1 \le i \le 5$.

1. Let $((i, \alpha), (j, \alpha)) \in \mathcal{I}_1^{*2}$. Then one should have $A_i[\alpha] \neq A_j[\alpha]$ and $g_1(i, \alpha) \neq g_2(\alpha)$. Therefore, we have

$$\Pr[OC_1] = 0.$$

2. Let $((i, \alpha), (j, \alpha)) \in \mathcal{I}_2^{*2}$. Then $M_i[\alpha] \neq M_j[\alpha]$ so $g_2(i, \alpha) \neq g_2(j, \alpha)$. Therefore, we have

$$\Pr[OC_2] = 0.$$

3. Since $IC_4 = OC_3$,

$$\Pr\left[\mathsf{OC}_3\right] \le \frac{2\,|\mathcal{I}_4|^2}{2^{2n}}.$$

4. Let $((i, \alpha), (j, \alpha)) \in \mathcal{I}_4^{*2}$. Then $C_i[\alpha] \neq C_j[\alpha]$ so $g_4(i, \alpha) \neq g_4(j, \alpha)$. Therefore, we have

$$\Pr[OC_4] = 0.$$

- 5. Let $(i, j) \in [q_e]^{*2}$. We distinguish two sub-cases.
 - (a) First, assume $m_i \neq m_j$. Without loss of generality, we can assume that $m_i < m_j$. In this case, $(V_i, T_i) = (V_j, T_j)$ if and only if

$$\begin{cases} X_j[a_j + m_j] = V_i \oplus \bigoplus_{\alpha=1}^{a_j + m_j - 1} X_j[\alpha]; \\ T_j = T_i. \end{cases}$$

Since $X_j[a_j + m_j]$ is chosen uniformly at random from the set of size at least $2^n - q_e$ and T_j is chosen uniformly at random from $\{0, 1\}^n$, one has

$$\Pr\left[(V_i, T_i) = (V_j, T_j)\right] \le \frac{1}{2^n (2^n - q_e)} \le \frac{2}{2^{2n}}$$

(b) Now assume that $m_i = m_j$. Since there is no redundant query, there exists at least one index *h* such that $M_i[h] \neq M_j[h]$. In this case, $(V_i, T_i) = (V_j, T_j)$ if and only if

$$\begin{cases} X_j[a_j+h] = V_i \oplus \bigoplus_{\alpha \neq a_j+h} X_j[\alpha]; \\ T_j = T_i. \end{cases}$$

Since $X_j[a_j + h]$ is chosen uniformly at random from the set of size at least $2^n - q_e$ and T_j is chosen uniformly at random from $\{0, 1\}^n$, one has

$$\Pr\left[(V_i, T_i) = (V_j, T_j)\right] \le \frac{1}{2^n (2^n - q_e)} \le \frac{2}{2^{2n}}.$$

🖄 Springer

To sum up, we have

$$\Pr\left[\mathsf{OC}_{5}\right] \leq \sum_{(i,j)\in[q_{e}]^{*2}} \frac{2}{2^{2n}} \leq \frac{2q_{e}^{2}}{2^{2n}}.$$

Now using $|\mathcal{I}_1| + |\mathcal{I}_2| \le \sigma$, $|\mathcal{I}_1| + |\mathcal{I}_3| \le \sigma$, and $|\mathcal{I}_i| \le \sigma$ for $1 \le i \le 4$, we conclude the lemma.

5 Security of ZLR

Theorem 2 Let \widetilde{E} : $\mathcal{K} \times \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a tweakable block cipher and ρ be a state update function given in Sect. 3.3. Then for nonnegative integers q_e , q_d , σ , l, and t such that q_e , $\sigma < 2^{n-1}$, we have

$$\mathsf{Adv}^{\mathsf{oae}}_{\mathsf{ZLR}[\tilde{E},\rho]}(q_e, q_d, \sigma, l, t) \leq \frac{6\sigma + 2q + 2q_d}{2^n} + \frac{\sigma l + 48\sigma^2 + 18q\sigma + 6q^2}{2^{2n}} + \mathsf{Adv}^{\mathsf{tprp}}_{\tilde{E}}(3\sigma + q, t + t'),$$

where $q = q_e + q_d$ and t' is the time complexity necessary to compute \tilde{E} for $3\sigma + q$ queries.

5.1 Proof setup

The proof of Theorem 2 is similar to the proof of DS-ZLR mode. Fix a (q_e, q_d, σ, l, t) adversary \mathcal{A} against ZLR $[\tilde{E}, \rho]$. Up to the TPRP security of \tilde{E}, \tilde{E} can be replaced by random tweakable permutation $\tilde{\pi}$ with the cost of

$$\operatorname{Adv}_{\tilde{E}}^{\operatorname{tprp}}(3\sigma + q, t + t'),$$

where t' is the time complexity necessary to compute \widetilde{E} for $3\sigma + q$ queries.

Let \$ denote the online random function defined as in Sect. 2.2. \mathcal{A} has to distinguish (ZLR.Enc, ZLR.Dec) and (\$, Rej) using q_e encryption queries and q_d decryption queries. In the real world, \mathcal{A} interacts with ZLR = (ZLR.Enc, ZLR.Dec). In the ideal world, \mathcal{A} interacts with (\$, Rej).

In the *i*-th encryption query, A queries with the associated data A_i and the message M_i , and get the ciphertext C_i and the tag T_i . In the *j*-th decryption query, A queries with the associated data A'_i , the ciphertext C'_i , and the tag T'_i and get $b'_i = M'_i$ or \bot . Then let

$$\tau_e = (A_i, M_i, C_i, T_i)_{i \in [q_e]} \tau_d = (A'_i, C'_i, T'_j, b'_j)_{j \in [q_d]},$$

denote the list of the encryption queries and the decryption queries, respectively. Let $q = q_e + q_d$ and we can rearrange the queries and their answers as

$$\{(A_i, M_i, C_i, T_i)_{i \in [q_e]}, (A_j, C_j, T_j, b_j)_{j \in [q_e+1,q]}\}.$$

Now for $i \in [q]$, set:

$$(A_i[1], \dots, A_i[a_i]) \xleftarrow{2n} A_i;$$
$$(C_i[1], \dots, C_i[m_i]) \xleftarrow{2n} C_i.$$

Similarly, for $i \in [q_e]$, set:

$$(M_i[1],\ldots,M_i[m_i]) \stackrel{2n}{\longleftarrow} M_i.$$

Let $l_i = a_i + m_i$ for $i \in [q]$, then $\sigma = \sum_{i \in [q]} l_i$ and $l = \max\{l_i : i \in [q]\}$.

To make the proof simple, we reveal the actual tuple of the masks $(\Delta_i)_{i \in [4]}$ to \mathcal{A} at the end of the interaction in the real world, or dummy tuple of masks $(\Delta_i)_{i \in [4]}$ that is chosen randomly from $(\{0, 1\}^n)^{*4}$ in the ideal world. With this information, \mathcal{A} can compute $\Delta_5 = \Delta_1 \oplus \Delta_3$ and $\Delta_6 = \Delta_2 \oplus \Delta_4$. We define some useful index sets that

$$\mathcal{P}_A = \{(i, \alpha) : i \in [q], \alpha \in [a_i]\};$$

$$\mathcal{P}_M = \{(i, \alpha) : i \in [q_e], \alpha \in [m_i]\};$$

$$\mathcal{P}_C = \{(i, \alpha) : i \in [q], \alpha \in [m_i]\},$$

which denote the set of the indices of the associated data, the message, and the ciphertext, respectively. For each $(i, \alpha) \in \mathcal{P}_A$, set

$$(A_{i,L}[\alpha], A_{i,R}[\alpha]) \xleftarrow{n} A_i[\alpha].$$

For each $(i, \alpha) \in \mathcal{P}_M$, set

$$(M_{i,L}[\alpha], M_{i,R}[\alpha]) \xleftarrow{n} M_i[\alpha].$$

Also, for each $(i, \alpha) \in \mathcal{P}_C$, set

$$(C_{i,L}[\alpha], C_{i,R}[\alpha]) \xleftarrow{n} C_i[\alpha].$$

For each $(i, \alpha) \in \mathcal{P}_A$, let

$$\hat{A}_{i,L}[\alpha] = A_{i,L}[\alpha] \oplus 2^{\alpha-1}\Delta_1, \qquad \qquad \hat{A}_{i,R}[\alpha] = A_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_2.$$

For each $(i, \alpha) \in \mathcal{P}_M$, let

$$\hat{M}_{i,L}[\alpha] = M_{i,L}[\alpha] \oplus 2^{\alpha-1} \Delta_3, \qquad \qquad \hat{M}_{i,R}[\alpha] = M_{i,R}[\alpha] \oplus 2^{\alpha-1} \Delta_4.$$

Also, for each $(i, \alpha) \in \mathcal{P}_C$, let

$$\hat{C}_{i,L}[\alpha] = C_{i,L}[\alpha] \oplus 2^{\alpha-1}\Delta_5, \qquad \qquad \hat{C}_{i,R}[\alpha] = C_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_6.$$

With these values, we reveal the actual internal states $X_i[\alpha]$, $Y_i[\alpha]$, and $Z_i[\alpha]$ variables in the real world. We set for the encryption queries:

- for $(i, \alpha) \in \mathcal{P}_A, X_i[\alpha] = \tilde{\pi}(\mathsf{Pad}_t(0 \parallel \alpha \parallel \hat{A}_{i,R}[\alpha]), \hat{A}_{i,L}[\alpha]);$
- for $(i, \alpha) \in \mathcal{P}_M$, $X_i[a_i + \alpha] = \tilde{\pi}(\mathsf{Pad}_t(1 \parallel \alpha \parallel \hat{M}_{i,R}[\alpha]), \hat{M}_{i,L}[\alpha]);$
- for $(i, \alpha) \in \mathcal{P}_C$, $Y_i[\alpha] = \tilde{\pi}^{-1}(\mathsf{Pad}_t(3 \parallel \alpha \parallel \hat{C}_{i,R}[\alpha]), \hat{C}_{i,L}[\alpha]);$
- for $(i, \alpha) \in \mathcal{P}_C$, $Z_i[\alpha] = \tilde{\pi}^{-1}(\mathsf{Pad}_t(2 \parallel \alpha \parallel \hat{Y}_i[\alpha]), \hat{C}_{i,R}[\alpha]).$

On the other hand, in the ideal world, for $i \in [q_e]$ and $\alpha \in [l_i]$, $X_i[\alpha]$ is chosen to satisfy following rules. For $i \in [q_e]$,

- if $\alpha \in [a_i]$ and there exists j < i such that $A_i[\alpha] = A_i[\alpha]$, set $X_i[\alpha] = X_i[\alpha]$;
- if $\alpha \in [m_i]$ and there exists j < i such that $M_i[\alpha] = M_j[\alpha]$, set $X_i[a_i + \alpha] = X_j[a_j + \alpha]$;
- if $\alpha \in [a_i]$, sample $X_i[\alpha] \leftarrow \{0, 1\}^n$ different from $X_j[\alpha]$ for all $j \in [q_e]$ satisfying $a_i \ge \alpha, A_i[\alpha] \ne A_j[\alpha]$, and $A_{i,R}[\alpha] = A_{j,R}[\alpha]$;
- if $\alpha \in [m_i]$, sample $X_i[a_i + \alpha] \leftarrow \{0, 1\}^n$ different from $X_j[a_j + \alpha]$ for all $j \in [q_e]$ satisfying $a_j < \alpha$, $M_i[\alpha] \neq M_j[\alpha]$, and $M_{i,R}[\alpha] = M_{j,R}[\alpha]$;

• otherwise, sample $X_i[\alpha] \leftarrow_{\$} \{0, 1\}^n$ uniformly at random.

Now $Y_i[\alpha]$ and $Z_i[\alpha]$ for $i \in [q_e]$ and $\alpha \in [m_i]$ can be given by (2) and (3), and those would be revealed. For $i \in [q_e + 1, q]$ and $\alpha \in [m_i]$, $Y_i[\alpha]$ and $Z_i[\alpha]$ are chosen satisfying following rules:

- if there exists j < i such that $C_i[\alpha] = C_i[\alpha]$, set $Y_i[\alpha] = Y_i[\alpha]$ and set $Z_i[\alpha] = Z_i[\alpha]$;
- if there exists j < i such that $C_i[\alpha] \neq C_i[\alpha]$ and $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, sample $Y_i[\alpha] \leftarrow_{\$}$ $\{0, 1\}^n$ different from $Y_k[\alpha]$;
- otherwise, sample $Y_i[\alpha] \leftarrow_{\$} \{0, 1\}^n$ and $Z_i[\alpha] \leftarrow_{\$} \{0, 1\}^n$ uniformly at random.

Finally, A attains the following transcript:

$$\tau = \left\{ (A_i, M_i, X_i, Y_i, Z_i, C_i, T_i)_{i \in [q_e]}, (A_i, X_i, Y_i, Z_i, C_i, T_i, b_i)_{i \in [q_e+1,q]} \right\} \\ \cup \left\{ (\Delta_{i,j})_{i \in [q], j \in [4]} \right\}.$$

5.2 Defining bad events

In this section, we define bad events. For $i \in [q]$, let U_i and V_i be the final state $S_i[l_i]$, which is defined in (4) and (5). To describe the bad cases, we will define some functions which take the indices as input. Let

- $\mathcal{I}_1 = \{(i, \alpha) \in \mathcal{P}_A : \forall j < i, A_i[\alpha] \neq A_j[\alpha]\};$ $\mathcal{I}_2 = \{(i, \alpha) \in \mathcal{P}_M : \forall j < i, M_i[\alpha] \neq M_j[\alpha]\};$ $\mathcal{I}_3 = \mathcal{I}_4 = \{(i, \alpha) \in \mathcal{P}_C : \forall j < i, C_i[\alpha] \neq C_j[\alpha]\},$

and for $r \in [4]$, let $f_r, g_r : \mathcal{I}_r \to (\{0, 1\}^n)^2$ be functions where

$f_1(i,\alpha) = (\hat{A}_{i,R}[\alpha], \hat{A}_{i,L}[\alpha]),$	$g_1(i,\alpha) = (\hat{A}_{i,R}[\alpha], X_i[\alpha]),$
$f_2(i,\alpha) = (\hat{M}_{i,R}[\alpha], \hat{M}_{i,L}[\alpha]),$	$g_2(i,\alpha) = (\hat{M}_{i,R}[\alpha], X_i[a_i + \alpha]),$
$f_3(i, \alpha) = (Y_i[\alpha], Z_i[\alpha]),$	$g_3(i,\alpha) = (Y_i[\alpha], \hat{C}_{i,R}[\alpha]),$
$f_4(i,\alpha) = (\hat{C}_{i,R}[\alpha], Y_i[\alpha]),$	$g_4(i,\alpha) = (\hat{C}_{i,R}[\alpha], \hat{C}_{i,L}[\alpha]).$

Note that f_r gives the pair of the tweak and the input of each tweakable block cipher call, and g_r gives the pair of the tweak and the output of each tweakable block cipher call. For $1 \le r \le s \le 4$ we define the following events.

- TwColl_r \Leftrightarrow there exists $(i, \alpha) \in \mathcal{I}_r$ and $v \in \{0, 1\}^n$ such that $f_r(i, \alpha) = (0, v)$;
- $\mathsf{IC}_{r,s} \Leftrightarrow$ there exists $(i, \alpha) \in \mathcal{I}_r$ and $(j, \beta) \in \mathcal{I}_s$ such that $(r, i, \alpha) \neq (s, j, \beta)$ and $f_r(i, \alpha) = f_s(j, \beta);$
- $OC_{r,s} \Leftrightarrow$ there exists $(i, \alpha) \in \mathcal{I}_r$ and $(j, \beta) \in \mathcal{I}_s$ such that $(r, i, \alpha) \neq (s, j, \beta)$ and $g_r(i, \alpha) = g_s(j, \beta).$

Also, For $r \in [4]$, let

- $\mathsf{IC}_{r,5} \Leftrightarrow$ there exists $i \in [q]$ and $(j, \beta) \in \mathcal{I}_r$ such that $(V_i, U_i) = f_r(j, \beta)$;
- $OC_{r,5} \Leftrightarrow$ there exists $i \in [q_e]$ and $(j, \beta) \in \mathcal{I}_r$ such that $(V_i, T_i) = g_r(j, \beta)$,

and let

- TwColl₅ \Leftrightarrow there exists $i \in [q]$ such that $V_i = 0$;
- $\mathsf{IC}_{5,5} \Leftrightarrow$ there exists different $i, j \in [q]$ such that $(V_i, U_i) = (V_i, U_i)$;
- $OC_{5,5} \Leftrightarrow$ there exists different $i, j \in [q_e]$ such that $(V_i, T_i) = (V_i, T_i)$.

A transcript τ is defined as *bad* if one of the following events occurs:

- 1. bad₁ \Leftrightarrow there exists $i, j \in [q_e]$ and $\alpha \in [\min\{m_i, m_j\}]$ such that $(A_i, M_i[: \alpha]) \neq (A_j, M_j[: \alpha])$ and $C_i[\alpha] = C_j[\alpha]$;
- 2. $\mathsf{bad}_2 \Leftrightarrow \bigvee_{1 < r < s < 5} (\mathsf{IC}_{r,s} \lor \mathsf{OC}_{r,s} \lor \mathsf{TwColl}_r).$

We denote Γ_{bad} as a set of all bad transcripts. We will now find the upper bound on the probability that each bad event will occur in the ideal world. Fix $i, j \in [q_e]$ and $\alpha \in [\min\{m_i, m_j\}]$ such that $(A_i, M_i[: \alpha]) \neq (A_j, M_j[: \alpha])$. Then, since $C_i[\alpha]$ and $C_j[\alpha]$ are chosen uniformly at random, one has

$$\Pr\left[\mathsf{bad}_{1}\right] \leq \frac{\sigma l}{2^{2n}}.\tag{12}$$

The conditional probability of bad_2 given that bad_1 has not happened is upper bounded as follows.

Lemma 7

$$\Pr\left[\mathsf{bad}_2 \land \neg \mathsf{bad}_1\right] \le \frac{48\sigma^2 + 18q\sigma + 6q^2}{2^{2n}} + \frac{6\sigma + 2q}{2^n}$$

The proof of this lemma is deferred to Sect. 5.4. We now consider good transcripts.

Lemma 8 For any $\tau \notin \Gamma_{\text{bad}}$,

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}}=\tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}}=\tau\right]} \ge 1 - \frac{2q_d}{2^n}.$$

The proof of this lemma is deferred to Sect. 5.3.

Finally, by Lemmas 7 and 8 and (12), we can conclude that Theorem 2 holds.

5.3 Analyzing good transcripts

Fix $\tau \notin \Gamma_{\text{bad}}$. For the proof, we define the following sets.

- $\mathcal{I}'_{3} = \{(i, \alpha) : i \in [q_{e} + q_{d}], \alpha \in [m_{i}], \forall j < i, (A_{i}, C_{i}[:\alpha]) \neq (A_{j}, C_{j}[:\alpha])\};\$
- $W_1[\alpha, v] = \{(i, \alpha) \in \mathcal{I}_1 : A_{i,R}[\alpha] = v \oplus 2^{\alpha-1}\Delta_2\};$
- $W_2[\alpha, v] = \{(i, \alpha) \in \mathcal{I}_2 : M_{i,R}[\alpha] = v \oplus 2^{\alpha-1} \Delta_4\};$
- $W_3[\alpha, v] = \{(i, \alpha) \in \mathcal{I}'_3 : C_{i,R}[\alpha] = v \oplus 2^{\alpha 1} \Delta_6\};$
- $W_4[\alpha, v] = \{(i, \alpha) \in \mathcal{I}_3^{\bar{i}} : Y_i[\alpha] = v\},\$

and following notations,

- $u_j[\alpha, v] = |W_j[\alpha, v]|$ for $j \in [4]$;
- $u_5[\alpha] = \left| \left\{ (i, \alpha) \in \mathcal{I}'_3 : \forall j < i, C_i[\alpha] \neq C_j[\alpha] \right\} \right|;$
- $u_6^e[v] = |\{i \in [q_e] : V_i = v\}|;$
- $u_6^d[v] = |\{i \in [q_e + 1, q_e + q_d] : V_i = v\}|.$

For $j \in [4]$, let

$$W_j^e[\alpha, v] = \left\{ (i, \alpha) \in W_j[\alpha, v] : i \in [q_e] \right\},\$$

and

$$W_{j}^{d}[\alpha, v] = W_{j}[\alpha, v] \setminus W_{j}^{e}[\alpha, v]$$

We also denote $u_j^e[\alpha, v] = \left| W_j^e[\alpha, v] \right|$ and $u_j^d[\alpha, v] = \left| W_j^d[\alpha, v] \right|$, so we have $u_j[\alpha, v] = u_j^e[\alpha, v] + u_j^d[\alpha, v]$.

First, we consider the ideal world. The probability that ciphertext C_1, \ldots, C_{q_e} is given is $\frac{1}{2^{2n|B|}}$ where $\mathcal{B} = \{(A_i, M_i[:\alpha]) : 1 \le i \le q_e, \alpha \in [m_i]\}$, and one that tags T_1, \ldots, T_{q_e} are given is $\frac{1}{2^{nq_e}}$. Let **X**, **Y**, **Z** be the distribution of $(X_1, \ldots, X_{q_e+q_d}), (Y_{q_e+1}, \ldots, Y_{q_e+q_d})$, and $(Z_{q_e+1}, \ldots, Z_{q_e+q_d})$, respectively. First, $X_i[\alpha]$ and $X_j[\alpha]$ are given differently if $A_{i,R}[\alpha] = A_{j,R}[\alpha]$ or $M_{i,R}[\alpha] = M_{j,R}[\alpha]$. Therefore, for each $v \in \{0, 1\}^n$ and $\alpha \in [a_i]$, the probability that $X_i[\alpha]$'s for $A_{i,R}[\alpha] = v$ are given according to associated data is $\frac{1}{(2^n)_{u_1[\alpha,v_1]}}$, where $v_1 = v \oplus 2^{\alpha-1}\Delta_2$. Similarly, for each $v \in \{0, 1\}^n$ and $\alpha \in [m_i]$, one that corresponding $X_i[\alpha]$'s for $M_{i,R}[\alpha] = v$ are given according to message is $\frac{1}{(2^n)_{u_2[\alpha,v_2]}}$, where $v_2 = v \oplus 2^{\alpha-1}\Delta_4$. Hence,

$$\Pr\left[\mathbf{X} = (X_1, \dots, X_{q_e+q_d})\right] = \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_1[\alpha, v_1]}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_2[\alpha, v_2]}}$$
$$= \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_1[\alpha, v]}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_2[\alpha, v]}}.$$

Also, $Y_i[\alpha]$ and $Y_j[\alpha]$ are given differently if $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, while $\{Y_i\}_{1 \le i \le q_e}$ is determined from $(X_1, \ldots, X_{q_e+q_d})$. Therefore, for each $v \in \{0, 1\}^n$ and $\alpha \in [l]$, the probability that corresponding $Y_i[\alpha]$'s are given is $\frac{1}{(2^n - u_3^e[\alpha, v_3])_{u_3^d[\alpha, v_3]}}$, where $v_3 = v \oplus 2^{\alpha-1}\Delta_6$. Hence similarly from the case above,

$$\Pr\left[\mathbf{Y} = (Y_{q_e+1}, \dots, Y_{q_e+q_d}) | \mathbf{X}\right] = \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n - u_3^e[\alpha, v])_{u_3^d[\alpha, v]}}.$$

Now, since $Z_i[\alpha]$'s are given uniformly at random in decryption queries,

$$\Pr\left[\mathbf{Z} = (Z_{q_e+1}, \dots, Z_{q_e+q_d})\right] = \prod_{1 \le \alpha \le l} \frac{1}{(2^n)^{u_5[\alpha]}}$$

Hence, we can conclude the following probability.

$$\Pr\left[\mathsf{T}_{\mathsf{id}} = \tau\right] = \frac{1}{2^{2n|\mathcal{B}|}} \times \frac{1}{2^{nq_e}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_1[\alpha,v]}} \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n)_{u_2[\alpha,v]}} \\ \times \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \frac{1}{(2^n - u_3^e[\alpha,v])_{u_3^d[\alpha,v]}} \\ \times \left(\prod_{1 \le \alpha \le l} \frac{1}{(2^n)^{u_5[\alpha]}}\right) \times \frac{1}{(2^n)_4}.$$
(13)

Note that $\frac{1}{(2^n)_4}$ is the probability that $\Delta_1, \Delta_2, \Delta_3$ and Δ_4 are given.

Springer

Now, we consider the real world. First, in decryption queries, the probability of attaining \perp for every answer is bounded below by

$$\prod_{v \in \{0,1\}^n} \left(1 - \frac{1}{2^n - u_6^e[v]} \right)^{u_6^a[v]} \ge \left(1 - \frac{1}{2^n - q_e} \right)^{q_d} \ge 1 - \frac{q_d}{2^n - q_e}.$$

If we fix $v \in \{0, 1\}^n$, $\tilde{\pi}$ takes v as a tweak if and only if one of the following conditions holds.

- 1. $A_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_2 = v;$ 2. $M_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_4 = v;$ 3. $Y_i[\alpha] = v;$
- 4. $C_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_6 = v;$
- 5. $V_i = v$.

Since the case bad_2 does not exist in any good transcript, the number of tweakable block ciphers in all queries that has v as tweak is

$$\sum_{1 \le \alpha \le l} (u_1[\alpha, v] + u_2[\alpha, v] + u_3[\alpha, v] + u_4[\alpha, v]) + u_6^e[v].$$

Since $\frac{1}{(2^n)_{a+b}} \ge \frac{1}{(2^n)_a(2^n)_b}$ for $a, b \ge 0$, we have

$$\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right] \ge \prod_{\substack{1 \le \alpha \le l \\ v \in \{0,1\}^n}} \frac{1}{(2^n)_{u_1[\alpha,v]}(2^n)_{u_2[\alpha,v]}(2^n)_{u_3[\alpha,v]}(2^n)_{u_4[\alpha,v]}} \\ \times \prod_{v \in \{0,1\}^n} \frac{1}{(2^n)_{u_6^e[v]}} \times \frac{1}{(2^n)_4}.$$
(14)

Note that $\frac{1}{(2^n)_4}$ is the probability that Δ_1 , Δ_2 , Δ_3 and Δ_4 are given. Since $\sum_{v \in \{0,1\}^n} u_6^e[v] = q_e$, we have

$$\prod_{v \in \{0,1\}^n} \frac{1}{(2^n)_{u_6^e[v]}} \ge \prod_{v \in \{0,1\}^n} \frac{1}{(2^n)^{u_6^e[v]}} = \frac{1}{(2^n)^{q_e}}.$$
(15)

Also,

$$\prod_{1 \le \alpha \le l} (2^n)^{u_5[\alpha]} \ge \prod_{1 \le \alpha \le l} (2^n)_{u_5[\alpha]} \ge \prod_{1 \le \alpha \le l} (2^n)_{u_4^d[\alpha]}.$$
(16)

Therefore by (13), (14), (15) and (16),

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} \ge \frac{2^{2n|\mathcal{B}|}}{\prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} \left[2^{2n|\mathcal{B}|} \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)_{\substack{u_3^e[\alpha,v] \\ 1 \le \alpha \le l}} \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)_{\substack{u_4^e[\alpha,v] \\ 1 \le \alpha \le l}} \times \left(1 - \frac{q_d}{2^n - q_e} \right) \\ \ge 1 - \frac{q_d}{2^n - q_e} \ge 1 - \frac{2q_d}{2^n}.$$

The last inequality follows since

$$|\mathcal{B}| \ge \sum_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} u_3^e[\alpha, v],$$

🖄 Springer

and hence,

$$2^{n|\mathcal{B}|} \ge \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)^{u_3^e[\alpha,v]} \ge \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)_{u_3^e[\alpha,v]},$$

and similarly,

$$2^{n|\mathcal{B}|} \ge \prod_{\substack{v \in \{0,1\}^n \\ 1 \le \alpha \le l}} (2^n)_{u_4^e[\alpha,v]},$$

which completes the proof.

5.4 Bounding the probability of bad events

Let

$$\mathsf{TwColl} = \bigvee_{i=1}^{5} \mathsf{TwColl}_{i},$$
$$\mathsf{IC} = \bigvee_{1 \le i \le j \le 5} \mathsf{IC}_{i,j},$$
$$\mathsf{OC} = \bigvee_{1 \le i \le j \le 5} \mathsf{OC}_{i,j}.$$

Note that $bad_2 = TwColl \lor IC \lor OC$. We calculate the probability of the each collision event in the following lemmas. The result of main theorem is derived directly.

Lemma 9

$$\Pr\left[\mathsf{TwColl}\right] \le \frac{6\sigma + 2q}{2^n}.$$

Proof We calculate each probability of TwColl_i for i = 1 to 5.

1. Fix $(i, \alpha) \in \mathcal{I}_1$ and $v \in \{0, 1\}^n$. Then $f_1(i, \alpha) = (0, v)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_1 = A_{i,L}[\alpha];\\ 2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus v, \end{cases}$$

and since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = (0,v)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

Therefore, we get

$$\Pr\left[\mathsf{TwColl}_{1}\right] \leq \sum_{v \in \{0,1\}^{n}} \frac{2|\mathcal{I}_{1}|}{2^{2n}} \leq \frac{2|\mathcal{I}_{1}|}{2^{n}}.$$

2. Fix $(i, \alpha) \in \mathcal{I}_2$ and $v \in \{0, 1\}^n$. Then $f_2(i, \alpha) = (0, v)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_3 = M_{i,L}[\alpha];\\ 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus v, \end{cases}$$

and since (Δ_3, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_2(i,\alpha) = (0,v)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

Therefore, we get

$$\Pr\left[\mathsf{TwColl}_2\right] \le \sum_{v \in \{0,1\}^n} \frac{2|\mathcal{I}_2|}{2^{2n}} \le \frac{2|\mathcal{I}_2|}{2^n}$$

3. Fix $(i, \alpha) \in \mathcal{I}_3$ and $v \in \{0, 1\}^n$. If $i \in [q_e]$, then $f_3(i, \alpha) = (0, v)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus \bigoplus_{\beta=1}^{a_i+\alpha} X_i[\beta], \\ X_i[\alpha+a_i] \oplus \bigoplus_{\beta=1}^{\alpha-1} 2^{\alpha-1}\Delta_4 = Q \oplus v, \end{cases}$$

where

$$Q = \bigoplus_{\beta=1}^{a_i} 2^{a_i + \alpha - \beta} \left(X[\beta] \oplus A_{i,R}[\beta] \oplus 2^{\beta - 1} \Delta_2 \right)$$
$$\oplus \bigoplus_{\beta=1}^{\alpha - 1} 2^{\alpha - \beta} \left(X[a_i + \beta] \oplus M_{i,R}[\beta] \right).$$

Since Δ_4 is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[\alpha + a_i]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_3(i,\alpha) = (0,v)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

Now assume that $i \notin [q_e]$. Then $f_3(i, \alpha) = (0, v)$ if and only if

$$\begin{cases} Y_i[\alpha] = 0; \\ Z_i[\alpha] = v, \end{cases}$$

and since $Z_i[\alpha]$ is chosen uniformly at random from $\{0, 1\}^n$ and $Y_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_3(i,\alpha) = (0,v)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}$$

By the above reasoning, we have

$$\Pr\left[\mathsf{TwColl}_3\right] \le \sum_{v \in \{0,1\}^n} \frac{2|\mathcal{I}_3|}{2^{2n}} \le \frac{2|\mathcal{I}_3|}{2^n}$$

4. Fix $(i, \alpha) \in \mathcal{I}_4$ and $v \in \{0, 1\}^n$. If $i \in [q_e]$, then $f_4(i, \alpha) = (0, v)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 \oplus 2^{\alpha-1}\Delta_4 = C_{i,R}[\alpha];\\ 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus v \oplus \bigoplus_{\beta=1}^{a_i+\alpha} X_i[\beta] \end{cases}$$

and since (Δ_2, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_4(i,\alpha) = (0,v)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

If $i \notin [q_e]$, then $f_4(i, \alpha) = (0, v)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 = C_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_4; \\ Y_i[\alpha] = v. \end{cases}$$

Since Δ_2 is chosen uniformly at random from $\{0, 1\}^n$ and $Y_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_4(i,\alpha) = (0,v)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

Therefore, we get

$$\Pr\left[\mathsf{TwColl}_4\right] \le \sum_{v \in \{0,1\}^n} \frac{2|\mathcal{I}_4|}{2^{2n}} \le \frac{2|\mathcal{I}_4|}{2^n}.$$

- 5. Fix $i \in [q]$. We distinguish two subcases.
 - (a) Assume that $i \in [q_e]$. Then $V_i = 0$ if and only if

$$X_i[1] = \sum_{\alpha=2}^{a_i+m_i} X_i[\alpha].$$

Since $X_i[1]$ is sampled from the set of size at least $2^n - q_e$, one has

$$\Pr[V_i = 0] \le \frac{1}{2^n - q_e} \le \frac{2}{2^n}.$$

(b) Assume that $i \notin [q_e]$. Then the equation $V_i = 0$ is equivalent to the system of equations

$$Y_i[1] = \bigoplus_{\alpha=1}^{a_i} X_i[\alpha] \oplus \bigoplus_{\alpha=2}^{m_i} (Y_i[\alpha] \oplus Z_i[\alpha]) \oplus Z_i[1].$$

Since $Y_i[1]$ is sampled from the set of size at least $2^n - q$, one has

$$\Pr[V_i = 0] \le \frac{1}{2^n - q} \le \frac{2}{2^n}.$$

By the above reasoning,

$$\Pr\left[\mathsf{TwColl}_{5}\right] \leq \sum_{i \in [q]} \frac{2}{2^{n}} \leq \frac{2q}{2^{n}}$$

Now using $|\mathcal{I}_1| + |\mathcal{I}_2| \le \sigma$, $|\mathcal{I}_1| + |\mathcal{I}_3| \le \sigma$, and $|\mathcal{I}_i| \le \sigma$ for $1 \le i \le 4$, we conclude the lemma.

Lemma 10

$$\Pr\left[\mathsf{IC}\right] \le \frac{4q^2 + 12q\sigma + 20\sigma^2}{2^{2n}}$$

Proof We calculate each probability of $IC_{i,j}$ for $1 \le i \le j \le 5$.

1. Fix $((i, \alpha), (j, \beta)) \in (\mathcal{I}_1)^{*2}$. If $\alpha = \beta$, one should have $A_i[\alpha] \neq A_j[\beta]$ and $f_1(i, \alpha) \neq f_1(j, \beta)$. Suppose $\alpha \neq \beta$. Then, $f_1(i, \alpha) = f_1(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_1 = A_{i,L}[\alpha] \oplus A_{j,L}[\beta];\\ (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2 = A_{i,R}[\alpha] \oplus A_{j,R}[\beta], \end{cases}$$

and since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = f_1(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}$$

Therefore, we get

$$\Pr\left[\mathsf{IC}_{1,1}\right] \le \frac{2|\mathcal{I}_1|^2}{2^{2n}}.$$

2. Fix $(i, \alpha) \in \mathcal{I}_1$ and $(j, \beta) \in \mathcal{I}_2$. Then the equation $f_1(i, \alpha) = f_2(j, \beta)$ is equivalent to the system of equations

$$2^{\alpha-1}\Delta_1 = A_{i,L}[\alpha] \oplus M_{j,L}[\beta] \oplus 2^{\beta-1}\Delta_3;$$

$$2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus 2^{\beta-1}\Delta_4.$$

Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

Pr
$$[f_1(i, \alpha) = f_2(j, \beta)] \le \frac{1}{2^n (2^n - 1)} \le \frac{2}{2^{2n}}.$$

Therefore,

$$\Pr\left[\mathsf{IC}_{1,2}\right] \le \sum_{(i,\alpha)\in\mathcal{I}_1}\sum_{(j,\beta)\in\mathcal{I}_2}\frac{2}{2^{2n}} \le \frac{2\,|\mathcal{I}_1|\,|\mathcal{I}_2|}{2^{2n}}.$$

- 3. Fix $(i, \alpha) \in \mathcal{I}_1$ and $(j, \beta) \in \mathcal{I}_3$. We distinguish two subcases.
 - (a) If $j \in [q_e]$, then the equation $f_1(i, \alpha) = f_3(j, \beta)$ is equivalent to the system of equations

$$\begin{cases} 2^{\alpha-1}\Delta_1 \oplus \bigoplus_{\gamma=1}^{\beta-1} 2^{\beta-1}\Delta_4 = A_{i,L}[\alpha] \oplus Q; \\ 2^{\beta-1}\Delta_4 = 2^{\alpha-1}\Delta_2 \oplus A_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j[\gamma], \end{cases}$$

where

$$Q = X[a_j + \beta] \oplus \bigoplus_{\gamma=1}^{a_j} 2^{a_j + \beta - \gamma} \left(X_j[\gamma] \oplus A_{j,R}[\gamma] \oplus 2^{\gamma - 1} \Delta_2 \right)$$
$$\oplus \bigoplus_{\gamma=1}^{\beta - 1} 2^{\beta - \gamma} \left(X_j[a_j + \gamma] \oplus M_{j,R}[\gamma] \right).$$

Since (Δ_1, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}$$

(b) Assume j ∉ [q_e]. If C_j[β] = C_{j'}[β] for j' ∈ [q_e], this case is same as the case that j ∈ [q_e]. Otherwise, the equation f₁(i, α) = f₃(j, β) is equivalent to the system of equations

$$2^{\alpha-1}\Delta_1 = A_{i,L}[\alpha] \oplus Z_j[\beta];$$

$$2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus Y_j[\beta].$$

Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{2^n(2^n - 1)} \le \frac{2}{2^{2n}}$$

By the above reasoning,

$$\Pr\left[\mathsf{IC}_{1,3}\right] \leq \sum_{(i,\alpha)\in\mathcal{I}_1}\sum_{(j,\beta)\in\mathcal{I}_3}\frac{2}{2^{2n}} \leq \frac{2\,|\mathcal{I}_1|\,|\mathcal{I}_3|}{2^{2n}}.$$

- 4. Fix $(i, \alpha) \in \mathcal{I}_1$ and $(j, \beta) \in \mathcal{I}_4$. We distinguish two subcases.
 - (a) Assume that $j \in [q_e]$. Then the equation $f_1(i, \alpha) = f_4(j, \beta)$ is equivalent to the system of equations

$$\begin{cases} 2^{\alpha-1}\Delta_1 \oplus 2^{\beta-1}\Delta_4 = A_{i,L}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j[\gamma];\\ 2^{\beta-1}\Delta_4 = A_{i,R}[\alpha] \oplus C_{j,R}[\beta] \oplus 2^{\alpha-1}\Delta_2 \oplus 2^{\beta-1}\Delta_2. \end{cases}$$

Since (Δ_1, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}$$

(b) Assume that $j \notin [q_e]$. Then the equation $f_1(i, \alpha) = f_4(j, \beta)$ is equivalent to the system of equations

$$\begin{cases} 2^{\alpha-1}\Delta_1 = A_{i,L}[\alpha] \oplus Y_j[\beta];\\ 2^{\beta-1}\Delta_4 = A_{i,R}[\alpha] \oplus C_{j,R}[\beta] \oplus 2^{\alpha-1}\Delta_2 \oplus 2^{\beta-1}\Delta_2. \end{cases}$$

Since (Δ_1, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

By the above reasoning,

$$\Pr\left[\mathsf{IC}_{1,4}\right] \le \sum_{(i,\alpha)\in\mathcal{I}_1}\sum_{(j,\beta)\in\mathcal{I}_4}\frac{2}{2^{2n}} \le \frac{2\,|\mathcal{I}_1|\,|\mathcal{I}_4|}{2^{2n}}.$$

- 5. Fix $(i, \alpha) \in \mathcal{I}_1$ and $j \in [q]$. We distinguish two subcases.
 - (a) Assume that $j \in [q_e]$. Then the equation $f_1(i, \alpha) = (V_j, U_j)$ is equivalent to the system of equations

$$\begin{cases} 2^{\alpha-1}\Delta_1 \oplus \left(\bigoplus_{\beta=1}^{a_j} 2^{a_j+m_j+1-\beta}\right) \Delta_2 = Q \oplus A_{i,L}[\alpha];\\ 2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus \bigoplus_{\beta=1}^{a_j+m_j} X_j[\beta], \end{cases}$$

$$Q = \bigoplus_{\beta=1}^{a_j} 2^{a_j + m_j + 1 - \beta} \left(X_j[\beta] \oplus A_{j,R}[\beta] \right)$$
$$\oplus \bigoplus_{\beta=1}^{m_j} 2^{m_j + 1 - \beta} \left(X_j[a_j + \beta] \oplus M_{j,R}[\beta] \oplus 2^{\beta - 1} \Delta_4 \right)$$

Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n(2^n - 1)} \le \frac{2}{2^{2n}}.$$

(b) Assume that $j \notin [q_e]$. Then the equation $f_1(i, \alpha) = (V_j, U_j)$ is equivalent to the system of equations

$$\begin{cases} 2^{\alpha-1}\Delta_1 = A_{i,L}[\alpha] \oplus U_j; \\ 2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus V_j. \end{cases}$$

Note that U_j and V_j are independent of Δ_1 and Δ_2 . Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_1(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - 1)} \le \frac{2}{2^{2n}}.$$

By the above reasoning, we have

$$\Pr\left[\mathsf{IC}_{1,5}\right] \le \sum_{(i,\alpha)\in\mathcal{I}_1}\sum_{j\in[q]}\frac{2}{2^{2n}} \le \frac{2q\,|\mathcal{I}_1|}{2^{2n}}$$

6. Fix $(i, \alpha) \in \mathcal{I}_2$ and $(j, \beta) \in \mathcal{I}_2$, where $(i, \alpha) \neq (j, \beta)$. If $\alpha = \beta$, then $M_i[\alpha] \neq M_j[\beta]$ so $f_2(i, \alpha) \neq f_2(j, \beta)$. Suppose $\alpha \neq \beta$. Then, $f_2(i, \alpha) = f_2(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_3 = M_{i,L}[\alpha] \oplus M_{j,L}[\beta];\\ (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 = M_{i,R}[\alpha] \oplus M_{j,R}[\beta], \end{cases}$$

where $2^{\alpha-1} \oplus 2^{\beta-1} \neq 0$. Since (Δ_3, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_2(i,\alpha) = f_2(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

Therefore, we get

$$\Pr\left[\mathsf{IC}_{2,2}\right] \leq \sum_{(i,\alpha)\in\mathcal{I}_2}\sum_{(j,\beta)\in\mathcal{I}_2}\frac{2}{2^{2n}} \leq \frac{2\,|\mathcal{I}_2|^2}{2^{2n}}.$$

- 7. Fix $(i, \alpha) \in \mathcal{I}_2$ and $(j, \beta) \in \mathcal{I}_3$. We distinguish two subcases.
 - (a) Assume that $j \in [q_e]$. Then the equation $f_2(i, \alpha) = f_3(j, \beta)$ is equivalent to the system of the equations

$$\begin{cases} 2^{\alpha-1}\Delta_3 \oplus X_j[a_j+\beta] = M_{i,L}[\alpha] \oplus Q; \\ X_j[a_j+\beta] = (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 \oplus M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j+\beta-1} X_j[\gamma], \end{cases}$$

$$Q = \bigoplus_{\gamma=1}^{a_j} 2^{a_j+\beta-\gamma} \left(X_j[\gamma] \oplus A_{j,R}[\gamma] \oplus 2^{\gamma-1} \Delta_2 \right)$$
$$\oplus \bigoplus_{\gamma=1}^{\beta-1} 2^{\beta-\gamma} \left(X_j[a_j+\gamma] \oplus M_{j,R}[\gamma] \oplus 2^{\gamma-1} \Delta_4 \right)$$

Since Δ_3 is chosen uniformly at random from $\{0, 1\}^n$ and $X_j[a_j + \beta]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_2(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

(b) Assume that $j \notin [q_e]$. Then the equation $f_2(i, \alpha) = f_3(j, \beta)$ is equivalent to the system of the equations

$$\begin{cases} 2^{\alpha-1}\Delta_3 = M_{i,L}[\alpha] \oplus Z_j[\beta];\\ 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus Y_j[\beta]. \end{cases}$$

Since (Δ_3, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_2(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

By the above reasoning, we have

$$\Pr\left[\mathsf{IC}_{2,3}\right] \leq \sum_{(i,\alpha)\in\mathcal{I}_2}\sum_{(j,\beta)\in\mathcal{I}_3}\frac{2}{2^{2n}} \leq \frac{2\,|\mathcal{I}_2|\,|\mathcal{I}_3|}{2^{2n}}.$$

8. Fix $(i, \alpha) \in \mathcal{I}_2$ and $(j, \beta) \in \mathcal{I}_4$. Then the equation $f_2(i, \alpha) = f_4(j, \beta)$ is equivalent to the system of the equations

$$\begin{cases} 2^{\alpha-1}\Delta_3 = M_{i,L}[\alpha] \oplus Y_j[\beta];\\ 2^{\beta-1}\Delta_2 = (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 \oplus M_{i,R}[\alpha] \oplus C_{j,R}[\beta]. \end{cases}$$

Note that $Y_j[\beta]$ is independent of Δ_2 and Δ_3 . Since (Δ_2, Δ_3) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_2(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{IC}_{2,4}\right] \le \sum_{(i,\alpha)\in\mathcal{I}_2}\sum_{(j,\beta)\in\mathcal{I}_4}\frac{2}{2^{2n}} \le \frac{2\,|\mathcal{I}_2|\,|\mathcal{I}_4|}{2^{2n}}.$$

9. Fix $(i, \alpha) \in \mathcal{I}_2$ and $j \in [q]$. If $j \in [q_e]$, then $f_2(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_3 \oplus \left(\bigoplus_{\beta=1}^{m_j} 2^{m_j}\right) \Delta_4 = M_{i,L}[\alpha] \oplus P; \\ 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus \bigoplus_{\beta=1}^{a_j+m_j} X_j[\beta], \end{cases}$$

$$P = \bigoplus_{\beta=1}^{a} 2^{a+m+1-\beta} \left(X[\beta] \oplus A_R[\beta] \oplus 2^{\beta-1} \Delta_2 \right)$$
$$\oplus \bigoplus_{\beta=1}^{m} 2^{m+1-\beta} \left(X[a+\beta] \oplus M_R[\beta] \right).$$

Since (Δ_3, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_2(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - 1)} \le \frac{2}{2^{2n}}.$$

If $j \notin [q_e]$, then $f_2(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_3 = M_{i,L}[\alpha] \oplus U_j; \\ 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus V_j. \end{cases}$$

Note that U_j and V_j are independent of Δ_3 and Δ_4 . Since (Δ_3, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[f_2(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n(2^n - 1)} \le \frac{2}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{IC}_{2,5}\right] \le \sum_{j \in [q]} \sum_{(i,\alpha) \in \mathcal{I}_2} \frac{2}{2^{2n}} \le \frac{2q |\mathcal{I}_2|}{2^{2n}}$$

10. Fix $((i, \alpha), (j, \beta)) \in (\mathcal{I}_3)^{*2}$ where $i \leq j$. If $j \in [q_e + 1, q_e + q_d]$, we have

$$\Pr[f_3(i,\alpha) = f_3(j,\beta)] \le \frac{1}{2^{2n}},$$

by the random choice of Y and Z variables in the ideal world. Suppose $j \in [q_e]$. Then, by the equations of Y-variables and Z-variables, $f_3(i, \alpha) = f_3(j, \beta)$ if and only if

$$\begin{cases} \bigoplus_{\gamma=1}^{a_i+\alpha} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j[\gamma] = P; \\ \bigoplus_{\gamma=1}^{a_i+\alpha} 2^{a_i+\alpha-\gamma} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} 2^{a_j+\beta-\gamma} X_j[\gamma] = Q, \end{cases}$$
(17)

where

$$\begin{split} P &= M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2, \\ Q &= \bigoplus_{\gamma=1}^{a_i} 2^{a_i+\alpha-\gamma} (A_{i,R}[\gamma] \oplus 2^{\gamma-1}\Delta_2) \oplus \bigoplus_{\gamma=1}^{\alpha-1} 2^{\alpha-\gamma} (M_{i,R}[\gamma] \oplus 2^{\gamma-1}\Delta_4) \\ &\oplus \bigoplus_{\gamma=1}^{a_j} 2^{a_j+\beta-\gamma} (A_{j,R}[\gamma] \oplus 2^{\gamma-1}\Delta_2) \oplus \bigoplus_{\gamma=1}^{\beta-1} 2^{\beta-\gamma} (M_{j,R}[\gamma] \oplus 2^{\gamma-1}\Delta_4). \end{split}$$

Let us take a look at each of the subcase below.

(a) If $\alpha < \beta$, (17) can be rewritten as

$$\begin{cases} X_i[a_i + \alpha] \oplus X_j[a_j + \alpha] \oplus X_j[a_j + \beta] = P'; \\ X_i[a_i + \alpha] \oplus 2^{\beta - \alpha} X_j[a_j + \alpha] \oplus X_j[a_j + \beta] = Q', \end{cases}$$
(18)

🖄 Springer

for some P' and Q'. Assume that $X_i[a_i + \alpha] = X_j[a_j + \alpha]$. Then (18) can be rewritten as

$$\begin{cases} X_j[a_j + \beta] = P'; \\ (2^{\beta - \alpha} + 1)X_j[a_j + \alpha] \oplus X_j[a_j + \beta] = Q'. \end{cases}$$

In this case, by the sampling process of $X_i[a_i + \alpha]$ and $X_j[a_j + \beta]$,

$$\Pr\left[f_3(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

If $X_i[a_i + \alpha] = X_j[a_j + \alpha]$, (18) can be rewritten as

$$\begin{cases} X_i[a_i + \alpha] \oplus X_j[a_j + \alpha] = P' \oplus X_j[a_j + \beta]; \\ X_i[a_i + \alpha] \oplus 2^{\beta - \alpha} X_j[a_j + \alpha] = Q' \oplus X_j[a_j + \beta]. \end{cases}$$

In this case, by the sampling process of $X_i[a_i + \alpha]$ and $X_i[a_i + \alpha]$,

$$\Pr\left[f_3(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

Therefore, no matter $M_i[\alpha] = M_j[\alpha]$ or not,

$$\Pr[f_3(i, \alpha) = f_3(j, \beta)] \le \frac{4}{2^{2n}}$$

(b) If $a_i < a_j$ and $\alpha = \beta$, (17) can be rewritten as

$$\begin{aligned} X_i[a_i] \oplus X_j[a_i] \oplus X_j[a_j] &= P'; \\ X_i[a_i] \oplus 2^{a_j - a_i} X_j[a_i] \oplus X_j[a_j] &= Q', \end{aligned}$$
(19)

for some P' and Q'. Assume that $X_i[a_i] = X_i[a_i]$. Then (19) can be rewritten as

$$\begin{cases} X_j[a_j] = P'; \\ (2^{a_j - a_i} + 1) X_j[a_i] \oplus X_j[a_j] = Q' \end{cases}$$

In this case, by the sampling process of $X_j[a_i]$ and $X_j[a_j]$, we have

$$\Pr\left[f_3(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

If $X_i[a_i] \neq X_j[a_i]$, then (19) can be rewritten as

$$\begin{cases} X_i[a_i] \oplus X_j[a_i] = P' \oplus X_j[a_j]; \\ X_i[a_i] \oplus 2^{a_j - a_i} X_j[a_i] = Q' \oplus X_j[a_j]. \end{cases}$$

In this case, by the sampling process of $X_i[a_i]$ and $X_i[a_i]$, we have

$$\Pr\left[f_3(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

Therefore, no matter $A_i[a_i] = A_j[a_i]$ or not,

$$\Pr[f_3(i, \alpha) = f_3(j, \beta)] \le \frac{4}{2^{2n}}$$

(c) If there exists two different $\gamma_1, \gamma_2 \leq \alpha$ such that $A_i[\gamma_1] \neq A_j[\gamma_1]$ and $A_i[\gamma_2] \neq A_j[\gamma_2]$, (17) can be rewritten as

$$\begin{cases} X_i[\gamma_1] \oplus X_j[\gamma_2] = P'; \\ 2^{a_i \oplus \alpha - \gamma_1} X_i[\gamma_1] \oplus 2^{a_i \oplus \alpha - \gamma_2} X_i[\gamma_2] = Q', \end{cases}$$

for some P' and Q'. Therefore, by the sampling process of $X_i[\gamma_1]$ and $X_j[\gamma_2]$, we get

$$\Pr\left[f_3(i,\alpha) = f_3(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

We can apply the similar argument if $(A_i, M_i[: \alpha])$ and $(A_j, M_j[: \alpha])$ are differ in two or more blocks.

(d) Let $a_i = a_j, \alpha = \beta$, and $M_i[\alpha] \neq M_j[\alpha]$ while $(A_i, M_i[\alpha - 1]) = (A_j, M_j[\alpha - 1])$, Then, (17) can be rewritten as

$$X_i[a_i + \alpha] \oplus X_j[a_i + \alpha] = M_{i,R}[\alpha] \oplus M_{j,R}[\alpha];$$

$$X_i[a_i + \alpha] \oplus X_j[a_i + \alpha] = 0,$$

so one should have $X_i[a_i + \alpha] = X_j[a_i + \alpha]$ and $M_{i,R}[\alpha] = M_{j,R}[\alpha]$ which contradicts the rules for choosing X variables. Therefore,

$$\Pr[f_3(i, \alpha) = f_3(j, \beta)] = 0,$$

and one can apply the similar argument if there exists only one different block between $(A_i, M_i[: \alpha])$ and $(A_j, M_j[: \alpha])$.

All in all, we get

$$\Pr\left[\mathsf{IC}_{3,3}\right] \le \frac{4|\mathcal{I}_3|^2}{2^{2n}}.$$

- 11. Fix $(i, \alpha) \in \mathcal{I}_3$ and $(j, \beta) \in \mathcal{I}_4$. Let us take a look at each of sub-case below.
 - (a) Let $i, j \in [q_e]$. Assume that $M_i[: \alpha]$ and $M_j[: \beta]$ are different in two or more blocks. We fix such distinct γ_1, γ_2 . If $\beta \le \alpha$, then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} 2^{a_i \oplus \alpha - \gamma_1} X_i[a_i + \gamma_1] \oplus 2^{a_i \oplus \alpha - \gamma_2} X_i[a_i + \gamma_2] = P'; \\ X_i[a_i + \gamma_1] \oplus X_i[a_i + \gamma_2] = Q', \end{cases}$$

for some P' and Q' which are independent of $X_i[a_i + \gamma_1]$ and $X_i[a_i + \gamma_2]$ By the sampling process of $X_i[a_i + \gamma_1]$ and $X_i[a_i + \gamma_2]$, we have

$$\Pr\left[f_3(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}$$

If $\beta > \alpha$, then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} X_j[a_j + \gamma_1] \oplus \bigoplus_{\delta=1}^{a_i} 2^{\delta-1} \Delta_2 = P'; \\ 2^{\beta-1} \Delta_2 = Y_i \oplus 2^{\beta-1} \Delta_4 \oplus C_{j,R}[\beta], \end{cases}$$

for some P' which is independent of $X_j[a_j + \gamma_1]$ and Δ_2 . By the sampling process of $X_j[a_j + \gamma_1]$ and the randomness of Δ_2 , we have

$$\Pr\left[f_3(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{(2^n - \sigma)(2^n - 1)} \le \frac{4}{2^{2n}}.$$

🖄 Springer

Therefore,

$$\Pr[f_3(i,\alpha) = f_4(j,\beta)] \le \frac{4}{2^{2n}}.$$

(b) Let *i*, *j* ∈ [*q_e*]. Assume that *M_i*[: α] and *M_j*[: β] are different in just a single block with index *h*. Then *f*₃(*i*, α) = *f*₄(*j*, β) if and only if

$$\begin{cases} X_i[a_i + h] = P'; \\ 2^{\alpha - h} X_i[a_i + h] \oplus X_j[a_j + h] = Q', \end{cases}$$

for some P' and Q'. Therefore, by the sampling process of $X_i[a_i+h]$ and $X_j[a_j+h]$, we have

$$\Pr\left[f_3(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

(c) Let $i, j \in [q_e]$ and $M_i[: \alpha] = M_j[: \beta]$. Note that $X_i[a_i + h] = X_j[a_j + h]$ for all $h \in [\alpha]$. If $\alpha = \beta > 2$, then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} X_i[a_i+1] \oplus X_i[a_i+2] = P' \\ (2^{\alpha-1} \oplus 1)X_i[a_i+1] \oplus (2^{\alpha-2} \oplus 1)X_i[a_i+2] = Q'. \end{cases}$$

If $\alpha = \beta = 2$, then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} X_i[a_i+1] \oplus X_i[a_i+2] = P'; \\ (2^{\alpha-1} \oplus 1)X_i[a_i+1] = Q'. \end{cases}$$

For both case, one has

$$\Pr[f_3(i,\alpha) = f_4(j,\beta)] \le \frac{4}{2^{2n}}.$$

Now assume $\alpha = \beta = 1$. Then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} \Delta_2 = P'; \\ \bigoplus_{\gamma=1}^{a_j} 2^{a_j + 1 - \gamma} \Delta_2 \oplus \Delta_4 = Q'. \end{cases}$$

Since (Δ_2, Δ_4) is chosen uniformly at random from $\{0, 1\}^{*2}$, one has

$$\Pr[f_3(i,\alpha) = f_4(j,\beta)] \le \frac{2}{2^{2n}}$$

(d) Let $i \in [q_e + 1, q]$ and $j \in [q_e]$. Then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_2 \oplus 2^{\beta-1}\Delta_4 = Y_i[\alpha] \oplus C_{j,R};\\ 2^{\beta-1}\Delta_4 = Z_i[\alpha] \oplus M_{j,R}[\alpha] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j[\gamma]. \end{cases}$$

Since (Δ_2, Δ_4) is chosen uniformly at random from $\{0, 1\}^{*2}$, one has

$$\Pr[f_3(i, \alpha) = f_4(j, \beta)] \le \frac{2}{2^{2n}}$$

(e) Let $i \in [q_e]$ and $j \in [q_e + 1, q]$. If $\alpha \ge 2$, then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} X_i[a_i+1] \oplus X_i[a_i+2] = P'; \\ X_i[a_i+1] \oplus 2X_i[a_i+2] = Q', \end{cases}$$

where P' and Q' are independent of $X_i[a_i + 1]$ and $X_i[a_i + 2]$. In this case, by the sampling process of $X_i[a_i + 1]$ and $X_i[a_i + 2]$, we have

$$\Pr\left[f_3(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

If $\alpha = 1$, then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} X_i[a_i+1] \oplus \Delta_4 = P'; \\ X_i[a_i+1] = Q', \end{cases}$$

where P' and Q' are independent of $X_i[a_i + 1]$ and Δ_4 . In this case, since $X_i[a_i + 1]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$ and Δ_4 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_2\}$, we have

$$\Pr\left[f_3(i,\alpha) = f_4(j,\beta)\right] \le \frac{1}{(2^n - 1)(2^n - \sigma)} \le \frac{4}{2^{2n}}.$$

(f) Let $i, j \in [q_e + 1, q]$. Then $f_3(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_2 = Y_i[\alpha] \oplus C_{j,R}[\beta] \oplus 2^{\beta-1}\Delta_4; \\ Z_i[\alpha] = Y_j[\beta]. \end{cases}$$

Since Δ_2 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_2\}$ and $Z_i[\alpha]$ are chosen uniformly at random from $\{0, 1\}^n$, respectively, we have

Pr
$$[f_3(i, \alpha) = f_4(j, \beta)] \le \frac{1}{2^n (2^n - 1)} \le \frac{2}{2^{2n}}.$$

To sum up, we have

$$\Pr\left[\mathsf{IC}_{3,4}\right] \le \sum_{(j,\beta)\in\mathcal{I}_4} \sum_{(i,\alpha)\in\mathcal{I}_3} \frac{4}{2^{2n}} \le \frac{4|\mathcal{I}_3||\mathcal{I}_4|}{2^{2n}}$$

- 12. Fix $(i, \alpha) \in \mathcal{I}_3$ and $j \in [q_e + q_d]$. Let us take a look at each of sub-case below.
 - (a) Assume that $i, j \in [q_e]$, and $M_i[: \alpha]$ and M_j are different in two or more blocks. Fix such distinct γ_1, γ_2 . If $\alpha \ge m_j$, then $f_3(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} X_i[a_i+\gamma_1] \oplus X_i[a_i+\gamma_2] = P';\\ 2^{a_i+\alpha-\gamma_1}X_i[a_i+\gamma_1] \oplus 2^{a_i+\alpha-\gamma_2}X_i[a_i+\gamma_2] = Q', \end{cases}$$

for some P' and Q' which are independent of $X_i[a_i + \gamma_1]$ and $X_i[a_i + \gamma_2]$. In this case, by the sampling process of $X_i[a_i + \gamma_1]$ and $X_i[a_i + \gamma_2]$,

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}$$

If $\alpha < m_j$, then $f_3(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} X_j[a_j + \gamma_1] \oplus X_j[a_j + \gamma_2] = P'; \\ 2^{a_j + m_j + 1 - \gamma_1} X_j[a_j + \gamma_1] \oplus 2^{a_j + m_j + 1 - \gamma_2} X_j[a_j + \gamma_2] = Q', \end{cases}$$

for some P' and Q' which are independent of $X_j[a_j + \gamma_1]$ and $X_j[a_j + \gamma_2]$. In this case, by the sampling process of $X_j[a_j + \gamma_1]$ and $X_j[a_j + \gamma_2]$,

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

🖄 Springer

Therefore, we have

$$\Pr\left[f_3(i,\alpha)=(V_j,U_j)\right] \le \frac{2}{2^{2n}}.$$

(b) Suppose $i, j \in [q_e]$, and M_i and M_j are differ in a single block with index γ . Then, by the equations of U-variables and V-variables specified in Sect. 3, $f_3(i, \alpha) = (V_j, U_j)$ can be rewritten as

$$\begin{cases} X_i[a_i + \gamma] \oplus X_j[a_j + \gamma] = P'; \\ X_i[a_i + \gamma] \oplus 2^{m_j + 1 - \gamma} X_j[a_j + \gamma] = Q', \end{cases}$$

for some P' and Q' which are independent of $X_i[a_i + \gamma]$ and $X_j[a_j + \gamma]$. By the sampling process of $X_i[a_i + \gamma]$ and $X_j[a_j + \gamma]$, we have

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)} \le \frac{4}{2^{2n}}$$

(c) Suppose $i = j \in [q_e]$. If $\alpha < m_i$, then $f_3(i, \alpha) = (V_i, U_i)$ if and only if

$$\begin{aligned} X_i[a_i + m_i] &= M_{i,R}[\alpha] \oplus 2^{\alpha - 1} \Delta_4 \oplus \bigoplus_{\beta = a_i + \alpha + 1}^{a_i + m_i} X_i[\beta];\\ 2X_i[a_i + m_i] \oplus (2^{m_i + 1 - \alpha} + 1) X_i[a_i + \alpha] &= Q', \end{aligned}$$

for some Q' which is independent of $X_i[a_i + \alpha]$ and $X_i[a_i + m_i]$. Note that $\alpha < m_i$ so $m_i - \alpha + 1 > 0$. Therefore, in this case, we have

$$\Pr\left[f_3(i,\alpha) = (V_i, U_i)\right] \le \frac{1}{(2^n - \sigma)} \le \frac{4}{2^{2n}}.$$

Now assume that $\alpha = m_i$. Then $f_3(i, m_i) = (V_i, U_i)$ can be rewritten as

$$\begin{cases} 2^{m_i-1}\Delta_4 = P';\\ 3X_i[m_i] \oplus \left(2^{m_i} \oplus \bigoplus_{\beta=1}^{m_i-1} (2^{m_i-1} \oplus 2^{m_i})\right) \Delta_4 = Q'. \end{cases}$$

 $X_i[m_i]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$ and Δ_4 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_2\}$, we get

$$\Pr\left[f_3(i,\alpha) = (V_i, U_i)\right] \le \frac{1}{(2^n - 1)(2^n - \sigma)} \le \frac{4}{2^{2n}}.$$

(d) Let $i \in [q_e + 1, q]$ and $C_i[\alpha] \neq C_j[\alpha]$. Then $f_3(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} Y_i[\alpha] = V_j; \\ Z_i[\alpha] = U_j \end{cases}$$

Since $Y_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$ and $Z_i[\alpha]$ are chosen uniformly at random from $\{0, 1\}^n$, we have

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - \sigma)} \le \frac{2}{2^{2n}}$$

(e) Let $j \in [q_e + 1, q]$ and there exists γ such that $(j, \gamma) \in \mathcal{I}_3$. Then, if we fix all X, Y, and Z variables consisting (V_j, U_j) except $Y_j[\gamma]$ and $Z_j[\gamma]$, there exists a 1-1 correspondence map $f : \{0, 1\}^{2n} \longrightarrow \{0, 1\}^{2n}$ between $(Y_j[\gamma], Z_j[\gamma])$ and (V_j, U_j) . Then $\Pr[f_3(i, \alpha) = (V_j, U_j)] = \Pr[f_3(i, \alpha) = f((Y_j[\gamma], Z_j[\gamma]))]$. Since $Y_j[\gamma]$

is chosen uniformly at random from the set of size at least $2^n - \sigma$ and $Z_j[\gamma]$ are chosen uniformly at random from $\{0, 1\}^n$, we get

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

(f) Let $i \in [q_e + 1, q]$, $C_i[\alpha] = C_j[\alpha]$, Since $(i, \alpha) \in \mathcal{I}_3$, one should have $j \in [q_e + 1, q_e + q_d]$ and $C_i[\gamma] \neq C_j[\gamma]$ for some γ . Suppose that $(j, \gamma) \notin \mathcal{I}_3$. If there exists some $j' \in [q_e + 1, q_e + q_d]$ such that $(j', \gamma) \in \mathcal{I}_3$ and $C_j[\gamma] = C_{j'}[\gamma]$, we can easily apply the same argument as (e). If there exists $j' \in [q_e]$ such that $(j', \gamma) \in \mathcal{I}_3$ and $C_{j'}[\gamma] = C_j[\gamma]$, there exists a 1-1 correspondence map between $(X_{j'}[\gamma], \Delta_4)$ and (V_j, U_j) . Since $Y_j[\gamma]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$ and $Z_j[\gamma]$ are chosen uniformly at random from $\{0, 1\}^n$, we get

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n(2^n - 1)} \le \frac{2}{2^{2n}}.$$

Moreover, we can apply same method for all remaining cases together with the condition $\neg bad_1$.

To sum up, we have

$$\Pr\left[f_3(i,\alpha) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{IC}_{3,5}\right] \le \frac{4|\mathcal{I}_3|q}{2^{2n}}$$

- (13) Fix $((i, \alpha), (j, \beta)) \in \mathcal{I}_4^{*2}$. Without loss of generality, let $i \leq j$. We distinguish some sub-cases as below.
 - (a) Let $i, j \in [q_e]$ and $\alpha \neq \beta$. Then $f_4(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2 \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 = C_{i,R}[\alpha] \oplus C_{j,R}[\beta];\\ (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 = M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_i+\alpha} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j[\gamma]. \end{cases}$$

Since (Δ_2, Δ_4) is chosen uniformly at random from $\{0, 1\}^{*2}$, one has

$$\Pr[f_4(i, \alpha) = f_4(j, \beta)] \le \frac{2}{2^{2n}}$$

(b) Let i, j ∈ [q_e] and α = β. (Now we use α instead of β.) Note that C_i[α] ≠ C_j[α] and M_i[: α] ≠ M_j[: α] since ((i, α), (j, α)) ∈ I^{*2}₄. Let h ∈ [α] the index such that M_i[h] ≠ M_j[h] Then f₄(i, α) = f₄(j, α) if and only if

$$\begin{cases} C_{i,R}[\alpha] = C_{j,R}[\alpha]; \\ X_i[h] = M_{i,R}[\alpha] \oplus M_{j,R}[\alpha] \oplus \bigoplus_{\gamma \neq a_i+h} X_i[\gamma] \oplus \bigoplus_{\gamma=1}^{a_j+\alpha} X_j[\gamma]. \end{cases}$$

Since $C_{i,R}[\alpha]$ is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[h]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_4(i,\alpha) = f_4(j,\alpha)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

🖄 Springer

(c) Let $i \in [q_e]$, $j \in [q_e + 1, q]$, and $\alpha \neq \beta$. Then $f_4(i, \alpha) = f_4(j, \beta)$ if and only if $\begin{cases}
(2^{\alpha - 1} \oplus 2^{\beta - 1})\Delta_2 \oplus (2^{\alpha - 1} \oplus 2^{\beta - 1})\Delta_4 = C_{i,R}[\alpha] \oplus C_{j,R}[\beta]; \\
2^{\alpha - 1}\Delta_4 = Y_j[\beta] \oplus M_{i,R}[\alpha] \oplus \bigoplus_{\gamma=1}^{a_i + \alpha} X_i[\gamma].
\end{cases}$

Since (Δ_2, Δ_4) is chosen uniformly at random from $\{0, 1\}^{*2}$, one has

$$\Pr\left[f_4(i,\alpha) = f_4(j,\beta)\right] \le \frac{2}{2^{2n}}$$

(d) Let $i \in [q_e]$, $j \in [q_e + 1, q]$, and $\alpha = \beta$. If $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, then $Y_i[\alpha] \neq Y_j[\alpha]$ by the sampling process. In this case, $\Pr[f_4(i, \alpha) = f_4(j, \alpha)] = 0$. If $C_{i,R}[\alpha] \neq C_{j,R}[\alpha]$, then similarly $\Pr[f_4(i, \alpha) = f_4(j, \alpha)] = 0$. Therefore,

$$\Pr[f_4(i, \alpha) = f_4(j, \alpha)] = 0.$$

(e) Let $i, j \in [q_e + 1, q]$. If $\alpha \neq \beta$, then $f_4(i, \alpha) = f_4(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2 = (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 \oplus C_{i,R}[\alpha] \oplus C_{j,R}[\beta];\\ Y_i[\alpha] = Y_i[\beta]. \end{cases}$$

Since Δ_2 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_4\}$ and $Y_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - q$, we have

$$\Pr[f_4(i, \alpha) = f_4(j, \beta)] \le \frac{4}{2^{2n}}$$

Let $\alpha = \beta$. If $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, then $Y_i[\alpha] \neq Y_j[\beta]$ by the sampling process, so the probability is zero. If $C_{i,R}[\alpha] = C_{j,R}[\alpha]$, then $C_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_2 \oplus 2^{\alpha-1}\Delta_4 \neq C_{j,R}[\alpha] \oplus 2^{\alpha-1}\Delta_2 \oplus 2^{\alpha-1}\Delta_4$ so the probability is zero.

To sum up, we have

$$\Pr\left[\mathsf{IC}_{4,4}\right] \le \frac{4 \, |\mathcal{I}_4|^2}{2^{2n}}.$$

14. Fix $(i, \alpha) \in \mathcal{I}_4$ and $j \in [q]$. We distinguish some sub-cases as below.

(a) Let $i, j \in [q_e]$ and $\alpha \neq m_i$. If $\alpha > m_i$, then $f_4(i, \alpha) = (V_i, U_i)$ if and only if

$$\begin{cases} X_i[a_i + \alpha] = M_{i,R}[\alpha] \oplus 2^{\alpha - 1} \Delta_4 \oplus \bigoplus_{\beta = 1}^{a_i + \alpha - 1} X_i[\beta] \oplus U_j; \\ C_{i,R}[\alpha] = 2^{\alpha - 1} \Delta_2 \oplus 2^{\alpha - 1} \Delta_4 \oplus V_j. \end{cases}$$

Therefore, by the randomness of $C_{i,R}[\alpha]$ and $X_i[a_i + \alpha]$, one has

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}$$

If $\alpha < m_i$, then $f_4(i, \alpha) = (V_i, U_i)$ if and only if

$$\begin{cases} 2X_j[a_j + m_j] = Y_i[\alpha] \oplus P; \\ X_j[a_j + m_j] \oplus C_{i,R}[\alpha] = 2^{\alpha - 1} \Delta_2 \oplus 2^{\alpha - 1} \Delta_4 \oplus \bigoplus_{\beta = 1}^{a_j + m_j - 1} X_j[\beta], \end{cases}$$

for some constant $P \in \{0, 1\}^n$, which is independent of $X_j[a_j + m_j]$ and $C_{i,R}[\alpha]$. Therefore, by the sampling process of $C_{i,R}[\alpha]$ and $X_j[a_j + m_j]$, one has

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}$$

(b) Let $i, j \in [q_e]$ and $\alpha = m_j$. Assume that $A_i \neq A_j$ and $a_i \geq a_j$. (We can apply the similar argument when $a_i < a_j$.) Then there exists $\gamma \in [a_i]$ such that $\gamma > a_j$ or $A_i[\gamma] \neq A_j[\gamma]$. In this case, $f_4(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} C_{i,R}[\alpha] \oplus X_i[\gamma] = P'; \\ X_i[\gamma] = Q', \end{cases}$$

for some P' and Q' which are independent of $C_{i,R}[\alpha]$ and $X_i[\gamma]$. Since $C_{i,R}[\alpha]$ is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[\gamma]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, we get

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - \sigma)} \le \frac{2}{2^{2n}}$$

(c) Let $i, j \in [q_e]$, $A_i = A_j$ and $\alpha = m_j$. Then $M_i \neq M_j$ since there is no redundant query. Let *h* be the index such that $M_i[h] \neq M_j[h]$. Then $f_4(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} X_i[a_i+h] \oplus 2^{m_j+1-h} X_j[a_j+h] = P; \\ X_j[a_j+h] = 2^{\alpha-1} \Delta_2 \oplus 2^{\alpha-1} \Delta_4 \oplus C_{i,R}[\alpha] \oplus \bigoplus_{\substack{\beta \in [m_j] \\ \beta \neq a_j+h}} X_j[\beta], \end{cases}$$

for some *P* which is independent of $X_i[a_i + h]$ and $X_j[a_j + h]$. Since $X_i[a_i + h]$ and $X_j[a_j + h]$ are chosen randomly from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}$$

(d) Let $i, j \in [q_e]$, $A_i = A_j$ and $M_i[: \alpha] = M_j$. Then $f_4(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_4 = M_i[\alpha];\\ 2^{\alpha-w_\alpha}\Delta_4 \oplus 3X_i[a_i+\alpha] = P, \end{cases}$$

for some constant *P*. Since Δ_4 is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[a_i + \alpha]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, we have

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

(e) Let $i \in [q_e + 1, q]$ and $j \in [q_e]$. If $C_i[\alpha] = C_{i'}[\alpha]$ for some $i' \in [q_e]$, it is one of the above cases. Otherwise, $f_4(i, \alpha) = (V_i, U_i)$ if and only if

$$\begin{cases} Y_i[\alpha] \oplus 2^{a_j + m_j} X_j[1] = P'; \\ X_j[1] = 2^{\alpha - 1} \Delta_2 \oplus 2^{\alpha - 1} \Delta_4 \oplus C_{j,R}[\alpha] \oplus \bigoplus_{\beta = 2}^{a_j + m_j} X_j[\beta], \end{cases}$$

for some constant P' which is independent of $Y_i[\alpha]$ and $X_j[1]$. $Y_i[\alpha]$ is sampled from the set of size at least $2^n - \sigma$ and $X_j[1]$ is sampled uniformly at random from the set of size at least $2^n - \sigma$. Therefore, we have

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

🖄 Springer

(f) Let $i \in [q_e]$ and $j \in [q_e + 1, q]$. There is no redundant query, $A_i \neq A_j$ or $C_i \neq C_j$. Assume that $A_i \neq A_j$ and $a_i \ge a_j$. (We can apply similar argument when $a_i < a_j$ or $C_i \neq C_j$.) Then there exists $\gamma \in [a_i]$ such that $\gamma > a_j$ or $A_i[\gamma] \neq A_j[\gamma]$. Then $f_4(i, \alpha) = (V_i, U_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 = 2^{\alpha-1}\Delta_4 \oplus C_{j,R}[\alpha] \oplus V_j;\\ \bigoplus_{\beta=1}^{a_j} 2^{\beta-1}\Delta_2 \oplus X_i[\gamma] = Q', \end{cases}$$

for some Q' which is independent of Δ_2 and $X_i[\gamma]$. In this case, $X_i[\gamma]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$. Also, Δ_2 is chosen uniformly at random from $\{0, 1\}^n$. Therefore, we have

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}.$$

(g) Let $i, j \in [q_e + 1, q]$. If $C_i[\alpha] = C_{i'}[\alpha]$ for some $i' \in [q_e]$, it is one of the above cases. Otherwise, $f_4(i, \alpha) = (V_j, U_j)$ if and only if

$$\begin{cases} C_{i,R}[\alpha] = V_j \oplus 2^{\alpha-1} \Delta_{i,2} \oplus 2^{\alpha-1} \Delta_{i,4}; \\ Y_i[\alpha] = U_j. \end{cases}$$

By the sampling process of $C_{i,R}[\alpha]$ and $Y_i[\alpha]$, we have

$$\Pr\left[f_4(i,\alpha) = (V_j, U_j)\right] \le \frac{1}{(2^n - \sigma)^2} \le \frac{4}{2^{2n}}.$$

By the above analysis, we have

$$\Pr\left[\mathsf{IC}_{4,5}\right] \le \frac{4q \, |\mathcal{I}_4|}{2^{2n}}.$$

- 15. Fix $i, j \in [q]^{*2}$. Without loss of generality, let $i \leq j$. We restore X values and R values using $\hat{\rho}^{-1}$. Then, since there is no redundant query, $A_i \neq A_j$ or $M_i \neq M_j$. We consider the following cases.
 - (a) If $a_i > a_j + 1$, then $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 2^{a_i+m_i-a_j} & 2^{a_i+m_i-a_j-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[a_j+1] \\ X_i[a_j+2] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

for some P' and Q' which are independent of $X_i[a_j + 1]$ and $X_i[a_j + 2]$. By the sampling process of $X_i[a_j+1]$ and $X_i[a_j+2]$, in this case $\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}$. We can apply the similar argument when $a_j > a_i + 1$ and get the same result.

(b) Assume that $a_i = a_j + 1$ and $A_i[\beta] \neq A_j[\beta]$ for some $\beta \in [a_j]$. Then $(V_i, U_i) = (V_i, U_j)$ if and only if

$$\begin{pmatrix} 2^{m_i+a_i-\beta+1} & 2^{m_i+1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[\beta] \\ X_i[a_i] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

for some P' and Q' which are independent of $X_i[\beta]$ and $X_i[a_i]$. By Lemma 6, we can conclude

$$\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}$$

Springer

(c) Assume that $a_i = a_j + 1$ and $A_i[: a_j] = A_j$. If $M_i[\beta] \neq M_j[\beta]$ or there exists $\beta \in [m_i]$, we can use the randomness of $X_i[a_i + \beta]$ and $X_i[a_i]$. More precisely, $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 2^{m_i-\beta+1} & 2^{m_i+1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[a_i+\beta] \\ X_i[a_i] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

for some P' and Q' which are independent of $X_i[a_i + \beta]$ and $X_i[a_i]$. If $M_i = M_j$, we have two cases, $X_i[a_i] = 0$ or $X_i[a_i] \neq 0$. $X_i[a_i] \neq 0$ implies $V_i \neq V_j$ (see (5)). Also, if $X_i[a_i] = 0$, then $U_i = U_j$ if and only if

$$\bigoplus_{\beta=1}^{m_i} 2^{m+1-\beta} (X_i[a_i+\beta] \oplus M_{i,R}[\beta]) \oplus 2^{m+1} A_{i,R}[a_i] = 0.$$

Therefore, $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X_i[a_i] \\ X_i[a_i + m_i] \end{pmatrix} = \begin{pmatrix} 0 \\ Q' \end{pmatrix},$$

where

$$Q' = \bigoplus_{\beta=1}^{m_i-1} 2^{m+1-\beta} (X_i[a_i + \beta] \oplus M_{i,R}[\beta]) \oplus M_{i,R}[m_i] \oplus 2^{m+1} A_{i,R}[a_i].$$

(see (4)). Therefore, by the sampling process of $X_i[a_i]$ and Lemma 6,

$$\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}$$

We can apply the similar argument when $a_i = a_i + 1$ and $A_i[: a_i] = A_i$.

(d) Assume that $a_i = a_j$. If there exist $\alpha, \beta \in [a_i]$ such that $A_i[\alpha] \neq A_j[\alpha]$ and $A_i[\beta] \neq A_j[\beta], (V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 2^{a_i+m_i-\alpha+1} & 2^{a_i+m_i-\beta+1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[\alpha] \\ X_i[\beta] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix}$$

for some P' and Q' which are independent of $X_i[\alpha]$ and $X_i[\beta]$. Then by Lemma 6, $\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{4}{2^{2n}}$. If there exists only one $\alpha \in [a_i]$ such that $A_i[\alpha] \ne A_j[\alpha]$, then $(V_i, U_i) = (V_j, U_j)$ if and only if

$$\begin{pmatrix} 2^{a_i+m_i-\alpha+1} & 2^{a_j+m_j-\alpha+1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_i[\alpha] \\ X_j[\alpha] \end{pmatrix} = \begin{pmatrix} P' \\ Q' \end{pmatrix},$$

for some P' and Q' which are independent of $X_i[\alpha]$ and $X_j[\alpha]$. Therefore,

$$\Pr\left[(V_i, U_i) = (V_j, U_j)\right] \le \frac{1}{2^n (2^n - 1)} \le \frac{4}{2^{2n}}$$

Therefore, we have

$$\Pr\left[\mathsf{IC}_{5,5}\right] \le \frac{4q^2}{2^{2n}}$$

🖉 Springer

All in all, we have

$$\Pr\left[\mathsf{IC}\right] \le \frac{4q^2 + 12q\sigma + 20\sigma^2}{2^{2n}}.$$

Lemma 11

$$\Pr[\mathsf{OC}] \le \frac{2q_e^2 + 6q_e\sigma + 28\sigma^2}{2^{2n}}$$

Proof We calculate each probability of $OC_{i,j}$ for $1 \le i \le j \le 5$.

1. Let $((i, \alpha), (j, \beta)) \in \mathcal{I}_1^{*2}$. If $\alpha = \beta$, then one should have $A_i[\alpha] \neq A_j[\beta]$ and $g_1(i, \alpha) \neq g_2(\beta)$. Suppose $\alpha \neq \beta$. Then $g_1(i, \alpha) = g_1(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2 = A_{i,R}[\alpha] \oplus A_{j,R}[\beta];\\ X_i[\alpha] = X_j[\beta], \end{cases}$$

and since Δ_2 is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr[g_1(i,\alpha) = g_1(j,\beta)] \le \frac{1}{2^n(2^n - \sigma)} \le \frac{2}{2^{2n}}$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{1,1}\right] \le \sum_{((i,\alpha),(j,\beta))\in\mathcal{I}_1^{*2}} \frac{2}{2^{2n}} \le \frac{2\,|\mathcal{I}_1|^2}{2^{2n}}.$$

2. Let $(i, \alpha) \in \mathcal{I}_1$ and $(j, \beta) \in \mathcal{I}_2$. Then $g_1(i, \alpha) = g_2(j, \beta)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 = 2^{\beta-1}\Delta_4 \oplus A_{i,R}[\alpha] \oplus M_{i,R}[\beta];\\ X_i[\alpha] = X_j[a_j + \beta]. \end{cases}$$

Since Δ_2 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_4\}$ and $X_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - \sigma$, one has

$$\Pr\left[g_1(i,\alpha) = g_2(j,\beta)\right] \le \frac{1}{(2^n - 1)(2^n - \sigma)} \le \frac{4}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{1,2}\right] \le \sum_{(j,\beta)\in\mathcal{I}_2} \sum_{(i,\alpha)\in\mathcal{I}_1} \frac{4}{2^{2n}} \le \frac{4\,|\mathcal{I}_1|\,|\mathcal{I}_2|}{2^{2n}}.$$

- 3. Let $(i, \alpha) \in \mathcal{I}_1$ and $(j, \beta) \in \mathcal{I}_3$. We distinguish two sub-cases.
 - (a) Assume $j \in [q_e]$. Then $g_1(i, \alpha) = g_3(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_4 \oplus C_j[\beta] = 2^{\beta-1}\Delta_2 \oplus X_i[\alpha]; \\ 2^{\beta-1}\Delta_4 = 2^{\alpha-1}\Delta_2 \oplus A_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j\gamma. \end{cases}$$

Since Δ_4 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_2\}$ and $C_j[\beta]$ is chosen uniformly at random from $\{0, 1\}^n$, respectively, one has

$$\Pr\left[g_1(i,\alpha) = g_3(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}$$

(b) Assume j ∉ [q_e]. If C_j[β] = C_{j'}[β] for j' ∈ [q_e], this case is same as the case that j ∈ [q_e]. Otherwise, g₁(i, α) = g₃(j, β) if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus Y_j[\beta];\\ 2^{\beta-1}\Delta_2 \oplus 2^{\beta-1}\Delta_4 = C_{i,R}[\beta] \oplus X_i[\alpha]. \end{cases}$$

Since (Δ_2, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[g_1(i,\alpha) = g_3(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}$$

To sum up, we have

$$\Pr\left[\mathsf{OC}_{1,3}\right] \le \sum_{(j,\beta)\in\mathcal{I}_3} \sum_{(i,\alpha)\in\mathcal{I}_1} \frac{2}{2^{2n}} \le \frac{2\,|\mathcal{I}_1|\,|\mathcal{I}_3|}{2^{2n}}.$$

4. Let $(i, \alpha) \in \mathcal{I}_1$ and $(j, \beta) \in \mathcal{I}_4$. Then $g_1(i, \alpha) = g_3(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_1 = X_i[\alpha] \oplus C_{i,L}[\beta] \oplus 2^{\beta-1}\Delta_3; \\ 2^{\beta-1}\Delta_4 = A_{i,R}[\alpha] \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2 \end{cases}$$

Since (Δ_1, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n \setminus \{\Delta_2, \Delta_3\})^{*2}$, one has

$$\Pr\left[g_1(i,\alpha) = g_4(j,\beta)\right] \le \frac{1}{(2^n - 2)(2^n - 3)} \le \frac{4}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{1,4}\right] \le \sum_{(j,\beta)\in\mathcal{I}_4} \sum_{(i,\alpha)\in\mathcal{I}_1} \frac{4}{2^{2n}} \le \frac{4\,|\mathcal{I}_1|\,|\mathcal{I}_4|}{2^{2n}}.$$

5. Let $(i, \alpha) \in \mathcal{I}_1$ and $j \in [q_e]$. Then $g_1(i, \alpha) = (V_j, T_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 = A_{i,R}[\alpha] \oplus \bigoplus_{\beta=1}^{a_j+m_j} X_j[\beta];\\ T_j = X_i[\alpha]. \end{cases}$$

Since Δ_2 and T_j are chosen uniformly at random from $\{0, 1\}^n$, respectively, one has

$$\Pr\left[g_1(i,\alpha)=(V_j,T_j)\right]\leq \frac{1}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{1,5}\right] \le \sum_{j \in [q_e]} \sum_{(i,\alpha) \in \mathcal{I}_1} \frac{1}{2^{2n}} \le \frac{q_e |\mathcal{I}_1|}{2^{2n}}$$

6. Let $((i, \alpha), (j, \beta)) \in \mathbb{Z}_2^{*2}$. If $\alpha = \beta$, then $M_i[\alpha] \neq M_j[\beta]$ so $g_2(i, \alpha) \neq g_2(j, \beta)$. Otherwise, $g_2(i, \alpha) = g_2(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 = M_{i,R}[\alpha] \oplus M_{j,R}[\beta];\\ X_i[a_i + \alpha] = X_j[a_j + \beta]. \end{cases}$$

Since Δ_4 is chosen uniformly at random from $\{0, 1\}^n$ and $X_i[a_i + \alpha]$ is chosen uniformly at random from the set of size at least $2^n - q_e$, we have

$$\Pr\left[g_2(i,\alpha) = g_2(j,\beta)\right] \le \frac{1}{2^n(2^n - q_e)} \le \frac{2}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{2,2}\right] \le \sum_{((i,\alpha),(j,\beta))\in \mathcal{I}_{2}^{*2}} \frac{2}{2^{2n}} \le \frac{2|\mathcal{I}_{2}|^{2}}{2^{2n}}.$$

7. Let $(i, \alpha) \in \mathcal{I}_2$ and $(j, \beta) \in \mathcal{I}_3$. We distinguish three sub-cases.

(a) Assume that $j \in [q_e]$ and $\alpha \neq \beta$. Then $g_2(i, \alpha) = g_3(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_2 \oplus 2^{\beta-1}\Delta_4 = X_i[a_i + \alpha] \oplus C_{j,R}[\beta];\\ (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4 = M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j+\beta} X_j[\gamma]. \end{cases}$$

Since (Δ_2, Δ_4) is chosen uniformly at random from $(\{0, 1\}^n)^{*2}$, one has

$$\Pr\left[g_2(i,\alpha) = g_3(j,\beta)\right] \le \frac{1}{2^n(2^n-1)} \le \frac{2}{2^{2n}}$$

(b) Now assume that $j \in [q_e]$ and $\alpha = \beta$. If $M_i[\alpha] = M_j[\beta]$, then $X_i[a_i + \alpha] = X_j[a_j + \beta]$ therefore $g_2(i, \alpha) = g_3(j, \beta)$ if and only if

$$\begin{cases} X_j[a_j + \beta] \oplus 2^{\beta - 1} \Delta_2 = C_{j,R}[\beta] \oplus 2^{\beta - 1} \Delta_4; \\ X_j[a_j + \beta] = M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j + \beta - 1} X_j[\gamma]. \end{cases}$$

Otherwise, $g_2(i, \alpha) = g_3(j, \beta)$ if and only if

$$2^{\beta-1}\Delta_2 = C_{j,R}[\beta] \oplus X_i[a_i + \alpha] \oplus 2^{\beta-1}\Delta_4;$$

$$X_j[a_j + \beta] = M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus \bigoplus_{\gamma=1}^{a_j+\beta-1} X_j[\gamma]$$

For both cases, since Δ_2 is chosen uniformly at random from $\{0, 1\}^n \setminus \Delta_4$ and $X_j[a_j + \beta]$ is chosen uniformly at random from the set of size at least $2^n - q_e$, one has

$$\Pr\left[g_2(i,\alpha) = g_3(j,\beta)\right] \le \frac{1}{(2^n - 1)(2^n - q_e)} \le \frac{4}{2^{2n}}$$

(c) Assume that $j \notin [q_e]$. Since $(j, \beta) \in \mathcal{I}_3$, $Y_j[\beta]$ is chosen uniformly at random from the set of size at least $2^n - q$. Now, $g_2(i, \alpha) = g_3(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_2 = C_{j,R}[\beta] \oplus X_i[a_i + \alpha] \oplus 2^{\beta-1}\Delta_4; \\ Y_j[\beta] = M_{i,R}[\alpha] \oplus M_{j,R}[\beta] \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4. \end{cases}$$

Since Δ_2 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_4\}$ and $Y_j[\beta]$ is chosen uniformly at random from the set of size at least $2^n - q$, one has

$$\Pr\left[g_2(i,\alpha) = g_3(j,\beta)\right] \le \frac{1}{(2^n - 1)(2^n - q)} \le \frac{4}{2^{2n}}.$$

To sum up, we have

$$\Pr\left[\mathsf{OC}_{2,3}\right] \le \sum_{(j,\beta)\in\mathcal{I}_3} \sum_{(i,\alpha)\in\mathcal{I}_2} \frac{4}{2^{2n}} \le \frac{4\,|\mathcal{I}_2|\,|\mathcal{I}_3|}{2^{2n}}.$$

8. Let $(i, \alpha) \in \mathcal{I}_2$ and $(j, \beta) \in \mathcal{I}_4$. Then $g_2(i, \alpha) = g_4(j, \beta)$ if and only if

$$2^{\beta-1}\Delta_1 = X_i[a_i + \alpha] \oplus C_{j,L}[\beta] \oplus 2^{\beta-1}\Delta_3;$$

$$2^{\beta-1}\Delta_2 = M_{i,R}[\alpha] \oplus C_{j,R}[\beta] \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4.$$

Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n \setminus \{\Delta_3, \Delta_4\})^{*2}$, one has

$$\Pr\left[g_2(i,\alpha) = g_4(j,\beta)\right] \le \frac{1}{(2^n - 2)(2^n - 3)} \le \frac{4}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{2,4}\right] \le \sum_{(j,\beta)\in\mathcal{I}_4} \sum_{(i,\alpha)\in\mathcal{I}_2} \frac{4}{2^{2n}} \le \frac{4|\mathcal{I}_2||\mathcal{I}_4|}{2^{2n}}.$$

9. Let $(i, \alpha) \in \mathcal{I}_2$ and $j \in [q_e]$. Then $g_2(i, \alpha) = (V_j, T_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus \bigoplus_{\beta=1}^{a_j+m_j} X_j[\beta];\\ T_j = X_i[a_i+\alpha]. \end{cases}$$

Since Δ_4 and T_i are chosen uniformly at random from $\{0, 1\}^n$, respectively, one has

$$\Pr\left[g_2(i,\alpha) = (V_j, T_j)\right] \le \frac{1}{2^{2n}}$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{2,5}\right] \le \sum_{j \in q_e} \sum_{(i,\alpha) \in \mathcal{I}_2} \frac{1}{2^{2n}} \le \frac{q_e |\mathcal{I}_2|}{2^{2n}}$$

10. Since $IC_{4,4} = OC_{3,3}$,

$$\Pr\left[\mathsf{OC}_{3,3}\right] \le \frac{4\,|\mathcal{I}_4|^2}{2^{2n}}.$$

11. Let $(i, \alpha) \in \mathcal{I}_3$ and $(j, \beta) \in \mathcal{I}_4$. Then $g_3(i, \alpha) = g_4(j, \beta)$ if and only if

$$\begin{cases} 2^{\beta-1}\Delta_2 = C_{j,R}[\beta] \oplus 2^{\beta-1}\Delta_4 \oplus Y_i[\alpha];\\ 2^{\alpha-1}\Delta_2 \oplus 2^{\beta-1}\Delta_1 = C_{i,R}[\alpha] \oplus C_{j,L}[\beta] \oplus 2^{\beta-1}\Delta_3 \oplus 2^{\alpha-1}\Delta_4. \end{cases}$$

Note that $Y_i[\alpha]$ is independent of Δ_1 and Δ_2 whether $i \in [q_e]$ or not. Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n \setminus \{\Delta_3, \Delta_4\})^{*2}$, one has

$$\Pr\left[g_3(i,\alpha) = g_4(j,\beta)\right] \le \frac{1}{(2^n - 2)(2^n - 3)} \le \frac{4}{2^{2n}}.$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{3,4}\right] \leq \sum_{(j,\beta)\in\mathcal{I}_4} \sum_{(i,\alpha)\in\mathcal{I}_3} \frac{4}{2^{2n}} \leq \frac{4\left|\mathcal{I}_3\right|\left|\mathcal{I}_4\right|}{2^{2n}}.$$

12. Let $(i, \alpha) \in \mathcal{I}_3$ and $j \in [q_e]$. We distinguish two sub-cases.

(a) Let $i \in [q_e]$. Then $g_3(i, \alpha) = (V_i, T_i)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_4 = M_{i,R}[\alpha] \oplus \bigoplus_{\beta=1}^{a_i+\alpha} X_i[\alpha] \oplus \bigoplus_{\beta=1}^{a_j+m_j} X_j[\beta];\\ T_j \oplus 2^{\alpha-1}\Delta_4 = C_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_2. \end{cases}$$

Since Δ_4 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_2\}$ and T_j is chosen uniformly at random from $\{0, 1\}^n$, respectively, one has

$$\Pr\left[g_3(i,\alpha) = (V_j, T_j)\right] \le \frac{1}{2^n (2^n - 1)} \le \frac{2}{2^{2n}}.$$

(b) Let $i \notin [q_e]$. If there exists $i' \in [q_e]$ such that $C_i[\alpha] = C_{i'}[\alpha]$, this case is same as the case that $i \in [q_e]$. Otherwise, $g_3(i, \alpha) = (V_j, T_j)$ if and only if

$$\begin{cases} Y_i[\alpha] = \bigoplus_{\beta=1}^{a_j+m_j} X_j[\beta]; \\ T_j = C_{i,R}[\alpha] \oplus 2^{\alpha-1} \Delta_2 \oplus 2^{\alpha-1} \Delta_4 \end{cases}$$

Since T_j is chosen uniformly at random from $\{0, 1\}^n$ and $Y_i[\alpha]$ is chosen uniformly at random from the set of size at least $2^n - q$, one has

$$\Pr\left[g_3(i,\alpha) = (V_j, T_j)\right] \le \frac{1}{2^n (2^n - q)} \le \frac{2}{2^{2n}}$$

To sum up, we have

$$\Pr\left[\mathsf{OC}_{3,5}\right] \le \sum_{j \in [q_e]} \sum_{(i,\alpha) \in \mathcal{I}_3} \frac{2}{2^{2n}} \le \frac{2q_e \, |\mathcal{I}_3|}{2^{2n}}$$

13. Let $((i, \alpha), (j, \beta)) \in \mathcal{I}_4^{*2}$. If $\alpha = \beta$, then $C_i[\alpha] \neq C_j[\beta]$ so $g_4(i, \alpha) \neq g_4(j, \beta)$. Now assume $\alpha \neq \beta$. Then $g_4(i, \alpha) = g_4(j, \beta)$ if and only if

$$\begin{cases} (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_1 = C_{i,L}[\alpha] \oplus C_{j,L}[\beta] \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_3; \\ (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_2 = C_{i,R}[\alpha] \oplus C_{j,R}[\beta] \oplus (2^{\alpha-1} \oplus 2^{\beta-1})\Delta_4. \end{cases}$$

Since (Δ_1, Δ_2) is chosen uniformly at random from $(\{0, 1\}^n \setminus \{\Delta_3, \Delta_4\})^{*2}$, one has

$$\Pr\left[g_4(i,\alpha) = g_4(j,\beta)\right] \le \frac{1}{(2^n - 2)(2^n - 3)} \le \frac{4}{2^{2n}}$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{4,4}\right] \le \frac{4 \, |\mathcal{I}_4|^2}{2^{2n}}$$

14. Let $(i, \alpha) \in \mathcal{I}_4$ and $j \in [q_e]$. Then $g_4(i, \alpha) = (V_j, T_j)$ if and only if

$$\begin{cases} 2^{\alpha-1}\Delta_2 = C_{i,R}[\alpha] \oplus 2^{\alpha-1}\Delta_4 \oplus V_j; \\ T_j = C_{i,L}[\alpha] \oplus 2^{\alpha-1}\Delta_1 \oplus 2^{\alpha-1}\Delta_3. \end{cases}$$

Note that V_j is independent of Δ_2 . Since Δ_2 is chosen uniformly at random from $\{0, 1\}^n \setminus \{\Delta_1, \Delta_3, \Delta_4\}$ and T_j is chosen uniformly at random from $\{0, 1\}^n$, respectively, one has

$$\Pr\left[g_4(i,\alpha) = (V_j, T_j)\right] \le \frac{2}{2^{2n}}$$

Therefore, we have

$$\Pr\left[\mathsf{OC}_{4,5}\right] \leq \sum_{j \in [q_e]} \sum_{(i,\alpha) \in \mathcal{I}_4} \frac{2}{2^{2n}} \leq \frac{2q_e\mathcal{I}_4}{2^{2n}}.$$

- 15. Let $(i, j) \in [q_e]^{*2}$. We distinguish two sub-cases.
 - (a) First, assume $m_i \neq m_j$. Without loss of generality, we can assume that $m_i < m_j$. In this case, $(V_i, T_i) = (V_j, T_j)$ if and only if

$$\begin{cases} X_j[a_j + m_j] = V_i \oplus \bigoplus_{\alpha=1}^{a_j + m_j - 1} X_j[\alpha]; \\ T_j = T_i. \end{cases}$$

Since $X_j[a_j + m_j]$ is chosen uniformly at random from the set of size at least $2^n - q_e$ and T_j is chosen uniformly at random from $\{0, 1\}^n$, one has

$$\Pr\left[(V_i, T_i) = (V_j, T_j)\right] \le \frac{1}{2^n (2^n - q_e)} \le \frac{2}{2^{2n}}.$$

(b) Now assume that $m_i = m_j$. Since there is no redundant query, there exists at least one index *h* such that $M_i[h] \neq M_j[h]$. In this case, $(V_i, T_i) = (V_j, T_j)$ if and only if

$$\begin{cases} X_j[a_j+h] = V_i \oplus \bigoplus_{\alpha \neq a_j+h} X_j[\alpha]; \\ T_j = T_i. \end{cases}$$

Since $X_j[a_j + h]$ is chosen uniformly at random from the set of size at least $2^n - q_e$ and T_j is chosen uniformly at random from $\{0, 1\}^n$, one has

$$\Pr\left[(V_i, T_i) = (V_j, T_j)\right] \le \frac{1}{2^n (2^n - q_e)} \le \frac{2}{2^{2n}}.$$

To sum up, we have

$$\Pr\left[\mathsf{OC}_{5,5}\right] \le \sum_{(i,j)\in[q_e]^{*2}} \frac{2}{2^{2n}} \le \frac{2q_e^2}{2^{2n}}$$

Now using $|\mathcal{I}_1| + |\mathcal{I}_2| \le \sigma$, $|\mathcal{I}_1| + |\mathcal{I}_3| \le \sigma$, and $|\mathcal{I}_i| \le \sigma$ for $1 \le i \le 4$, we conclude the lemma.

We distinguish 35 cases, which is denoted by TwColl, IC, or OC. All in all, since $|\mathcal{I}_r| \leq \sigma$ for $r \in [4]$, one get

$$\Pr\left[\mathsf{bad}_2 \land \neg \mathsf{bad}_1\right] \le \frac{48\sigma^2 + 18q\sigma + 6q^2}{2^{2n}} + \frac{6\sigma + 2q}{2^n}.$$

6 Conclusion

In this paper, we proposed two tweakable block cipher-based online authenticated encryption schemes ZLR and DS-ZLR, following the Encrypt-Mix-Encrypt paradigm. Our schemes turn out to provide *n*-bit OAE security, supporting pipelined computation as well as online nonce-misuse resistance. We believe that our AE schemes will be useful in protocols where high security and efficiency are required at the same time, in particular, when latency is critical and online properties are required, for example, for VoIP, teleconference and Car2X communications. It is open if the provable security of ZLR and DS-ZLR are tight, and if they also provide more advanced security notions such as Release of Unverified Plaintext (RUP) security. We leave them as interesting topics for further research.

Acknowledgements This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No.2021R1F1A1047146).

Author contributions W.C, S.H, and B.L. discussed the main idea of this submission, and they wrote most of the manuscript. J.L supervised the overall research direction, and revised the manuscript. All the authors reviewed the manuscript.

Funding Open Access funding enabled and organized by KAIST.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

- Andreeva E., Bilgin B., Bogdanov A., Luykx A., Mennink B., Mouha N., Yasuda K.: APE: authenticated permutation-based encryption for lightweight cryptography. In: Fast Software Encryption: 21st International Workshop, FSE 2014, London, UK, March 3–5: Revised Selected Papers 21, pp. 168–186. Springer, Berlin (2015).
- 2. Andreeva E., Bogdanov A., Luykx A., Mennink B., Tischhauser E., Yasuda K.: AES-COPA v (2015).
- Andreeva E., Lallemand V., Purnal A., Reyhanitabar R., Roy A., Vizár D.: Forkcipher: a new primitive for authenticated encryption of very short messages. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 153–182. Springer, Cham (2019).
- 4. Andreeva E., Bhati A.S., Preneel B., Vizár D.: 1, 2, 3, fork: counter mode variants based on a generalized forkcipher. In: Cryptology ePrint Archive (2021).
- Bao Z., Guo J., Iwata T., Minematsu K.: ZOCB and ZOTR: tweakable blockcipher modes for authenticated encryption with full absorption. In: IACR Transactions on Symmetric Cryptology, pp. 1–54 (2019).
- Bellare M., Rogaway P., Wagner D.: The EAX mode of operation. In: Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5–7: Revised Papers 11, pp. 389–407. Springer, Berlin (2004).
- Bertoni G., Daemen J., Peeters M., Van Assche G.: Duplexing the sponge: single-pass authenticated encryption and other applications. In: Selected Areas in Cryptography: 18th International Workshop, SAC: Toronto, ON, Canada, August 11–12, 2011, Revised Selected Papers 18, pp. 320–337. Springer, Berlin (2012).
- Bhattacharya S., Nandi M.: Revisiting variable output length XOR pseudorandom function. In: IACR Transactions on Symmetric Cryptology, pp. 314–335 (2018).
- 9. Chakraborti A., Datta N., Jha A., Lopez C.M., Nandi M., Sasaki Y.: Lotus-aead and locus-aead. Submission to the NIST Lightweight Cryptography Project (2019).
- Chakraborti A., Datta N., Jha A., Mancillas-López C., Nandi M.: Light-OCB: parallel lightweight authenticated cipher with full security. In: International Conference on Security, Privacy, and Applied Cryptography Engineering, pp. 22–41. Springer, Cham (2021).
- Daemen J., Mennink B., Van Assche G.: Full-state keyed duplex with built-in multi-user support. In: Advances in Cryptology-ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part II 23, pp. 606–637. Springer (2017).
- Datta N., Nandi M.: ELmE: A misuse resistant parallel authenticated encryption. In: Information Security and Privacy: 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7–9, 2014. Proceedings 19, pp. 306–321. Springer (2014).
- Fleischmann E., Forler C., Lucks S.: McOE: A family of almost foolproof on-line authenticated encryption schemes. In: Fast Software Encryption: 19th International Workshop, FSE 2012, Washington, DC, USA, March 19–21: Revised Selected Papers, pp. 196–215. Springer, Berlin (2012).
- Grochow T., List E., Nandi M.: Dovemac: a tbc-based PRF with smaller state, full security, and high rate. In: IACR Transactions on Symmetric Cryptology, pp. 43–80 (2019).

- Gueron S., Lindell Y.: GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 109–119 (2015).
- Hoang V.T., Tessaro S.: Key-alternating ciphers and key-length extension: exact bounds and multi-user security. In: Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14–18, 2016, Proceedings, Part I 36, pp. 3–32. Springer, Berlin (2016).
- Hoang V.T., Krovetz T., Rogaway P.: Robust authenticated-encryption AEZ and the problem that it solves. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 15–44. Springer, Berlin (2015).
- Hoang V.T., Reyhanitabar R., Rogaway P., Vizár D.: Online authenticated-encryption and its nonce-reuse misuse-resistance. In: Advances in Cryptology–CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16–20, 2015, Proceedings, Part I 35, pp. 493–517. Springer, Berlin (2015).
- Iwata T., Minematsu K., Peyrin T., Seurin Y.: ZMAC: a fast tweakable block cipher mode for highly secure message authentication. In: Annual International Cryptology Conference, pp. 34–65. Springer, Cham (2017).
- 20. Jean J., Nikolic I., Peyrin T., Seurin Y.: Deoxys v1. 41. Submitted to CAESAR, p. 124 (2016).
- Krovetz T., Rogaway P.: The software performance of authenticated-encryption modes. In: Fast Software Encryption: 18th International Workshop, FSE: Lyngby, Denmark, February 13–16, 2011, Revised Selected Papers 18, pp. 306–327. Springer, Berlin (2011).
- 22. Leuven E.A.K., Leuven A.L.K., Leuven B.M.K.: COLM v1 (2016).
- Liskov M., Rivest R.L., Wagner D.: Tweakable block ciphers. In: Advances in Cryptology. CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings 22, pp. 31–46. Springer, Berlin (2002).
- McGrew D.A., Viega J.: The security and performance of the Galois/counter mode (GCM) of operation. In: International Conference on Cryptology in India, pp. 343–355. Springer, Berlin (2004).
- 25. Minematsu K., Iwata T.: Tweak-length extension for tweakable blockciphers. In: IMA International Conference on Cryptography and Coding, pp. 77–93. Springer, Cham (2015).
- Patarin J.: The "coefficients H" technique. In: International Workshop on Selected Areas in Cryptography, pp. 328–345. Springer, Berlin (2008).
- Peyrin T., Seurin Y.: Counter-in-tweak: authenticated encryption modes for tweakable block ciphers. In: Annual International Cryptology Conference, pp. 33–63. Springer, Berlin (2016).
- Rogaway P., Shrimpton T.: A provable-security treatment of the key-wrap problem. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 373–390. Springer, Berlin (2006).
- 29. Whiting D., Housley R., Ferguson N.: Counter with cbc-mac (ccm) (No. rfc3610) (2003).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.