

PAE: Towards More Efficient and BBB-secure AE From a Single Public Permutation*

Arghya Bhattacharjee¹, Ritam Bhaumik², Avijit Dutta³, Eik List⁴

Indian Statistical Institute
École polytechnique fédérale de Lausanne, Switzerland
Institute for Advancing Intelligence, TCG CREST
Nanyang Technological University, Singapore
bhattacharjeearghya29@gmail.com, ritam.bhaumik@epfl.ch avirocks.dutta13@gmail.com,
eik.list@ntu.edu.sg

Abstract. Four recent trends have emerged in the evolution of authenticated encryption schemes: (1) Regarding simplicity, the adoption of public permutations as primitives allows for sparing a key schedule and the need for storing round keys; (2) using the sums of permutation outputs, inputs, or outputs has been a well-studied means to achieve higher security beyond the birthday bound; (3) concerning robustness, schemes should provide graceful security degradation if a limited amount of nonces repeats during the lifetime of a key, and (4) Andreeva et al.’s ForkCipher approach can increase the efficiency of a scheme since they can use fewer rounds per output branch compared to full-round primitives.

In this work, we improve on the state of the art by combining those aspects for efficient authenticated encryption. We propose PAE, an efficient nonce-based AE scheme that employs a public permutation and one call to an XOR-universal hash function. PAE provides $O(2n/3)$ -bit security and high throughput by combining forked public-permutation-based variants of nEHtM and an Encrypted Davies-Meyer. Thus, it can use a single, in part round-reduced, public permutation for most operations, spare a key schedule, and guarantee security beyond the birthday bound even under limited nonce reuse.

Keywords: Symmetric-key cryptography · Permutation · Provable Security.

1 Introduction

Public-permutation-based Authenticated Encryption. Designing secure and efficient authenticated-encryption schemes is a key task in symmetric-key cryptography. Its understanding has been increasing continuously over the past decade, where one can identify at least four recent trends in the design of symmetric-key schemes: using public permutations; providing beyond-birthday-bound (BBB) security; offering additional robustness against, and graceful security degradation under, nonce reuse; and using forked primitives for higher efficiency. The use of public permutations has been established as a promising approach for designing AE schemes since the selection of Keccak as the SHA-3 standard and the proposal of Duplex. Since then, a plenty of AE schemes have been build out of public permutation that includes Ascon [21], Oribatida [10], Beetle [11], Elephant [7,6], ISAP [20], ISAP+ [8],

*An extended abstract of this paper is included in the proceedings of ICICS 2023.

Gimli [5], Xoodyak [19], APE [1], APE+ [33] etc.¹ Public permutations can spare an often sophisticated study of the key-schedule effects on the security of the primitive and save implementations from the need for computing and storing numerous round keys.

Compared to schemes based on block or stream ciphers, a permutation-based construction often possess the disadvantage of security guarantees. When simply replacing keyed with unkeyed primitives in an existing scheme, the result would suffer from a birthday-bound security limitation. While this is less of an issue when the primitive’s block length is high or the message-processing rate is low, both measures considerably reduce the efficiency. For higher security in settings where bigger permutations or small rates are undesirable, a second research trend has emerged from the use of summing multiple states, after a series of works [14,16,17,18,27] established the sum of outputs from independent permutations as an effective means for increasing the security beyond the birthday bound.

For nonce-based authenticated encryption, a third desideratum of AE schemes is robustness against occasional nonce repetitions. When possible, the security of schemes should not collapse when relatively few nonces are repeated (as would, for example, that of GCM) but rather degrade gracefully – usually to the birthday bound. Thus, one should study its security in the faulty-nonce model [23] and study the effects of nonce repetitions in depth.

On top of those three, modern schemes should be efficient, and, given that numerous metrics of efficiency exist, we consider throughput in this work. For this purpose, Andreeva et al. introduced ForkCiphers and the Iterate-Fork-Iterate paradigm [2] as a promising higher-level concept. At its core, Iterate-Fork-Iterate means to iterate a set of rounds, to fork (i.e. copy) the middle state into multiple branches, and to iterate over more rounds of separate reduced permutations on each branch to produce multiple independent outputs. Since the forked state is secret, forked primitives can use fewer rounds than the full permutation and therefore can achieve higher efficiency.

Contribution. In this work, we propose PAE, a nonce-based authenticated encryption scheme built from a public permutation that improves on the state of the art in all four aspects above. For encryption, it uses a forked and public-permutation-based variant of Encrypted Davies-Meyer [27]. For authentication, it forks the well-known nonce-based Encrypt-Hash-then-MAC [29] to obtain a more efficient variant of [15,22]. PAE provides $O(2n/3)$ -bit security when instantiated with public permutations also if up to $O(2^{n/3})$ queries repeat nonces. Thus, PAE can achieve high efficiency and BBB security simultaneously. Note that PAE achieves BBB security w.r.t. the number of queries or the number of query blocks, not w.r.t. the query length. We implemented our proposal on ARM-32 microcontrollers with Chaskey-8 [31] and two parallel instances of the hash function from MAC611 [25] showcasing the efficiency on such platforms.

In the remainder, we give the necessary preliminaries in Section 2, properly define our proposal in Section 3, and give our analysis in Section 4, before we report on the results of an implementation for microcontrollers in Section 6.

2 Preliminaries

Notations. For a set \mathcal{X} , $X \leftarrow \mathcal{X}$ denotes that X is sampled uniformly at random from \mathcal{X} and is independent of all other random variables defined so far. $\{0, 1\}^n$ denotes the set of all

¹We deliberately keep block cipher and tweakable block cipher based AE schemes out of the discussion as this paper studies only permutation based AE.

binary strings of length n and $\{0, 1\}^*$ denotes the set of all binary strings of finite arbitrary length. For any element $x \in \{0, 1\}^*$, $|x|$ denotes the number of bits in x . For any two elements $x, y \in \{0, 1\}^*$, $x||y$ denotes the concatenation of x followed by y . For $x, y \in \{0, 1\}^n$, $x \oplus y$ denotes the bitwise xor of x and y . For a sequence of elements $(x_1, x_2, \dots, x_s) \in \{0, 1\}^*$, x_a^i denotes the a -th block of i -th element x_i . The set of all permutations over \mathcal{X} is denoted as $\text{Perm}(\mathcal{X})$ and Perm denotes the set of all permutations over $\{0, 1\}^n$. For integers $1 \leq b \leq a$, $(a)_b$ denotes $a(a-1)\dots(a-b+1)$, where $(a)_0 = 1$ by convention. $[q]$ refers to the set $\{1, \dots, q\}$ and $[q_1, q_2]$ to the set $\{q_1, q_1 + 1, \dots, q_2 - 1, q_2\}$.

Nonce-based AE From a Public Permutation. A nonce-based authenticated encryption (AE) scheme \mathcal{E} is a triplet of algorithms $\mathcal{E} = (\mathcal{E}.\text{KGen}, \mathcal{E}.\text{Enc}, \mathcal{E}.\text{Dec})$, where the key-generation algorithm $\mathcal{E}.\text{KGen}$, on input 1^n , returns a n -bit key $k \leftarrow \mathcal{K}$. The encryption algorithm $\mathcal{E}.\text{Enc}$ is a function

$$\mathcal{E}.\text{Enc} : \mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{M} \rightarrow \mathcal{C} \times \mathcal{T},$$

that takes as input a key $k \in \mathcal{K}$ (key space) a unique nonce $\nu \in \mathcal{N}$ (nonce space), an associated data $A \in \mathcal{AD}$ (associated data space) and a message $M \in \mathcal{M}$ (message space) and it returns a ciphertext, tag pair $(C, T) \in \mathcal{C} \times \mathcal{T}$, where \mathcal{C} is called the ciphertext space and \mathcal{T} is called the tag space. We assume that $\mathcal{E}.\text{Enc}$ makes internal calls to the n -bit public random permutations $\mathbf{P} = (\mathbf{P}_1, \dots, \mathbf{P}_d)$ for $d \geq 1$ and $n \in \mathbb{N}$, where all of the d permutations are independent and uniformly sampled from Perm . We write $\mathcal{E}.\text{Enc}_k^{\mathbf{P}}$ to denote $\mathcal{E}.\text{Enc}_k$ with uniform k and uniform \mathbf{P} . Likewise, the decryption algorithm $\mathcal{E}.\text{Dec}$ is a function

$$\mathcal{E}.\text{Dec} : \mathcal{K} \times \mathcal{N} \times \mathcal{AD} \times \mathcal{C} \times \mathcal{T} \rightarrow \mathcal{M} \cup \{\perp\},$$

that takes as input a key, nonce, associated data, ciphertext, and tag and returns either a valid message or the abort symbol \perp . Again, we assume that $\mathcal{E}.\text{Dec}$ makes internal calls to the n -bit public random permutations \mathbf{P} . We write $\mathcal{E}.\text{Dec}_k^{\mathbf{P}}$ to denote $\mathcal{E}.\text{Dec}_k$ with uniform k and uniform \mathbf{P} . The correctness condition of the public permutation-based authenticated encryption scheme says that for every $k \in \mathcal{K}$, $\nu \in \mathcal{N}$, $A \in \mathcal{A}$, $M \in \mathcal{M}$, and d -tuple of n -bit permutations \mathbf{P} ,

$$\mathcal{E}.\text{Dec}_k^{\mathbf{P}}(\nu, A, \mathcal{E}.\text{Enc}_k^{\mathbf{P}}(\nu, A, M)) = M.$$

A distinguisher \mathbf{D} is given access to either of the pair of oracles $(\mathcal{E}.\text{Enc}_k^{\mathbf{P}}, \mathcal{E}.\text{Dec}_k^{\mathbf{P}})$ in the real world or a pair of oracles $(\text{Rand}, \text{Rej})$ in the ideal world, where the oracle Rand returns (C, T) that is uniformly sampled from $\mathcal{C} \times \mathcal{T}$ on input (ν, A, M) and the oracle Rej always returns \perp on input (ν, A, C, T) . Apart from making queries to this pair of oracles in either of the worlds, \mathbf{D} can also make queries to the permutations \mathbf{P} and \mathbf{P}^{-1} in both of these worlds. We call the distinguisher \mathbf{D} to be *nonce-respecting* if \mathbf{D} never makes any queries to the encryption oracle with repeating nonces. However, \mathbf{D} is allowed to make queries to the decryption oracle with repeating nonces. We define the nonce based AE advantage of \mathbf{D} against \mathcal{E} in the public permutation model as

$$\text{Adv}_{\mathcal{E}}^{\text{nAE}}(\mathbf{D}) := \left| \Pr \left[\mathbf{D}^{(\mathcal{E}.\text{Enc}_k^{\mathbf{P}}, \mathcal{E}.\text{Dec}_k^{\mathbf{P}}, \mathbf{P}, \mathbf{P}^{-1})} \Rightarrow 1 \right] - \Pr \left[\mathbf{D}^{(\text{Rand}, \text{Rej}, \mathbf{P}, \mathbf{P}^{-1})} \Rightarrow 1 \right] \right|,$$

where \mathbf{D} is a nonce-respecting adversary and the above probability is defined over the randomness of $k \leftarrow \mathcal{K}$, $\mathbf{P}_1, \dots, \mathbf{P}_d \leftarrow \text{Perm}$ and the randomness of the distinguisher (if any). In this paper, we omit the time of the distinguisher and assume that the distinguisher is

computationally unbounded and hence deterministic. We say D is a (q_e, q_d, q_p) distinguisher if D makes total q_e encryption queries, q_d decryption queries and q_p primitive queries that include both the forward and inverse queries. We write

$$\mathbf{Adv}_{\mathcal{E}}^{\text{nAE}}(q_e, q_d, q_p) := \max_D \mathbf{Adv}_{\mathcal{E}}^{\text{nAE}}(D),$$

where the maximum is taken over all (q_e, q_d, q_p) -distinguishers D .

Almost-XOR-Universal and Almost-regular Hash Function. Let \mathcal{K}_h and \mathcal{X} be two non-empty finite sets and H be a keyed function $H : \mathcal{K}_h \times \mathcal{X} \rightarrow \{0, 1\}^n$. Then, H is called an ϵ_{axu} -almost-xor-universal (axu) hash function, if for any distinct $x, x' \in \mathcal{X}$ and for any $y \in \{0, 1\}^n$,

$$\Pr [k_h \leftarrow \mathcal{K}_h : H_{k_h}(x) \oplus H_{k_h}(x') = y] \leq \epsilon_{\text{axu}}.$$

Moreover, H is said to be an ϵ_{reg} -almost-regular (ar) hash function, if for any $x \in \mathcal{X}$ and for any $y \in \{0, 1\}^n$,

$$\Pr [k_h \leftarrow \mathcal{K}_h : H_{k_h}(x) = y] \leq \epsilon_{\text{reg}}.$$

Pairwise Independent Hash Function. Let \mathcal{K}_h and \mathcal{X} be two non-empty finite sets and H be a keyed function $H : \mathcal{K}_h \times \mathcal{X} \rightarrow \{0, 1\}^n$. Then, H is said to be an δ -pairwise independent hash function, if for any distinct $x, x' \in \mathcal{X}$ and for any $y, y' \in \{0, 1\}^n$,

$$\Pr [k_h \leftarrow \mathcal{K}_h : H_{k_h}(x) = y, H_{k_h}(x') = y'] \leq \delta.$$

If H is an ϵ_{axu} -almost-xor universal hash function, then $H'_{(k_h, k)} := H_{k_h} \oplus k$, where $k \in \{0, 1\}^n$ is independently sampled over k_h , is $\epsilon_{\text{axu}}/2^n$ -pairwise independent hash function. This is because for any $x \neq x'$ and for any $y, y' \in \{0, 1\}^n$,

$$\begin{aligned} & \Pr [k_h \leftarrow \mathcal{K}_h, k \leftarrow \{0, 1\}^n : H'_{(k_h, k)}(x) = y, H'_{(k_h, k)}(x') = y'] \\ &= \Pr [k_h \leftarrow \mathcal{K}_h, k \leftarrow \{0, 1\}^n : H_{k_h}(x) \oplus k = y, H_{k_h}(x') \oplus k = y'] \\ &= \Pr [k_h \leftarrow \mathcal{K}_h, k \leftarrow \{0, 1\}^n : H_{k_h}(x) \oplus k = y, H_{k_h}(x) \oplus H_{k_h}(x') = y \oplus y'] \\ &\leq \epsilon_{\text{axu}}/2^n. \end{aligned}$$

3 Definition of PAE

In this section, we propose PAE, a beyond-birthday-bound secure nonce-based authenticated encryption scheme based on public permutation in the faulty nonce model. Our construction employs two basic components: the first is a public-permutation-based variable-output-length PRF ForkEDM_p and the other one is a public-permutation- and nonce-based MAC ForknEHtM_p . We combine them in Encrypt-then-MAC style to obtain a nonce-based authenticated encryption scheme built on public permutations. In particular, on input (ν, a, m) , the encryption function first determines the number of blocks ℓ in the message m and then invokes the ForkEDM_p module with input (ν, ℓ) to generate ℓ many keystream blocks, which is then masked with the message blocks in one-time padding style to generate the ciphertext blocks. Then, it invokes the permutation-based MAC ForknEHtM_p with input the nonce, the associated data, and the ciphertext to generate the tag t . The decryption module of PAE works in a similar way. An algorithmic description of the construction is given in Algorithm 1. In the following, we show that PAE is a nonce-based authenticated encryption scheme built

Algorithm 1 Encryption and Decryption Function of PAE.

<pre> 1: function PAE.ENC[P, H]_{k_h, k}(ν, A, M) 2: (k₀, k₁) ← k 3: (M₁, ..., M_ℓ) ←ⁿ M 4: S ← ForkEDM_p[P]_{k₀, k₁}(ν, ℓ) 5: (S₁, ..., S_ℓ) ←ⁿ S 6: for i ← 1..ℓ do 7: C_i ← msb_{M_i}(S_i) ⊕ M_i 8: C ← (C₁ C₂ ... C_ℓ) 9: T ← ForkNEHTM_p[P, H]_{k_h, k₀, k₁}(ν, A, C) 10: return (C, T) </pre> <hr/> <pre> 11: function FORKEDM_p[P]_{k₀, k₁}(ν, ℓ) 12: X̂ ← P(fix₁₁(ν ⊕ k₀)) 13: for i ← 1..ℓ do 14: S_i ← P(fix₁₀(X̂ ⊕ 2ⁱ⁻¹ · (ν ⊕ k₀ ⊕ k₁))) ⊕ 2ⁱ⁻¹ · k₁ 15: S ← (S₁ ... S_ℓ) 16: return S </pre>	<pre> 21: function PAE.DEC[P, H]_{k_h, k}(ν, A, C, T) 22: (k₀, k₁) ← k 23: T* ← ForkNEHTM_p[P, H]_{k_h, k₀, k₁}(ν, A, C) 24: if T ≠ T* then 25: return ⊥ 26: (C₁, ..., C_ℓ) ←ⁿ C 27: S ← ForkEDM_p[P]_{k₀, k₁}(ν, ℓ) 28: (S₁, ..., S_ℓ) ←ⁿ S 29: for i ← 1..ℓ do 30: M_i ← msb_{C_i}(S_i) ⊕ M_i 31: M ← (M₁ M₂ ... M_ℓ) 32: return M </pre> <hr/> <pre> 33: function FORKNEHTM_p[P, H]_{k_h, k₀, k₁}(ν, A, C) 34: Ẑ ← P(fix₁₁(ν ⊕ k₁)) 35: Γ ← A C 36: T ← P(fix₀₀(Ẑ ⊕ k₀)) ⊕ P(fix₀₁(H_{k_h}(Γ) ⊕ Ẑ ⊕ k₀)) 37: return T </pre>
---	---

on n -bit public permutations that is secure roughly upto $2^{2n/3}$ encryption queries and 2^n decryption queries in the faulty nonce model.

Theorem 1 (AE Bound of PAE). *Let $\mathcal{M}, \mathcal{AD}$ and \mathcal{K}_h be three finite and non-empty sets. Let $P_0, P_1, P_2 \leftarrow \text{Perm}$ be three independent n -bit public random permutations and $H : \mathcal{K}_h \times \mathcal{M} \rightarrow \{0, 1\}^n$ be an n -bit ϵ_{axu} -almost xor universal and ϵ_{reg} -almost regular hash function. Moreover, let $\mathbf{K} = (k_0, k_1, k_2, k_3) \leftarrow \{0, 1\}^n$ denote the tuple of n -bit round keys, $K_h \leftarrow \mathcal{K}_h$ be a randomly sampled hash key and ρ and μ be two fixed parameters. Then the AE advantage for any $(\mu, q_e, q_d, \ell, \sigma)$ -nonce respecting adversary against PAE that makes at most μ faulty encryption queries out of q_e encryption, q_d decryption, and q_p primitive queries such that each message is at most ℓ blocks long, is given by*

$$\begin{aligned}
& \text{Adv}_{\text{PAE}}^{\text{nAE}}(\mu, q_e, q_d, \ell, \sigma) \\
& \leq \frac{1}{2^{2n}} \left(430\ell^2 \mu \sigma_e q_p^2 + 50211\ell^4 \sigma_e^2 q_p + 120\ell \sigma_e q_e q_p + 16q_e q_d q_p + 48\mu^2 q_p^2 \right. \\
& \quad + 5292\mu^2 q_e^2 + 1488\mu^2 q_e q_p + 240\ell \mu^2 q_e^{3/2} + 6000\ell^2 \mu^2 q_e + 2880\ell q_e^{5/2} \\
& \quad + 420\ell \sigma_e^2 \sqrt{q_e} + 3\ell^4 q_e^3 + 72\sigma_e^3 + 2q_d + \epsilon_{\text{reg}}(16\mu q_e q_d q_p^2 + 8q_e^2 q_p^2) \\
& \quad \left. + \epsilon_{\text{axu}}(12q_e^4 + 48q_e^3 q_p + 48q_e^2 q_p^2 + 1440\ell q_e^{5/2} q_p + 5520\ell q_e^{7/2} + 6000\ell^2 q_e^3) \right) \\
& + \frac{1}{2^n} \left(q_e^{3/2} + 2\ell^2 q_e + \mu(2q_e + q_d) + 14\ell \sqrt{q_e} q_p + (3\ell + 16)\mu q_p + 2\ell^2 \mu^2 \right. \\
& \quad \left. + \epsilon_{\text{axu}}(4q_e^3 + 4\mu q_e q_p^2 + 22\ell q_e^2 q_p) + \epsilon_{\text{reg}}(12q_e q_p^2 + 8\mu q_d q_p^2) \right) \\
& + 5\mu q_e \epsilon_{\text{axu}},
\end{aligned}$$

where $\xi = 2^n / 8q_e$.

Comparison. We note that the direction of using the sum of permutations with pruned primitives in encryption schemes has been proposed by Mennink and Neves [28] and has been transferred to public permutations recently [9]. In contrast to [9], we can simplify the domain separation and can use fewer rounds in the individual primitives. Compared to the very aggressive heuristic arguments in [28], our proposals are more robust. Naturally, our

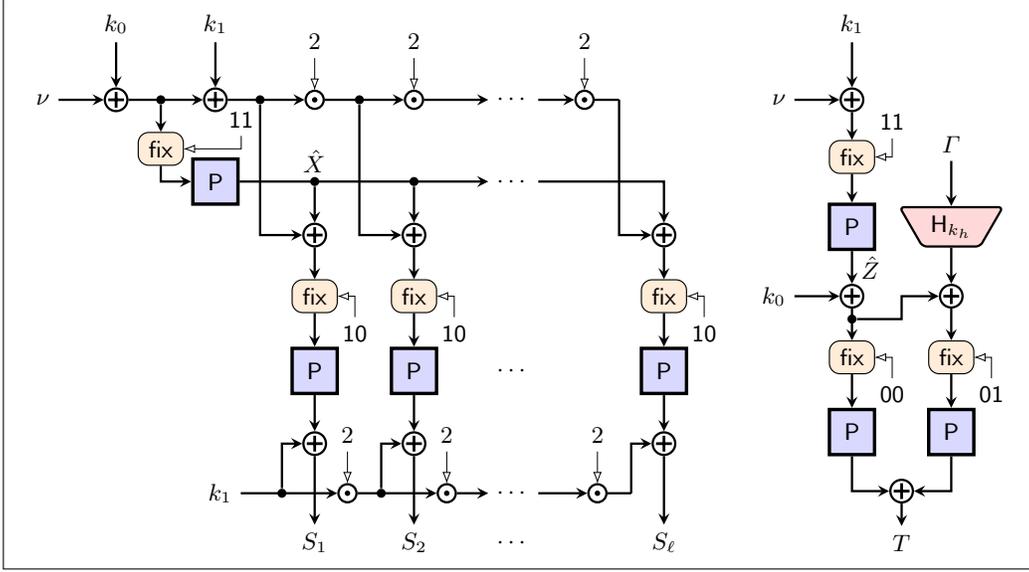


Fig. 1: The components of PAE, ForkEDM_p (left) and ForknEHtM_p (right). $S = (S_1, \dots, S_\ell)$ is used as a keystream to compute $C = M \oplus S$. $\Gamma = A||C$ is the input to H_{k_h} . The function `fix` replaces the first two bits of the input with a fixed constant.

authentication ForknEHtM_p is very similar to nEHtM_p^{*} as proposed by Chen et al. [15] and achieves a similar level of security. However, we can use forked primitives with fewer rounds while maintaining security.

4 Proof of Theorem 1

In this section, we prove Theorem 1. We shall often refer to the construction PAE[P, H] as simply PAE when the underlying primitives are assumed to be understood. To bound the AE advantage of the construction, we bound the distinguishing advantage of the two random systems: (i) the pair of oracles (PAE.Enc, PAE.Dec) for an n -bit random permutation P in the real world and (ii) the pair of oracles (Rand, Rej) in the ideal world. Let D be a computationally unbounded deterministic distinguisher that interacts with a pair of oracles in either of two worlds. We assume that D makes q_e encryption queries $(\nu_1, A^1, M^1), \dots, (\nu_{q_e}, A^{q_e}, M^{q_e})$ and receives $(C^1, T_1), \dots, (C^{q_e}, T_{q_e})$ as the corresponding responses. We also assume that D makes q_d decryption queries $(\nu'_1, A'^1, C'^1, T'_1), \dots, (\nu'_{q_d}, A'^{q_d}, C'^{q_d}, T'_{q_d})$ and receives (O^1, \dots, O^{q_d}) as the corresponding responses, where for each $i \in [q_d]$, $O^i \in \{0, 1\}^* \cup \{\perp\}$. For $i \in [q_e]$, we assume that M^i contains ℓ_i blocks (even when the last block is incomplete) and the total number of encryption message blocks as σ_e , where $\sigma_e = \ell_1 + \ell_2 + \dots + \ell_{q_e}$. Similarly, for $i \in [q_d]$, we assume that the ciphertext C'^i contains ℓ'_i blocks (even when the last block is incomplete) and the total number of decryption ciphertext blocks as σ_d , where $\sigma_d = \ell'_1 + \ell'_2 + \dots + \ell'_{q_d}$. In the real world, for each $i \in [q_e]$, we have

$$(C^i, T_i) \leftarrow \text{PAE.Enc}[P, H]_{k, k_h}(\nu_i, A^i, M^i)$$

Algorithm 2 Random oracle for the ideal world. Table $\text{Tb}_1[\nu]$ stores the updated number of keystream blocks for nonce ν and $\text{Tb}_2[\nu]$ stores the updated keystream blocks for nonce ν of length $\text{Tb}_1[\nu]$.

<pre> 11: procedure INITIALIZE 12: $\mathcal{D} \leftarrow \emptyset$; 13: $\text{Tb}_1[\cdot] \leftarrow \emptyset$ 14: $\text{Tb}_2[\cdot] \leftarrow \emptyset$ </pre>	<pre> 21: function QUERY(ν_i, A^i, M^i) 22: if $\nu_i \in \mathcal{D} \subseteq \{0, 1\}^n$ then $\nu_i = \nu$ 23: if $\ell_i = \text{Tb}_1[\nu]$ then $S^i \leftarrow \text{Tb}_2[\nu]$ 24: if $\ell_i < \text{Tb}_1[\nu]$ then $S^i \leftarrow (\text{Tb}_2[\nu])_{[n\ell_i]}$ 25: if $\ell_i > \text{Tb}_1[\nu]$ then 26: $R \leftarrow (\{0, 1\}^n)^{\ell_i - \text{Tb}_1[\nu]}$; $S^i \leftarrow \text{Tb}_2[\nu] \parallel R$ 27: $\text{Tb}_1[\nu] \leftarrow \ell_i$ 28: else 29: $S^i \leftarrow (\{0, 1\}^n)^{\ell_i}$; $\text{Tb}_2[\nu_i] \leftarrow S^i$; $\text{Tb}_1[\nu_i] \leftarrow \ell_i$ 30: $\mathcal{D} \leftarrow \mathcal{D} \cup \{\nu_i\}$ 31: $T_i \leftarrow \{0, 1\}^n$ 32: return $(S^i \oplus M^i, T_i)$ </pre>
---	---

for an n -bit uniform public random permutation P and for $2n$ -bit random keys $k = (k_0, k_1)$ with an independently chosen hash key k_h for the hash function H . Similarly, for each $i \in [qd]$, we have

$$O^i \leftarrow \text{PAE.Dec}[P, H]_{k, k_h}(\nu'_i, A^i, C^i, T'_i)$$

for an n -bit uniform public random permutation P_0 and for $2n$ -bit random keys $k = (k_0, k_1)$ with an independently chosen hash key k_h for H , where

$$O^i = \begin{cases} M^i & \text{if } (C^i, T'_i) \leftarrow \text{PAE.Enc}[P, H]_{k, k_h}(\nu'_i, A^i, M^i) \\ \perp & \text{otherwise} \end{cases}$$

Sampling in the Ideal World. In the ideal world, the outputs are sampled in a different way. We assume that all the queried messages to the encryption oracle, i.e., the Rand oracle of D are of length multiple of n , i.e., the last message block of the queried message is a complete block. Now, the encryption oracle in the ideal world, i.e., Rand , on the i -th encryption query (ν_i, A^i, M^i) works as shown in Alg. 2. If the nonce in the i -th queried message ν_i collides with some previously queried nonce, say ν_j for $j < i$, and $\ell_i = \ell_j$, then the output of the j -th query is assigned to the output of the i -th query. If $\ell_i < \ell_j$, then the output of the i -th query is assigned with the first $n\ell_i$ bits of the output of the j -th query. Finally, if $\ell_i > \ell_j$, then the output of the i -th query is the concatenation of the output of the j -th query with a random binary string of length $n(\ell_i - \ell_j)$ bits. If the nonce in the i -th query is fresh, it returns a uniformly sampled $n\ell_i$ -bit string. Finally, it uniformly and independently samples an n -bit tag T_i and returns ciphertext and tag to D .

Upon querying to the decryption oracle Rej of the ideal world with i -th decryption query (ν'_i, A^i, C^i, T'_i) , D always receives the authentication failure message \perp . Note that this is different from the real world because D receives the corresponding message M^i as the response of the decryption query (ν'_i, A^i, C^i, T'_i) from the real world if the authentication of the decryption query (ν'_i, A^i, C^i, T'_i) succeeds; otherwise D receives \perp .

Primitive Queries. As the proof is carried out in the random permutation model, we allow D to query the underlying permutation of the construction in both the forward and the

inverse direction. If the permutation query to P is a forward query, then we denote the query as U_j and the corresponding response as V_j . Similarly, if the permutation query to P is a backward query (i.e., inverse permutation query), then we denote the query as V_j and the corresponding response as U_j . We allow D to make forward queries to the underlying permutation P by setting the first two bits of the query to b , where $b \in \{00, 01, 10, 11\}$. Similarly, we allow D to make inverse query to the underlying permutation P^{-1} . Let

$$\text{Tr}_p^b = \{(U_1^b, V_1), (U_2^b, V_2), \dots, (U_{q_b^p}^b, V_{q_b^p}^b)\},$$

denote the transcript of q_b^p primitive queries, where $b \in \{00, 01, 10, 11\}$, such that for each $i \in [q_b^p]$, U_i^b denotes the input (resp. output) of the forward (resp. inverse) query with its two most significant bits set to b and V_i denotes the output (resp. input) of the corresponding forward (resp. inverse) query. For $b \in \{00, 01, 10, 11\}$, we denote \mathcal{U}^b to the set of input (resp. output) of the forward (resp. inverse) primitive queries to P (resp. P^{-1}) with its two most significant bits set to b and \mathcal{V}^b denotes the set of corresponding output (resp. input) of the forward (resp. inverse) primitive queries to P (resp. P^{-1}), i.e.,

$$\mathcal{V}^b := \{v : \exists u \in \mathcal{U}^b, v = \mathsf{P}(u)\}.$$

Let us define $\mathcal{U} := \mathcal{U}^{00} \cup \mathcal{U}^{01} \cup \mathcal{U}^{10} \cup \mathcal{U}^{11}$ as well as \mathcal{V} and Tr_p analogously. \mathcal{U} denotes the set of all inputs (resp. outputs) of the forward (resp. inverse) primitive queries and \mathcal{V} denotes the set of all corresponding outputs (resp. inputs) of the forward (resp. inverse) primitive queries. We also record the history of all the primitive queries of D in Tr_p , called the transcript of primitive queries. We also summarize the interaction of D with the encryption and decryption oracles in either of the two worlds in a transcript $\text{Tr} = \text{Tr}_e \cup \text{Tr}_d$, where

$$\text{Tr}_e = \{(\nu_1, A^1, M^1, C^1, T_1), (\nu_2, A^2, M^2, C^2, T_2), \dots, (\nu_{q_e}, A^{q_e}, M^{q_e}, C^{q_e}, T_{q_e})\}$$

is called the transcript of the encryption queries and

$$\text{Tr}_d = \{(\nu'_1, A'^1, C'^1, T'_1, O'^1), (\nu'_2, A'^2, C'^2, T'_2, O'^2), \dots, (\nu'_{q_d}, A'^{q_d}, C'^{q_d}, T'_{q_d}, O'^{q_d})\}$$

is called the transcript of the decryption queries. Once D is done with all its queries and responses, the challenger releases some additional information before D submits its decision bit. In fact, when D interacts with the oracles in the real world, the challenger releases the underlying $2n$ -bit keys $k = (k_0, k_1)$ and the hash key k_h which are used in the construction. It also releases the intermediate variables $\hat{Z}_i = \mathsf{P}(\nu_i \oplus k_1)$ for each $i \in [q_e] \cup [q_d]$, which are generated from the ForknEHtM_p construction. On the other hand, when D interacts with the oracles in the ideal world, the challenger samples a $2n$ -bit key $k = (k_0, k_1)$ uniformly at random and a random hash key k_h from the set of all hash keys and releases them to D . In addition to this, the ideal world computes $\hat{Z}_i = \mathsf{P}(\nu_i \oplus k_1)$ for every encryption queries and computes $\hat{Z}'_i = \mathsf{P}(\nu'_i \oplus k_1)$ for every decryption queries and release them to D . The overall attack transcript becomes $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$, where

$$\text{Tr}_e^* = \{(\nu_1, A^1, M^1, C^1, T_1, \hat{Z}_1), \dots, (\nu_{q_e}, A^{q_e}, M^{q_e}, C^{q_e}, T_{q_e}, \hat{Z}_{q_e})\}$$

be the transcript of the encryption queries and

$$\text{Tr}_d^* = \{(\nu'_1, A'^1, C'^1, T'_1, O'^1, \hat{Z}'_1), \dots, (\nu'_{q_d}, A'^{q_d}, C'^{q_d}, T'_{q_d}, O'^{q_d}, \hat{Z}'_{q_d})\}$$

be the transcript of the decryption queries. The transcript of the primitive queries remains the same. Let X_{re} denote the random variable that takes a transcript Tr^* realized in the real

world. Similarly, X_{id} denotes the random variable that takes a transcript Tr^* realized in the ideal world. The probability of realizing a transcript Tr^* in the ideal (resp. real) world is called the *ideal (resp. real) interpolation probability*. A transcript Tr^* is said to be attainable with respect to D if its ideal interpolation probability is non-zero, and AttT denotes the set of all such attainable transcripts and $\Phi : \text{Att} \rightarrow [0, \infty)$ be a non-negative function that maps any attainable transcripts to a non-negative real value. Following these notations, we now state the main theorem of the Expectation Method [13]:

Theorem 2 (Expectation Method). *Let $\text{AttT} = \text{GoodT} \sqcup \text{BadT}$ be a partition of the set of attainable transcripts. Let $\text{Tr}^* \in \text{GoodT}$ be an arbitrary good transcript such that*

$$\frac{p_{\text{re}}(\text{Tr}^*)}{p_{\text{id}}(\text{Tr}^*)} := \frac{\Pr[X_{\text{re}} = \text{Tr}^*]}{\Pr[X_{\text{id}} = \text{Tr}^*]} \geq 1 - \Phi(\tau),$$

and there exists $\epsilon_{\text{bad}} \geq 0$ such that $\Pr[X_{\text{id}} \in \text{BadT}] \leq \epsilon_{\text{bad}}$. Then

$$\mathbf{Adv}_{\text{PAE}}^{\text{nAE}}(D) \leq \mathbf{E}[\Phi(X_{\text{id}})] + \epsilon_{\text{bad}}. \quad (1)$$

To prove the security of the construction using the Expectation Method, we identify the set of bad transcripts and upper bound their probabilities in the ideal world. Then we find a lower bound for the ratio of the real to ideal interpolation probability for a good transcript.

Definition and Probability of Bad Transcripts. We have to bound the probability of bad transcripts in the ideal world. We say that an encryption query $(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^*$ is *non-colliding* if $\forall (\nu^*, A^*, M^*, C^*, T^*, \hat{Z}^*) \in \text{Tr}_e^*, T \neq T^*$. For the sake of notational simplicity, we write $S_\alpha^i = M_\alpha^i \oplus C_\alpha^i$. We also write $I^i := A^i || C^i$ (resp. $I'^i := A^i || C'^i$) to denote the input of the hash in the i -th encryption query (resp. decryption query). Now, we characterize the set of bad transcripts as follows. The main crux of identifying bad events is to identify the two-fold collisions between the construction and primitive queries or the collision between construction queries. In total, we consider six sets of bad events:

- A. Collisions between construction and primitive queries for ForkEDM_p .
- B. Collisions between two construction queries for ForkEDM_p .
- C. Collisions between construction and primitive queries for ForknEHtM_p .
- D. Collisions between two construction queries for ForknEHtM_p .
- E. Verification queries for ForknEHtM_p .
- F. Bad events between ForkEDM_p and ForknEHtM_p .

Then, an attainable transcript $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$ is called a **bad** transcript if any one of those events occur. Recall that $\text{BadT} \subseteq \text{AttT}$ be the set of all attainable bad transcripts and $\text{GoodT} = \text{AttT} \setminus \text{BadT}$ is the set of all attainable good transcripts. We bound the probability of bad transcripts in the ideal world as follows:

Lemma 1. *With X_{id} and BadT defined as above, as $\sigma_e \geq q_e \geq \mu$,*

$$\begin{aligned} \Pr[X_{\text{id}} \in \text{BadT}] \leq & \frac{234\ell^2 \mu \sigma_e q_p^2}{2^{2n}} + \frac{131\ell^4 \sigma_e^2 q_p}{2^{2n}} + \frac{2\ell^2 q_e}{2^n} + \frac{3\ell^4 q_e^3}{2^{2n}} + \frac{14\ell \sqrt{q_e} q_p}{2^n} + \frac{2\ell^2 \mu^2}{2^n} + \frac{q_e^{3/2}}{2^n} \\ & + \frac{4\mu q_e q_p^2 \epsilon_{\text{axu}}}{2^n} + \frac{22\ell q_e^2 q_p \epsilon_{\text{axu}}}{2^n} + \frac{8q_e^2 q_p^2 \epsilon_{\text{reg}}}{2^{2n}} + 5\mu q_e \epsilon_{\text{axu}} + \frac{q_e^2 \epsilon_{\text{axu}}}{2\xi} + \frac{12q_e q_p^2 \epsilon_{\text{reg}}}{2^n} \\ & + \frac{(3\ell + 16)\mu q_p}{2^n} + \frac{\mu(2q_e + q_d)}{2^n} + \frac{16q_e q_d q_p}{2^{2n}} + \frac{8\mu q_d q_p^2 \epsilon_{\text{reg}}}{2^n} + \frac{16\mu q_e q_d q_p^2 \epsilon_{\text{reg}}}{2^{2n}}. \end{aligned}$$

Proof of the lemma is postponed to Appendix A. However, we summarize the terms in Table 1.

Table 1: Upper bounds for the individual bad events.

	Event index i					
	1,7,13	2,8,14	3,9,15	4,10,16	5,11,17	6,12,18
A1..6	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{16\sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e^2 q_p}{2^{2n}}$	$\frac{\ell^2 q_e q_p^2}{2^{2n}}$	$\frac{\ell^2 q_e \sigma_e q_p}{2^{2n}}$
A7..11	$\frac{4\sigma_e^2 q_p}{2^{2n}}$	$\frac{4\ell^2 q_e q_p^2}{2^{2n}}$	$\frac{16\ell \mu \sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e^2 q_p}{2^{2n}}$	$\frac{4\ell^4 q_e^2 q_p}{2^{2n}}$	
B1..6	$\frac{\ell^2 q_e}{2^n}$	$\frac{\ell^4 q_e}{2^{2n}}$	$\frac{\sqrt{q_e q_p}}{2^n}$	$\frac{\ell \sqrt{q_e q_p}}{2^n}$	$\frac{\ell^2 q_e}{2^n}$	$\frac{\ell^2 q_e^2}{2^{2n}} + \frac{\ell^2 \mu^2}{2^n}$
B7	$\frac{\ell^4 q_e^2}{2^{2n}} + \frac{\ell^2 \mu^2}{2^n}$					
C1..6	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{4\mu q_e q_p^2 \epsilon_{\text{axu}}}{2^n} + \frac{4q_p}{2^n}$	$\frac{4q_e q_p^2 \epsilon_{\text{reg}}}{2^n}$	$\frac{16q_e^2 q_p}{2^{2n}} + \frac{16q_e^2 q_p \epsilon_{\text{axu}}}{2^{2n}}$	$\frac{4\mu q_p}{2^n}$
C7..11	$\frac{4q_e q_p^2}{2^{2n}}$	$\frac{4q_e q_p^2}{2^{2n}}$	$\frac{16\mu q_e q_p^2}{2^{2n}}$	$\frac{4q_e^2 q_p^2 \epsilon_{\text{reg}}}{2^{2n}}$	$\frac{4q_e^2 q_p^2 \epsilon_{\text{reg}}}{2^{2n}}$	
D1..6	$\frac{q_e}{2^n}$	$\mu^2 \epsilon_{\text{axu}}$	$2\mu^2 \epsilon_{\text{axu}} + 2\mu q_e \epsilon_{\text{axu}} + \frac{2\mu q_e}{2^n}$	$\frac{\mu^2}{2^n}$	$\frac{q_e^2}{2^{2n}} + \frac{q_e \epsilon_{\text{axu}}}{2^n}$	$\frac{2}{2^n}$
D7..10	$\frac{q_e^2 \epsilon_{\text{axu}}}{2^n}$	$\frac{4\sqrt{q_e q_p}}{2^n}$	$\frac{4\sqrt{q_e q_p}}{2^n}$	$\frac{4\sqrt{q_e q_p}}{2^n}$		
E1..5	$\frac{4q_d q_p^2 \epsilon_{\text{reg}}}{2^n}$	$\frac{\mu q_d}{2^n}$	$\frac{16q_e q_d q_p}{2^{2n}}$	$\frac{4\mu q_d q_p^2 \epsilon_{\text{reg}}}{2^n}$	$\frac{16\mu q_e q_d q_p^2 \epsilon_{\text{reg}}}{2^{2n}}$	
F1..6	$\frac{1}{2^n}$	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{4q_e q_p^2 \epsilon_{\text{reg}}}{2^n}$	$\frac{4q_e^2 q_p}{2^{2n}}$	$\frac{4q_e^2 q_p}{2^{2n}}$
F7..12	$\frac{3/2}{2^n}$	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{4q_e^2 q_p}{2^{2n}}$	$\frac{4\mu q_p}{2^n}$
F13..18	$\frac{8\mu q_p}{2^n}$	$\frac{4q_e \sigma_e q_p}{2^{2n}}$	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{4q_e^2 q_p \epsilon_{\text{axu}}}{2^n}$	$\frac{4q_e^2 q_p}{2^{2n}}$	$\frac{\mu \ell q_p}{2^n}$
F19..24	$\frac{2\ell \mu q_p}{2^n}$	$\frac{\sigma_e^2 q_p}{2^{2n}}$	$\frac{\sigma_e q_p^2}{2^{2n}}$	$\frac{\ell q_e^2 q_p \epsilon_{\text{axu}}}{2^n}$	$\frac{4\sigma_e^2 q_p}{2^{2n}}$	$\frac{16q_e q_p^2}{2^{2n}}$
F25..30	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{16q_e^2 q_p}{2^{2n}}$	$\frac{16q_e^2 q_p}{2^{2n}}$	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e^2 q_p}{2^{2n}}$	$\frac{4q_e q_p^2 \epsilon_{\text{reg}}}{2^{2n}}$
F31..36	$\frac{16q_e q_p^2}{2^{2n}}$	$\frac{16q_e^2 q_p}{2^{2n}}$	$\frac{16q_e^2 q_p}{2^{2n}}$	$\frac{4\sigma_e q_p^2}{2^{2n}}$	$\frac{4\sigma_e^2 q_p}{2^{2n}}$	$\frac{16\mu^2 q_p^2}{2^{2n}}$

5 Analysis of Good Transcripts

Let $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h) \in \text{GoodT}$ be an attainable good transcript and we define

$$p(\text{Tr}^*) := \Pr[\text{P} \leftarrow \text{Perm} : \text{PAE}_{k_0, k_1, k_h}^{\text{P}} \mapsto (\text{Tr}_e^*, \text{Tr}_d^*) \mid \text{P} \mapsto \text{Tr}_p].$$

We call a permutation P compatible to an attainable good transcript $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$ if $\text{PAE}_{k_0, k_1, k_h}^{\text{P}} \mapsto (\text{Tr}_e^*, \text{Tr}_d^*)$ and $\forall (U^b, V) \in \text{Tr}_p, \text{P}(U^b) = V$ holds. Note that, $\text{PAE}_{k_0, k_1, k_h}^{\text{P}} \mapsto (\text{Tr}_e^*, \text{Tr}_d^*)$ holds implies that for every $(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^*$,

$$(A) := \begin{cases} S \leftarrow \text{ForkEDM}_p[\text{P}]_{k_0, k_1}(\nu, \lfloor \frac{|M|}{n} \rfloor), \\ C \leftarrow M \oplus S_{\lfloor |M| \rfloor}, \\ \hat{Z} \leftarrow \text{P}(\text{fix}_{11}(\nu \oplus k_1)), \\ T \leftarrow \text{P}(\text{fix}_{00}(\hat{Z} \oplus k_0)) \oplus \text{P}(\text{fix}_{01}(\hat{Z} \oplus k_0 \oplus \mathbf{H}_{k_h}(C))) \end{cases}$$

holds and for every $(\nu', A', C', T', O', \hat{Z}') \in \text{Tr}_d^*$,

$$(B) := \begin{cases} \hat{Z}' \leftarrow \text{P}(\text{fix}_{11}(\nu' \oplus k_1)) \\ T' \neq \text{ForknEHtM}_p[\text{P}, \text{H}]_{k_0, k_1, k_h}(\nu', A', C') \end{cases}$$

holds. For an attainable good transcript $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$, we call that a permutation P is compatible with Tr_e^* (resp. Tr_d^*) if (A) (resp. (B)) holds. We call P is compatible with $\text{Tr}_e^* \cup \text{Tr}_d^*$ if P is compatible to both Tr_e^* and Tr_d^* . For an attainable good transcript $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$, we define

$$\text{Comp}(\text{Tr}^*) := \{\text{P} : \text{P} \text{ is compatible to } \text{Tr}_e^* \cup \text{Tr}_d^*\}.$$

For a good attainable transcript Tr^* , we have

$$\Pr[\mathbf{X}_{\text{re}} = \text{Tr}^*] = \frac{1}{|\mathcal{K}_h|} \cdot \frac{1}{N^2} \cdot \underbrace{\Pr[\mathbf{P} \leftarrow \text{Perm} : \mathbf{P} \in \text{Comp}(\text{Tr}^*) \mid \mathbf{P} \mapsto \text{Tr}_p]}_{\mathfrak{p}(\text{Tr}^*)} \cdot \frac{1}{(N)_{q_p}}$$

As the encryption oracle of the ideal world always outputs uniform random n -bit strings on each input query and the decryption oracle always returns \perp , we have

$$\Pr[\mathbf{X}_{\text{id}} = \text{Tr}^*] = \frac{1}{|\mathcal{K}_h|} \cdot \frac{1}{N^2} \cdot \frac{1}{N^{\sigma_e}} \cdot \frac{1}{(N)_{q_p}}.$$

5.1 Establishing A Lower Bound on $\mathfrak{p}(\text{Tr}^*)$

First of all, for a good transcript $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$ and for $b \in \{00, 01, 10, 11\}$, recall that \mathcal{U}^b is the set of all domain points of the forward primitive queries to permutation \mathbf{P} and the range points of the inverse primitive queries to permutation \mathbf{P} with its two most significant bits are set to b and \mathcal{V}^b is the set of all the corresponding range points of the forward primitive queries to permutation \mathbf{P} such that the two most significant bits of the queries are set to b and the domain points of the inverse primitive queries to permutation \mathbf{P} such that the two most significant bits of the corresponding response is b . Moreover, \mathcal{U} is the set of all domain points of the forward primitive queries to \mathbf{P} and the range points of the inverse primitive queries to \mathbf{P} . Similarly, \mathcal{V} is the set of all range points of the forward primitive queries to \mathbf{P} and the domain points of the inverse primitive queries to \mathbf{P} . Since $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h)$ is good, we can partition the set of encryption queries Tr_e^* into disjoint groups as follows:

$$\begin{aligned} \mathcal{Q}_1 &:= \{(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^* : \text{fix}_{11}(\nu \oplus k_0) \in \mathcal{U}^{11}\}, \\ \mathcal{Q}_2 &:= \{(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^* : \alpha \in [\ell], S_\alpha \oplus 2^{\alpha-1}k_1 \in \mathcal{V}\} \\ \mathcal{Q}_3 &:= \{(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^* : \text{fix}_{11}(\nu \oplus k_1) \in \mathcal{U}^{11}\} \\ \mathcal{Q}_4 &:= \{(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^* : \text{fix}_{00}(\hat{Z} \oplus k_0) \in \mathcal{U}^{00}\} \\ \mathcal{Q}_5 &:= \{(\nu, A, M, C, T, \hat{Z}) \in \text{Tr}_e^* : \text{fix}_{01}(\hat{Z} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma)) \in \mathcal{U}^{01}\} \\ \mathcal{Q}_0 &:= \text{Tr}_e^* \setminus \cup_{i=1}^5 \mathcal{Q}_i \end{aligned}$$

Having defined the sets, we claim that the sets are disjoint and they exhaust the entire set of attainable good transcripts.

Proposition 1. *Let $\text{Tr}^* = (\text{Tr}_e^*, \text{Tr}_d^*, \text{Tr}_p, k_0, k_1, k_h) \in \text{GoodT}$ be a good transcript. Then the sets $(\mathcal{Q}_0, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_4, \mathcal{Q}_5)$ are pairwise disjoint.*

Note that, since Tr^* is a good transcript, we have, $\alpha_1 = |\mathcal{Q}_1| \leq \sqrt{q_e}$ and $\alpha_2 = |\mathcal{Q}_2| \leq \sqrt{q_e}$. Similarly, we have $\alpha_3 = |\mathcal{Q}_3| \leq \sqrt{q_e}$, $\alpha_4 = |\mathcal{Q}_4| \leq \sqrt{q_e}$ and finally $\alpha_5 = |\mathcal{Q}_5| \leq \sqrt{q_e}$. For $i \in \{0, 1, \dots, 5\}$, let \mathbf{E}_i denote the event $\text{PAE.Enc}_{k_0, k_1, k_h}^{\mathbf{P}} \mapsto \mathcal{Q}_i$. Now, it is easy to see that

$$\mathfrak{p}(\text{Tr}^*) = \underbrace{\Pr[\wedge_{i=1}^5 \mathbf{E}_i \mid \mathbf{P} \mapsto \text{Tr}_p]}_{\mathfrak{p}_1(\text{Tr}^*)} \cdot \underbrace{\Pr[\mathbf{E}_0 \wedge \text{PAE.Dec}_{k_0, k_1, k_h}^{\mathbf{P}} \mapsto \text{Tr}_d^* \mid \wedge_{i=1}^5 \mathbf{E}_i \wedge \mathbf{P} \mapsto \text{Tr}_p]}_{\mathfrak{p}_2(\text{Tr}^*)} \quad (2)$$

Thus, it is enough to establish a good lower bound on $\mathfrak{p}_1(\text{Tr}^*)$ and $\mathfrak{p}_2(\text{Tr}^*)$.

5.2 Lower Bound of $\mathbf{p}_1(\mathbf{Tr}^*)$

To lower bound $\mathbf{p}_1(\mathbf{Tr}^*)$, we define 5×5 sets. For all $k \in \{1, \dots, 5\}$, let

$$\begin{aligned} \mathcal{D}_1^k &:= \{\text{fix}_{11}(\nu_i \oplus k_0) : (\nu_i, A^i, M^i, C^i, T_i, \hat{Z}_i) \in \mathcal{Q}_k\}, \\ \mathcal{R}_1^k &:= \{S_\alpha^i \oplus 2^{\alpha-1}k_1, \forall \alpha \in [\ell_i] : (\nu_i, A^i, M^i, C^i, T_i, \hat{Z}_i) \in \mathcal{Q}_k\}, \\ \mathcal{I}_1^k &:= \{\text{fix}_{11}(\nu_i \oplus k_1) : (\nu_i, A^i, M^i, C^i, T_i, \hat{Z}_i) \in \mathcal{Q}_k\}, \\ \mathcal{D}_2^k &:= \{(\text{fix}_{00}(\hat{Z}_i \oplus k_0), \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^i))) : (\nu_i, A^i, M^i, C^i, T_i, \hat{Z}_i) \in \mathcal{Q}_k\}, \\ \mathcal{R}_2^k &:= \{T_i : (\nu_i, A^i, M^i, C^i, T_i, \hat{Z}_i) \in \mathcal{Q}_k\}. \end{aligned}$$

In the following, the goal is to establish upper bounds for the probabilities of E.1 to E.5 to occur. Since the process is repetitive (although there are subtle differences for each event), we will report only the bound here and the detailed treatment of each of the events are given in Appendix B.

$$\begin{aligned} \mathbf{p}_1(\mathbf{Tr}^*) &\geq \frac{1}{(2^n - q_p)_{\Delta_1}} \cdot \frac{1}{(2^n - q_p - \Delta_1 - 2\alpha_1)_{\Delta_2}} \cdot \left(1 - \sum_{i=1}^k \frac{18\rho_i^2 \binom{\mu_i}{2}}{2^{2n}}\right) \\ &\quad \cdot \frac{1}{(2^n - q_p - (\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4) - 2(\alpha_1 + \alpha_2 + \alpha_3))_{2\alpha_4}} \\ &\quad \cdot \frac{1}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - \Delta_5 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4))_{2\alpha_5}}, \end{aligned}$$

where $\Delta_1 = (\ell_1 + \dots + \ell_{\alpha_1} + \alpha_1)$, $\Delta_2 = (\ell_1 + \dots + \ell_{\alpha_2} + \alpha_2)$, $\Delta_3 = (\ell_1 + \dots + \ell_{\alpha_3} + \alpha_3)$, $\Delta_4 = (\ell_1 + \dots + \ell_{\alpha_4} + \alpha_4)$, and $\Delta_5 = (\ell_1 + \dots + \ell_{\alpha_5} + \alpha_5)$.

5.3 Lower Bound of $\mathbf{p}_2(\mathbf{Tr}^*)$

To lower bound $\mathbf{p}_2(\mathbf{Tr}^*)$, we first note that all the inputs to and outputs from the permutation are fresh, i.e., they have not collided with any primitive query input or output. Let $\delta = \Delta_1 + \Delta_2 + \Delta_3 + \Delta_4 + \Delta_5 + 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5)$. Hence, using the results from [24] and [15], we have

$$\begin{aligned} \mathbf{p}_2(\mathbf{Tr}^*) &\geq \left(1 - \frac{28(q_p + \delta)\sigma_e^2}{2^{2n}} - \frac{4(q_p + \delta)^2\sigma_e}{2^{2n}} - \frac{24\sigma_e^3}{2^{2n}}\right) \cdot \frac{(2^n - q_p - \delta)_{2\alpha_0}}{2^{n\alpha_0}} \\ &\quad \cdot \left(1 - \sum_{i=1}^k \frac{6\rho_i^2 \binom{\mu_i}{2}}{2^{2n}} - \frac{2q_d}{2^n}\right). \end{aligned} \quad (3)$$

By taking the ratio of $\mathbf{p}_1(\mathbf{Tr}^*) \times \mathbf{p}_2(\mathbf{Tr}^*)$ to 2^{nq_e} and finally, by applying the Expectation Method [26], we have

$$\begin{aligned} \mathbf{E}[\Phi(X_{\text{id}})] &\leq \frac{28(q_p + \delta)\sigma_e^2}{2^{2n}} + \frac{4(q_p + \delta)^2\sigma_e}{2^{2n}} + \frac{24\sigma_e^3}{2^{2n}} + \frac{12q_e^4\epsilon_{\text{axu}}}{2^{2n}} + \frac{12\mu^2q_e^2}{2^{2n}} + \frac{48q_e^3}{2^{2n}} \\ &\quad + \frac{48(q_p + \delta)q_e^3\epsilon_{\text{axu}}}{2^{2n}} + \frac{48\mu^2(q_p + \delta)q_e}{2^{2n}} + \frac{192(q_p + \delta)q_e^2}{2^{2n}} \\ &\quad + \frac{48(q_p + \delta)^2q_e^2\epsilon_{\text{axu}}}{2^{2n}} + \frac{48\mu^2(q_p + \delta)^2}{2^{2n}} + \frac{192(q_p + \delta)^2q_e}{2^{2n}} + \frac{2q_d}{2^{2n}}. \end{aligned} \quad (4)$$

Table 2: Performance, code size, and stack consumption in bytes of primitives on 32-bit ARM Cortex-M3 for Sparkle and Cortex-M4 for Chaskey as in our implementation; unr. = unrolled.

Primitive	Version	Inv. throughput c/b (cycles)	Code size bytes	Stack bytes
Sparkle 256 [4]	7 steps	18.9 (605)	316 + 32	40
Sparkle 384 [4]	7 steps	22.5 (1 079)	452 + 32	48
Sparkle 384 [4]	7 steps unr.	19.4 (930)	2 820	48
ChaCha20 [32]	12 steps	20.6 (1 487)	734	232
Chaskey	8 rounds	6.4 (103)	56	16
Chaskey	8 rounds unr.	6.3 (100)	250	16

Finally, by assuming the maximum message length of ℓ blocks and $\alpha_i \leq \sqrt{q_e}$ for $i \in [5]$, we have $\delta \leq 10\sqrt{q_e} + 5\ell\sqrt{q_e}$. By plugging in the upper bound of δ in the above equations, and using $\sigma_e \geq q_e \geq \mu$, we obtain the following.

$$\mathbf{E}[\Phi(X_{\text{id}})] \leq \frac{1}{2^{2n}} \left(5980\sigma_e^2 q_p + 420\ell\sigma_e^2 \sqrt{q_e} + 196\sigma_e q_p^2 + 44100\ell^2 \sigma_e^2 + 120\ell\sigma_e q_e q_p + 12q_e^4 \epsilon_{\text{axu}} \right. \\ \left. + 5292\mu^2 q_e^2 + 48q_e^3 q_p \epsilon_{\text{axu}} + 5520\ell q_e^{7/2} \epsilon_{\text{axu}} + 48q_e^2 q_p^2 \epsilon_{\text{axu}} + 48\mu^2 q_p^2 + 1440\ell q_e^{5/2} q_p \epsilon_{\text{axu}} \right. \\ \left. + 1488\mu^2 q_e q_p + 240\ell\mu^2 q_e^{3/2} + 2880\ell q_e^{5/2} + 6000\ell^2 q_e^3 \epsilon_{\text{axu}} + 6000\ell^2 \mu^2 q_e + 72\sigma_e^3 + 2q_d \right).$$

6 Software Implementation for 32-bit Microcontrollers

Since we employ public permutations, our construction can spare the necessary overhead of a key schedule, spare state from precomputed round keys, and can use smaller primitives for a sufficient security level as needed for lightweight implementations. We propose an instantiation that we implemented on 32-bit microcontrollers and evaluate its efficiency with respect to cycles per byte and memory usage.

Primitive Choice and Rationale. We can employ a smaller primitive for a sufficient security level than duplex-based constructions. The 128-bit Chaskey permutation is small, efficient, and easy to implement on Microcontrollers. Moreover, the sum of permutations allowed reduced individual permutations. Therefore, we decided to instantiate our construction with Chaskey-8 [30,31] for the public permutation and two parallel instances of the MAC-611 hash function [25] operating modulo $2^{61} - 1$.

Environment. We evaluated our instantiation on an NXP FRDM-KV31F board which has an ARM Cortex M4 KV31F512VLL12 MCU processor at 120 MHz, 96 kB SRAM, and 512 kB of flash memory. We implemented our construction mostly in C with some assembly code from [25], and code for Chaskey by Mouha.², compiled with `arm-none-eabi-gcc v10.3.1` in NXP MCUXpresso v11. For measuring the number of used cycles, we employed the Data Watchpoint and Trace (DWT) flags that are implemented on Cortex M4.³ We measured

²<https://mouha.be/chaskey/>

³<https://mcuoneclipse.com/2017/01/30/cycle-counting-on-arm-cortex-m-with-dwt/>

Table 3: Performance in cycles per byte (cycles) on 32-bit ARM Cortex M3 for Schwaemm and on Cortex-M4 for [32] and our implementations. (*) = asymptotic.

Construction	Inv. throughput in c/b (cycles)	
	64 bytes	1 536 bytes
Schwaemm-128-128 [4]	68.5 (4 384)	45.9 (70 440)
Schwaemm-256-128 [4]	73.7 (4 715)	37.2 (57 109)
ChaCha20-Poly1305 [32]		28.4(*) (-)
PAE with Chaskey-8-Poly1305 [This work]	45.3 (2 902)	24.2 (37 145)
PAE with Chaskey-8-MAC611 [This work]	41.8 (2 676)	22.7 (34 797)

cycles on the target chip (not a simulator) for fixed messages and empty associated data and a 64- as well as 1 536-byte message and averaged over 100 measurements each.

To determine the the code size of the individual functions, we used the usual GNU `size` utility and MCUXpresso. To evaluate the stack usage, we used Beer’s script based on `arm-none-eabi-objdump`.⁴ Since nested functions reduce the code size but increase the stack size, we limited the depth from top-level functions to one level inside them. We compiled with flags `-Os` for smaller code and with `-O3 -fomit-framepointer` for versions optimized for low cycles per byte, respectively. Table 2 shows the number of cycles, code size, and stack usage of the primitives. Table 3 illustrates the performance of the construction and its hashing components over longer messages.

Results and Discussion. Chaskey is particularly lightweight with only 56 bytes when optimized for size, and 250 when eight rounds are fully unrolled. For comparison, a reduced-round version of Ascon weighs about 1 810 bytes, and one of Sparkle 384, the fastest instance among the Sparkle family, needs 2 820 bytes [4]. The disadvantage of our instantiation is the need of computing two 64-bit hashes and the need of multiple 128-bit keys. Though, we spare to compute any complex key schedule in the sense that the only key-update procedure involves doubling a key in $\mathbb{F}_{2^{128}}$.

Our instantiation excels in inverse throughput. In [3], Beierle et al. showcased highly optimized versions of Sparkle and Schwaemm. Among the Sparkle family of permutations, Sparkle-384 peaked at around 19 cycles per byte on Cortex-M3; In the context of the AE scheme Schwaemm, Schwaemm-256-128 topped their proposals by encrypting messages at 37 cycles per byte, which was a top value among the NIST LWC finalists.

Instantiating PAE with Chaskey and the hash function of MAC611 from [25] yielded competitive results in our implementations, of less than 23 cycles per byte for longer messages. Motivated by the results of [32] with a generic composition of ChaCha20 and Poly1305, we also considered Poly1305 as an appropriate alternative hash function. Our implementation could achieve already similarly competitive results, of less than 25 cycles per byte for longer messages. Combined with eight-round Chaskey, there seems to be room for an asymptotic optimum of even as low as about 15 cycles per byte for either instance that could be addressed in future work. Moreover, we emphasize that those results employ no SIMD instruction sets such as NEON as they are unavailable in Cortex-M4 and earlier architectures.

⁴<https://dlbeer.co.nz/oss/avstack.html>

7 Summary

This work proposes PAE, a highly efficient AE scheme from public permutations that provides $O(2n/3)$ -bit security even under a few faulty nonces. It demonstrates that the Iterate-Fork-Iterate(-Many) paradigm can increase efficiency even on lightweight platforms and from public permutations. Future works can consider further tightening the gap to the asymptotic optimum of implementation. Also, as PAE achieves BBB security w.r.t. the number of queries or the number of query blocks but not w.r.t. the query length, future works can try to achieve that with similar constructions. Moreover, while we consider using an alternative hash function based on the same public permutation, future works can try to tackle the open problem to derive its security bound.

References

1. E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda. APE: authenticated permutation-based encryption for lightweight cryptography. In C. Cid and C. Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 168–186. Springer, 2014.
2. E. Andreeva, V. Lallemand, A. Purnal, R. Reyhanitabar, A. Roy, and D. Vizár. Forkeipher: A New Primitive for Authenticated Encryption of Very Short Messages. In S. D. Galbraith and S. Moriai, editors, *ASIACRYPT II*, volume 11922 of *LNCS*, pages 153–182. Springer, 2019.
3. C. Beierle, A. Biryukov, L. C. dos Santos, J. Großschädl, A. Moradi, L. Perrin, A. R. Shahmirzadi, A. Udovenko, V. Velichkov, and Q. Wang. An update on the lwc finalist sparkle. *NIST Lightweight Cryptography*, 2022.
4. C. Beierle, A. Biryukov, L. C. dos Santos, J. Großschädl, L. Perrin, A. Udovenko, V. Velichkov, and Q. Wang. Schwaemm and esch: Lightweight authenticated encryption and hashing using the sparkle permutation family, May 17 2021.
5. D. J. Bernstein, S. Kölbl, S. Lucks, P. M. C. Massolino, F. Mendel, K. Nawaz, T. Schneider, P. Schwabe, F. Standaert, Y. Todo, and B. Viguier. Gimli : A cross-platform permutation. In W. Fischer and N. Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 299–320. Springer, 2017.
6. T. Beyne, Y. L. Chen, C. Dobraunig, and B. Mennink. Dumbo, jumbo, and delirium: Parallel authenticated encryption for the lightweight circus. *IACR Trans. Symmetric Cryptol.*, 2020(S1):5–30, 2020.
7. T. Beyne, Y. L. Chen, C. Dobraunig, and B. Mennink. Multi-user security of the elephant v2 authenticated encryption mode. In R. AlTawy and A. Hülsing, editors, *Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers*, volume 13203 of *Lecture Notes in Computer Science*, pages 155–178. Springer, 2021.
8. A. Bhattacharjee, A. Chakraborti, N. Datta, C. Mancillas-López, and M. Nandi. sf ISAP+: sf ISAP with fast authentication. In T. Isobe and S. Sarkar, editors, *Progress in Cryptology - INDOCRYPT 2022 - 23rd International Conference on Cryptology in India, Kolkata, India, December 11-14, 2022, Proceedings*, volume 13774 of *Lecture Notes in Computer Science*, pages 195–219. Springer, 2022.
9. A. Bhattacharjee, A. Dutta, E. List, and M. Nandi. CENCPP*: beyond-birthday-secure encryption from public permutations. *Des. Codes Cryptogr.*, 90(6):1381–1425, 2022.
10. A. Bhattacharjee, C. M. López, E. List, and M. Nandi. The oribatida v1.3 family of lightweight authenticated encryption schemes. *J. Math. Cryptol.*, 15(1):305–344, 2021.

11. A. Chakraborti, N. Datta, M. Nandi, and K. Yasuda. Beetle family of lightweight and secure authenticated encryption ciphers. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):218–241, 2018.
12. S. Chen, R. Lampe, J. Lee, Y. Seurin, and J. P. Steinberger. Minimizing the two-round even-mansour cipher. *J. Cryptol.*, 31(4):1064–1119, 2018.
13. S. Chen and J. P. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version at <https://eprint.iacr.org/2013/222>.
14. Y. L. Chen. A modular approach to the security analysis of two-permutation constructions. In S. Agrawal and D. Lin, editors, *ASIACRYPT I*, volume 13791 of *LNCS*, pages 379–409. Springer, 2022.
15. Y. L. Chen, A. Dutta, and M. Nandi. Multi-user BBB security of public permutations based MAC. *Cryptogr. Commun.*, 14(5):1145–1177, 2022.
16. Y. L. Chen, E. Lambooj, and B. Mennink. How to Build Pseudorandom Functions from Public Random Permutations. In A. Boldyreva and D. Micciancio, editors, *CRYPTO I*, volume 11692 of *LNCS*, pages 266–293. Springer, 2019.
17. Y. L. Chen, B. Mennink, and B. Preneel. Categorization of Faulty Nonce Misuse Resistant Message Authentication. In M. Tibouchi and H. Wang, editors, *ASIACRYPT III*, volume 13092 of *LNCS*, pages 520–550. Springer, 2021.
18. B. Cogliati and Y. Seurin. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In M. Robshaw and J. Katz, editors, *CRYPTO I*, volume 9814 of *LNCS*, pages 121–149. Springer, 2016.
19. J. Daemen, S. Hoffert, M. Peeters, G. V. Assche, and R. V. Keer. Xoodyak, a lightweight cryptographic scheme. *IACR Trans. Symmetric Cryptol.*, 2020(S1):60–87, 2020.
20. C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, B. Mennink, R. Primas, and T. Unterluggauer. Isap v2.0. *IACR Trans. Symmetric Cryptol.*, 2020(S1):390–416, 2020.
21. C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schl affer. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.*, 34(3):33, 2021.
22. A. Dutta and M. Nandi. BBB Secure Nonce Based MAC Using Public Permutations. In A. Nitaj and A. M. Youssef, editors, *AFRICACRYPT*, volume 12174 of *LNCS*, pages 172–191. Springer, 2020.
23. A. Dutta, M. Nandi, and S. Talnikar. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In Y. Ishai and V. Rijmen, editors, *EUROCRYPT I*, volume 11476 of *LNCS*, pages 437–466. Springer, 2019.
24. A. Dutta, M. Nandi, and S. Talnikar. Permutation based EDM: an inverse free BBB secure PRF. *IACR Trans. Symmetric Cryptol.*, 2021(2):31–70, 2021.
25. S. Duval and G. Leurent. Lightweight MACs from Universal Hash Functions. In S. Bela id and T. G uneysu, editors, *CARDIS*, volume 11833 of *LNCS*, pages 195–215. Springer, 2019.
26. V. T. Hoang and S. Tessaro. Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. In M. Robshaw and J. Katz, editors, *CRYPTO I*, volume 9814 of *LNCS*, pages 3–32. Springer, 2016.
27. B. Mennink and S. Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In J. Katz and H. Shacham, editors, *CRYPTO, Part III*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017.
28. B. Mennink and S. Neves. Optimal PRFs from Blockcipher Designs. *IACR Trans. Symmetric Cryptol.*, 2017(3):228–252, 2017.
29. K. Minematsu. How to thwart birthday attacks against macs via small randomness. In S. Hong and T. Iwata, editors, *FSE*, volume 6147 of *LNCS*, pages 230–249. Springer, 2010.
30. N. Mouha. Chaskey: A MAC Algorithm for Microcontrollers - Status Update and Proposal of Chaskey-12 -. *IACR Cryptol. ePrint Arch.*, page 1182, 2015.
31. N. Mouha, B. Mennink, A. V. Herrewewege, D. Watanabe, B. Preneel, and I. Verbauwhede. Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In A. Joux and A. M. Youssef, editors, *SAC*, volume 8781 of *LNCS*, pages 306–323. Springer, 2014.

32. F. D. Santis, A. Schauer, and G. Sigl. ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications. In D. Atienza and G. D. Natale, editors, *DATE*, pages 692–697. IEEE, 2017.
33. P. Zhang. Permutation-based lightweight authenticated cipher with beyond conventional security. *Security and Communication Networks*, 2021:1–9, 10 2021.

A Proof of Lemma 2

We restate the lemma to aid the reader.

Lemma 2. *With X_{id} and BadT defined as above, as $\sigma_e \geq q_e \geq \mu$,*

$$\begin{aligned} \Pr[X_{\text{id}} \in \text{BadT}] \leq & \frac{234\ell^2 \mu \sigma_e q_p^2}{2^{2n}} + \frac{131\ell^4 \sigma_e^2 q_p}{2^{2n}} + \frac{2\ell^2 q_e}{2^n} + \frac{3\ell^4 q_e^3}{2^{2n}} + \frac{14\ell \sqrt{q_e} q_p}{2^n} + \frac{2\ell^2 \mu^2}{2^n} + \frac{q_e^{3/2}}{2^n} \\ & + \frac{4\mu q_e q_p^2 \epsilon_{\text{axu}}}{2^n} + \frac{22\ell q_e^2 q_p \epsilon_{\text{axu}}}{2^n} + \frac{8q_e^2 q_p^2 \epsilon_{\text{reg}}}{2^{2n}} + 5\mu q_e \epsilon_{\text{axu}} + \frac{q_e^2 \epsilon_{\text{axu}}}{2\xi} + \frac{12q_e q_p^2 \epsilon_{\text{reg}}}{2^n} \\ & + \frac{(3\ell + 16)\mu q_p}{2^n} + \frac{\mu(2q_e + q_d)}{2^n} + \frac{16q_e q_d q_p}{2^{2n}} + \frac{8\mu q_d q_p^2 \epsilon_{\text{reg}}}{2^n} + \frac{16\mu q_e q_d q_p^2 \epsilon_{\text{reg}}}{2^{2n}}. \end{aligned}$$

A.1 Analysis of Events A_i

The events A_i study collisions between construction and primitive queries for ForkEDM_p .

1. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, S_\alpha^i \oplus 2^{\alpha-1} k_1 = V_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A1] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

2. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{10}$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, \text{fix}_{10}(V_{j_1} \oplus 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A2] \leq \frac{16\sigma_e q_p^2}{2^{2n}}.$$

3. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{10}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ and $\exists b \in \{00, 01, 10, 11\}$ such that the following holds:

$$\begin{cases} S_\alpha^i \oplus 2^{\alpha-1} k_1 = V_{j_1}, \\ (b \parallel ([U_{j_1} \oplus 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)]_{n-2})) = V_{j_2}. \end{cases}$$

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A3] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

4. $\exists i_1, i_2 \in [q_e], \alpha \in [\ell_{i_1}], \beta \in [\ell_{i_2}], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{10}$ and $\exists b \in \{00, 01, 10, 11\}$ such that the following holds:

$$\begin{cases} S_\alpha^i \oplus 2^{\alpha-1} k_1 = V_{j_1}, \\ (b \| ([U_{j_1} \oplus 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)]_{n-2})) = S_\beta^{i_2} \oplus 2^{\beta-1} k_1. \end{cases}$$

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A4] \leq \frac{4\sigma_e^2 q_p}{2^{2n}}.$$

5. $\exists i \in [q_e], \alpha \neq \beta \in [\ell_i], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $S_\alpha^i \oplus 2^{\alpha-1} k_1 = V_{j_1}, S_\beta^i \oplus 2^{\beta-1} k_1 = V_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of S_α^i and S_β^i . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A5] \leq \frac{\ell^2 q_e q_p^2}{2^{2n}}.$$

6. $\exists i_1, i_2 \in [q_e], \alpha \neq \beta \in [\ell_{i_1}], \gamma \in [\ell_{i_2}], (U_j, V_j) \in \text{Tr}_p$ such that $S_\alpha^{i_1} \oplus 2^{\alpha-1} k_1 = V_j, S_\beta^{i_1} \oplus 2^{\beta-1} k_1 = S_\gamma^{i_2} \oplus 2^{\gamma-1} k_1$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of $S_\alpha^{i_1}$ and $S_\beta^{i_1}$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A6] \leq \frac{\ell^2 q_e \sigma_e q_p}{2^{2n}}.$$

7. $\exists i_1, i_2 \in [q_e], \alpha \in [\ell_{i_1}], \beta \in [\ell_{i_2}], (U_j, V_j) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_j, S_\alpha^{i_1} \oplus 2^{\alpha-1} k_1 = S_\beta^{i_2} \oplus 2^{\beta-1} k_1$.

W.l.o.g., suppose $i_1 > i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and $S_\alpha^{i_1}$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A7] \leq \frac{4\sigma_e^2 q_p}{2^{2n}}.$$

8. $\exists i \in [q_e], \alpha \neq \beta \in [\ell_i], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{10}$ and $\exists b \in \{00, 01, 10, 11\}$ such that the following holds:

$$\begin{cases} S_\alpha^i \oplus 2^{\alpha-1} k_1 = V_{j_1}, \\ \text{fix}_{10} \left((b \| ([U_{j_1}]_{n-2} \oplus [2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)]_{n-2})) \oplus 2^{\beta-1}(\nu_i \oplus k_0 \oplus k_1) \right) = U_{j_2}. \end{cases}$$

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A8] \leq \frac{4\ell^2 q_e q_p^2}{2^{2n}}.$$

9. $\exists i_1 \neq i_2 \in [q_e], \alpha \in [\ell_{i_1}], \beta \in [\ell_{i_2}], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that the following holds:

$$\begin{cases} \text{fix}_{11}(\nu_{i_1} \oplus k_0) = U_{j_1}, \\ \text{fix}_{11}(\nu_{i_2} \oplus k_0) = U_{j_2}, \\ [V_{j_1} \oplus 2^{\alpha-1}(\nu_{i_1} \oplus k_0 \oplus k_1)]_{n-2} = [V_{j_2} \oplus 2^{\beta-1}(\nu_{i_2} \oplus k_0 \oplus k_1)]_{n-2}. \end{cases}$$

The first two equations can be rewritten as $U_{j_1} \oplus \text{fix}_{11}(\nu_{i_1}) = U_{j_2} \oplus \text{fix}_{11}(\nu_{i_2}) = \text{fix}_{11}(k_0)$. We observe that if we fix any three indices, e.g., j_1, i_1 , and j_2 , the fourth index (in this case i_2) gets fixed. For a fixed value of the indices j_1, i_1 and j_2 , the probability of the event is upper bounded by $(\mu/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A9] \leq \frac{16\ell\mu\sigma_e q_p^2}{2^{2n}}.$$

10. $\exists i_1 \neq i_2 \in [q_e], \alpha \in [\ell_{i_1}], \beta \in [\ell_{i_2}], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{10}$ such that the following condition holds:

$$\begin{cases} S_\alpha^{i_1} \oplus 2^{\alpha-1}k_1 = V_{j_1}, \\ S_\beta^{i_2} \oplus 2^{\beta-1}k_1 = V_{j_2}, \\ [U_{j_1} \oplus 2^{\alpha-1}(\nu_{i_1} \oplus k_0 \oplus k_1)]_{n-2} = [U_{j_2} \oplus 2^{\beta-1}(\nu_{i_2} \oplus k_0 \oplus k_1)]_{n-2}. \end{cases}$$

The first two equations can be rewritten as $2^{1-\alpha}S_\alpha^{i_1} \oplus 2^{1-\alpha}V_{j_1} = 2^{1-\beta}S_\beta^{i_2} \oplus 2^{1-\beta}V_{j_2} = k_1$. We observe that if we fix any three indices, e.g., i_1, j_1 , and j_2 , the fourth index (in this case i_2) gets fixed. For a fixed value of the indices i_1, j_1 and i_2 , the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A10] \leq \frac{4\sigma_e^2 q_p}{2^{2n}}.$$

11. $\exists i_1 \neq i_2 \in [q_e], \alpha, \gamma \in [\ell_{i_1}], \beta, \delta \in [\ell_{i_2}], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{10}$ and $\exists b, b' \in \{00, 01, 10, 11\}$ such that the following holds:

$$\begin{cases} S_\alpha^{i_1} \oplus 2^{\alpha-1}k_1 = V_{j_1}, \\ S_\beta^{i_2} \oplus 2^{\beta-1}k_1 = V_{j_2}, \\ \text{fix}_{10}(b \| ([U_{j_1} \oplus 2^{\alpha-1}(\nu_{i_1} \oplus k_0 \oplus k_1)]_{n-2}) \oplus 2^{\gamma-1}(\nu_{i_1} \oplus k_0 \oplus k_1)) \\ = \text{fix}_{10}(b' \| ([U_{j_2} \oplus 2^{\beta-1}(\nu_{i_2} \oplus k_0 \oplus k_1)]_{n-2}) \oplus 2^{\delta-1}(\nu_{i_2} \oplus k_0 \oplus k_1)). \end{cases}$$

The first two equations can be rewritten as $2^{1-\alpha}S_\alpha^{i_1} \oplus 2^{1-\alpha}V_{j_1} = 2^{1-\beta}S_\beta^{i_2} \oplus 2^{1-\beta}V_{j_2} = k_1$. We observe that if we fix any three indices, e.g., i_1, j_1 , and j_2 , the fourth index (in this case i_2) gets fixed. For a fixed value of the indices i_1, j_1 and i_2 , the probability of the

event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[A11] \leq \frac{4\ell^4 q_e^2 q_p}{2^{2n}}.$$

A.2 Analysis of Events B_i

Next, we consider the events B_i that upper bound probabilities for collisions between two construction queries for ForkEDM $_p$.

1. $\exists i \in [q_e], \alpha \neq \beta \in [\ell_i]$ such that $S^i[\alpha] \oplus 2^{\alpha-1}k_1 = S^i[\beta] \oplus 2^{\beta-1}k_1$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[B1] \leq \frac{\ell^2 q_e}{2^n}.$$

2. $\exists i, i', i'' \in [q_e], \alpha \neq \beta \in [\ell_i], \gamma \in [\ell_{i'}], \delta \in [\ell_{i''}]$ such that $S^i[\alpha] \oplus 2^{\alpha-1}k_1 = S^{i'}[\gamma] \oplus 2^{\gamma-1}k_1, S^i[\beta] \oplus 2^{\beta-1}k_1 = S^{i''}[\delta] \oplus 2^{\delta-1}k_1$.

W.l.o.g., suppose $i' > i$ and $i'' > i$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of $S^{i'}[\gamma]$ and $S^{i''}[\delta]$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[B2] \leq \frac{\ell^4 q_e^3}{2^{2n}}.$$

3. $\#\{(i, j) \in [q_e] \times [q_p] : \nu_i \oplus k_0 = u_j\} \geq \sqrt{q_e}$.

For a fixed value of the set of indices, the probability of the event $\nu_i \oplus k_0 = u_j$ is upper bounded by $(1/2^n)$ due to the randomness of k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$E[\#\{(i, j) \in [q_e] \times [q_p] : \nu_i \oplus k_0 = u_j\}] = \frac{q_e q_p}{2^n}.$$

Using Markov's inequality, we obtain

$$\Pr[B3] \leq \frac{\sqrt{q_e q_p}}{2^n}.$$

4. $\#\{(i, j) \in [q_e] \times [q_p], \alpha \in [\ell_i] : S^i[\alpha] \oplus 2^{\alpha-1}k_1 = v_j\} \geq \sqrt{q_e}$.

For a fixed value of the set of indices, the probability of the event $S^i[\alpha] \oplus 2^{\alpha-1}k_1 = v_j$ is upper bounded by $(1/2^n)$ due to the randomness of k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$E[\#\{(i, j) \in [q_e] \times [q_p], \alpha \in [\ell_i] : S^i[\alpha] \oplus 2^{\alpha-1}k_1 = v_j\}] = \frac{\ell q_e q_p}{2^n}.$$

Using Markov's inequality, we obtain

$$\Pr[B4] \leq \frac{\ell \sqrt{q_e q_p}}{2^n}.$$

5. $\exists i \in [q_e], \alpha \neq \beta \in [\ell_i]$ such that $(\nu_i \oplus k_0 \oplus k_1)(2^{\alpha-1} \oplus 2^{\beta-1}) = 0$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of k_0 or k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[B5] \leq \frac{\ell^2 q_e}{2^n}.$$

6. $\exists i \neq j \in [q_e], \alpha \in [\ell_i], \beta \in [\ell_j]$ such that $S^i[\alpha] = S^j[\beta], 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1) = 2^{\beta-1}(\nu_j \oplus k_0 \oplus k_1)$.

W.l.o.g., suppose $i > j$. If $\alpha \neq \beta$, then for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of $S^i[\alpha]$ and k_0 . Else if $\alpha = \beta$, then for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of $S^i[\alpha]$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[B6] \leq \frac{\ell^2 q_e^2}{2^{2n}} + \frac{\ell^2 \mu^2}{2^n}.$$

7. $\exists i \neq j \in [q_e], \alpha \neq \alpha' \in [\ell_i], \beta \neq \beta' \in [\ell_j]$ such that $S^i[\alpha] = S^j[\beta], (2^{\alpha-1} \oplus 2^{\alpha'-1})(\nu_i \oplus k_0 \oplus k_1) = (2^{\beta-1} \oplus 2^{\beta'-1})(\nu_j \oplus k_0 \oplus k_1)$.

W.l.o.g., suppose $i > j$. If $(2^{\alpha-1} \oplus 2^{\alpha'-1}) \neq (2^{\beta-1} \oplus 2^{\beta'-1})$, then for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of $S^i[\alpha]$ and k_0 . Else if $(2^{\alpha-1} \oplus 2^{\alpha'-1}) = (2^{\beta-1} \oplus 2^{\beta'-1})$, then for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of $S^i[\alpha]$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[B7] \leq \frac{\ell^4 q_e^2}{2^{2n}} + \frac{\ell^2 \mu^2}{2^n}.$$

A.3 Analysis of Events C_i

The events C_i are concerned with collision probabilities between construction and primitive queries for ForknEHtM $_p$.

1. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $\text{fix}_{11}(\nu_i \oplus k_1) = U_{j_1}, \text{fix}_{00}(V_{j_1} \oplus k_0) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C1] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

2. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{11}(\nu_i \oplus k_1) = U_{j_1}, \text{fix}_{01}(V_{j_1} \oplus k_0 \oplus H_{k_h}(I^i)) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C2] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

3. $\exists i_1 \neq i_2 \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_1) = U_{j_1}, \text{fix}_{11}(\nu_{i_2} \oplus k_1) = U_{j_2}, \text{fix}_{01}(V_{j_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1})) = \text{fix}_{01}(V_{j_2} \oplus \mathbf{H}_{k_h}(\Gamma^{i_2}))$.

When $\Gamma^{i_1} = \Gamma^{i_2}$, it forces an equality in the first $n-2$ bits of V_{j_1} and V_{j_2} , thus limiting the choice of indices to $4q_p$, and the probability of the event is at most $(1/2^{n-2})$ from the randomness of k_1 . When $\Gamma^{i_1} \neq \Gamma^{i_2}$, the first two equations can be rewritten as $U_{j_1} \oplus \text{fix}_{11}(\nu_{i_1}) = U_{j_2} \oplus \text{fix}_{11}(\nu_{i_2}) = \text{fix}_{11}(k_1)$. We observe that if we fix any three indices, e.g., j_1, i_1 and j_2 , the fourth index (in this case i_2) gets fixed. For a fixed value of the indices j_1, i_1 and j_2 , the probability of the event is upper bounded by $(\mu/2^{n-2})\epsilon_{\text{axu}}$ due to the randomness of k_1 and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C3] \leq \frac{4\mu q_e q_p^2 \epsilon_{\text{axu}}}{2^n} + \frac{4q_p}{2^n}.$$

4. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_1}, \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^i)) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}$ due to the randomness of k_0 and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C4] \leq \frac{4q_e q_p^2 \epsilon_{\text{reg}}}{2^n}.$$

5. $\exists i_1, i_2 \in [q_e], (U, V) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U, \hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1}) = \hat{Z}_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma^{i_2})$. W.l.o.g., suppose $i_1 < i_2$. When $\nu_{i_1} = \nu_{i_2}$, for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{axu}}$ due to the randomness of k_0 and k_h (since this implies $\Gamma^{i_1} \neq \Gamma^{i_2}$). Otherwise, the probability is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ by the randomness of k_0 , and either \hat{Z}_{i_2} or k_1 (the latter when ν_{i_2} is obtained from a backward primitive query by guessing k_1). Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C5] \leq \frac{16q_e^2 q_p}{2^{2n}} + \frac{16q_e^2 q_p \epsilon_{\text{axu}}}{2^n}.$$

6. $i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{01}$ such that $\nu_{i_1} = \nu_{i_2}, \text{fix}_{01}(\hat{Z}_{i_1} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{i_1})) = U$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})$ due to the randomness of k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C6] \leq \frac{4\mu q_p}{2^n}.$$

7. $i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $\text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_1}, V_{j_1} \oplus T_i = V_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and T_i . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C7] \leq \frac{4q_e q_p^2}{2^{2n}}.$$

8. $i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{01}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^i)) = U_{j_1}, V_{j_1} \oplus T_i = V_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and T_i . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C8] \leq \frac{4q_e q_p^2}{2^{2n}}.$$

9. $i_1 \neq i_2 \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_{j_1}, \text{fix}_{00}(\hat{Z}_{i_2} \oplus k_0) = U_{j_2}, V_{j_1} \oplus T_{i_1} = V_{j_2} \oplus T_{i_2}$.

W.l.o.g., suppose $i_1 < i_2$. The first two equations can be rewritten as $U_{j_1} \oplus \text{fix}_{00}(\hat{Z}_{i_1}) = U_{j_2} \oplus \text{fix}_{00}(\hat{Z}_{i_2}) = \text{fix}_{00}(k_0)$. We observe that if we fix any three indices, e.g., j_1, i_1 and j_2 , the fourth index (in this case i_2) gets fixed. For a fixed value of the indices j_1, i_1 and j_2 , the probability of the event is upper bounded by $(\mu/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and T_{i_2} . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C9] \leq \frac{16\mu q_e q_p^2}{2^{2n}}.$$

10. $i_1 \neq i_2 \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{01}(\hat{Z}_{i_1} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{i_1})) = U_{j_1}, \text{fix}_{01}(\hat{Z}_{i_2} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{i_2})) = U_{j_2}, V_{j_1} \oplus T_{i_1} = V_{j_2} \oplus T_{i_2}$.

W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}(1/2^n)$ due to the randomness of k_0, k_h and T_{i_2} . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C10] \leq \frac{4q_e^2 q_p^2 \epsilon_{\text{reg}}}{2^{2n}}.$$

11. $i_1 \neq i_2 \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_{j_1}, \text{fix}_{01}(\hat{Z}_{i_2} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{i_2})) = U_{j_2}, V_{j_1} \oplus T_{i_1} = V_{j_2} \oplus T_{i_2}$.

W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}(1/2^n)$ due to the randomness of k_0, k_h and T_{i_2} . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[C11] \leq \frac{4q_e^2 q_p^2 \epsilon_{\text{reg}}}{2^{2n}}.$$

A.4 Analysis of Events D_i

The events D_i study collisions between two construction queries for ForknEHtM_p .

1. $\exists i \in [q_e]$ such that $T_i = \mathbf{0}$.

For a fixed value of the index, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of T_i . Applying the union bound over all possible values of the index, we obtain

$$\Pr[D1] \leq \frac{q_e}{2^n}.$$

2. $\exists i_1, i_2 \in [q_e]$ such that $\nu_{i_1} = \nu_{i_2}, \mathbf{H}_{k_h}(\Gamma^{i_1}) = \mathbf{H}_{k_h}(\Gamma^{i_2})$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by ϵ_{axu} due to the randomness of k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[D2] \leq \mu^2 \epsilon_{\text{axu}}.$$

3. $\exists i_1, i_2, i_3 \in [q_e]$ such that $\nu_{i_1} = \nu_{i_2}, \hat{Z}_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma^{i_2}) = \hat{Z}_{i_3} \oplus \mathbf{H}_{k_h}(\Gamma^{i_3})$.
 W.l.o.g., suppose $i_2 < i_3$. If $\Gamma^{i_2} \neq \Gamma^{i_3}$, then ν_{i_2} may or may not be equal to ν_{i_3} , and for a fixed value of the set of indices, the probability of the event is upper bounded by ϵ_{axu} due to the randomness of k_h . And if $\Gamma^{i_2} = \Gamma^{i_3}$ then $\nu_{i_2} \neq \nu_{i_3}$, and for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of either \hat{Z}_{i_3} or k_1 (the latter when ν_{i_3} is obtained from a backward primitive query by guessing k_1). Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[D3] \leq 2\mu^2 \epsilon_{\text{axu}} + 2\mu q_e \epsilon_{\text{axu}} + \frac{2\mu q_e}{2^n}.$$

4. $\exists i_1 \neq i_2 \in [q_e]$ such that $\nu_{i_1} = \nu_{i_2}, T_{i_1} = T_{i_2}$.
 W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of T_{i_2} . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[D4] \leq \frac{\mu^2}{2^n}.$$

5. $\exists i_1 \neq i_2 \in [q_e]$ such that $\hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1}) = \hat{Z}_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma^{i_2}), T_{i_1} = T_{i_2}$.
 W.l.o.g., suppose $i_1 < i_2$. When $\nu_{i_1} \neq \nu_{i_2}$, for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of T_{i_2} , and either \hat{Z}_{i_2} or k_1 (the latter when ν_{i_2} is obtained from a backward primitive query by guessing k_1). When $\nu_{i_1} = \nu_{i_2}$, we know that $\Gamma^{i_1} \neq \Gamma^{i_2}$, so the probability of the event is upper bounded by $(1/2^n)\epsilon_{\text{axu}}$ by the randomness of T_{i_2} and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[D5] \leq \frac{q_e^2}{2^{2n}} + \frac{q_e^2 \epsilon_{\text{axu}}}{2^n}.$$

6. $\#\{i \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p : T_i = V_{j_1} \oplus V_{j_2}\} \geq \frac{p^2 q_m}{2^n} + p\sqrt{3nq_m}$.
 By using the sum-capture lemma [12], we obtain

$$\Pr[D6] \leq \frac{2}{2^n}.$$

7. $\{i_1, i_2, \dots, i_\xi\} \subseteq [q_e]$ such that $\hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1}) = \hat{Z}_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma^{i_2}) = \dots = \hat{Z}_{i_\xi} \oplus \mathbf{H}_{k_h}(\Gamma^{i_\xi})$.
 By using the result of the multi-collision theorem, i.e., Theorem 4 of [23], we obtain

$$\Pr[D7] \leq \frac{q_e^2 \epsilon_{\text{axu}}}{2^\xi}.$$

8. $\#\{i \in [q_e], (U, V) \in \text{Tr}_p^{11} : \text{fix}_{11}(\nu_i \oplus k_1) = U\} \geq \sqrt{q_e}$.

For a fixed value of the set of indices, the probability of the event $\text{fix}_{11}(\nu_i \oplus k_1) = U$ is upper bounded by $(1/2^{n-2})$ due to the randomness of k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$E[\#\{i \in [q_e], (U, V) \in \text{Tr}_p^{11} : \text{fix}_{11}(\nu_i \oplus k_1) = U\}] = \frac{4q_e q_p}{2^n}.$$

Using Markov's inequality, we obtain

$$\Pr[D8] \leq \frac{4\sqrt{q_e} q_p}{2^n}.$$

9. $\#\{i \in [q_e], (U, V) \in \text{Tr}_p^{00} : \text{fix}_{00}(\hat{Z}_i \oplus k_0) = U\} \geq \sqrt{q_e}$.

For a fixed value of the set of indices, the probability of the event $\text{fix}_{00}(\hat{Z}_i \oplus k_0) = U$ is upper bounded by $(1/2^{n-2})$ due to the randomness of k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$E[\#\{i \in [q_e], (U, V) \in \text{Tr}_p^{00} : \text{fix}_{00}(\hat{Z}_i \oplus k_0) = U\}] = \frac{4q_e q_p}{2^n}.$$

Using Markov's inequality, we obtain

$$\Pr[D9] \leq \frac{4\sqrt{q_e} q_p}{2^n}.$$

10. $\#\{i \in [q_e], (U, V) \in \text{Tr}_p^{01} : \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^i)) = U\} \geq \sqrt{q_e}$.

For a fixed value of the set of indices, the probability of the event $\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^i)) = U$ is upper bounded by $(1/2^{n-2})$ due to the randomness of k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$E[\#\{i \in [q_e], (U, V) \in \text{Tr}_p^{01} : \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^i)) = U\}] = \frac{4q_e q_p}{2^n}.$$

Using Markov's inequality, we obtain

$$\Pr[D10] \leq \frac{4\sqrt{q_e} q_p}{2^n}.$$

A.5 Analysis of Events E_i

Next, the events E_i consider the verification queries for ForknEHtM_p .

1. $i \in [qd], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{00}(\hat{Z}'_i \oplus k_0) = U_{j_1}, \text{fix}_{01}(\hat{Z}'_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma'^i)) = U_{j_2}, T'_i = V_{j_1} \oplus V_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}$ due to the randomness of k_0 and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[E1] \leq \frac{4qdq_p^2 \epsilon_{\text{reg}}}{2^n}.$$

2. $i_1 \in [q_e], i_2 \in [q_d]$ such that $\nu_{i_1} = \nu'_{i_2}, \hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1}) = \hat{Z}'_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma'^{i_2}), T_{i_1} = T'_{i_2}$.
 Since $\nu_{i_1} = \nu'_{i_2}$, we have $\hat{Z}_{i_1} = \hat{Z}'_{i_2}$. Since $T^{i_1} = T'^{i_2}$, Γ^{i_1} and Γ'^{i_2} cannot be equal, so for a fixed set of indices, the probability of this event is upper bounded by $1/2^n$. Since each encryption nonce can be repeated at most μ times, applying union-bound gives

$$\Pr[E2] \leq \frac{\mu q_d}{2^n}.$$

3. $i_1 \in [q_e], i_2 \in [q_d], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_{j_1}, \text{fix}_{00}(\hat{Z}'_{i_2} \oplus k_0) = U_{j_2}, \text{fix}_{01}(\hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1})) = \text{fix}_{01}(\hat{Z}'_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma'^{i_2})), T'_{i_2} = V_{j_1} \oplus V_{j_2} \oplus T_{i_1}$.
 W.l.o.g., suppose the i_1 -th encryption query is done after the i_2 -th decryption query. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 , and either \hat{Z}_{i_1} or k_1 (the latter when ν_{i_1} is obtained from a backward primitive query by guessing k_1). Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[E3] \leq \frac{16q_e q_d q_p}{2^{2n}}.$$

4. $i_1 \in [q_e], i_2 \in [q_d], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\nu_{i_1} = \nu'_{i_2}, \text{fix}_{01}(\hat{Z}_{i_1} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{i_1})) = U_{j_1}, \text{fix}_{01}(\hat{Z}'_{i_2} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma'^{i_2})) = U_{j_2}, T'_{i_2} = V_{j_1} \oplus V_{j_2} \oplus T_{i_1}$.
 If the encryption query is not done after the other three relevant queries, or none of the permutation queries is both forward and done after the other three relevant queries, then for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}$ due to the randomness of k_0 and k_h . Else, for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}(1/2^{n-2})$ due to the randomness of k_0, k_h and either T_{i_1} or V_{j_1} or V_{j_2} . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[E4] \leq \frac{4\mu q_d q_p^2 \epsilon_{\text{reg}}}{2^n}.$$

5. $i_1 \neq i_2 \in [q_e], i_3 \in [q_d], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_{j_1}, \nu_{i_2} = \nu'_{i_3}, \text{fix}_{01}(\hat{Z}_{i_2} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{i_2})) = U_{j_2}, \text{fix}_{01}(\hat{Z}'_{i_3} \oplus \mathbf{H}_{k_h}(\Gamma'^{i_3})) = \text{fix}_{01}(\hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1})), T'_{i_3} = V_{j_1} \oplus V_{j_2} \oplus T_{i_1} \oplus T_{i_2}$.
 W.l.o.g., suppose the i_1 -th encryption query is done after the i_3 -th decryption query. If one of the encryption queries is not done after the other four relevant queries, or one of the permutation queries is both forward and done after the other four relevant queries, then for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}(1/2^{n-2})$ due to the randomness of k_0, k_h , and either \hat{Z}_{i_1} or k_1 (the latter when ν_{i_1} is obtained from a backward primitive query by guessing k_1). Else for a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}(1/2^{n-2})(1/2^n)$ due to the randomness of k_0, k_h , either \hat{Z}_{i_1} or k_1 (the latter when ν_{i_1} is obtained from a backward primitive query by guessing k_1) and either T_{i_1} or T_{i_2} or V_{j_1} or V_{j_2} . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[E5] \leq \frac{16\mu q_e q_d q_p^2 \epsilon_{\text{reg}}}{2^{2n}}.$$

A.6 Analysis of Events F_i

Finally, the events F_i consider auxiliary bad events between ForkEDM_p and ForknEHtM_p .

1. $k_0 = k_1$.

$$\Pr[F1] \leq \frac{1}{2^n}.$$

2. $\exists i \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, \text{fix}_{11}(\nu_i \oplus k_1) = U_{j_2}$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F2] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

3. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, \text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the first equation is upper bounded by $(1/2^{n-2})$ due to the randomness of k_0 . If $\hat{Z}_i \notin \text{Tr}_p^{11}$ or if $\hat{Z}_i \in \text{Tr}_p^{11}$ such that \hat{Z}_i is the output of a forward permutation query, then the probability of the second equation is upper bounded by $(1/2^{n-2})$ due to the randomness of \hat{Z}_i . Else if $\hat{Z}_i \in \text{Tr}_p^{11}$ such that \hat{Z}_i is the input of a backward permutation query, or in other words, $\text{fix}_{11}(\nu_i \oplus k_1)$ is the output of a backward permutation query, then the probability of the second equation is upper bounded by $(1/2^{n-2})$ due to the randomness of k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F3] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

4. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(I^i)) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{reg}}$ due to the randomness of k_0 and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F4] \leq \frac{4q_e q_p^2 \epsilon_{\text{reg}}}{2^n}.$$

5. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}$ such that $\nu_{i_1} \oplus k_0 = \nu_{i_2} \oplus k_1, \text{fix}_{11}(\nu_{i_1} \oplus k_0) = U$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F5] \leq \frac{4q_e^2 q_p}{2^{2n}}.$$

6. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}$ such that $\nu_{i_1} \oplus k_0 = \nu_{i_2} \oplus k_1, \text{fix}_{11}(\nu_{i_2} \oplus k_1) = U$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F6] \leq \frac{4q_e^2 q_p}{2^{2n}}.$$

7. $\#\{(i_1, i_2) \in [q_e] \times [q_e] : \nu_{i_1} \oplus \nu_{i_2} = k_0 \oplus k_1\} \geq \sqrt{q_e}$.
 For a fixed value of the set of indices, the probability of the event $\nu_{i_1} \oplus \nu_{i_2} = k_0 \oplus k_1$ is upper bounded by $(1/2^n)$ due to the randomness of k_0 or k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$E[\#\{(i_1, i_2) \in [q_e] \times [q_e] : \nu_{i_1} \oplus \nu_{i_2} = k_0 \oplus k_1\}] = \frac{q_e^2}{2^n}.$$

Using Markov's inequality, we obtain

$$\Pr[F7] \leq \frac{q_e^{3/2}}{2^n}.$$

8. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $S_\alpha^i \oplus 2^{\alpha-1}k_1 = V_{j_1}, \text{fix}_{11}(\nu_i \oplus k_1) = U_{j_2}$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of S_α^i and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F8] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

9. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $S_\alpha^i \oplus 2^{\alpha-1}k_1 = V_{j_1}, \text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_2}$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F9] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

10. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{01}$ such that $S_\alpha^i \oplus 2^{\alpha-1}k_1 = V_{j_1}, \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^i)) = U_{j_2}$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F10] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

11. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_0) = U, \nu_{i_1} \oplus k_1 = \nu_{i_2} \oplus k_0$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F11] \leq \frac{4q_e^2 q_p}{2^{2n}}.$$

12. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_0) = U, \nu_{i_1} = \nu_{i_2}$.
 For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})$ due to the randomness of k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F12] \leq \frac{4\mu q_p}{2^n}.$$

13. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_0) = U, \hat{Z}_{i_1} = \hat{Z}_{i_2}$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})$ due to the randomness of k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F13] \leq \frac{8\mu q_p}{2^n}.$$

14. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}, \alpha \in [\ell_{i_2}]$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_0) = U, \hat{Z}_{i_1} = S_\alpha^{i_2} \oplus 2^{\alpha-1}k_1$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F14] \leq \frac{4q_e \sigma_e q_p}{2^{2n}}.$$

15. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{11}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, \hat{Z}_i = V_{j_2}$.
In other words, $\exists i \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_i \oplus k_0) = U_{j_1}, \text{fix}_{11}(\nu_i \oplus k_1) = U_{j_2}$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F15] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

16. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_0) = U, \hat{Z}_{i_1} \oplus \mathbf{H}_{k_h}(\Gamma^{i_1}) = \hat{Z}_{i_2} \oplus \mathbf{H}_{k_h}(\Gamma^{i_2})$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})\epsilon_{\text{axu}}$ due to the randomness of k_0 , and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F16] \leq \frac{4q_e^2 q_p \epsilon_{\text{axu}}}{2^n}.$$

17. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p$ such that $S_\alpha^{i_1} \oplus 2^{\alpha-1}k_1 = V, \text{fix}_{11}(\nu_{i_1} \oplus k_0) = \text{fix}_{11}(\nu_{i_2} \oplus k_1)$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^{n-2})$ due to the randomness of k_1 and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F17] \leq \frac{4q_e^2 q_p}{2^{2n}}.$$

18. $\exists i_1 \neq i_2 \in [q_e], (U, V) \in \text{Tr}_p, \alpha \in [\ell_{i_1}]$ such that $S_\alpha^{i_1} \oplus 2^{\alpha-1}k_1 = V, \nu_{i_1} = \nu_{i_2}$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F18] \leq \frac{\mu \ell q_p}{2^n}.$$

19. $\exists i_1 \neq i_2 \in [q_e], \alpha \in [\ell_{i_1}], (U_{j_1}, V_{j_1}) \in \text{Tr}_p$ such that $S_\alpha^{i_1} \oplus 2^{\alpha-1}k_1 = V_{j_1}, \hat{Z}_{i_1} = \hat{Z}_{i_2}$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)$ due to the randomness of k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F19] \leq \frac{2\ell\mu q_p}{2^n}.$$

20. $\exists i_1 \neq i_2 \in [q_e], \alpha_1 \in [\ell_{i_1}], \alpha_2 \in [\ell_{i_2}], (U_{j_1}, V_{j_1}) \in \text{Tr}_p$ such that $S_{\alpha_1}^{i_1} \oplus 2^{\alpha_1-1}k_1 = V_{j_1}, S_{\alpha_2}^{i_2} \oplus 2^{\alpha_2-1}k_1 = \hat{Z}_{i_1}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of $S_{\alpha_1}^{i_1}$ and $S_{\alpha_2}^{i_2}$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F20] \leq \frac{\sigma_e^2 q_p}{2^{2n}}.$$

21. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $S_{\alpha}^i \oplus 2^{\alpha-1}k_1 = V_{j_1}, \hat{Z}_i = V_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)(1/2^n)$ due to the randomness of S_{α}^i and either \hat{Z}_i or k_1 (the latter when ν_i is obtained from a backward primitive query by guessing k_1). Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F21] \leq \frac{\sigma_e q_p^2}{2^{2n}}.$$

22. $\exists i_1 \neq i_2 \in [q_e], \alpha \in [\ell_{i_1}], (U_{j_1}, V_{j_1}) \in \text{Tr}_p$ such that $S_{\alpha}^{i_1} \oplus 2^{\alpha-1}k_1 = V_{j_1}, \hat{Z}_{i_1} \oplus H_{k_h}(\Gamma^{i_1}) = \hat{Z}_{i_2} \oplus H_{k_h}(\Gamma^{i_2})$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^n)\epsilon_{\text{axu}}$ due to the randomness of k_1 and k_h . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F22] \leq \frac{\ell q_e^2 q_p \epsilon_{\text{axu}}}{2^n}.$$

23. $\exists i_1, i_2 \in [q_e], \alpha_1 \in [\ell_{i_1}], \alpha_2 \in [\ell_{i_2}], (U_j, V_j) \in \text{Tr}_p^{11}$ such that $\text{fix}_{11}(\nu_{i_1} \oplus k_1) = U_j, S_{\alpha_1}^{i_1} \oplus 2^{\alpha_1-1}k_1 = S_{\alpha_2}^{i_2} \oplus 2^{\alpha_2-1}k_1$.

W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_1 and $S_{\alpha_2}^{i_2}$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F23] \leq \frac{4\sigma_e^2 q_p}{2^{2n}}.$$

24. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_1}, \text{fix}_{11}(\nu_i \oplus k_0) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of either \hat{Z}_i or k_1 (the latter when ν_i is obtained from a backward primitive query by guessing k_1) and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F24] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

25. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_1}, \text{fix}_{11}(\nu_i \oplus k_1) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F25] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

26. $\exists i_1, i_2 \in [q_e], (U_j, V_j) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_j, \text{fix}_{11}(\nu_{i_1} \oplus k_0) = \text{fix}_{11}(\nu_{i_2} \oplus k_1)$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F26] \leq \frac{16q_e^2 q_p}{2^{2n}}.$$

27. $\exists i_1, i_2 \in [q_e], (U_j, V_j) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_j, \text{fix}_{11}(\nu_{i_1} \oplus k_1) = \text{fix}_{11}(\nu_{i_2} \oplus k_0)$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F27] \leq \frac{16q_e^2 q_p}{2^{2n}}.$$

28. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{00}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $\text{fix}_{00}(\hat{Z}_i \oplus k_0) = U_{j_1}, S_\alpha^i \oplus 2^{\alpha-1} k_1 = V_{j_2}$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F28] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

29. $\exists i_1, i_2 \in [q_e], \alpha_1 \in [\ell_{i_1}], \alpha_2 \in [\ell_{i_2}], (U_j, V_j) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_j, S_{\alpha_1}^{i_1} \oplus 2^{\alpha_1-1} k_1 = S_{\alpha_2}^{i_2} \oplus 2^{\alpha_2-1} k_1$.

W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and $S_{\alpha_2}^{i_2}$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F29] \leq \frac{4\sigma_e^2 q_p}{2^{2n}}.$$

30. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{01}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus H_{k_h}(\Gamma^i)) = U_{j_1}, \text{fix}_{11}(\nu_i \oplus k_0) = U_{j_2}$.

For a fixed value of the set of indices, the probability of the event is upper bounded by $\epsilon_{\text{reg}}(1/2^{n-2})$ due to the randomness of k_h and k_0 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F30] \leq \frac{4q_e q_p^2 \epsilon_{\text{reg}}}{2^n}.$$

31. $\exists i \in [q_e], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{01}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{11}$ such that $\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^i)) = U_{j_1}, \text{fix}_{11}(\nu_i \oplus k_1) = U_{j_2}$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F31] \leq \frac{16q_e q_p^2}{2^{2n}}.$$

32. $\exists i_1, i_2 \in [q_e], (U_j, V_j) \in \text{Tr}_p^{01}$ such that $\text{fix}_{01}(\hat{Z}_{i_1} \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^{i_1})) = U_j, \text{fix}_{11}(\nu_{i_1} \oplus k_0) = \text{fix}_{11}(\nu_{i_2} \oplus k_1)$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F32] \leq \frac{16q_e^2 q_p}{2^{2n}}.$$

33. $\exists i_1, i_2 \in [q_e], (U_j, V_j) \in \text{Tr}_p^{01}$ such that $\text{fix}_{01}(\hat{Z}_{i_1} \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^{i_1})) = U_j, \text{fix}_{11}(\nu_{i_1} \oplus k_1) = \text{fix}_{11}(\nu_{i_2} \oplus k_0)$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F33] \leq \frac{16q_e^2 q_p}{2^{2n}}.$$

34. $\exists i \in [q_e], \alpha \in [\ell_i], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{01}, (U_{j_2}, V_{j_2}) \in \text{Tr}_p$ such that $\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^i)) = U_{j_1}, S_\alpha^i \oplus 2^{\alpha-1}k_1 = V_{j_2}$.
For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and k_1 . Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F34] \leq \frac{4\sigma_e q_p^2}{2^{2n}}.$$

35. $\exists i_1, i_2 \in [q_e], \alpha_1 \in [\ell_{i_1}], \alpha_2 \in [\ell_{i_2}], (U_{j_1}, V_{j_1}) \in \text{Tr}_p^{01}$ such that $\text{fix}_{01}(\hat{Z}_{i_1} \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^{i_1})) = U_{j_1}, S_{\alpha_1}^{i_1} \oplus 2^{\alpha_1-1}k_1 = S_{\alpha_2}^{i_2} \oplus 2^{\alpha_2-1}k_1$.
W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^n)$ due to the randomness of k_0 and $S_{\alpha_2}^{i_2}$. Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F35] \leq \frac{4\sigma_e^2 q_p}{2^{2n}}.$$

36. $\exists i_1, i_2 \in [q_e], (U_{j_1}, V_{j_1}), (U_{j_2}, V_{j_2}) \in \text{Tr}_p^{00}$ such that $\text{fix}_{00}(\hat{Z}_{i_1} \oplus k_0) = U_{j_1}, \text{fix}_{00}(\hat{Z}_{i_2} \oplus k_0) = U_{j_2}, \nu_{i_1} = \nu_{i_2}$.
W.l.o.g., suppose $i_1 < i_2$. For a fixed value of the set of indices, the probability of the event is upper bounded by $(1/2^{n-2})(1/2^{n-2})$ due to the randomness of k_0 and either \hat{Z}_{i_2} or k_1 (the latter when ν_{i_2} is obtained from a backward primitive query by guessing k_1). Applying the union bound over all possible values of the set of indices, we obtain

$$\Pr[F36] \leq \frac{16\mu^2 q_p^2}{2^{2n}}.$$

Let

$$\begin{aligned} \text{Dom}^{11}(\mathsf{P}) &\leftarrow \mathcal{I}_1^1, \quad \text{Dom}^{10}(\mathsf{P}) \leftarrow \mathcal{X}_1^1, \quad \text{Ran}^{10}(\mathsf{P}) \leftarrow \mathcal{R}_1^1 \\ \text{Dom}^{00}(\mathsf{P}) &\leftarrow \{\text{fix}_{00}(\hat{Z}_i \oplus k_0) : (\nu_i, A^i, M^i, C^i, T^i, Z^i) \in \mathcal{Q}_1\} \\ \text{Dom}^{01}(\mathsf{P}) &\leftarrow \{\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathsf{H}_{k_h}(\Gamma^i)) : (\nu_i, A^i, M^i, C^i, T^i, Z^i) \in \mathcal{Q}_1\} \end{aligned}$$

Note that, $|\text{Dom}^{11}(\mathsf{P})| = \alpha_1$, $|\text{Dom}^{10}(\mathsf{P})| = |\text{Ran}^{10}(\mathsf{P})| = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_1})$ and finally $|\text{Dom}^{00}(\mathsf{P})| = |\text{Dom}^{01}(\mathsf{P})| = \alpha_1$.

B.2 Bounding $\Pr[\mathbf{E.2}]$

As the transcript is good, due to $\overline{\mathsf{F.17}}$, $\mathcal{D}_1^2 \cap \mathcal{I}_1^2 = \emptyset$. Now, we define $\mathcal{X}_1^2 := \{\text{fix}_{10}(\mathsf{P}(\text{fix}_{11}(\nu_i \oplus k_0) \oplus 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)) : \alpha \in [\ell_i], S_\alpha^i \oplus 2^{\alpha-1}k_1 \in \mathcal{V}\}$. As $S_\alpha^i \oplus 2^{\alpha-1}k_1 \in \mathcal{V}$, it implies that $S_\alpha^i \oplus 2^{\alpha-1}k_1 = v_{j_i}$. Thus, we have

$$\begin{aligned} \mathcal{X}_1^2 &:= \{(\text{fix}_{10}(u_{j_1} \oplus (2^{\alpha-1} \oplus 2^{\beta-1})(\nu_i \oplus k_0 \oplus k_1)))_{\alpha, \beta \in [\ell_1]}, \dots, \\ &\quad (\text{fix}_{10}(u_{j_{\alpha_2}} \oplus (2^{\alpha-1} \oplus 2^{\beta-1})(\nu_i \oplus k_0 \oplus k_1)))_{\alpha, \beta \in [\ell_{\alpha_1}]} \}. \end{aligned}$$

Now, as the transcript is good, we have the following:

1. for each $j \in [\alpha_2]$, $\alpha \in [\ell_j]$, $\text{fix}_{10}(u_j \oplus (2^{\alpha-1} \oplus 2^{\beta-1})(\nu_j \oplus k_1)) \notin \mathcal{U}^{10}$; otherwise A.3 and A.8 would hold.
2. for each $j \neq j' \in [\alpha_2]$, $\alpha, \beta \in [\ell_j]$, and $\alpha', \beta' \in [\ell_{j'}]$, $\text{fix}_{10}(u_j \oplus (2^{\alpha-1} \oplus 2^{\beta-1})(\nu_j \oplus k_0 \oplus k_1)) \neq \text{fix}_{10}(u_{j'} \oplus (2^{\alpha'-1} \oplus 2^{\beta'-1})(\nu_{j'} \oplus k_0 \oplus k_1))$; otherwise A.10 and A.11 would hold.

Similarly, for the set \mathcal{R}_1^2 , as the transcript is good, we have the following:

1. for each $j \in [\alpha_2]$ and $\alpha' \neq \alpha \in [\ell_j]$, $S_{\alpha'}^j \oplus 2^{\alpha'-1}k_1 \notin \mathcal{V}$, where $S_\alpha^j \oplus 2^{\alpha-1}k_1 \in \mathcal{V}$; otherwise A.5 would hold.
2. for each $j \in [\alpha_2]$ such that $S_\alpha^j \oplus 2^{\alpha-1}k_1 \in \mathcal{V}$, then for $\alpha' \in [\ell_j]$, $S_{\alpha'}^j \oplus 2^{\alpha'-1}k_1 \neq S_\beta^{j'} \oplus 2^{\beta-1}k_1$ for $j' \in [q_e]$ and $\beta \in [\ell_{j'}]$; otherwise A.6 would hold.

As a result, the set \mathcal{X}_1^2 is permutation compatible with \mathcal{R}_1^2 and $|\mathcal{X}_1^2| = |\mathcal{R}_1^2| = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_2})$. Now, we consider the set \mathcal{I}_1^2 . It is easy to see that due to $\overline{\mathsf{F.8}}$, each element $\text{fix}_{11}(\nu_i \oplus k_1)$ of \mathcal{I}_1^2 does not belong to \mathcal{U}^{11} . Similarly, due to $\overline{\mathsf{F.18}}$, each element of \mathcal{I}_1^2 are distinct. Therefore, $|\mathcal{I}_1^2| = \alpha_2$. Similarly, all the elements $\hat{Z}_1, \hat{Z}_2, \dots, \hat{Z}_{\alpha_2}$ are distinct (due to $\overline{\mathsf{F.19}}$), do not collide with any $S_\alpha^j \oplus 2^{\alpha-1}k_1$ (due to $\overline{\mathsf{F.20}}$), and finally, they do not collide with any primitive query output (due to $\overline{\mathsf{F.21}}$). As a result, the set \mathcal{I}_1^2 is permutation compatible with $(\hat{Z}_1, \hat{Z}_2, \dots, \hat{Z}_{\alpha_2})$.

Now, we consider \mathcal{D}_2^2 and \mathcal{R}_2^2 . As the transcript is good, we have the following:

1. for each $j \in [\alpha_2]$, $\text{fix}_{00}(\hat{Z}_j \oplus k_0) \notin \mathcal{U}^{00}$ and $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \mathsf{H}_{k_h}(\Gamma^j)) \notin \mathcal{U}^{01}$; otherwise F.9 or F.10 would hold.
2. for each $j \neq j' \in [\alpha_2]$, $\hat{Z}_j \oplus \mathsf{H}_{k_h}(\Gamma^j) \neq \hat{Z}_{j'} \oplus \mathsf{H}_{k_h}(\Gamma^{j'})$; otherwise F.22 would hold.

Summing up everything above, we see that permutation P is fixed on a total of

$$\Delta_2 := (\ell_1 + \ell_2 + \dots + \ell_{\alpha_2} + \alpha_2)$$

Let $\Delta_3 = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_3} + \alpha_3)$. Summing up everything above, we have

$$\Pr[\text{E.3}] = \frac{h_{\Delta_3}^3}{(2^n - q_p - \Delta_1 - \Delta_2 - 2\alpha_1 - 2\alpha_2)_{\Delta_3}} \cdot \frac{h_{2\alpha_3}^3}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - 2(\alpha_1 + \alpha_2))_{2\alpha_3}} \quad (7)$$

where $h_{\Delta_3}^3$ denotes the number of solutions to \mathcal{E}_3^1 and $h_{2\alpha_3}^3$ denotes the number of solutions to the bivariate system of affine equations \mathcal{E}_3^2 . It is easy to see that

$$h_{\Delta_3}^3 = \prod_{i=0}^{\Delta_3-1} (2^n - q_p - i - \Delta_1 - \Delta_2 - 2\alpha_1 - 2\alpha_2).$$

Therefore,

$$\Pr[\text{E.3}] = \frac{h_{2\alpha_3}^3}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - 2(\alpha_1 + \alpha_2))_{2\alpha_3}} \quad (8)$$

Finally, we have

$$\begin{aligned} \text{Dom}^{11}(\text{P}) &\leftarrow \mathcal{D}_1^3 \cup \text{Dom}^{11}(\text{P}), \quad \text{Dom}^{10}(\text{P}) \leftarrow \mathcal{X}_1^3 \cup \text{Dom}^{10}(\text{P}), \quad \text{Ran}^{10}(\text{P}) \leftarrow \mathcal{R}_1^3 \cup \text{Ran}^{10}(\text{P}) \\ \text{Dom}^{00}(\text{P}) &\leftarrow \{\text{fix}_{00}(\hat{Z}_i \oplus k_0) : (\nu_i, A^i, M^i, C^i, T^i, Z^i) \in \mathcal{Q}_3\} \cup \text{Dom}^{00}(\text{P}) \\ \text{Dom}^{01}(\text{P}) &\leftarrow \{\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \text{H}_{k_h}(\Gamma^i)) : (\nu_i, A^i, M^i, C^i, T^i, Z^i) \in \mathcal{Q}_3\} \cup \text{Dom}^{01}(\text{P}) \end{aligned}$$

Note that, $|\text{Dom}^{11}(\text{P})| = (\alpha_1 + 2\alpha_2 + \alpha_3)$, $|\text{Dom}^{10}(\text{P})| = |\text{Ran}^{10}(\text{P})| = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_1}) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_2} - \alpha_2) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_3})$ and finally $|\text{Dom}^{00}(\text{P})| = |\text{Dom}^{01}(\text{P})| = (\alpha_1 + \alpha_2 + \alpha_3)$.

B.4 Bounding $\Pr[\text{E.4}]$

As the transcript is good, due to $\overline{\text{F.26}}$ and $\overline{\text{F.27}}$, $\mathcal{D}_1^4 \cap \mathcal{I}_1^4 = \emptyset$. Now, we define $\mathcal{X}_1^4 := \{\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_i \oplus k_0)) \oplus 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)) : \alpha \in [\ell_i], \text{fix}_{00}(\hat{Z}_i \oplus k_0) \in \mathcal{U}^{00}\}$. For each $j \in [\alpha_4]$, $\text{fix}_{00}(\hat{Z}_j \oplus k_0) \in \mathcal{U}^{00}$. For the set \mathcal{R}_1^4 , as the transcript is good, we have the following:

1. for each $j \in [\alpha_4]$ and $\alpha \in [\ell_j]$, $S_\alpha^j \oplus 2^{\alpha-1}k_1 \notin \mathcal{V}$; otherwise F.28 would hold.
2. for each $j \in [\alpha_4]$, $\alpha \in [\ell_j]$, such that $\text{fix}_{00}(\hat{Z}_j \oplus k_0) \in \mathcal{U}^{00}$, then $S_\alpha^j \oplus 2^{\alpha-1}k_1 \neq S_{\alpha'}^{j'} \oplus 2^{\alpha'-1}k_1$ for $j' \in [q_e]$ and $\alpha' \in [\ell_{j'}]$; otherwise F.29 would hold.

As a result, we have the following: for each $j \in [\alpha_4]$,

$$\mathcal{E}_4^1 := \begin{cases} \text{P}(\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_j \oplus k_0)) \oplus \nu_j \oplus k_0 \oplus k_1)) = S_1^j \oplus k_1 \\ \text{P}(\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_j \oplus k_0)) \oplus 2(\nu_j \oplus k_0 \oplus k_1))) = S_2^j \oplus 2k_1 \\ \vdots \\ \text{P}(\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_j \oplus k_0)) \oplus 2^{\ell_j-1}(\nu_j \oplus k_0 \oplus k_1))) = S_{\ell_j}^j \oplus 2^{\ell_j-1}k_1 \end{cases}$$

Now, we consider the set \mathcal{I}_1^4 , where $\mathcal{I}_1^4 := \{\text{fix}_{11}(\nu_1 \oplus k_1), \text{fix}_{11}(\nu_2 \oplus k_1), \dots, \text{fix}_{11}(\nu_{\alpha_4} \oplus k_1)\}$. Since, for each $j \in [\alpha_4]$, $\text{fix}_{00}(\hat{Z}_j \oplus k_0) \in \mathcal{U}^{00}$, we have $\text{fix}_{11}(\nu_j \oplus k_1) \notin \mathcal{U}^{11}$ for $j \in [\alpha_4]$; otherwise the condition C.1 would have hold. Moreover, due to $\overline{\text{F.36}}$, each $\text{fix}_{11}(\nu_j \oplus k_1)$ are distinct. It is easy to see that due to $\overline{\text{C.4}}$, for each $j \in [\alpha_4]$, $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \text{H}_{k_h}(\Gamma)) \notin \mathcal{U}^{01}$. Moreover, due to $\overline{\text{C.5}}$, for $j \neq j' \in [\alpha_4]$, $\hat{Z}_j \oplus \text{H}_{k_h}(\Gamma^j) \neq \hat{Z}_{j'} \oplus \text{H}_{k_h}(\Gamma^{j'})$. We also have, for each $j \in [\alpha_4]$, due to $\overline{\text{C.7}}$, $V_{i_j} \oplus T_j \notin \mathcal{V}$, where $\hat{Z}_j \oplus k_0 = U_{i_j}$. Moreover, due to $\overline{\text{C.9}}$, we

also have $V_{i_j} \oplus T_j \neq V_{i_{j'}} \oplus T_{j'}$, where $\text{fix}_{00}(\hat{Z}_j \oplus k_0) = U_{i_j}$ and $\text{fix}_{00}(\hat{Z}_{j'} \oplus k_0) = U_{i_{j'}}$. Let $\text{fix}_{00}(\hat{Z}_j \oplus k_0) = U_{i_j}$ for $j \in [\alpha_4]$ and $(U_{i_j}, V_{i_j}) \in \text{Tr}_p^{00}$. Therefore, we have the following:

$$\mathcal{E}_4^2 := \begin{cases} \text{P}(\text{fix}_{01}(\hat{Z}_1 \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^1))) = T_1 \oplus V_{i_1} \\ \text{P}(\text{fix}_{01}(\hat{Z}_2 \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^2))) = T_2 \oplus V_{i_2} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{P}(\text{fix}_{01}(\hat{Z}_{\alpha_4} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{\alpha_4}))) = T_{\alpha_4} \oplus V_{i_{\alpha_4}} \end{cases}$$

Let $\Delta_4 = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_4} + \alpha_4)$. Note that, the permutation P is fixed on $\Delta_4 + \alpha_4$ many input-output pairs. Summing up everything above, we have

$$\begin{aligned} \text{Pr}[\text{E.4}] &= \frac{h_{\Delta_4}^4}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - 2(\alpha_1 + \alpha_2 + \alpha_3))_{\Delta_4}} \\ &\quad \cdot \frac{1}{(2^n - q_p - (\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4) - 2(\alpha_1 + \alpha_2 + \alpha_3))_{\alpha_4}} \\ &\quad \cdot \frac{1}{(2^n - q_p - (\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4) - 2(\alpha_1 + \alpha_2 + \alpha_3) - \alpha_4)_{\alpha_4}} \end{aligned}$$

where $h_{\Delta_4}^4$ denotes the number of solutions to \mathcal{E}_4^1 . It is easy to see that

$$h_{\Delta_4}^4 = \prod_{i=0}^{\Delta_4-1} (2^n - q_p - i - \Delta_1 - \Delta_2 - \Delta_3 - 2\alpha_1 - 2\alpha_2 - 2\alpha_3).$$

Therefore,

$$\begin{aligned} \text{Pr}[\text{E.4}] &= \frac{1}{(2^n - q_p - (\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4) - 2(\alpha_1 + \alpha_2 + \alpha_3))_{\alpha_4}} \\ &\quad \cdot \frac{1}{(2^n - q_p - (\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4) - 2(\alpha_1 + \alpha_2 + \alpha_3) - \alpha_4)_{\alpha_4}} \end{aligned} \quad (9)$$

Finally, we have

$$\begin{aligned} \text{Dom}^{11}(\text{P}) &\leftarrow \mathcal{D}_1^4 \cup \mathcal{I}_1^4 \cup \text{Dom}^{11}(\text{P}), \quad \text{Dom}^{10}(\text{P}) \leftarrow \mathcal{X}_1^4 \cup \text{Dom}^{10}(\text{P}), \quad \text{Ran}^{10}(\text{P}) \leftarrow \mathcal{R}_1^4 \cup \text{Ran}^{10}(\text{P}) \\ \text{Dom}^{01}(\text{P}) &\leftarrow \{\text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^i)) : (\nu_i, A^i, M^i, C^i, T^i, Z^i) \in \mathcal{Q}_4\} \cup \text{Dom}^{01}(\text{P}) \\ \text{Ran}^{01}(\text{P}) &\leftarrow \{V_{i_1} \oplus T_1, \dots, V_{i_{\alpha_4}} \oplus T_{\alpha_4}\} \end{aligned}$$

Note that, $|\text{Dom}^{11}(\text{P})| = (\alpha_1 + 2\alpha_2 + \alpha_3 + 2\alpha_4)$, $|\text{Dom}^{10}(\text{P})| = |\text{Ran}^{10}(\text{P})| = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_1}) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_2} - \alpha_2) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_3}) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_4})$ and finally $|\text{Dom}^{00}(\text{P})| = (\alpha_1 + \alpha_2 + \alpha_3)$ and $|\text{Dom}^{01}(\text{P})| = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$.

B.5 Bounding $\text{Pr}[\text{E.5}]$

As the transcript is good, due to $\overline{\text{F.32}}$ and $\overline{\text{F.33}}$, $\mathcal{D}_1^5 \cap \mathcal{I}_1^5 = \emptyset$. Now, we define $\mathcal{X}_1^5 := \{\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_i \oplus k_0)) \oplus 2^{\alpha-1}(\nu_i \oplus k_0 \oplus k_1)) : \alpha \in [\ell_i], \text{fix}_{01}(\hat{Z}_i \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^i)) \in \mathcal{U}^{01}\}$. For each $j \in [\alpha_5]$, $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^j)) \in \mathcal{U}^{01}$. Moreover, for the set \mathcal{R}_1^5 , as the transcript is good, we have the following:

1. for each $j \in [\alpha_5]$ and $\alpha \in [\ell_j]$, $S_\alpha^j \oplus 2^{\alpha-1}k_1 \notin \mathcal{V}$; otherwise F.34 would hold.
2. for each $j \in [\alpha_5]$, $\alpha \in [\ell_j]$, such that $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^j)) \in \mathcal{U}^{01}$, then $S_\alpha^j \oplus 2^{\alpha-1}k_1 \neq S_{\alpha'}^{j'} \oplus 2^{\alpha'-1}k_1$ for $j' \in [q_e]$ and $\alpha' \in [\ell_{j'}]$; otherwise F.35 would hold.

As a result, we have the following: for each $j \in [\alpha_5]$,

$$\mathcal{E}_5^1 := \begin{cases} \text{P}(\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_j \oplus k_0)) \oplus \nu_j \oplus k_0 \oplus k_1)) = S_1^j \oplus k_1 \\ \text{P}(\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_j \oplus k_0)) \oplus 2(\nu_j \oplus k_0 \oplus k_1))) = S_2^j \oplus 2k_1 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{P}(\text{fix}_{10}(\text{P}(\text{fix}_{11}(\nu_j \oplus k_0)) \oplus 2^{\ell_j-1}(\nu_j \oplus k_0 \oplus k_1))) = S_{\ell_j}^j \oplus 2^{\ell_j-1}k_1 \end{cases}$$

Now, we consider the set \mathcal{I}_1^5 , where $\mathcal{I}_1^5 := \{\text{fix}_{11}(\nu_1 \oplus k_1), \text{fix}_{11}(\nu_2 \oplus k_1), \dots, \text{fix}_{11}(\nu_{\alpha_5} \oplus k_1)\}$. Since, for each $j \in [\alpha_5]$, $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^j)) \in \mathcal{U}^{01}$, we have $\text{fix}_{11}(\nu_j \oplus k_1) \notin \mathcal{U}^{11}$ for $j \in [\alpha_5]$; otherwise the condition C.2 would have hold. Moreover, due to $\overline{\text{C.6}}$, each $\text{fix}_{11}(\nu_j \oplus k_1)$ are distinct. It is easy to see that due to $\overline{\text{C.4}}$, for each $j \in [\alpha_5]$, $\text{fix}_{00}(\hat{Z}_j \oplus k_0) \notin \mathcal{U}^{00}$. Moreover, due to $\overline{\text{C.6}}$, for $j \neq j' \in [\alpha_5]$, $\hat{Z}_j \neq \hat{Z}_{j'}$. We also have, for each $j \in [\alpha_5]$, due to $\overline{\text{C.8}}$, $V_{i_j} \oplus T_j \notin \mathcal{V}$, where $\hat{Z}_j \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^j) = U_{i_j}$. Moreover, due to $\overline{\text{C.10}}$, we also have $V_{i_j} \oplus T_{i_j} \neq V_{i_{j'}} \oplus T_{i_{j'}}$, where $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^j)) = U_{i_j}$ and $\text{fix}_{01}(\hat{Z}_{j'} \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^{j'})) = U_{i_{j'}}$. Let $\text{fix}_{01}(\hat{Z}_j \oplus k_0 \oplus \mathbf{H}_{k_h}(\Gamma^j)) = U_{i_j}$ for $j \in [\alpha_5]$ and $(U_{i_j}, V_{i_j}) \in \text{Tr}_p^{01}$. Therefore, we have the following:

$$\mathcal{E}_5^2 := \begin{cases} \text{P}(\text{fix}_{00}(\hat{Z}_1 \oplus k_0)) = T_1 \oplus V_{i_1} \\ \text{P}(\text{fix}_{00}(\hat{Z}_2 \oplus k_0)) = T_2 \oplus V_{i_2} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{P}(\text{fix}_{00}(\hat{Z}_{\alpha_5} \oplus k_0)) = T_{\alpha_5} \oplus V_{i_{\alpha_5}} \end{cases}$$

Let $\Delta_5 = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_5} + \alpha_5)$. Note that, the permutation P is fixed on $\Delta_5 + \alpha_5$ many input-output pairs. Summing up everything above, we have

$$\begin{aligned} \text{Pr}[\text{E.5}] &= \frac{h_{\Delta_5}^5}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4))_{\Delta_5}} \\ &\quad \cdot \frac{1}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - \Delta_5 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4))_{\alpha_5}} \\ &\quad \cdot \frac{1}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - \Delta_5 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) - \alpha_5)_{\alpha_5}} \end{aligned}$$

where $h_{\Delta_5}^5$ denotes the number of solutions to \mathcal{E}_5^1 . It is easy to see that

$$h_{\Delta_5}^5 = \prod_{i=0}^{\Delta_5-1} (2^n - q_p - i - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)).$$

Therefore,

$$\begin{aligned} \text{Pr}[\text{E.5}] &= \frac{1}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - \Delta_5 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4))_{\alpha_5}} \\ &\quad \cdot \frac{1}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - \Delta_5 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) - \alpha_5)_{\alpha_5}} \quad (10) \end{aligned}$$

Finally, we have

$$\begin{aligned}\text{Dom}^{11}(\mathbb{P}) &\leftarrow \mathcal{D}_1^5 \cup \mathcal{I}_1^5 \cup \text{Dom}^{11}(\mathbb{P}), \quad \text{Dom}^{10}(\mathbb{P}) \leftarrow \mathcal{X}_1^5 \cup \text{Dom}^{10}(\mathbb{P}), \quad \text{Ran}^{10}(\mathbb{P}) \leftarrow \mathcal{R}_1^5 \cup \text{Ran}^{10}(\mathbb{P}) \\ \text{Dom}^{00}(\mathbb{P}) &\leftarrow \{\text{fix}_{00}(\hat{Z}_i \oplus k_0) : (\nu_i, A^i, M^i, C^i, T^i, Z^i) \in \mathcal{Q}_5\} \cup \text{Dom}^{01}(\mathbb{P}) \\ \text{Ran}^{00}(\mathbb{P}) &\leftarrow \{V_{i_1} \oplus T_1, \dots, V_{i_{\alpha_5}} \oplus T_{\alpha_5}\}\end{aligned}$$

Note that, $|\text{Dom}^{11}(\mathbb{P})| = (\alpha_1 + 2\alpha_2 + \alpha_3 + 2\alpha_4 + 2\alpha_5)$, $|\text{Dom}^{10}(\mathbb{P})| = |\text{Ran}^{10}(\mathbb{P})| = (\ell_1 + \ell_2 + \dots + \ell_{\alpha_1}) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_2} - \alpha_2) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_3}) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_4}) + (\ell_1 + \ell_2 + \dots + \ell_{\alpha_5})$ and finally $|\text{Dom}^{01}(\mathbb{P})| = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$ and $|\text{Dom}^{00}(\mathbb{P})| = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_5)$.

Due to Theorem 1 of [15], we have

$$\begin{aligned}h_{2\alpha_1}^1 &\geq \frac{(2^n - q_p - \Delta_1)_{2\alpha_1}}{2^{n\alpha_1}} \cdot \left(1 - \sum_{i=1}^k \frac{6\rho_i^2 \binom{\mu_i}{2}}{2^{2n}}\right) \\ h_{2\alpha_2}^2 &\geq \frac{(2^n - q_p - \Delta_1 - \Delta_2 - 2\alpha_1)_{2\alpha_2}}{2^{n\alpha_2}} \cdot \left(1 - \sum_{i=1}^k \frac{6\rho_i^2 \binom{\mu_i}{2}}{2^{2n}}\right) \\ h_{2\alpha_3}^3 &\geq \frac{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - 2(\alpha_1 + \alpha_2))_{2\alpha_3}}{2^{n\alpha_3}} \cdot \left(1 - \sum_{i=1}^k \frac{6\rho_i^2 \binom{\mu_i}{2}}{2^{2n}}\right).\end{aligned}$$

Hence,

$$\begin{aligned}p_1(\text{Tr}^*) &\geq \frac{1}{(2^n - q_p)_{\Delta_1}} \cdot \frac{1}{(2^n - q_p - \Delta_1 - 2\alpha_1)_{\Delta_2}} \cdot \left(1 - \sum_{i=1}^k \frac{18\rho_i^2 \binom{\mu_i}{2}}{2^{2n}}\right) \\ &\cdot \frac{1}{(2^n - q_p - (\Delta_1 + \Delta_2 + \Delta_3 + \Delta_4) - 2(\alpha_1 + \alpha_2 + \alpha_3))_{2\alpha_4}} \\ &\cdot \frac{1}{(2^n - q_p - \Delta_1 - \Delta_2 - \Delta_3 - \Delta_4 - \Delta_5 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4))_{2\alpha_5}}\end{aligned}$$