# Tight Security Bound of 2k-LightMAC_Plus

Nilanjan Datta[1], Avijit Dutta[1] and Samir Kundu[2]

1. Institute for Advancing Intelligence, TCG-CREST, Kolkata
2. Indian Statistical Institute, Kolkata.
nilanjan.datta@tcgcrest.org, avijit.dutta@tcgcrest.com,
samirkundu3@gmail.com

**Abstract.** In ASIACRYPT'17, Naito proposed a beyond-birthday-bound variant of the LightMAC construction, called LightMAC_Plus, which is built on three independently keyed $n$-bit block ciphers, and showed that the construction achieves $2n/3$-bits PRF security. Later, Kim et al. claimed (without giving any formal proof) its security bound to $2^{3n/4}$. In FSE'18, Datta et al. have proposed a two-keyed variant of the LightMAC_Plus construction, called 2k-LightMAC_Plus, which is built on two independently keyed $n$-bit block ciphers, and showed that the construction achieves $2n/3$-bits PRF security. In this paper, we show a tight security bound on the 2k-LightMAC_Plus construction. In particular, we show that it provably achieves security up to $2^{3n/4}$ queries. We also exhibit a matching attack on the construction with the same query complexity and hence establishing the tightness of the security bound. To the best of our knowledge, this is the first work that provably shows a message length independent $3n/4$-bit tight security bound on a block cipher based variable input length PRF with two block cipher keys.

**Keywords:** LightMAC_Plus, H-Coefficient technique, Beyond Birthday Bound, Double Block Hash-then-Sum, 2k-LightMAC_Plus

## 1 Introduction

In FSE'16 [LPTY16], Luykx et al. have proposed LightMAC, which has been standardized by ISO/IEC standardization process. LightMAC is a block cipher based PRF that operates in parallel mode, i.e., for an $n$-bit block cipher $\mathsf{E}$ instantiated with two independently sampled keys $K_1, K_2$, and with a global counter size $s$, the LightMAC function is defined as follows:

$$\mathsf{LightMAC}_{\mathsf{E}_{K_1,K_2}}(M) = \mathsf{E}_{K_2}\left(\sum_{i=1}^{\ell-1} \mathsf{E}_{K_1}(\langle i \rangle_s \| M[i]) \oplus \mathsf{pad}_n(M[\ell])\right),$$

where $\langle i \rangle_s$ denotes the $s$ bit encoding of the integer $i$ and $(M[1], \ldots, M[\ell])$ denotes the $n-s$ bit parsing of message $M$, where each $M[i]$ is an $n-s$ bit string, and $\mathsf{pad}_n$ is an injective function that takes a message and appends to it a suitable number of $10^*$ to make the length of the padded string to be exactly $n$. However, this design comes at the cost of a reduced rate of construction, where the rate of a construction is determined by the ratio of the total number of $n$-bit message blocks in a message $M$ to the total number of primitive calls with block size $n$ required to process the message $M$. Despite having a reduced rate, the design of LightMAC is simple in the sense that it minimizes all auxiliary operations other than having the block cipher calls, which allows to have a low overhead cost, and hence obtains a more compact implementation than PMAC [BR02]. Moreover, due to the inherent parallelism in the design of the scheme, LightMAC outperforms all the other popular sequential MAC constructions in terms of throughput in the parallel computing infrastructure.

### 1.1 Beyond Birthday Bound Secure Variants of LightMAC

Over the years, there have been many proposals of variants of LightMAC construction achieving beyond the birthday bound security. In 2017, Naito [Nai17] proposed LightMAC_Plus construction based on three block cipher keys and showed that the construction is secure against all adversaries that make roughly $2^{2n/3}$ queries. In fact, LightMAC_Plus is the first beyond the birthday bound-secure PRF which is proven to have a message length independent security bound. In the same paper, the author has also proposed LightMAC_Plus2 [Nai17] that provides a higher security bound than LightMAC_Plus or LightMAC, but it comes at the increased number of block cipher calls. In CT-RSA'18 [Nai18], Naito has improved the bound of the LightMAC_Plus construction from $q^3/2^{2n}$ to $q_t^2 q_v/2^{2n}$, where $q_t$ is the number of tagging queries and $q_v$ is the number of verification queries. This security bound implies that LightMAC_Plus is secure up to $2^n$ tagging queries if the number of verification queries is 1. Later, in [LNS18], Leurent et al. have shown a forging attack on the construction that achieves a constant success probability when the number of tagging queries is $2^{3n/4}$ and the number of verification queries is 1, which in turn invalidates the security claim of Naito [Nai18] on LightMAC_Plus. In EUROCRYPT'20, Kim et al. [KLL20] have claimed an improved security bound (but did not supply any formal proof to back up the claim) of LightMAC_Plus construction from $2n/3$-bits to $3n/4$-bits (ignoring the maximum message length), and due to the result of [LNS18], the improved bound of LightMAC_Plus turns out to be the tight one.

In FSE'19, Datta et al. [DDNP18] proposed a two-keyed variant of LightMAC_Plus, called 2K-LightMAC_Plus, where the sum function used in the finalization phase uses the same block cipher key that is independent to the block cipher key used in the internal hash computation of 2K-LightMAC_Plus. Authors have shown that 2K-LightMAC_Plus achieves $2n/3$-bits security bound. In [Nai18], Naito has proposed a single-keyed variant of LightMAC_Plus, dubbed as LightMAC_Plus-1k, in which a single block cipher key is used in the entire construction. However, the $2n$-bits output $(\Sigma, \Theta)$ of the internal hash computation is domain separated by setting their two most significant bits to it 10 and 11, respectively. Moreover, the checksum of the message blocks after padded with the string $0^{n-s}$ is masked with the $\Sigma$ value. Author has shown that LightMAC_Plus-1k achieves $2n/3$-bits security. Recently, Song [Son21] proposed another variant of the single-keyed

LightMAC_Plus construction dubbed as 1k-LightMAC_Plus, in which a single block cipher is used throughout the construction and the $2n$-bit hash value is domain separated by setting their most significant bit to 0 and 1 respectively. It has been shown in [Son21] that 1k-LightMAC_Plus also achieves $2n/3$-bits security bound. Therefore, to summarize, only the LightMAC_Plus construction has been claimed to achieve a tight $3n/4$-bit security bound [KLL20], and all its existing reduced-keyed variants achieve only $2n/3$-bits security. Therefore, the motivation for this paper stems from asking the question

> *Can we prove a tight $3n/4$-bit security bound on any reduced-keyed variants of the* LightMAC_Plus *construction ?*

### 1.2 Our Contribution

In this paper, we answer the above question affirmatively and show that the construction achieves a tight security bound up to $2^{3n/4}$ queries (ignoring the maximum message length). In particular, we have shown an upper bound on the PRF advantage of 2k-LightMAC_Plus in roughly of the order of $2^{3n/4}$ queries, provided the maximum number of message blocks in a query is at most $\min\{2^{n-2}-1, 2^s\}$, and the total number of distinct message blocks across all queries is at most $2^n$, where $n$ denotes the block size of the block cipher and $s$ denotes the size of the block counter. Moreover, we have also shown a matching PRF attack on the construction with query complexity in roughly of the order of $2^{3n/4}$ queries. The schematic diagram of 2k-LightMAC_Plus is shown in Fig. 1. However, to prove the security bound of the construction, we deeply rely on the result of the mirror theory, where we lower the bound on the number of solutions of a given system of equations. The following result establishes an upper bound on the PRF advantage of 2k- LightMAC_Plus against all information-theoretic adversaries.

**Theorem 1.** *Let $\mathcal{K}$ be a finite and non-empty set. Let $\mathsf{E} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Then, the PRF advantage for any $(q, \ell, \sigma, t)$ adversary against* 2k-LightMAC_Plus[E] *is given by,*

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{2k\text{-}LightMAC\_Plus[E]}}(q,\ell,\sigma,t) \le 2\mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(\sigma+2q,t') + \frac{96q^4}{2^{3n}} + \frac{8\sqrt{2}q^2}{2^{3n/2}} + \frac{7q^{4/3}}{2^n} + \frac{39q^{8/3}}{2^{2n}} + \frac{244q^2}{2^{2n}} + \frac{32q^3}{2^{3n}} + \frac{6\sigma}{2^n} + \frac{q}{2^n} + \frac{8}{2^n},$$

*where $\ell \le \min\{2^{n-2}-1, 2^s\}$, is the maximum number of message blocks in a query, $\sigma \le 2^n$, is the total number of distinct message blocks queried, and $t' = O((\sigma+2q)t)$.*

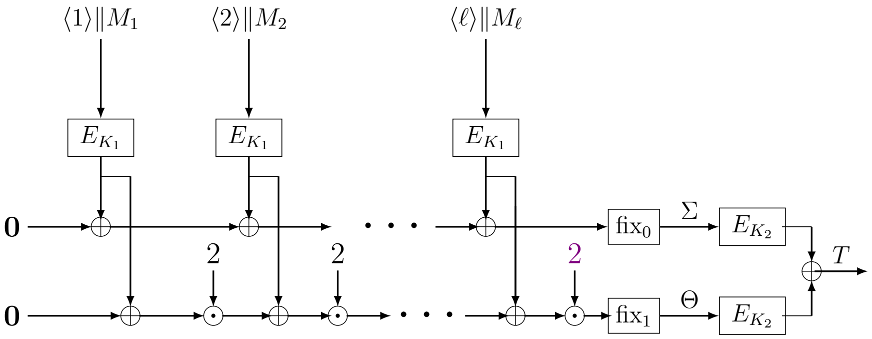

Fig. 1: Pictorial description of the 2k-LightMAC_Plus [DDNP18].

## 2 Preliminaries

General Notations: For $q \in \mathbb{N}$, we write $[q]$ to denote the set $\{1, \ldots, q\}$. For a natural number $n$, $\{0,1\}^n$ denotes the set of all binary strings of length $n$ and $\{0,1\}^*$ denotes the set of all binary strings of arbitrary length. For a natural number $n$, we call the elements of $\{0,1\}^n$ *block*s. For any binary string $x \in \{0,1\}^*$, $|x|$ denotes the length i.e., the number of bits in $x$. For $x, y \in \{0,1\}^n$, we write $z = x \oplus y$ to denote the bitwise xor of $x$ and $y$. For two binary strings $x, y \in \{0,1\}^*$, we write $x\|y$ to denote the concatenation of $x$ followed by $y$. For a natural number $n$ and $x \in \{0,1\}^*$, we write $(x_1, x_2, \ldots, x_{l-1}, x_l) \xleftarrow{n} x$ to denote the $n$-bit parsing of $x$, where $|x_i| = n$ for all $i \in [l-1]$ and $0 < |x_l| \leq n-1$. For any $n \in \mathbb{N}$, we define an injective function $\mathsf{pad}_n$ that takes an arbitrary string $x \in \{0,1\}^*$ and returns $y \in (\{0,1\}^n)^*$, defined as follows:

$$\mathsf{pad}_n(x) \overset{\Delta}{=} x\|10^d,$$

where $d$ is the smallest integer such that $|\mathsf{pad}_n(x)|$ is a multiple of $n$. For two positive integers $i, s$ such that $i < 2^s$, we write $\langle i\rangle_s$ to denote the $s$-bit representation of integer $i$. For $b \in \{0,1\}$, we consider the function $\mathsf{fix}_b$ that takes an $n$-bit binary string $x$ and returns $x$ except its least significant bit is changed to bit $b$. For $b \in \{10, 11\}$, we consider the function $\mathsf{fix}_b$ that takes an $n$-bit binary string $x$ and returns $x$ except its two most significant bits are changed to $b$. For a pair of positive integers $(i,j), (i',j') \in \mathbb{Z}^+ \times \mathbb{Z}^+$, we write $(i,j) \preceq (i',j')$ to denote that either $i < i'$ or ($i = i'$ and $j < j'$).
We write a $q$-tuple $\widetilde{x} = (x_1, \ldots, x_q)$ as $(x_i)_{i \in [q]}$. When all the elements of a tuple $\widetilde{x} = (x_1, \ldots, x_q)$ are distinct, then by abusing of notation, we often write $\widetilde{x}$ as the set $\widetilde{x} = \{x_i : i \in [q]\}$. We write $\mathcal{X}^{(q)}$ to denote the set of all $q$ tuples whose all elements are distinct, i.e.,

$$\mathcal{X}^{(q)} = \{(x_1, \ldots, x_q) : x_i \neq x_j, \forall i \neq j\}.$$

We write $x \leftarrow y$ to denote the assignment of the variable $y$ into $x$. For a set $\mathcal{X}$, $\mathsf{X} \leftarrow_{\$} \{0,1\}^n$ denotes that $\mathsf{X}$ is sampled uniformly at random from $\{0,1\}^n$ and independent to all random variables defined so far. For a tuple of random variables $(X_1, \ldots, X_q)$, we write $(X_1, \ldots, X_q) \leftarrow_{\$} \{0,1\}^n$ to denote that each $X_i$ is sampled uniformly from $\{0,1\}^n$ and independent to all other previously sampled random variables. Similarly, we write $(X_1, \ldots, X_q) \xleftarrow{\text{wor}} \{0,1\}^n$ to denote that each $X_i$ is sampled uniformly from $\{0,1\}^n \setminus \{X_1, \ldots, X_{i-1}\}$, i.e., $X_i \leftarrow_{\$} \{0,1\}^n \setminus \{X_1, \ldots, X_{i-1}\}$. For integers $1 \leq b \leq a$, we write $(a)_b$ to denote $a(a-1)\ldots(a-b+1)$, where $(a)_0 = 1$ by convention.

We denote the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ as $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$. We write $\mathsf{Func}_{\mathcal{X}}$ when $\mathcal{Y} = \{0,1\}^n$. Sometimes, we omit the set $\mathcal{X}$ from $\mathsf{Func}_{\mathcal{X}}$ and simply write $\mathsf{Func}$ when the domain is clear from the context. The set of all permutations over $\mathcal{X}$ is denoted as $\mathsf{Perm}(\mathcal{X})$. When $\mathcal{X} = \{0,1\}^n$, then we omit $\mathcal{X}$ and simply write $\mathsf{Perm}$ to denote the set of all permutations over $\{0,1\}^n$. We say that an $n$-bit permutation $\mathsf{P} \in \mathsf{Perm}$ maps a $q$-tuple $\widetilde{x}$ to an another $q$-tuple $\widetilde{y}$, denoted as $\widetilde{x} \overset{\mathsf{P}}{\mapsto} \widetilde{y}$, where each element of the $\widetilde{x}$ tuple and the $\widetilde{y}$ tuple is an $n$-bit string, if the following holds:

$$\forall i \in [q], \quad \mathsf{P}(x_i) = y_i.$$

We say that a $q$-tuple $\widetilde{x}$ is permutation compatible with an another $q$-tuple $\widetilde{y}$, where each element of both the tuples is an $n$-bit string, if there exists at least one permutation $\mathsf{P} \in \mathsf{Perm}$ such that $\widetilde{x} \overset{\mathsf{P}}{\mapsto} \widetilde{y}$.

### 2.1 Psuedorandom Function and Pseudorandom Permutation

Let $\mathsf{F} : \{0,1\}^k \times \mathcal{X} \to \{0,1\}^n$ be a family of keyed functions from $\mathcal{X}$ to $\{0,1\}^n$. We define the pseudorandom function (prf) advantage of $\mathsf{F}$ with respect to a distinguisher $\mathscr{A}$ as follows:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}}(\mathscr{A}) \overset{\Delta}{=} \Delta_{\mathscr{A}}[\mathsf{F}_K; \mathsf{R}] = \left|\Pr[K \leftarrow \{0,1\}^k : \mathscr{A}^{\mathsf{F}_K} = 1] - \Pr[\mathsf{R} \leftarrow \mathsf{Func} : \mathscr{A}^{\mathsf{R}} = 1]\right|.$$

When $\mathcal{X} = \{0,1\}^n$ such that for every $K \in \{0,1\}^k$, the function $\mathsf{E}_K : \{0,1\}^n \to \{0,1\}^n$ is bijective, then we call $\mathsf{F}$ to be a family of pseudorandom permutation. We say that $\mathsf{F}$ is $(q, \ell, \sigma, \mathtt{t}, \epsilon)$ secure if the maximum pesudorandom function (permutation) advantage of $\mathsf{F}$ is $\epsilon$ where the maximum is taken over all distinguishers $\mathscr{A}$ that makes $q$ queries to its oracle such that the total number of message blocks queried across all $q$ queries is $\sigma$, $\ell$ being the maximum number of message blocks among all $q$ queries, and the adversary runs for time at most $\mathtt{t}$, i.e.,

$$\mathbf{Adv}^{\mathrm{W}}_{\mathsf{F}}(q, \ell, \sigma, \mathtt{t}) \overset{\Delta}{=} \max_{\mathscr{A} \in \mathcal{C}} \mathbf{Adv}^{\mathrm{W}}_{\mathsf{F}}(\mathscr{A}),$$

where $W$ is either prf or prp, $\mathcal{C}$ is the class of all distinguishers $\mathscr{A}$ that makes at most $q$ queries such that the total number of message blocks queried across all $q$ queries is $\sigma$, and $\ell$ being the maximum number of message blocks among all $q$ queries with run time at most $\mathtt{t}$.

The following result from linear algebra will be very useful in establishing the security bound of our construction. Proof of this result can be found in Proposition 1 of [DDN+17].

**Lemma 1.** *Let* $(Z_1, \ldots, Z_q) \xleftarrow{\text{wor}} \mathcal{X} \subseteq \{0,1\}^n$ *with* $|\mathcal{X}| = N > q$*. Let* $A$ *be a* $k \times q$ *binary matrix with rank* $r$*. We denote the column vector* $(Z_1, \ldots, Z_q)^{\mathtt{tr}}$ *as* $\widetilde{\mathsf{Z}}$*. Then, for any* $\widetilde{\mathsf{c}} \in (\{0,1\}^n)^k$*, we have*

$$\Pr[A \cdot \widetilde{\mathsf{Z}} = \widetilde{\mathsf{c}}] \leq \frac{1}{(N-q+r)_r}.$$

### 2.2 Mirror Theory

Consider an undirected edge-labelled acylic graph $\mathsf{G} = (\mathcal{V}, \mathcal{E}, \mathcal{L})$ with edge labelling function $\mathcal{L} : \mathcal{E} \to \{0,1\}^n$, where $\mathcal{V} = \{P_1, \ldots, P_\alpha\}$ be the set of vertices of the graph. For an edge $\{P_i, P_j\} \in \mathcal{E}$, we write $\mathcal{L}(\{P_i, P_j\}) = \lambda_{ij}$. For a path $\mathcal{P}$ and a cycle $\mathcal{C}$ in the graph $\mathsf{G}$, we define the label of the path and the label of the cycle as

$$\mathcal{L}(\mathcal{P}) \triangleq \sum_{e \in \mathcal{P}} \mathcal{L}(e),\ \mathcal{L}(\mathcal{C}) \triangleq \sum_{e \in \mathcal{C}} \mathcal{L}(e).$$

We say the graph $\mathsf{G}$ is **good** if the graph is acylic and for all paths $\mathcal{P}$ of arbitrary length in the graph $\mathsf{G}$, one has $\mathcal{L}(\mathcal{P}) \neq \mathbf{0}$. For such a good graph $\mathsf{G}$, we associate a system of bivariate affine equations as follows:

$$\mathcal{E}_{\mathsf{G}} = Y_i \oplus Z_j = \lambda_{ij}\ \forall\ \{Y_i, Z_j\} \in \mathcal{E}.$$

Note that, in the above system of bivariate affine equations, the variables are the vertices of the associated graph. We say that two variables are involved in an equation, if the corresponding vertices are connected by an edge in the graph. The constants of the equations are the label of the corresponding edges. Therefore, for the system of affine equations $\mathcal{E}_{\mathsf{G}}$, the variables are $Y_i$'s and $Z_i$'s. Now, we define an equivalence relation $\sim$ over $\mathcal{V}$ such that $u \sim v$ if and only if $(u, v) \in \mathcal{E}$. This equivalence relation induces a partition on $\mathcal{V}$ and each partition is called a component. The size of a component refers to the number of elements (i.e., the number of vertices) in the partition. The set of components in $\mathsf{G}$ is denoted by $\mathsf{comp}(\mathsf{G}) = (\mathsf{C}_1 \sqcup \ldots \sqcup \mathsf{C}_\alpha \sqcup \mathsf{D}_1 \sqcup \ldots \sqcup \mathsf{D}_\beta)$ where we assume that there are $\alpha$ many components of $\mathsf{G}$ (i.e., $\mathsf{C}_1, \ldots, \mathsf{C}_\alpha$) with component size greater than 2 and $\beta$ many components of $\mathsf{G}$ (i.e., $\mathsf{D}_1, \ldots, \mathsf{D}_\beta$) having component size exactly 2. We write $\mathsf{C}$ to denote $\mathsf{C}_1 \sqcup \ldots \sqcup \mathsf{C}_\alpha$ and $\mathsf{D}$ to denote $\mathsf{D}_1 \sqcup \ldots \sqcup \mathsf{D}_\beta$. We write $q_c$ to denote the total number of edges in $\mathsf{C}$ and $q$ denotes the total number of edges in the graph $\mathsf{G}$. Then, it is easy to see that $q = q_c + \beta$.

**Notations:** For the $i$-th component of $\mathsf{C}$, i.e., $\mathsf{C}_i$, which is acyclic and edge-labelled graph, let $\mathcal{V}_{\mathsf{C}_i}$ be the set of vertices of the component $\mathsf{C}_i$ and $w_i$ denotes the cardinality of the set $\mathcal{V}_{\mathsf{C}_i}$. Let $\mathcal{V}_{\mathsf{C}}$ denotes the set of vertices of $\mathsf{C}$. For $1 \leq i \leq \alpha$, we write $\sigma_i = w_1 + w_2 + \ldots + w_i$, with the convention that $\sigma_0 = 0$. Note that $q_c = \sigma_\alpha - \alpha$ as each component $\mathsf{C}_i$ is a tree. Let $h(\mathsf{G})$ denote the number of solutions to the graph $\mathsf{G}$. Let $h_c(i)$ denote the number of solutions for the subgraph $\mathsf{C}_1 \sqcup \mathsf{C}_2 \sqcup \ldots \sqcup \mathsf{C}_i$ and $h_d(i)$ denote the number of solutions for the subgraph $\mathsf{C} \sqcup \mathsf{D}^i$ where $\mathsf{D}^i \overset{\Delta}{=} \mathsf{D}_1 \sqcup \mathsf{D}_2 \sqcup \ldots \sqcup \mathsf{D}_i$. Therefore, $h_d(0) = h_c(\alpha)$ and $h_d(\beta) = h(\mathsf{G})$.

**Definition 1.** *Let $\mathcal{E}_\mathsf{G}$ be a system of equations corresponding to a good acyclic edge-labeled graph $\mathsf{G}$ (as defined above). An injective function $\Phi : \mathcal{V} \to \{0,1\}^n$, is said to be an injective solution to $\mathcal{E}_\mathsf{G}$ if $\Phi(P_i) \oplus \Phi(P_j) = \lambda_{ij}$ for all $\{P_i, P_j\} \in \mathcal{E}$ such that $\mathcal{L}(\{P_i, P_j\}) = \lambda_{ij}$.*

In [DDD21], authors have proved that if $\mathsf{G}$ is a good acyclic edge-labeled graph such that it is decomposed into finitely many components of size greater than 2 and exactly 2, then the number of injective solutions chosen from $\{0,1\}^n$, to $\mathcal{E}_\mathsf{G}$, is very close to the average number of solutions until the number of edges in $\mathcal{E}$ is roughly $2^{3n/4}$. Formally, the result is as follows:

**Theorem 2.** *Let $\mathsf{G} = (\mathcal{V}, \mathcal{E}, \mathcal{L})$ be a good acylic edge-labelled graph with $|\mathcal{E}| = q$ edges and $s$ vertices such that $\mathsf{G}$ is decomposed into $\alpha$ many components $\mathsf{C}_1 \sqcup \ldots \sqcup \mathsf{C}_\alpha$ of size at least 3 and $\beta$ many components $\mathsf{D}_1 \sqcup \ldots \sqcup \mathsf{D}_\beta$ of size exactly 2. For $1 \leq i \leq \alpha$, let $w_i$ be the total number of vertices of $\mathsf{C}_1 \sqcup \ldots \sqcup \mathsf{C}_i$ and $q_c$ be the total number of edges in $\mathsf{C}_1 \sqcup \ldots \sqcup \mathsf{C}_\alpha$. Let $\sigma_\alpha = w_1 + w_2 + \ldots + w_\alpha$ be the total number of vertices of $\mathsf{C}_1 \sqcup \mathsf{C}_2 \sqcup \ldots \sqcup \mathsf{C}_\alpha$. Then the total number of injective solutions to $\mathcal{E}_\mathsf{G}$ which are chosen from $\{0,1\}^n$ is at least:*

$$\frac{(2^n)_s}{2^{nq}} \left( 1 - \frac{9q_c^2}{4 \cdot 2^n} - \frac{9q_c^2 q}{2^{2n}} - \frac{24q^2 q_c}{2^{2n}} - \frac{6qq_c}{2^{2n}} - \frac{40q^2}{2^{2n}} - \frac{16q^4}{2^{3n}} \right).$$

We refer the interested reader to [DDD21] for proof of the result.

## 3 Proof of Theorem 1

As the first step of the proof, we replace the underlying block ciphers $\mathsf{E}_{K_1}$ and $\mathsf{E}_{K_2}$ of the construction with a pair of uniformly sampled $n$-bit random permutations $\mathsf{P}_1$ and $\mathsf{P}_2$ at the cost of the prp advantage of $\mathsf{E}$ and denote the resulting construction as $\textsf{2k-LightMAC\_Plus}^*[\mathsf{P}_1, \mathsf{P}_2]$, i.e.,

$$\mathbf{Adv}^{\mathrm{PRF}}_{\textsf{2k-LightMAC\_Plus[E]}}(q, \sigma, t) \leq 2\mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(\sigma, t') + \mathbf{Adv}^{\mathrm{PRF}}_{\textsf{2k-LightMAC\_Plus}^*[\mathsf{P}_1,\mathsf{P}_2]}(q, \sigma).$$

We write 2k-LightMAC_Plus or 2k-LightMAC_Plus$^*$ instead of 2k-LightMAC_Plus[E] or 2k-LightMAC_Plus$^*[\mathsf{P}_1, \mathsf{P}_2]$ whenever the primitives are understood from the context. Now, our goal is to upper bound the information-theoretic PRF security of 2k-LightMAC_Plus$^*$. For doing this, we bound the PRF security of 2k-LightMAC_Plus$^*$ in terms of the distinguishing advantage of an information-theoretic distinguisher $\mathsf{D}$ in distinguishing the output of 2k-LightMAC_Plus$^*$ from the output of an ideal world that consists of a random function $\mathsf{RF}$ which outputs a random $n$-bit tag $T$ on every input $M \in \mathcal{M}$. We assume that the distinguisher $\mathsf{D}$ makes $q$ queries to the oracle in either of the two worlds and at the end of the interaction, the oracle releases some additional information to $\mathsf{D}$. If $\mathsf{D}$ interacts with the oracle in the real world, then it releases $\widetilde{\Sigma} = (\Sigma_1, \Sigma_2, \ldots, \Sigma_q)$ and $\widetilde{\Theta} = (\Theta_1, \Theta_2, \ldots, \Theta_q)$. However, if $\mathsf{D}$ interacts with the oracle in the ideal world, then the oracle also releases $\widetilde{\Sigma}$, $\widetilde{\Theta}$ tuple, where the tuple $\widetilde{\Sigma}$, and $\widetilde{\Theta}$ are computed in the ideal world as described in the following section.

### 3.1 Description of the Ideal World

The ideal oracle consists of two phases: (i) online phase in which for each queried message $M^i$, the oracle samples the response $T_i$ uniformly at random from $\{0,1\}^n$ and returns it to the distinguisher $\mathsf{D}$. If it happens that any of the sampled responses are all zero strings, then we set the bad flag $\mathsf{Bad\text{-}Tag}$ to 1 and abort the game, i.e.,

$$\mathsf{Bad\text{-}Tag} \leftarrow 1 : \exists i \in [q] : T_i = 0^n.$$

When all the queries and responses are over, the offline phase of the ideal world begins. In this phase, we consider a function $\mathcal{L}_1$, which is initially undefined at every point of its domain. The oracle of the ideal world computes $X^i_j = \langle j \rangle_s \| M^i_j$ values for all $i \in [q], j \in [\ell_i]$ and samples $Y^i_j$ as follows: (a) if $X^i_j$ is fresh in $\widetilde{X}$, then $Y^i_j$ is uniformly sampled from outside of the set $\mathsf{Ran}(\mathcal{L}_1)$ followed by including it to the set $\mathsf{Ran}(\mathcal{L}_1)$; (ii) on the other hand, if $X^i_j$ collides with some previous $X^{i'}_{j'}$ value, where $(i', j') \preceq (i, j)$, then $Y^i_j$ is set to the value $Y^{i'}_{j'}$. When all the $Y^i_j$, for $i \in [q], j \in [\ell_i]$ are determined, the oracle computes the tuple $(\Sigma_i, \Theta_i)$ for all $i \in [q]$ as

$$\Sigma_i = \mathsf{fix}_0(Y^i_1 \oplus Y^i_2 \oplus \ldots \oplus Y^i_{\ell_i}), \Theta_i = \mathsf{fix}_1(2^{\ell_i} Y^i_1 \oplus 2^{\ell_i - 1} Y^i_2 \oplus \ldots \oplus 2 Y^i_{\ell_i}).$$

After the computation of the tuple $(\widetilde{\Sigma}, \widetilde{\Theta})$ is over, we set the bad flag $\mathsf{Bad1}$ to 1, if there exists two pairs $(\Sigma_i, \Theta_i)$ and $(\Sigma_j, \Theta_j)$ such that $(\Sigma_i, \Theta_i) = (\Sigma_j, \Theta_j)$ holds, i.e.,

$$\mathsf{Bad1} \leftarrow 1 : \exists i \neq j \in [q] : (\Sigma_i, \Theta_i) = (\Sigma_j, \Theta_j).$$

Moreover, we set the bad flag $\mathsf{Bad2}$ to 1, if there exists two pairs $(\Sigma_i, T_i)$ and $(\Sigma_j, T_j)$ such that $(\Sigma_i, T_i) = (\Sigma_j, T_j)$ holds, i.e.,

$$\mathsf{Bad2} \leftarrow 1 : \exists i \neq j \in [q] : (\Sigma_i, T_i) = (\Sigma_j, T_j).$$

Similarly, we set the bad flag $\mathsf{Bad3}$ to 1, if there exists two pairs $(\Theta_i, T_i)$ and $(\Theta_j, T_j)$ such that $(\Theta_i, T_i) = (\Theta_j, T_j)$ holds, i.e.,

$$\mathsf{Bad3} \leftarrow 1 : \exists i \neq j \in [q] : (\Theta_i, T_i) = (\Theta_j, T_j).$$

We set the bad flag $\mathsf{Bad4}$ to 1 if there exists three distinct indices $i_1, i_2, i_3 \in [q]$ such that $\Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} = 0^n$ holds, i.e.,

$$\mathsf{Bad4} \leftarrow 1 : \exists i_1, i_2, i_3 \in [q] : \Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} = 0^n.$$

We set the bad flag $\mathsf{Bad5}$ to 1 if there exists four distinct indices $i_1, i_2, i_3, i_4 \in [q]$ such that $\Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, \Sigma_{i_3} = \Sigma_{i_4}$ holds, i.e.,

$$\mathsf{Bad5} \leftarrow 1 : \exists i_1, i_2, i_3, i_4 \in [q] : \Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, \Sigma_{i_3} = \Sigma_{i_4}.$$

We set the bad flag $\mathsf{Bad6}$ to 1 if there exists four distinct indices $i_1, i_2, i_3, i_4 \in [q]$ such that $\Theta_{i_1} = \Theta_{i_2}, \Sigma_{i_2} = \Sigma_{i_3}, \Theta_{i_3} = \Theta_{i_4}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} \oplus T_{i_4} = 0^n$ holds, i.e.,

$$\mathsf{Bad6} \leftarrow 1 : \exists i_1, i_2, i_3, i_4 \in [q] : \Theta_{i_1} = \Theta_{i_2}, \Sigma_{i_2} = \Sigma_{i_3}, \Theta_{i_3} = \Theta_{i_4}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} \oplus T_{i_4} = 0^n.$$

Finally, we set the bad flag $\mathsf{Bad7}$ to 1 if the number of colliding pairs for $\Sigma$ or $\Theta$ values is at least $q^{2/3}$, i.e.,

$$\mathsf{Bad7} \leftarrow 1 : \begin{cases} |\{(i,j) : i \neq j \in [q], \Sigma_i = \Sigma_j\}| \geq q^{2/3} \text{ or} \\ |\{(i,j) : i \neq j \in [q], \Theta_i = \Theta_j\}| \geq q^{2/3}. \end{cases}$$

The offline phase of the ideal world is depicted in Fig. 2.

Therefore, we summarize the interaction of $\mathsf{D}$ with the oracle in the following attack transcript

$$\tau = \{(M_1, T_1, \Sigma_1, \Theta_1), (M_2, T_2, \Sigma_2, \Theta_2), \ldots, (M_q, T_q, \Sigma_q, \Theta_q)\}.$$

Let $\mathsf{T}_{\mathrm{re}}$ denote the random variable that takes a transcript $\tau$ realized in the real world. Similarly, $\mathsf{T}_{\mathrm{id}}$ denotes the random variable that takes a transcript $\tau$ realized in the ideal world. The probability of realizing a transcript $\tau$ in the ideal (resp. real) world is called the *ideal* (*resp. real*) *interpolation probability.* A transcript $\tau$ is said to be attainable with respect to $\mathsf{D}$ if its ideal interpolation probability is non-zero, and $\Theta$ denotes the set of all such attainable transcripts. Following these notations, we now state the main theorem of the H-Coefficient technique [Pat08]:

**Theorem 3 (H-Coefficident Technique).** *Let* $\Theta = \mathsf{GoodT} \sqcup \mathsf{BadT}$ *be a partition of the set of attainable transcripts. Suppose there exists* $\epsilon_{\mathrm{ratio}} \geq 0$ *such that for any* $\tau \in \mathsf{GoodT}$*,*

$$\frac{\mathsf{p}_{\mathrm{re}}(\tau)}{\mathsf{p}_{\mathrm{id}}(\tau)} \triangleq \frac{\Pr[\mathsf{T}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{T}_{\mathrm{id}} = \tau]} \geq 1 - \epsilon_{\mathrm{ratio}},$$

*and there exists* $\epsilon_{\mathrm{bad}} \geq 0$ *such that* $\Pr[\mathsf{T}_{\mathrm{id}} \in \mathsf{BadT}] \leq \epsilon_{\mathrm{bad}}$*. Then*

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{2k\text{-}LightMAC\_Plus}^*}(\mathsf{D}) \leq \epsilon_{\mathrm{ratio}} + \epsilon_{\mathrm{bad}}. \tag{1}$$

Therefore, to prove the security of the construction using the H-Coefficient technique, we need to identify the set of bad transcripts and compute an upper bound for their probability in the ideal world. Then we need to lower bound the ratio of the real to ideal interpolation probability for a good transcript.

```
Offline Phase of $\mathcal{O}_{\text{ideal}}$, Initialize $\mathcal{L}_1 = \emptyset$

$\forall i \in [q]$ : compute $(\Sigma_i, \Theta_i) \leftarrow$ $\mathsf{Internal}^{\mathcal{L}_1}(M^i)$
    $\forall j \in [\ell_i]$ :  $X^i_j \leftarrow \langle j \rangle_s \| M^i_j$;
    if $\mathcal{L}_1(X^i_j) = \top$, then
        $\mathcal{L}_1(X^i_j) \leftarrow Y^i_j \xleftarrow{\$} \overline{\mathsf{Ran}(\mathcal{L}_1)}$;
    else $Y^i_j \leftarrow \mathcal{L}_1(X^i_j)$;
    $\Sigma_i := \mathsf{fix}_0(Y^i_1 \oplus \cdots \oplus Y^i_{\ell_i})$;
    $\Theta_i := \mathsf{fix}_1(2^{\ell_i} Y^i_1 \oplus \cdots \oplus 2^2 Y^i_{\ell_i - 1} \oplus 2 Y^i_{\ell_i})$;
    return $(\Sigma_i,\ \Theta_i)$;
Let $\widetilde{\Sigma} = (\Sigma_1, \ldots, \Sigma_q), \widetilde{\Theta} = (\Theta_1, \ldots, \Theta_q)$;
if $\exists i \neq j \in [q] : (\Sigma_i, \Theta_i) = (\Sigma_j, \Theta_j)$, then $\boxed{\mathsf{Bad1} \leftarrow 1}$ , $\perp$;
if $\exists i \neq j \in [q] : (\Sigma_i, T_i) = (\Sigma_j, T_j)$, then $\boxed{\mathsf{Bad2} \leftarrow 1}$ , $\perp$;
if $\exists i \neq j \in [q] : (\Theta_i, T_i) = (\Theta_j, T_j)$, then $\boxed{\mathsf{Bad3} \leftarrow 1}$ , $\perp$;
if $\exists i_1, i_2, i_3 \in [q] : \Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} = 0^n$, then $\boxed{\mathsf{Bad4} \leftarrow 1}$ , $\perp$;
if $\exists i_1, i_2, i_3, i_4 \in [q] : \Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, \Sigma_{i_3} = \Sigma_{i_4}$, then $\boxed{\mathsf{Bad5} \leftarrow 1}$ , $\perp$;
if $\exists i_1, i_2, i_3, i_4 \in [q] : \Theta_{i_1} = \Theta_{i_2}, \Sigma_{i_2} = \Sigma_{i_3}, \Theta_{i_3} = \Theta_{i_4}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} \oplus T_{i_4} = 0^n$,
 then $\boxed{\mathsf{Bad6} \leftarrow 1}$ , $\perp$;
 $\mathcal{F}_\Sigma \leftarrow \{(i,j) \in [q]^2 : \exists i \neq j,\ \Sigma^i = \Sigma^j\}$; $\mathcal{F}_\Theta \leftarrow \{(i,j) \in [q]^2 : \exists i \neq j,\ \Theta^i = \Theta^j\}$;
 if $|\mathcal{F}_\Sigma| \geq q^{2/3} \vee |\mathcal{F}_\Theta| \geq q^{2/3}$, then $\boxed{\mathsf{Bad7} \leftarrow 1}$ , $\perp$;
 return $\left( (\widetilde{X}_i, \widetilde{Y}_i)_{i \in [q]}, (\widetilde{\Sigma}, \widetilde{\Theta}) \right)$;
```

Fig. 2: Offline phase of the Ideal oracle $\mathcal{O}_{\text{ideal}}$: Boxed statements denote bad events. Whenever a bad event is set to 1, the oracle immediately aborts (denoted as $\perp$) and returns the remaining values of the transcript in any arbitrary manner. So, if we proceed further we can surely assume that the event $\perp$ (and so any bad event so far) does not hold. We write $\top$ when the value of a variable is not defined.

### 3.2 Definition and Probability of Bad Transcripts

In this section, we define and bound the probability of bad transcripts in the ideal world. We say that an attainable transcript $\tau$ is a **bad** transcript if anyone the bad flags, defined in the offline phase of the ideal world as shown in Fig. 2, is set to 1. Recall that $\mathsf{BadT} \subseteq \Theta$ be the set of all attainable bad transcripts and $\mathsf{GoodT} = \Theta \setminus \mathsf{BadT}$ be the set of all attainable good transcripts. We bound the probability of bad transcripts in the ideal world as follows. Before we proceed to bound the above events in the ideal world, we state the following two lemmas that upper bounds the collision probability between two $\varSigma$ (or $\varTheta$) values for two distinct queries. We emphasize that the following result will be frequently used in upper bounding the probability of the above bad events.

**Lemma 2.** *For distinct two messages $M_\alpha$ and $M_\beta$, we have*

$$(i)\ \Pr[\varSigma_\alpha = \varSigma_\beta] \le \frac{4}{2^n}, \quad (ii)\ \Pr[\varTheta_\alpha = \varTheta_\beta] \le \frac{4}{2^n}.$$

**Proof.** We prove only $(i)$ as the proof of $(ii)$ is exactly similar to $(i)$. Suppose the number of blocks of $M_\alpha$ and $M_\beta$ be $\ell_\alpha$ and $\ell_\beta$ respectively. Without loss of generality, we assume that $\ell_\alpha \le \ell_\beta$. Now,

$$\varSigma_\alpha = \varSigma_\beta \Rightarrow \mathsf{msb}_{n-1}\Bigg(\underbrace{\bigoplus_{i=1}^{\ell_\alpha} Y_\alpha[i] \oplus \bigoplus_{i=1}^{\ell_\beta} Y_\beta[i]}_{\mathfrak{F}}\Bigg) = 0^{n-1}. \tag{2}$$

For computing the probability of the above event, we consider the following three cases.

1. $(\ell_\alpha = \ell_\beta) \wedge (\exists a \in [\ell_\alpha] : X_\alpha[a] \neq X_\beta[a]) \wedge (\forall i \in [\ell_\alpha] \setminus \{a\} : X_\alpha[i] = X_\beta[i])$
2. $(\ell_\alpha = \ell_\beta) \wedge (\exists a, b \in [\ell_\alpha] : X_\alpha[a] \neq X_\beta[a] \wedge X_\alpha[b] \neq X_\beta[b])$
3. $(\ell_\alpha \neq \ell_\beta)$.

**Case 1:** Since $X_\alpha[a] \neq X_\beta[a] \Rightarrow Y_\alpha[a] \neq Y_\beta[a]$ and $X_\alpha[i] = X_\beta[i] \Rightarrow Y_\alpha[i] = Y_\beta[i]$, for $i \in [\ell_\alpha] \setminus \{a\}$, $\mathfrak{F} \neq 0^n$. So, the probability of $\varSigma_\alpha = \varSigma_\beta$ is $1/2^{n-1}$.

**Case 2:** Suppose $\exists a_1, a_2, \ldots, a_j \in [\ell_\alpha]$, $j \ge 2$ such that, for all $i \in [j]$, $X_\alpha[a_i] \neq X_\beta[a_i]$. After eliminating all the same outputs between $\{Y_\alpha[i] : 1 \le i \le \ell_\alpha\}$ and $\{Y_\beta[i] : 1 \le i \le \ell_\beta\}$, we have

$$\mathfrak{F} = \bigoplus_{i=1}^{j} \left(Y_\alpha[a_i] \oplus Y_\beta[a_i]\right).$$

Since $\mathfrak{F}$ has at most $\ell_\alpha + \ell_\beta$ outputs, the probability of $\mathfrak{F} = 0^n$ is $1/(2^n - \ell_\alpha - \ell_\beta - 1)$.

**Case 3:** Without loss of generality, we assume that $\ell_\alpha < \ell_\beta$. Similarly from the previous case, after eliminating the same outputs between $\{Y_\alpha[i] : 1 \le i \le \ell_\alpha\}$

and $\{Y_\beta[i] : 1 \leq i \leq \ell_\beta\}$, we have

$$\mathfrak{F} = \bigoplus_{i=1}^{j} Y_\alpha[a_i] \oplus \bigoplus_{i=1}^{k} Y_\beta[a_i],$$

where $a_1, \ldots, a_j \in [\ell_\alpha]$ and $b_1, \ldots, b_k \in [\ell_\beta]$. Also, by the similar argument of case 2, we have the probability of $\mathfrak{F} = 0^n$ is at most $1/(2^n - \ell_\alpha - \ell_\beta - 1)$. Hence,

$$\begin{aligned} \Pr[\Sigma_\alpha = \Sigma_\beta] &\leq \frac{2}{(2^n - \ell_\alpha - \ell_\beta - 1)} \\ &\leq \frac{4}{2^n}, \text{ assuming } \ell_\alpha + \ell_\beta \leq 2^{n-1}. \end{aligned} \qquad \square$$

Now, we are ready to bound the probability of the above bad events and hence, we bound the probability of realizing a bad transcript in the ideal world as follows:

**Lemma 3 (Bad Lemma).** *Let us define the event* $\mathsf{BadT} := \mathsf{Bad\text{-}Tag} \vee \mathsf{Bad1} \vee \mathsf{Bad2} \vee \mathsf{Bad3} \vee \mathsf{Bad4} \vee \mathsf{Bad5} \vee \mathsf{Bad6} \vee \mathsf{Bad7}_a \vee \mathsf{Bad7}_b$. *Let* $\tau'$ *be any attainable transcript and* $\mathsf{X}_{\mathrm{id}}$ *be defined as above. Then*

$$\Pr[\mathsf{X}_{\mathrm{id}} \in \mathsf{BadT}] \leq \frac{204q^2}{2^{2n}} + \frac{80q^4}{2^{3n}} + \frac{8\sqrt{2}q^2}{2^{3n/2}} + \frac{8}{2^n} + \frac{q}{2^n} + \frac{6\sigma}{2^n} + \frac{4q^{4/3}}{2^n} + \frac{32q^3}{2^{3n}}.$$

**Proof.** We upper bound the probability of individual bad events in the ideal world and then by the virtue of the union bound, we sum up the bounds to obtain the overall bound on the probability of bad transcripts in the ideal world.

**1. <u>Bound for $\mathsf{Bad\text{-}Tag}$ :</u>** For a fixed $i \in [q]$, the probability that $T_i = 0^n$ is exactly $2^{-n}$, which follows from the uniform sampling of the output for the $i$-th query in the ideal world. Therefore, by varying over all possible choices fo $i$, we have

$$\Pr[\mathsf{Bad\text{-}Tag}] = \Pr[\exists i \in [q] : T_i = 0^n] \leq \frac{q}{2^n}. \tag{3}$$

**2. <u>Bound for $\mathsf{Bad1}$ :</u>** For a fixed $i \neq j \in [q]$, $(\Sigma_i, \Theta_i) = (\Sigma_j, \Theta_j)$ implies the following two equations:

$$\mathcal{E} = \begin{cases} \underbrace{\mathsf{msb}_{n-1}\Big( (Y_i[1] \oplus \ldots \oplus Y_i[\ell_i]) \oplus (Y_j[1] \oplus \ldots \oplus Y_j[\ell_j]) \Big)}_{S_1} = 0^{n-1} \\ \underbrace{\mathsf{msb}_{n-1}\Big( (2^{\ell_i} Y_i[1] \oplus \ldots \oplus 2Y_i[\ell_i]) \oplus (2^{\ell_j} Y_j[1] \oplus \ldots \oplus 2Y_j[\ell_j]) \Big)}_{S_2} = 0^{n-1}, \end{cases}$$

where $\ell_i$ and $\ell_j$ denotes the number of blocks of message $M_i$ and $M_j$. We bound the probability of the above equation holds in the three disjoint cases as follows:

1. $(\ell_i = \ell_j) \wedge (\exists a \in [\ell_i] : X_i[a] \neq X_j[a]) \wedge (\forall \alpha \in [\ell_i] \setminus \{a\} : X_i[\alpha] = X_j[\alpha])$
2. $(\ell_i = \ell_j) \wedge (\exists a, b \in [\ell_i] : X_i[a] \neq X_j[a] \wedge X_i[b] \neq X_j[b])$
3. $(\ell_i \neq \ell_j)$.

**Case 1:** Since $X_i[a] \neq X_j[a] \Rightarrow Y_i[a] \neq Y_j[a]$ and $X_i[\alpha] = X_j[\alpha] \Rightarrow Y_i[\alpha] = Y_j[\alpha]$, for $\alpha \in [\ell_i] \setminus \{a\}$, $\bigoplus_{t=1}^{\ell_i} Y_i[t] \oplus \bigoplus_{t=1}^{\ell_j} Y_j[t] \neq 0^{n-1}$. So, the probability of $S_1 = 0^{n-1}$ is $1/2^n$ and also the probability of $S_2 = 0^{n-1}$ is $1/2^{n-1}$. Thus, the probability that satisfies equation $\mathcal{E}$ is $1/2^{2n-2}$.

**Case 2:** Suppose $\exists a_1, a_2, \ldots, a_p \in [\ell_i]$, $p \geq 2$ such that, for all $t \in [p]$, $X_i[a_t] \neq X_j[a_t]$. After eliminating all the same outputs between $\{Y_i[\alpha] : 1 \leq \alpha \leq \ell_i\}$ and $\{Y_j[\alpha] : 1 \leq \alpha \leq \ell_j\}$, we have

$$S_1 = \mathsf{msb}_{n-1}\left(\bigoplus_{t=1}^{p} (Y_i[a_t] \oplus Y_j[a_t])\right), \; S_2 = \mathsf{msb}_{n-1}\left(\bigoplus_{t=1}^{p} 2^{\ell_i - a_t + 1} (Y_i[a_t] \oplus Y_j[a_t])\right). \tag{4}$$

Note that, there are at most $\ell_i + \ell_j$ outputs in $S_1$ and $S_2$. Therefore, the numbers of possibilities for $Y_i[a_1]$ and $Y_i[a_2]$ are at least $2^n - (\ell_i + \ell_j - 2)$ and $2^n - (\ell_i + \ell_j - 1)$ respectively. Therefore, by fixing the values to the other output variables of equations in $\mathcal{E}$, the equations in $\mathcal{E}$ provide a unique solution for $Y_i[a_1]$ and $Y_i[a_2]$. As a result, the probability that equation $\mathcal{E}$ is satisfied is at most $4/(2^n - (\ell_i + \ell_j - 2))(2^n - (\ell_i + \ell_j - 1))$.

**Case 3:** Without loss of generality, we assume that $\ell_i < \ell_j$. Similar to the previous case, after eliminating the same outputs between $\{Y_i[\alpha] : 1 \leq \alpha \leq \ell_i\}$ and $\{Y_j[\alpha] : 1 \leq \alpha \leq \ell_j\}$, we have

$$\begin{aligned} S_1 &= \mathsf{msb}_{n-1}\left(\bigoplus_{t=1}^{p_1} Y_i[a_t] \oplus \bigoplus_{t=1}^{p_2} Y_j[a_t]\right), \\ S_2 &= \mathsf{msb}_{n-1}\left(\bigoplus_{t=1}^{p_1} 2^{\ell_i - a_t + 1} Y_i[a_t] \oplus \bigoplus_{t=1}^{p_2} 2^{\ell_j - a_t + 1} Y_j[a_t]\right), \end{aligned} \tag{5}$$

where $a_1, \ldots, a_{p_1} \in [\ell_i]$ and $b_1, \ldots, b_{p_2} \in [\ell_j]$. By $\ell_i < \ell_j$, we have $\ell_j \in \{b_1, \ldots, b_{p_2}\}$ and $\ell_j \neq 1$. Since, there are at most $\ell_i + \ell_j$ outputs in $S_1$ and in $S_2$, the number of possibilities for $Y_j[b_1]$ and $Y_j[\ell_j]$ is at least $(2^n - (\ell_i + \ell_j - 2))(2^n - (\ell_i + \ell_j - 1))$. By fixing the values to the other output variables of equations in $\mathcal{E}$, the equations in $\mathcal{E}$ provide a unique solution for $Y_j[b_1]$ and $Y_j[\ell_j]$. As a result, the probability that equation $\mathcal{E}$ is satisfied is at most $4/(2^n - (\ell_i + \ell_j - 2))(2^n - (\ell_i + \ell_j - 1))$.

Therefore, we see that for each of the above case, equations in $\mathcal{E}$ holds with probability at most $4/(2^n - (\ell_i + \ell_j - 2))(2^n - (\ell_i + \ell_j - 1))$. Therefore, we have

$$\Pr[\mathsf{Bad1}] \leq \frac{4\binom{q}{2}}{(2^n - (\ell_i + \ell_j - 2))(2^n - (\ell_i + \ell_j - 1))} \leq \frac{8q^2}{2^{2n}}, \tag{6}$$

where the second last inequality follows due to the fact that $\ell_i + \ell_j - 1 \leq 2^{n-1}$.

**3. Bound for $\mathsf{Bad2}$:** To bound the probability of the event $\mathsf{Bad2}$, for a fixed choice of indices $i \neq j \in [q]$,

$$\Pr[\Sigma_i = \Sigma_j, T_i = T_j] \overset{(1)}{=} \Pr[\Sigma_i = \Sigma_j] \cdot \Pr[T_i = T_j] \overset{(2)}{=} \frac{4}{2^n} \times \frac{1}{2^n} = \frac{4}{2^{2n}},$$

where (1) follows due to the fact that the distribution of $T_i$ is independent over the distribution of $\Sigma_i$ in the ideal world and (2) follows from Lemma 2 and from the event that $T_i = T_j$ holds with probability $2^{-n}$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\mathsf{Bad2}] = \Pr[\exists i \neq j \in [q] : (\Sigma_i, T_i) = (\Sigma_j, T_j)] \leq \frac{2q^2}{2^{2n}} \tag{7}$$

**4. Bound for $\mathsf{Bad3}$:** We bound the probability of the event $\mathsf{Bad3}$ in a similar way as we have bounded the probability of the event $\mathsf{Bad2}$. Using the exact argument as used in bounding the probability of the event $\mathsf{Bad2}$, we similarly bound the probability of the event $\mathsf{Bad3}$ and hence, we have

$$\Pr[\mathsf{Bad3}] \leq \frac{2q^2}{2^{2n}}. \tag{8}$$

**5.Bound for $\mathsf{Bad4}$:** To obtain the bound for $\mathsf{Bad4}$, we first define an auxiliary bad event

$$\mathsf{Aux\text{-}Bad} := Y_i[j] \in \{0^n, 0^{n-1}1\}.$$

It is easy to see that $\mathsf{Pr}[\mathsf{Aux\text{-}Bad}] \leq \frac{2\sigma}{2^n}$, if $\sigma$ is the total number of blocks over all the $q$ queries. Now we will obtain the bound for $\mathsf{Bad4}$ assuming that the auxiliary bad doesn't occur. Suppose $\ell$ be the maximum number of message blocks among all the $q$ queries. After fixing a triplet $(i_1, i_2, i_3)$, $\Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}$ can be represented by a system of three linear equations as follows:

$$\begin{aligned} \Sigma'_{i_1} &= \Sigma'_{i_2} \oplus 0^{n-1}b_1 \Leftrightarrow \bigoplus_{j=1}^{t} A_{1,j} \cdot Y[j] = 0^{n-1}b_1, \\ \Theta'_{i_2} &= \Theta'_{i_3} \oplus 0^{n-1}b_2 \Leftrightarrow \bigoplus_{j=1}^{t} A_{2,j} \cdot Y[j] = 0^{n-1}b_2, \end{aligned} \tag{9}$$

for some $A_{\alpha,\beta}$, $b_{ij}$, where $i \in [2], j \in [2]$ and $t \leq 3\ell$. The $i$-th row of the augmented matrix $(A|B)$ is denoted as $(A|B)_i$ and we denote the $i$-th row of the coefficient matrix $A$ as $A_i$ for $i = 1, 2$. Now, we assume that $b_1 = b_2 = 0$. If $\mathsf{Aux\text{-}Bad}$ doesn't occur then (i) $A_1$ contains at least three 1's, and (ii) $A_2$ contains at least two distinct entries and at most two $2^\alpha$ for each $\alpha$. Thus, $A_2$ is not a multiple of $A_1$, and hence rank of $A$ is at least 2. For other choices of $b_1, b_2$ also we can also show that the rank of $A$ is at least 2. Thus, for a fixed choice of indices $i_1, i_2, i_3 \in [q]$ as follows:

$$\Pr[\Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} = 0^n \wedge \overline{\mathsf{Aux\text{-}Bad}}]$$

$$
\begin{aligned}
&= \Pr[\Sigma_{i_1} = \Sigma_{i_2}, \Theta_{i_2} = \Theta_{i_3} \wedge \overline{\textsf{Aux-Bad}}] \cdot \Pr[T_{i_1} \oplus T_{i_2} \oplus T_{i_3} = 0^n] \\
&= \frac{4}{(2^n - 3\ell)(2^n - 3\ell - 1)} \times \frac{1}{2^n - 2} \\
&\leq \frac{32}{2^{3n}},
\end{aligned}
$$

assuming $\ell \leq 2^{n-2} - 1$. Here we have used the facts that the distribution of $T_{i_1}, T_{i_2}, T_{i_3}$ are chosen uniformly at random and they are independent over the distribution of $\Sigma_i$ in the ideal world. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\textsf{Bad4}] \leq \Pr[\textsf{Aux-Bad}] + \Pr[\textsf{Bad4} \wedge \overline{\textsf{Aux-Bad}}] \leq \frac{2\sigma}{2^n} + \frac{32q^3}{2^{3n}}. \tag{10}$$

**6.<u>Bound for Bad5:</u>** To obtain the bound for $\textsf{Bad5}$, we first define an auxiliary bad event

$$\textsf{Aux-Bad} := Y_i[j] \in \{0^n, 0^{n-1}1\}.$$

It is easy to see that $\textsf{Pr[Aux-Bad]} \leq \frac{2\sigma}{2^n}$, if $\sigma$ is the total number of blocks over all the $q$ queries. Now we will obtain the bound for $\textsf{Bad5}$ conditioned on the auxiliary bad doesn't happen. Suppose $\ell$ be the maximum number of message blocks among all the $q$ queries. For the $\Sigma$ and $\Theta$ collision we can simply eliminate all the same input blocks. Let us denote

$$\textsf{Bad5}_{i_1,i_2,i_3,i_4} \Leftrightarrow \Sigma_{i_1} = \Sigma_{i_2} \wedge \Theta_{i_2} = \Theta_{i_3} \wedge \Sigma_{i_3} = \Sigma_{i_4},$$

for $(i_1, i_2, i_3, i_4) \in [q]^4$. Therefore,

$$\textsf{Bad5} \Leftrightarrow \bigvee_{(i_1,i_2,i_3,i_4)\in[q]^4} \textsf{Bad5}_{i_1,i_2,i_3,i_4}.$$

After fixing a quadruple $(i_1, i_2, i_3, i_4)$, $\textsf{Bad5}_{i_1,i_2,i_3,i_4}$ can be represented by a system of three linear equations as follows;

$$
\begin{aligned}
\Sigma'_{i_1} = \Sigma'_{i_2} \oplus 0^{n-1}b_1 &\Leftrightarrow \bigoplus_{j=1}^{t} A_{1,j} \cdot Y[j] = 0^{n-1}b_1, \\
\Theta'_{i_2} = \Theta'_{i_3} \oplus 0^{n-1}b_2 &\Leftrightarrow \bigoplus_{j=1}^{t} A_{2,j} \cdot Y[j] = 0^{n-1}b_2, \\
\Sigma'_{i_3} = \Sigma'_{i_4} \oplus 0^{n-1}b_3 &\Leftrightarrow \bigoplus_{j=1}^{t} A_{3,j} \cdot Y[j] = 0^{n-1}b_3,
\end{aligned} \tag{11}
$$

for some $A_{\alpha,\beta}$, $b_i$, where $i \in [3]$. Suppose

$$B = \begin{bmatrix} 0^{n-1}b_1 \\ 0^{n-1}b_2 \\ 0^{n-1}b_3 \end{bmatrix}$$

Therefore, $(A|B)$ be the augmented matrix and $A$ be the coefficient matrix of the system of equations. The $i$-th row of the augmented matrix is denoted by $(A|B)_i$ and the $i$-th row of the coefficient matrix is denoted by $A_i$ for $i = 1, 2, 3$. We analyse the following cases depending on the $B$ matrix as follows.

**Case 1.** **$B$ is all zero matrix**. We fix $(i_1, i_2, i_3, i_4)$ and consider the matrix $A$. First let us consider the case $\ell_{i_2} = \ell_{i_3}$. Now assuming that Aux-Bad doesn't occur, we have the following four properties:

(P1) Both $A_1$ and $A_3$ contains at least three 1's. This is due to the fact that there are $\Sigma'$ collisions in $A_1$ and $A_3$,
(P2) All the entries of $A_2$ should look like $2^\beta$ for some $\beta$,
(P3) $A_2$ contains at most two $2^\alpha$ for each $\alpha$, and
(P4) Since there is $\Theta$ collision for $A_2$, it contains at least two distinct elements.

It is easy to see that the above properties ensure that $A_2$ is not a multiple of $A_1$, and hence rank of the coefficient matrix $A$ is at least 2. This implies that, either rank of $A$ is 3, or $A_1 = A_3$, or $A_2 = xA_1 + yA_3$, for some nonzero values $x, y$. We define three cases as follows:

(a) $\mathcal{T}_1 \overset{\Delta}{=} \{(i_1, i_2, i_3, i_4) \in [q]^4 : A \text{ has rank } 3\}$,
(b) $\mathcal{T}_2 \overset{\Delta}{=} \{(i_1, i_2, i_3, i_4) \in [q]^4 : A_1 = A_3\}$,
(c) $\mathcal{T}_3 \overset{\Delta}{=} \{(i_1, i_2, i_3, i_4) \in [q]^4 : A_2 = xA_1 \oplus yA_3 \text{ for some non-zero x,y}\}$.

**Case (1a):** Since the matrix is full ranked, the probability of $Y$-variables which satisfies system of equation is bounded by $1/(2^n - t)(2^n - t - 1)(2^n - t - 2)$. So we have

$$\Pr\left[\bigvee_{(i_1,i_2,i_3,i_4)\in\mathcal{T}_1} \mathsf{Bad5}_{i_1,i_2,i_3,i_4}\right] \leq \frac{q^4}{(2^n - 4\ell)(2^n - 4\ell - 1)(2^n - 4\ell - 2)} \leq \frac{8q^4}{2^{3n}}, \tag{12}$$

as $t \leq 4\ell$.

**Case (1b):** To bound the probability of $\mathsf{Bad5}_{i_1,i_2,i_3,i_4}$ for $(i_1, i_2, i_3, i_4) \in \mathcal{T}_2$, we define an equivalence relation $\sim$ on $[q]^2$, where $(i_1, i_2) \sim (i_3, i_4)$ implies $A_1 = A_3$ for $A$, which means that $\Sigma'_{i_1} = \Sigma'_{i_2} \Leftrightarrow \Sigma'_{i_3} = \Sigma'_{i_4}$. Assume that the relation $\sim$ partitions $[q]^2$ into $r$ many subsets, namely $\mathcal{I}_1, \ldots, \mathcal{I}_r$, i.e., $[q]^2 = \mathcal{I}_1 \sqcup \cdots \sqcup \mathcal{I}_r$. Now, we consider the event $\Sigma'_{i_1} = \Sigma'_{i_2}$ for all $(i_1, i_2) \in \mathcal{I}_j$, $j = 1, \ldots, r$, denoted by $\mathcal{F}_j$. Then, we have

$$\Pr[\mathcal{F}_j] \leq 2/2^n.$$

Therefore, we have

$$\Pr\left[\bigvee_{(i_1,i_2,i_3,i_4)\in\mathcal{T}_2} \mathsf{Bad5}_{i_1,i_2,i_3,i_4}\right] \leq \Pr\left[\bigvee_{j\in[r]} \bigvee_{(i_1,i_2),(i_3,i_4)\in\mathcal{I}_j} \mathsf{Bad5}_{i_1,i_2,i_3,i_4}\right]$$

$$\leq \sum_{j=1}^{r} \Pr[\mathcal{F}_j]\dot{\Pr}\left[\bigvee_{(i_1,i_2),(i_3,i_4)\in\mathcal{I}_j} \left(\Theta'_{i_2} = \Theta'_{i_3}\right) \middle| \mathcal{F}_j\right]$$

$$\leq \sum_{j=1}^{r} \frac{2}{2^n}.\min\left\{\frac{2|\mathcal{I}_j|^2}{2^n}, 1\right\}, \tag{13}$$

where $\ell \leq 2^n/16$. Using the given condition $\sum_{j=1}^{r} |\mathcal{I}_j| = q^2$, min $\left\{\frac{2|\mathcal{I}_j|^2}{2^n}, 1\right\}$ have maximum value when $r = \lfloor q^2/2^{\frac{n-1}{2}} \rfloor + 1$ and $|\mathcal{I}_j| = 2^{\frac{n-1}{2}}$, for $j = 1, \ldots, r-1$ and $|\mathcal{I}_r| = q^2 - (r-1)2^{\frac{n-1}{2}}$. Hence,

$$\Pr\left[\bigvee_{(i_1,i_2,i_3,i_4)\in\mathcal{T}_2} \mathsf{Bad5}_{i_1,i_2,i_3,i_4}\right] \leq \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{2}{2^n}. \tag{14}$$

**Case (1c):** Now we consider the case $(i_1, i_2, i_3, i_4) \in \mathcal{T}_3$. Properties (P1) - (P4) ensure that (i) $A_1$ and $A_3$ intersect at most two positions and can not be disjoint, and (ii) $A_2$ can have at most three different elements. So, we can find a submatrix of order $3 \times 3$

$$\begin{bmatrix} 1 & 1 & 0 \\ 2^\alpha & 2^\alpha \oplus 2^\beta & 2^\beta \\ 0 & 1 & 1 \end{bmatrix},$$

where $\alpha \neq \beta$. Since all the elements of $A_2$ is a power of 2, there must exist some $\gamma$ such that $2^\alpha \oplus 2^\beta = 2^\gamma$. We define

$$\mathsf{NEQ}_{i,j} \overset{\Delta}{=} \{\mu \in [\min\{\ell_i, \ell_j\}] : M_i[\mu] \neq M_j[\mu]\} \sqcup \{\mu : \min\{\ell_i, \ell_j\} < \mu \leq \max\{\ell_i, \ell_j\}\}.$$

Since $xA_1 \oplus yA_3$ gives at most three nonzero elements in $A_2$, $\mathsf{NEQ}_{i_2,i_3} = \{\alpha, \beta, \gamma\}$. Now consider that $M_{i_2}$ and $M_{i_3}$ are given with $\mathsf{NEQ}_{i_2,i_3} = \{\alpha, \beta, \gamma\}$, where $2^\alpha \oplus 2^\beta \oplus 2^\gamma = 0$ and $\alpha < \beta < \gamma$. We have to find $M_{i_1}$ and $M_{i_4}$ such that $(i_1, i_2, i_3, i_4) \in \mathcal{T}_3$. In this scenario, $A_2$ is determined uniquely. After choosing distinct $x, y \in \{2^\alpha, 2^\beta, 2^\gamma\}$, $A_1$ and $A_3$ are fix, such that $xA_1 \oplus yA_3 = A_2$. If $A_2$ contains every nonzero element exactly twice and if $x = 2^\alpha$ and $y = 2^\beta$, then we can find a submatrix of order $3 \times 6$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 2^\alpha & 2^\beta & 2^\gamma & 2^\alpha & 2^\beta & 2^\gamma \\ 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

with other elements are 0's. As, there are at most two possibilities that $M_{i_1}$ yielding $A_1$ and $M_{i_4}$ yielding $A_3$ each, $M_{i_1}$ and $M_{i_4}$ can be chosen at most 24 possible ways. Therefore we have,

$$\Pr\left[\bigvee_{(i_1,i_2,i_3,i_4)\in\mathcal{T}_3} \mathsf{Bad5}_{i_1,i_2,i_3,i_4}\right] \leq \frac{24\binom{q}{2}}{(2^n - 4\ell - 1)(2^n - 4\ell - 2)} \leq \frac{96q^2}{2^{2n}}. \tag{15}$$

By considering all the three sub-cases we have

$$\Pr\left[\bigvee_{(i_1,i_2,i_3,i_4)\in\mathcal{T}_1 \bigsqcup \mathcal{T}_2 \bigsqcup \mathcal{T}_3} \mathsf{Bad5}_{i_1,i_2,i_3,i_4}\right] \leq \frac{8q^4}{2^{3n}} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{2}{2^n} + \frac{96q^2}{2^{2n}}. \quad (16)$$

Now we consider the case where $\ell_{i_2} \neq \ell_{i_3}$. W.l.o.g. assume that $\ell_{i_2} > \ell_{i_3}$. We observe that property (P1), (P4) remains as it is, and property (P2) gets modified to the fact that all the entries of $A_2$ should now look like $2^{\beta}$ or $2^{\ell_{i_2}-\ell_{i_3}+\beta}$ for some $\beta$. Similar to the previous analysis, this may results in three sub-cases 1a, 1b, and 1c. We can easily bound 1a and 1b identically. Now we claim that 1c can not happen in this case. This is due to the fact that (i) The length difference in the two messages ensures that the contribution of $Y$-variables can not be canceled out (as the coefficients are different depending on the length of the message), (ii) one can have at least 2 different and at most 3 different entries in $A_2$, (iii) Both $A_1$, $A_3$, and $A_1 \oplus A_3$ must contain at least 3 1's. Combining the cases, we have

$$\Pr[\mathsf{Bad5\text{-}1} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{8q^4}{2^{3n}} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{2}{2^n} + \frac{96q^2}{2^{2n}}. \quad (17)$$

**Case 2: <u>$B$ is a non-zero matrix.</u>** Let us fix $(i_1, i_2, i_3, i_4)$. Now depending on the values of $b_1, b_2, b_3$ we have the cases as follows:

**Case (2a):** This case corresponds to $b_1 = b_3 = 0$, and $b_2 = 1$. In this event, it is clear that $(A|B)_2$ can not be written as a linear combination of $(A|B)_1$ and $(A|B)_3$. So, the rank of $(A|B)$ is either 2 or 3. Thus, we have

$$\Pr[\mathsf{Bad5\text{-}2a} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{8q^4}{2^{3n}} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{2}{2^n}.$$

**Case (2b):** This case corresponds to $b_1 = b_3 = 1$, and $b_2 = 0$. In this event $A_2$ follows the conditions (P2)-(P4). Since $A_2$ contains at least 2 distinct elements and $b_1 = b_3 = 1, b_2 = 0$, $(A|B)_2$ can not written as a linear combination of $(A|B)_1$ and $(A|B)_3$. So, the rank of $(A|B)$ is either 2 or 3. Thus, we have

$$\Pr[\mathsf{Bad5\text{-}2b} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{8q^4}{2^{3n}} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{2}{2^n}.$$

**Case (2c):** This case corresponds to $b_1 \neq b_3$, and $b_2 = 0$. In this event $(A|B)_1 \neq (A|B)_3$. Also, there exists at least one column in $(A|B)$ where the corresponding elements of $A_1$ and $A_3$ are distinct. Due to this reason $(A|B)_2$ can not written as a linear combination of $(A|B)_1$ and $(A|B)_3$. So, the rank of $(A|B)$ is 3. Thus, we have

$$\Pr[\mathsf{Bad5\text{-}2c} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{16q^4}{2^{3n}}.$$

**Case (2d):** This case corresponds to $b_1 \neq b_3$, and $b_2 = 1$. This is the same as **Case 2c**. Thus the probability of this event is bounded by

$$\Pr[\mathsf{Bad5\text{-}2d} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{16q^4}{2^{3n}}.$$

**Case (2e):** This case corresponds to $b_1 = b_2 = b_3 = 1$. In this event, any of the cases may happen among Case 1a, Case 1b and Case 1c. Thus the probability of this event is bounded by

$$\Pr[\mathsf{Bad5\text{-}2e} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{8q^4}{2^{3n}} + \frac{2\sqrt{2}q^2}{2^{3n/2}} + \frac{2}{2^n} + \frac{96q^2}{2^{2n}}.$$

Thus, summing all the above five cases, we have

$$\Pr[\mathsf{Bad5\text{-}2} \mid \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{56q^4}{2^{3n}} + \frac{6\sqrt{2}q^2}{2^{3n/2}} + \frac{6}{2^n} + \frac{96q^2}{2^{2n}}. \tag{18}$$

Finally, combining all the cases, we obtain:

$$\begin{aligned}\Pr[\mathsf{Bad5}] &\leq \Pr[\mathsf{Bad5} \mid \overline{\mathsf{Aux\text{-}Bad}}] + \Pr[\mathsf{Aux\text{-}Bad}] \\ &\leq \Pr[\mathsf{Bad5\text{-}1} \mid \overline{\mathsf{Aux\text{-}Bad}}] + \Pr[\mathsf{Bad5\text{-}2} \mid \overline{\mathsf{Aux\text{-}Bad}}] + \Pr[\mathsf{Aux\text{-}Bad}] \\ &\leq \frac{64q^4}{2^{3n}} + \frac{8\sqrt{2}q^2}{2^{3n/2}} + \frac{2\sigma + 8}{2^n} + \frac{192q^2}{2^{2n}}. \end{aligned} \tag{19}$$

**7. Bound for Bad6:** To obtain the bound for $\mathsf{Bad6}$, we first define an auxiliary bad event

$$\mathsf{Aux\text{-}Bad} := Y_i[j] \in \{0^n, 0^{n-1}1\}.$$

It is easy to see that $\mathsf{Pr}[\mathsf{Aux\text{-}Bad}] \leq \frac{2\sigma}{2^n}$, if $\sigma$ is the total number of blocks over all the $q$ queries. Now we will obtain the bound for $\mathsf{Bad6}$ assuming that the auxiliary bad doesn't occur. Suppose $\ell$ be the maximum number of message blocks among all the $q$ queries. After fixing a quadruple $(i_1, i_2, i_3, i_4)$, $\Theta_{i_1} = \Theta_{i_2}, \Sigma_{i_2} = \Sigma_{i_3}, \Theta_{i_3} = \Theta_{i_4}$ can be represented by a system of three linear equations as follows:

$$\begin{aligned} \Theta'_{i_1} = \Theta'_{i_2} \oplus 0^{n-1}b_1 &\Leftrightarrow \bigoplus_{j=1}^{t} A_{1,j} \cdot Y[j] = 0^{n-1}b_1, \\ \Sigma'_{i_2} = \Sigma'_{i_3} \oplus 0^{n-1}b_2 &\Leftrightarrow \bigoplus_{j=1}^{t} A_{2,j} \cdot Y[j] = 0^{n-1}b_2, \\ \Theta'_{i_3} = \Theta'_{i_4} \oplus 0^{n-1}b_3 &\Leftrightarrow \bigoplus_{j=1}^{t} A_{3,j} \cdot Y[j] = 0^{n-1}b_3, \end{aligned} \tag{20}$$

for some $A_{\alpha,\beta}$, $b_\alpha$, where $\alpha \in [3]$ and $t \leq 4\ell$. The $i$-th row of the augmented matrix $(A|B)$ is denoted as $(A|B)_i$ and we denote the $i$-th row of the coefficient matrix $A$ as $A_i$ for $i = 1, 2$. Now we claim that if $\mathsf{Bad\text{-}Aux}$ doesn't occur, then rank of $A$ is at least 2, for any choice of $(b_1, b_2)$. Thus, for a fixed choice of indices $i_1, i_2, i_3, i_4 \in [q]$ as follows:

$$\begin{aligned}&\Pr[\Theta_{i_1} = \Theta_{i_2}, \Sigma_{i_2} = \Sigma_{i_3}, \Theta_{i_3} = \Theta_{i_4}, T_{i_1} \oplus T_{i_2} \oplus T_{i_3} \oplus T_{i_4} = 0^n \wedge \overline{\mathsf{Aux\text{-}Bad}}]\\ &= \Pr[\Theta_{i_1} = \Theta_{i_2}, \Sigma_{i_2} = \Sigma_{i_3}, \Theta_{i_3} = \Theta_{i_4} \wedge \overline{\mathsf{Aux\text{-}Bad}}] \cdot \Pr[T_{i_1} \oplus T_{i_2} \oplus T_{i_3} \oplus T_{i_4} = 0^n]\\ &= \frac{4}{(2^n - 4\ell)(2^n - 4\ell - 1)} \times \frac{1}{2^n - 3} = \frac{16}{2^{3n}},\end{aligned}$$

assuming $\ell \leq 2^{n-2} - 1$. Note that, we have used the facts that the distribution of $T_{i_1}, T_{i_2}, T_{i_3}, T_{i_4}$ are chosen uniformly at random and they are independent over the distribution of $Y_i$ values in the ideal world. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\mathsf{Bad6}] \leq \Pr[\mathsf{Aux\text{-}Bad}] + \Pr[\mathsf{Bad6} \wedge \overline{\mathsf{Aux\text{-}Bad}}] \leq \frac{2\sigma}{2^n} + \frac{16q^4}{2^{3n}}. \qquad (21)$$

**8. Bound for $\mathsf{Bad7}_a$ and $\mathsf{Bad7}_b$:** We bound only the probability of the event $\mathsf{Bad7}_a$ as the analysis of bounding the probability of the event $\mathsf{Bad7}_b$ is exactly similar to that of bounding the probability of the event $\mathsf{Bad7}_a$. To bound the probability of the event $\mathsf{Bad7}_a$, we define an indicator random variable. For each $i \neq j \in [q]$, we define $\mathbb{X}_{i,j}$ which is defined as follows:

$$\mathbb{X}_{i,j} = \begin{cases} 1, & \text{if } \Sigma_i = \Sigma_j \\ 0, & \text{otherwise} \end{cases}$$

Note that, $\Pr[\mathbb{X}_{i,j} = 1] = \Pr[\Sigma_i = \Sigma_j]$ and therefore, from Lemma 2, we have

$$\Pr[\mathbb{X}_{i,j} = 1] = \frac{4}{2^n}.$$

We define another random variable $\mathbb{X} := \sum_{i,j} \mathbb{X}_{i,j}$. Therefore, we have

$$\begin{aligned}\Pr[\mathsf{Bad7}_a] &= \Pr[|\{(i,j) \in [q] \times [q] : i \neq j, \Sigma_i = \Sigma_j\}| > q^{2/3}]\\ &= \Pr[\mathbb{X} > q^{2/3}] \leq \frac{\mathbf{E}[\mathbb{X}]}{q^{2/3}} \leq \frac{4\binom{q}{2}}{2^n \cdot q^{2/3}} \leq \frac{2q^{4/3}}{2^n}. \qquad (22)\end{aligned}$$

Using the exact argument as used in bounding the probability of the event $\mathsf{Bad7}_a$, we similarly bound the probability of the event $\mathsf{Bad7}_b$ and hence, we have

$$\Pr[\mathsf{Bad7}_b] \leq \frac{2q^{4/3}}{2^n} \qquad (23)$$

Finally, the result follows as sum the probabilities of all these bad events. □

### 3.3 Analysis of Good Transcript

In this section, we lower bound the ratio of the probability of realizing a good transcript $\tau$ in the real and the ideal world. Let $\tau$ be a good transcript, where

$$\tau = \{(M_1, T_1, \widetilde{X}_1, \widetilde{Y}_1, \Sigma_1, \Theta_1), (M_2, T_2, \widetilde{X}_2, \widetilde{Y}_2, \Sigma_2, \Theta_2), \ldots, (M_q, T_q, \widetilde{X}_q, \widetilde{Y}_q, \Sigma_q, \Theta_q)\}.$$

In order to compute the real or ideal interpolation probability, let $\sigma$ denote the distinct number of message blocks among all $q$ queries. As a result of that, the ideal interpolation probability becomes $2^{-nq}/(2^n)_\sigma$.

Now, to compute the real interpolation probability, we first note that the permutation $\mathsf{P}_1$ is invoked on a total of $\sigma$ distinct input-output pairs and $\mathsf{P}_2$ is invoked on at most $2q$ input-output pairs. Therefore, we have

$$\begin{aligned}
\Pr[\mathsf{T}_{\rm re} = \tau] &= \Pr[\mathsf{P}_1(X^i_j) = Y^i_j, \forall i \in [q], j \in [\ell_i], \mathsf{P}_2(\mathit{\Sigma}_i) \oplus \mathsf{P}_2(\mathit{\Theta}_i) = T_i, \forall i \in [q]] \\
&= \Pr[\mathsf{P}_1(X^i_j) = Y^i_j, \forall i \in [q], j \in [\ell_i]] \cdot \Pr[\underbrace{\mathsf{P}_2(\mathit{\Sigma}_i) \oplus \mathsf{P}_2(\mathit{\Theta}_i) = T_i, \forall i \in [q]]}_{\mathsf{E}} \\
&= \frac{1}{(2^n)_\sigma} \cdot \Pr[\mathsf{E}] \qquad (24)
\end{aligned}$$

Therefore, it now boils down to compute a lower bound on the probability of the event $\mathsf{E}$. To do this, we first consider that $\tau$ is a good transcript. As a result of it, none of the bad flags defined in the offline phase of the ideal world have been set to 1. Now, we consider the tuple $\widetilde{\mathit{\Sigma}} = (\mathit{\Sigma}_1, \mathit{\Sigma}_2, \ldots, \mathit{\Sigma}_q), \widetilde{\mathit{\Theta}} = (\mathit{\Theta}_1, \mathit{\Theta}_2, \ldots, \mathit{\Theta}_q)$ corresponding to the good transcript $\tau$. From the two tuples $\widetilde{\mathit{\Sigma}}$ and $\widetilde{\mathit{\Theta}}$, we construct an edge labeled graph $\mathsf{G}$ as follows: for each $i \in [q], \mathit{\Sigma}_i$ and $\mathit{\Theta}_i$ represents the vertices of the graph and for each $i \in [q]$, we put an edge between the vertices $\mathit{\Sigma}_i$ and $\mathit{\Theta}_i$ with the label of the edge being $T_i$. Moreover, for any $i \neq j$, if $\mathit{\Sigma}_i = \mathit{\Sigma}_j$, then we merge the corresponding two vertices into one. Similarly, for any $i \neq j$, if $\mathit{\Theta}_i = \mathit{\Theta}_j$, then we merge the corresponding two vertices into one. This will end up with an edge-labeled graph having the following properties:

1. The graph does not have any cycle of length 2, otherwise the bad event $\mathsf{Bad1}$ would have been hold true.
2. The label of an edge of any path is non-zero, otherwise bad event $\mathsf{Bad\text{-}Tag}$ would have been hold true.
3. For a path of length two in the graph, the xor of the label of the edges of the path is non-zero, otherwise, the bad event $\mathsf{Bad2}$ or the bad event $\mathsf{Bad3}$ would have been hold true.
4. The graph does not have any odd length cycle.
5. The graph contains path of length three, which we call $\mathsf{N}$ path, such that the xor of the label of the edges of the path is non-zero, otherwise bad event $\mathsf{Bad4}$ would have been hold true.
6. The graph does not have any $\mathsf{M}$-path, otherwise bad event $\mathsf{Bad5}$ would have been hold true. A pictorial description of the $\mathsf{M}$ path is shown in $(b)$ of Fig. 3
7. The graph contains a $\mathsf{W}$ path such that the xor of the label of the edges of the path is non-zero, otherwise bad event $\mathsf{Bad6}$ would have been hold true. A pictorial description of the $\mathsf{W}$ path is shown in $(a)$ of Fig. 3

8. The last three properties ensure that the graph does not have any cycle of length 4 or above and it does not have any path of length more than 4. Hence, the graph $\mathsf{G}$ becomes acyclic. Therefore, $\mathsf{G}$ is a collection of some disjoint components.
9. Finally, due to $\overline{\mathsf{Bad7}_a}$ and $\overline{\mathsf{Bad7}_b}$, each component is of size at most $q^{2/3}$.

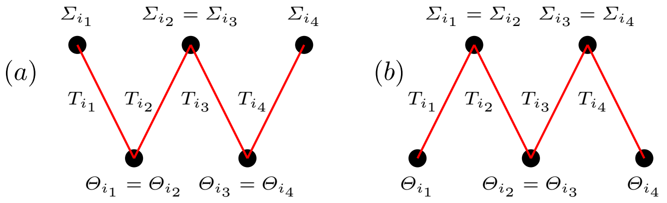
$\Sigma_{i_1}$
$\Sigma_{i_2} = \Sigma_{i_3}$
$\Sigma_{i_4}$
$(a)$
$T_{i_1}$
$T_{i_2}$
$T_{i_3}$
$T_{i_4}$
$\Theta_{i_1} = \Theta_{i_2}$
$\Theta_{i_3} = \Theta_{i_4}$
$\Sigma_{i_1} = \Sigma_{i_2}$
$\Sigma_{i_3} = \Sigma_{i_4}$
$(b)$
$T_{i_1}$
$T_{i_2}$
$T_{i_3}$
$T_{i_4}$
$\Theta_{i_1}$
$\Theta_{i_2} = \Theta_{i_3}$
$\Theta_{i_4}$

Fig. 3: $(a)$ represents a $\mathsf{W}$-path and $(b)$ represents a $\mathsf{M}$-path.

Therefore, computing a lower bound on the probability of the event $\mathsf{E}$ is equivalent to computing a lower bound on the number of injective solutions which are chosen from $\{0,1\}^n$ to $\mathcal{E}_{\mathsf{G}}$. Therefore, by applying Theorem 2, we have

$$\Pr[\mathsf{E}] \geq \frac{1}{2^{nq}}\left(1 - \epsilon_{\text{ratio}}\right). \tag{25}$$

Therefore, from Eqn. (24) and Eqn. (25), we have

$$\Pr[\mathsf{T}_{\text{re}} = \tau] \geq \frac{1}{(2^n)_\sigma} \cdot \frac{1}{2^{nq}} \cdot \left(1 - \epsilon_{\text{ratio}}\right) \tag{26}$$

where $\epsilon_{\text{ratio}}$ is defined as follows:

$$\epsilon_{\text{ratio}} \triangleq \frac{9q_c^2}{4 \cdot 2^n} + \frac{9q_c^2 q}{2^{2n}} + \frac{24q^2 q_c}{2^{2n}} + \frac{6qq_c}{2^{2n}} + \frac{40q^2}{2^{2n}} + \frac{16q^4}{2^{3n}}. \tag{27}$$

where $q_c$ denotes the total number of edges in the components having size greater than two. Since $q_c \leq q^{2/3} \leq q$, we have

$$\epsilon_{\text{ratio}} \leq \frac{9q^{4/3}}{4 \cdot 2^n} + \frac{9q^{7/3}}{2^{2n}} + \frac{24q^{8/3}}{2^{2n}} + \frac{6q^{5/3}}{2^{2n}} + \frac{40q^2}{2^{2n}} + \frac{16q^4}{2^{3n}} \tag{28}$$

Finally, the result follows by taking the ratio of real to ideal interpolation probability, and by combining Lemma 3 and Eqn. (28). □

## 4 Matching Attack on 2k-LightMAC_Plus

In this section, we show a distinguishing attack on 2k-LightMAC_Plus with $2^{3n/4}$ query complexity which establishes the proven security bound of 2k-LightMAC_Plus is tight. The distinguishing attack essentially follows a similar technique as described in [LNS18]. Broadly speaking, we first make a sufficient number of queries to the construction so that it satisfies a given relation $\mathcal{R}$. Once, we get a quadruple that satisfies the relation $\mathcal{R}$; we try to distinguish. Note that we have assumed that $s \leq n/4$ for the attack. Details of the attack are given as follows:

1. Perform the following for different choices of $x \leq 2^{3n/4}$:
   (a) Make queries to the construction 2k-LightMAC_Plus on the following three inputs: (i) $0\|x$, (ii) $1\|x$, (iii) $2\|x$.
   (b) $L[x] \triangleq \|_{i=0}^{2}\Big(\textsf{2k-LightMAC\_Plus}(i\|x)\Big)$.
2. For each $(x_1, x_2, x_3, x_4)$ such that $L[x_1] \oplus L[x_2] \oplus L[x_3] \oplus L[x_4] = 0^{3n}$, do the following:
   (a) Make four additional queries to the construction 2k-LightMAC_Plus with the following inputs: (i) $3\|x_1$, (ii) $3\|x_2$, (iii) $3\|x_3$, (iv) $3\|x_4$.
   (b) If $\bigoplus_{i=1}^{4}\textsf{2k-LightMAC\_Plus}(3\|x_i) = 0^n$ output 1.
3. Output 0.

### 4.1 Attack Idea

Due to the presence of collisions in the fix functions in the finalization process, we can construct a matching attack by utilizing differences in $\Sigma'$ and/or $\Theta'$ that are absorbed by the fix functions. Our approach involves finding a quadruple of messages $(M_1 := u\|x_1, M_2 := u\|x_2, M_3 := u\|x_4, M_4 := u\|x_4)$ such that two values collide within half of the state. Specifically, we search for quadruples that satisfy a relation $\mathcal{R}(M_1, M_2, M_3, M_4)$ defined as:

$$\mathcal{R}(M_1, M_2, M_3, M_4) \triangleq \begin{cases} \Sigma'(M_1) = \Sigma'(M_2) \oplus 0^{n-1}1 \\ \Theta'(M_2) = \Theta'(M_3) \oplus 0^{n-1}1 \\ \Sigma'(M_3) = \Sigma'(M_4) \oplus 0^{n-1}1 \\ \Theta'(M_4) = \Theta'(M_2) \oplus 0^{n-1}1 \end{cases}$$

Note that, a quadruple $(M_1, M_2, M_3, M_4)$ satisfies the relation $\mathcal{R}$, we must have

$$\bigoplus_{i=1}^{4} \textsf{2k-LightMAC\_Plus}(M_i) = 0^n.$$

Now, it is easy to see that our choice of messages, as shown in the attack algorithm, ensures the following:

$$\mathcal{R}(M_1, M_2, M_3, M_4) \Leftrightarrow \begin{cases} \mathsf{E}_{K_1}(\langle 2\rangle\|x_1) = \mathsf{E}_{K_1}(\langle 2\rangle\|x_2) \oplus 0^{n-1}1 \\ 2\mathsf{E}_{K_1}(\langle 2\rangle\|x_2) = 2\mathsf{E}_{K_1}(\langle 2\rangle\|x_3) \oplus 0^{n-1}1 \\ \mathsf{E}_{K_1}(\langle 2\rangle\|x_3) = \mathsf{E}_{K_1}(\langle 2\rangle\|x_4) \oplus 0^{n-1}1 \\ 2\mathsf{E}_{K_1}(\langle 2\rangle\|x_4) = 2\mathsf{E}_{K_1}(\langle 2\rangle\|x_1) \oplus 0^{n-1}1 \end{cases}$$

$$\Leftrightarrow \begin{cases} \bigoplus_{i=1}^{4} \mathsf{E}_{K_1}(\langle 2\rangle\|x_i) = 0^n \\ \mathsf{E}_{K_1}(\langle 2\rangle\|x_1) = \mathsf{E}_{K_1}(\langle 2\rangle\|x_2) \oplus 0^{n-1}1 \\ \mathsf{E}_{K_1}(\langle 2\rangle\|x_1) = \mathsf{E}_{K_1}(\langle 2\rangle\|x_4) \oplus 0^{n-1}1 \end{cases}$$

Therefore, $\mathcal{R}$ defines a $3n$-bit relation which is independent of $u$, so that several quadruples can be made easily that satisfy $\mathcal{R}$. Now we consider a list:

$$L = \{\textsf{2k-LightMAC\_Plus}(0\|x)\|\textsf{2k-LightMAC\_Plus}(1\|x)\|\textsf{2k-LightMAC\_Plus}(2\|x)\},$$

where $x \in [2^{3n/4}]$ and looking for a quadruples $(x_1, x_2, x_3, x_4)$ such that $L(x_1) \oplus L(x_2) \oplus L(x_3) \oplus L(x_4) = 0^{3n}$. This leads to an attack: we look for a quadruple $(x_1, x_2, x_3, x_4)$ such that

$$\forall u \in \{0, 1, 2\}, \ \bigoplus_{i=1}^{4} \textsf{2k-LightMAC\_Plus}(u\|x_i) = 0^n.$$

We expect on average one random quadruple (with $2^{3n}$ potential quadruples, and a $3n$-bit filtering), and one quadruple satisfying $\mathcal{R}$ (also a $3n$-bit condition). The correct quadruple is checked with 4 extra queries (as given in line 2(a) of the algorithm). It is easy to see that the distinguisher succeeds with probability $(1 - \frac{1}{2^n})$. This is due to the fact that the probability that line 2(b) gets executed for (i) the real construction is 1, and for (ii) a random function is $\frac{1}{2^n}$.

### 4.2 Attack Complexity

It is easy to see that the number of queries made by the adversary is $\tilde{\mathcal{O}}(2^{3n/4})$. The searching required for step (iii) is done with at most $\tilde{\mathcal{O}}(2^{3n})$ operations, and using $\mathcal{O}(2^{3n/4})$ memory size (to store all the lists). We would like to point out that one can improve on the time complexity of the attack following the technique used in [LNS18], that can report a quadruple used in line 2(a) in $\tilde{\mathcal{O}}(2^{3n/2})$ operations.

## 5 Conclusion

To the best of our knowledge, this is the first work that provably shows a message length-independent $3n/4$-bit tight security bound for a block cipher-based variable input length PRF with two block cipher keys. Proving a similar security bound for 1k-LightMAC_Plus is an interesting research problem. To prove the security of the 1k-LightMAC_Plus construction, we require to solve a combinatorial problem, called *mirror theory over a restricted set*, a variant of the mirror theory result, that considers establishing a lower bound on the solutions of a given system of bivariate affine equations which are chosen from a non-empty finite subset of $\{0,1\}^n$.

## References

[BR02] John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In *EUROCRYPT 2002*, pages 384–397, 2002.

[DDD21] Nilanjan Datta, Avijit Dutta, and Kushankur Dutta. Improved security bound of (E/D)WCDM. *IACR Trans. Symmetric Cryptol.*, 2021(4):138–176, 2021.

[DDN+17] Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Single key variant of pmac_plus. *IACR Trans. Symmetric Cryptol.*, 2017(4):268–305, 2017.

[DDNP18] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block hash-then-sum: A paradigm for constructing bbb secure prf. *IACR Transactions on Symmetric Cryptology*, 2018(3):36–92, 2018.

[KLL20] Seongkwang Kim, ByeongHak Lee, and Jooyoung Lee. Tight security bounds for double-block hash-then-sum macs. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 435–465. Springer, 2020.

[LNS18] Gaëtan Leurent, Mridul Nandi, and Ferdinand Sibleyras. Generic attacks against beyond-birthday-bound macs. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 306–336. Springer, 2018.

[LPTY16] Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. A MAC mode for lightweight block ciphers. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 43–59, 2016.

[Nai17] Yusuke Naito. Blockcipher-based macs: Beyond the birthday bound without message length. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, volume 10626 of *Lecture Notes in Computer Science*, pages 446–470. Springer, 2017.

[Nai18] Yusuke Naito. Improved security bound of lightmac_plus and its single-key variant. In Nigel P. Smart, editor, *Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, volume 10808 of *Lecture Notes in Computer Science*, pages 300–318. Springer, 2018.

[Pat08] Jacques Patarin. The "coefficients h" technique. In *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, pages 328–345, 2008.

[Son21] Haitao Song. A single-key variant of lightmac_plus. *Symmetry*, 13(10):1818, 2021.