Multi User Security of LightMAC and LightMAC_Plus

Nilanjan Datta[1] and Shreya Dey[1,2] and Avijit Dutta[1] and Devdutto Kanungo[3]

[1] Institute for Advancing Intelligence, TCG CREST, Kolkata, India.
[2] Ramakrishna Mission Vivekananda Educational and Research Institute, India.
[3] PricewaterhouseCoopers, Kolkata, India.
nilanjan.datta@tcgcrest.org,shreya.dey@tcgcrest.org,avijit.dutta@tcgcrest.org,
kitunscool@gmail.com

Abstract. In FSE'16, Luykx et al. have proposed LightMAC that provably achieves a query length independent PRF security bound. To be precise, the construction achieves security roughly in the order of $O(q^2/2^n)$, when instantiated with two independently keyed n-bit block ciphers and q is the total number of queries made by the adversary. Subsequently, in ASIACRYPT'17, Naito proposed a beyond-birthday-bound variant of the LightMAC construction, dubbed as LightMAC_Plus, that is built on three independently keyed n-bit block ciphers and achieves $2n/3$-bits PRF security. Security analyses of these two constructions have been conducted in the single-user setting, where we assume that the adversary has the access to a single instance of the construction. In this paper, we investigate, for the first time, the security of the LightMAC and the LightMAC_Plus construction in the context of multi-user setting, where we assume that the adversary has access to more than one instances of the construction. In particular, we have shown that LightMAC remains secure roughly up to $2^{n/2}$ construction queries and 2^k ideal-cipher queries in the ideal-cipher model and LightMAC_Plus maintains security up to approximately $2^{2n/3}$ construction queries and $2^{2k/3}$ ideal-cipher queries in the ideal-cipher model, where n denotes the block size and k denotes the key size of the block cipher.

Keywords: LightMAC, LightMAC_Plus, Multi-user Security, Mirror Theory, Beyond Birthday Bound.

1 Introduction

In the last several decades, the research interest in lightweight cryptography has seen remarkable growth in the cryptographic community. Lightweight cryptography ensures to protect communications in resource-constrained environments. Due to the advent of the Internet of Things (IoT), lightweight cryptography has gained a significant momentum in the last decade or so. As a consequence of that, the cryptographic community started to realize standardizing the lightweight cryptographic algorithms through various competitions and projects, most notably the CAESAR competition [13], NIST lightweight cryptography standardization project [41] and the ISO/IEC standardization [1]. In this regard, ISO/IEC 29192-6:2019 standard [1] specifies three message authentication code (or MAC) algorithms for lightweight applications; LightMAC [31], Tsudik's keymode [46] and Chaskey-12 [35].

1.1 LightMAC Construction

In FSE'16 [31], Luykx et al. have proposed LightMAC, which has been standardized by the ISO/IEC standardization process. LightMAC is a block cipher based PRF that operates in parallel mode, i.e., for an n-bit block cipher 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:

$$\mathsf{LightMAC}_{\mathsf{E}_{K_1,K_2}}(M) = \mathsf{E}_{K_2}\Bigg(\overbrace{\sum_{\alpha=1}^{\ell-1} \underbrace{\mathsf{E}_{K_1}(\langle\alpha\rangle_s \| M[\alpha])}_{V[\alpha]} \oplus \mathsf{pad}_n(M[\ell])}^{\mathsf{LightMAC\text{-}Hash}_{\mathsf{E}_{K_1}}}\Bigg),$$

where $\langle i\rangle_s$ denotes the s bit encoding of the integer i, $(M[1], \ldots, M[\ell-1])$ denotes the $n-s$ bit parsing of message M, where each $M[i]$ is an $n-s$ bit string, and 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. 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. 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.

Besides of having the implementation and the performance benefit of LightMAC, one of the other features of LightMAC that makes it more attractive, is its provable security bound. While the security bounds of all its contender candidates, such as PMAC [10], OMAC [25], CBC-MAC [3], XCBC [9] etc., degrade linearly with the maximum length of the message, LightMAC achieves a message length independent security bound. Assuming the maximum length of the message $\ell_{\max} \leq (n-s)2^s$, LightMAC is proved to have a PRF bound of $O(q^2/2^n)$, where q denotes the number of queries. However, some variants of PMAC, e.g., PMAC-with-parity [49], PMAC3 [39] etc., achieve message length independent security bound for a wide range of $\ell_{\max}$, they come at the cost of a significant increase in the design complexity.

Related Works on LightMAC. Now we briefly discuss related works on LightMAC and LightMAC_Plus. Shen et al. [43] have proposed two simple variants of LightMAC construction, dubbed as LedMAC1 and LedMAC2. LedMAC1 avoids an unnecessary padding of LightMAC that allows messages up to length $(n-s)2^s + s - 1$ bits without degrading the security bound. On the other hand, LedMAC2 reduces the number of keys of LedMAC1 from two to one and achieves a similar level of security as that of LightMAC. However, for LedMAC2, the maximum length of the message is $(n-s)2^{s-1} + s - 2$ bits at the cost of degradation of the security from $q^2/2^n$ to $q\sigma/2^n$, where σ denotes the total number of message blocks across all q queries. In [15], Chattopadhyay et al. minimized the number of block cipher keys of LightMAC from 2 to 1 and showed that LightMAC instantiated with a single block cipher key, dubbed as 1k-LightMAC, achieves security bound of $O(q^2/2^n)$ while restricting the query length up to $(n-s)\min\{2^{n/4}, 2^s\}$ bits. They have also proposed the domain-separated variant of 1k-LightMAC construction, called LightMAC-ds and showed that it achieves a similar security bound as that of LightMAC with maximum message length up to $(n-s)2^{s-1}$ bits.

1.2 LightMAC_Plus: BBB Secured Variant of LightMAC

In ASIACRYPT'17, Naito proposed a beyond birthday bound secure variant of LightMAC construction called LightMAC_Plus. Similar to the LightMAC construction, LightMAC_Plus is a block cipher based PRF that operates in parallel mode, i.e., for an n-bit block cipher E instantiated with three independently sampled keys K_1, K_2, K_3, and with a global counter size s, the LightMAC_Plus function is defined as follows:

$$\mathsf{LightMAC\_Plus}_{\mathsf{E}_{K_1,K_2,K_3}}(M) = \mathsf{E}_{K_2}(\Sigma) \oplus \mathsf{E}_{K_3}(\Theta),$$

where

$$\Sigma \;:=\; \Bigg(\sum_{\alpha=1}^{\ell} \underbrace{\mathsf{E}_{K_1}(\langle\alpha\rangle_s \| M'[\alpha])}_{V[\alpha]}\Bigg),\ \Theta := \Bigg(\sum_{\alpha=1}^{\ell} 2^{\ell-\alpha}\, \underbrace{\mathsf{E}_{K_1}(\langle\alpha\rangle_s \| M'[\alpha])}_{V[\alpha]}\Bigg).$$

Here $\langle i\rangle_s$ denotes the s bit encoding of the integer i, $M' \leftarrow \mathsf{pad}_{n-s}(M)$ 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. Like LightMAC construction, LightMAC_Plus comes with a reduced rate but with higher security guarantee. Naito has shown that LightMAC_Plus provably achieves a message length independent PRF security of up to $2^{2n/3}$ queries. Later in [26], Kim et al. have claimed an improved security bound of the construction from $2^{2n/3}$ queries to $2^{3n/4}$. However, their claim has not been backed up by any formal proof.

Related Works on LightMAC_Plus. Naito [37] proposed LightMAC_Plus2, along with LightMAC_Plus, that provides higher security bound than LightMAC_Plus, but comes at the increased number of block cipher calls. In CT-RSA'18 [38], Naito has improved the bound of 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 upto 2^n tagging queries if the number of verification queries is 1. Later, in [29], 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 [38] on LightMAC_Plus. In EUROCRYPT'20, Kim et al. [27] have shown an improved security bound of LightMAC_Plus construction from $2n/3$-bits to $3n/4$-bits (ignoring the maximum message length) without a formal proof. Due to the result of [29], the improved bound of LightMAC_Plus turns out to be the tight one.

In FSE'20, Datta et al. [19] 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, which has been recently improved to $3n/4$-bits [17]. In [38], 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 (Σ, Θ) of the internal hash computation is domain separated by setting their two most significant bits to 10 and 11 respectively. Moreover, the checksum of the message blocks after padded with the string 0^{n-s}, is masked with the Σ value. Author has shown that LightMAC_Plus-1k construction achieves $2n/3$-bits security.

Recently, Song [45] 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. As a result of that, from the efficiency viewpoint, 1k-LightMAC_Plus is a better choice over LightMAC_Plus-1k. It has been shown in [45] that 1k-LightMAC_Plus also achieves $2n/3$-bits security bound. In [18], Datta et al. have proposed a forkcipher based variant of the LightMAC_Plus construction and shown it to be secure up to $2^{(n+s)/2}$ queries, where s denotes the size of the block counter.

1.3 Multi User Security

The security analysis for all the above-mentioned constructions has been conducted in a single-user setting, where the adversary has access to the keyed construction for a single unknown randomly sampled key. This setup, known as the *single-user security model*, involves the adversary targeting one specific machine, in which the cryptographic algorithm is deployed, to compromise its security. However, in practice, cryptographic algorithms are usually deployed across multiple machines. For instance, AES-GCM [32, 33] is now widely used in the TLS protocol to protect web traffic and is currently used by billions of users daily. In such multi-user scenarios, the adversary's goal is to compromise the security of at least one user. This approach, known as the *multi-user security model*, considers the adversary's success as a combination of single-user successes.

The notion of multi-user (mu) security was introduced by Biham [7] in symmetric cryptanalysis and by Bellare, Boldyreva, and Micali [2] in the context of public-key encryption. In the multi-user setting, attackers have access to multiple machines and each of the machines implement a cryptographic algorithm F instantiated with independent secret keys. In the multi-user game an attacker can adaptively distribute its queries across multiple machines with independent keys. Multi-user security considers attackers that succeed in compromising the security of at least one machine, among others.

Multi-user security for block ciphers differs from that for modes. In the single-key setup, attacks on block ciphers like AES don't improve with more data complexity. However, in the multi-key environment, they do, as observed by Biham [7] and refined (time-memory-data trade-off) by Biryukov et al. [8]. This highlights how it's easier to recover a block cipher key from a large group than targeting a specific one. This principle extends to other deterministic symmetric-key algorithms, as done for MACs by Chatterjee et al.[14]. Generally, an adversary's multi-user advantage for a cryptographic algorithm is at most u times its single-user advantage. Hence, a multi-user security bound with a factor u can be easily established. Bellare and Tackmann [5] formalized a multi-user secure authenticated encryption scheme and analyzed countermeasures against multi-key attacks in TLS 1.3. However, their derived security bound also includes the factor u, implying a significant security drop in constructions like AES-GCM in large-scale deployments.

As evident from [4, 5, 11, 23, 24, 30, 36], it is a challenging problem to study the security degradation of cryptographic primitives with the number of users, even when their security in the single-user setting is well understood. Research on the multi-user security of MACs is relatively limited in the literature, with notable works by Chatterjee et al. [14], Morgan et al. [34], Bellare et al. [6], and two recent works of Shen et al. [44] and Datta et al. [20]. The first two employ a generic reduction approach for MACs, multiplying the single-user security by the number of users, while the latter employs a dedicated analysis method. In [44], Shen et al. demonstrated the multi-user security of various DbHtS [19] constructions with $2^{2n/3}$ construction queries and 2^k ideal-cipher queries. In [20], Datta et al. have shown multi-user security of two-keyed DbHtS [19] construction with $2^{3n/4}$ construction queries and 2^k ideal-cipher queries. However, these results cannot be directly applied to the multi-user security of LightMAC and LightMAC_Plus. Therefore, to address the applicability of the LightMAC and LightMAC_Plus constructions in practical setting, we ask the following:

> *How does the security of* LightMAC *and* LightMAC_Plus *degrade in the multi-user setting ?*

1.4 Our Contribution

In this paper, we address the above question and study the multi-user security of LightMAC and LightMAC_Plus constructions.

I. Multi-user Security of LightMAC. We first show that LightMAC is secured in the multi-user setting against all adversaries that make a total of $2^{n/2}$ queries and up to a total of 2^k ideal-cipher queries, where we have assumed that the underlying block cipher of the LightMAC construction is an ideal cipher. Unlike the single user security bound of LightMAC construction, the achieved bound is not ℓ-free, where ℓ denotes the maximum number of message blocks. However, we have shown that (i) if we restrict the number of ideal-cipher queries up to $2^{3k/4}$ and $\ell \leq 2^{n/4}/k$, or (ii) if we restrict the number of users up to $2^{n/4}$, then we achieve an ℓ-free multi-user security bound of LightMAC construction. We would like to mention that in the single-user setting, we obtained ℓ-free bound on LightMAC construction when $\ell \leq 2^{n/2}$, while we need $\ell \leq 2^{n/4}/k$ for achieving ℓ-free bound on multi-user security of LightMAC. Yet, this loss may not matter, as most applications use message sizes of at most $2^{n/4}$ blocks.

Remark 1. Concurrent to this work, Naito [40] have independently studied the multi-user security of Hash-then-Encrypt type MACs and showed security up to $O(q_u q\epsilon_{\text{axu}} + q\epsilon_{\text{reg}} + (p + \ell q)/2^k)$, where ϵ_{axu} denotes the almost-xor universal advantage and ϵ_{reg} denotes the regular advantage of the underlying hash function in the ideal cipher model. Moreover, q_u is the maximum number of queries per user, q (resp. p) denotes the number of construction (resp. primitive) queries, and ℓ denotes the maximum number of message blocks. Alongside, Naito has also shown multi-user security bound of CBC [3], EMAC [12], XCBC [9] and TMAC [28] up to $O(\ell q_u q/2^n + p/2^k)$.

II. Multi-user Security of LightMAC_Plus. For LightMAC_Plus, we have shown that the construction is secured in the multi-user setting against all adversaries that make a total of $2^{2n/3}$ queries and up to a total of $2^{2k/3}$ ideal-cipher queries, where we have assumed that the underlying block cipher of the LightMAC_Plus construction is an ideal cipher. We would like to mention here that unlike the single user security bound of the LightMAC_Plus construction, the proposed multi-user security bound of LightMAC_Plus is not ℓ-free. However, if we assume that $k \geq 4n/3$, then we obtain an ℓ-free security bound of the LightMAC_Plus construction, provided $\ell \leq 2^{n/3}/k$. We would like to note that for LightMAC_Plus construction, the security for primitive queries is $2k/3$ bits, which is smaller than the key size. On the other hand, in the standard model, the multi-user security is $k - \log_2 u$ bits. Moreover, LightMAC_Plus achieves $3n/4$-bit security in the standard model, which is better than the current bound. We believe that improving the multi-user security bound of LightMAC_Plus construction in the ideal-cipher model from $2n/3$ bits to $3n/4$ bits is hard problem.

Remark 2. The single-user security bound for the LightMAC and LightMAC_Plus constructions is established in the standard model. The overall bound includes an information-theoretic term that is ℓ-free, and a computational term that relies on the security of the underlying block cipher, which involves an upper limit on the number of queried blocks. Our bounds give a clearer picture of what happens under the hood. However, we would like to clarify that a proof in the ideal cipher model, where we treat E as an ideal block cipher, uniformly sampled from the set of all block ciphers, does not guarantee the security of the LightMAC(_Plus) construction for any instantiation of the construction with an actual block cipher. We have given a comparison of the proven bounds of LightMAC and LightMAC_Plus constructions both in the single-user and the multi-user setting in Table 1.

1.5 A Generic Overview of the Proof Approach

In this section we briefly describe the approach of the multi-user security proof of the LightMAC and LightMAC_Plus construction as follows:

I. Proof Approach of LightMAC: We prove the security of the construction using the H-Coefficient technique [42], where we release the block cipher keys of all the users and all the intermediate output values V in both the worlds along with the usual query-response pairs. This allows the challenger in both the worlds to compute Σ values for defining bad transcripts in terms of it and the released keys. Note that LightMAC uses two keys K_1 and K_2, where K_1 is used to compute the Σ values, which we customarily refer to as *hash key* and K_2 is used to compute the tags which is customarily referred to as *prf key*.

1. If the prf-key collides with an ideal cipher key for an user, and one of the tag values of that user collide with the output value of the corresponding ideal-cipher query, then in the real world, the corresponding Σ value will match with the input of the corresponding ideal-cipher query with probability 1, but that event holds in the ideal world with low probability, which in turn allows a distinguisher to distinguish between the real and the ideal world. Hence, we consider this event to be bad (see Bad1 of Sect. 4.2). A pictorial description of the event is shown in Fig. 1.

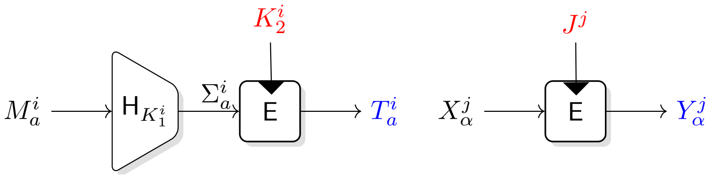

Figure 1: Description of the event Bad1: The key K_2^i of i-th user matches with ideal cipher key J^j and response to the a-th query of same user collide with the output value Y_α^j of the corresponding ideal-cipher query. $\mathsf{H}_{K_1^i}$ denotes the $\text{LightMAC-Hash}_{\mathsf{E}_{K_1^i}}$ construction

2. Symmetric to the above event, if the prf-key collides with an ideal cipher key for an user, and one of the Σ values of that user collide with the input value of the corresponding ideal-cipher query, then in the real world, the corresponding tag value will match with the output of the corresponding ideal-cipher query with probability 1, but that event holds in the ideal world with low probability, which in turn allows a distinguisher to distinguish between the real and the ideal world. Hence, we consider this event to be bad (see Bad2 of Sect. 4.2). A pictorial description of the event is shown in Fig. 2.

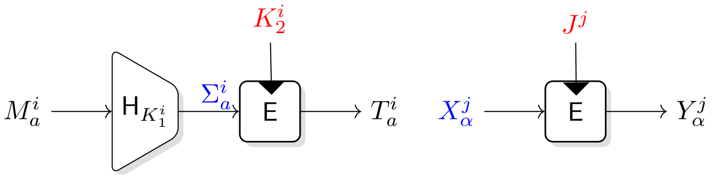

Figure 2: Description of the event Bad2: The key K_2^i of i-th user matches with ideal cipher key J^j and input to the a-th query of same user collide with the input value Y_α^j of the corresponding ideal-cipher query.

3. Finally, we disallow the collision between two Σ values for any user (see Bad3 of Sect. 4.2). A pictorial description of the event is shown in Fig. 3.

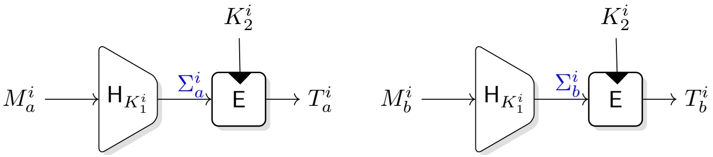

Figure 3: Description of the event $\mathsf{Bad3}$: Σ values of two queries for an user collides with each other.

4. However, to ease the analysis of bounding the above bad events, we would like to ensure that for any user i, its hash key K_1^i and prf key K_2^i should be fresh, i.e., they should not collide with any other user keys. If there is such collision in the hash keys or prf keys or collision between hash key and prf key among two users, then we set the bad event to true (see $\mathsf{BadK1}$, $\mathsf{BadK2}$ of Sect. 4.2).

5. Similarly, to ease analysis of bounding the event $\mathsf{Bad1}$, we would like to ensure that for any user i, each response should be distinct. If there is a collision in the tag value between two users or the collision between two tags for any user i, then we set the bad event to true (see $\mathsf{BadCollT}$ of Sect. 4.2). As mentioned before, this event is required while bounding $\mathsf{Bad1}$. This is to ensure that while bounding $\mathsf{Bad1}$, all the tag values are distinct. Details of the analysis can be found in Sect. 4.2.

If the bad events do not hold, then we count the total number of block cipher calls to lower bound the real interpolation probability and compute the ideal interpolation probability and prove that the ratio of the former to the later is at least 1. However, the non-triviality of the security analysis lies in the way we upper bound the probability of some crucial bad events within our target security bound. We cannot really bound the event $\mathsf{Bad3}$ as one seems to bound it in the standard model. Recall that, we are proving the security of the constructions in the ideal-cipher model, where the adversary is given access to evaluate the block cipher on its own. Therefore, it is plausible to assume that the adversary is well-informed about all the V values (during the block cipher evaluations) that define the event $\Sigma_a^i = \Sigma_b^i$. In that case, we are no longer left with any randomness that will bound the above bad event. However, the good news is that should the above situation hold, it must be the case that the i-th user key K_1^i collides with a chosen ideal-cipher key J^j which contributes to 2^{-k} probability to the event. Now, if one varies over all possible choices of (i, a, b, j), then the probability becomes $q^2p/2^k$, which makes our bound worse. The trick that we apply here is that, we will not allow the choices of j to vary upto p. We will restrict this choice to some parameter μ, which is of the order $2^{k-n}k\ell$, where ℓ denotes the maximum number of message blocks. For this choice of μ, we restore our target bound, at the cost of introducing an extra event that dictates the number of j exceeds μ holds with a low probability. Details of the analysis can be found in Sect. 4.2.

II. Proof Approach of $\mathsf{LightMAC\_Plus}$: Like $\mathsf{LightMAC}$ construction, we prove the security of the $\mathsf{LightMAC\_Plus}$ construction using the H-Coefficient technique [42], where we release the block cipher keys of all the users and all the intermediate output values V in both the worlds along with the usual query-response pairs. This allows the challenger in both the worlds to compute (Σ, Θ) values for defining bad transcripts in terms of it and the released keys. Note that $\mathsf{LightMAC\_Plus}$ uses three keys K_1, K_2 and K_3, where K_1 is used to compute the (Σ, Θ) values, which we customarily refer to as *hash key* and K_2, K_3 is used to compute the tags. We refer to K_2 as *σ-prf key* and K_3 as *θ-prf key*.

We first impose some bad conditions on user keys which mainly says that a pair of keys should not collide for two different users (see $\mathsf{BadK1}$-$\mathsf{BadK3}$ of Sect. 5.1). Moreover, if the prf key collides for two different users, then both of their corresponding hash keys should not collide with ideal-cipher keys (see BadK4 of Sect. 5.1). We also require that for an user, it should not be the case that both of its prf keys collide with ideal-cipher keys (see BadK5 of Sect. 5.1). Finally, it should not be the case that both prf keys of an user collide with each other (see BadK6 of Sect. 5.1). Moreover, if the has key of an user i collides with σ-prf key (resp. θ-prf key) of an another user i', then none of the message blocks preprended with appropriate block counter of user i should not collide with Σ (resp. Θ) value of user i'.

Followed by the definition of bad events on user keys, we now define bad events based on the input and key collision as follows:

1. If σ-prf key (resp. θ-prf key) for any user collides with an ideal cipher key, then its Σ (resp. Θ) value should not collide with the corresponding ideal-cipher input query. Otherwise, in the real world, one determines the block cipher output of Σ (resp. Θ), which does not hold true in the ideal world (see Bad1, Bad2 of Sect. 5.1).

2. If the hash key for any user collides with an ideal-cipher key, then its corresponding Σ value should not collide with other Σ value. Similarly, its corresponding Θ value should not collide with other Θ value (see Bad3, Bad4 of Sect. 5.1).

3. It should not be the case that for an user i, if two of its Σ (resp. Θ) value collides, then their corresponding T value should be distinct. Otherwise, it will imply the collision of Θ (resp. Σ) values in the real world, whereas in the ideal world such event should hold with low probability (see Bad5, Bad6 of Sect. 5.1).

4. If σ-prf key for two user collides with each other, then their corresponding Σ value or Θ value should not collide with each other (see Bad7, Bad8 of Sect. 5.1). Similarly, if θ-prf key for two user collides with each other, then their corresponding Θ value or Σ value should not collide with each other (see Bad9, Bad10 of Sect. 5.1).

5. If two of Σ (resp. Θ) values of an user collide with each other then, the corresponding Θ (resp. Σ) value should be distinct (see Bad11, Bad12 of Sect. 5.1).

6. Finally, the number of colliding Σ values or Θ values for an user i should be at most $q_i^{1/2}$, where q_i denotes the number of queries of the i-th user (see Bad13, Bad14).

If the bad events do not happen, then we lower bound the ratio of the real to ideal interpolation probability. Bounding the ideal interpolation probability is a straightforward analysis. On the other hand, to lower bound the real interpolation probability, we do the following: we divide the the set of users in two classes: (i) set of users whose one of the prf keys collide with an ideal-cipher key and (ii) set of users whose none of the prf keys collide with any ideal-cipher key. For the first class of users, we further divide them into a finite number of partitions based on the relation that two users belong to the same equivalent classes, if their corresponding prf keys collide with the same ideal-cipher key and then count the number of solutions to the system of equations by using the result of mirror theory over restricted set:

$$\mathsf{E}_{K_2^i}(\Sigma_a^i) \oplus \mathsf{E}_{K_3^i}(\Theta_a^i) = T_a^i.$$

Similarly, for the second class of users, we further divide them into a finite number of partitions based on the relation that two users belong to the same equivalent classes, if their corresponding prf keys collide with each other and then count the number of solutions to the system of equations by applying the result of mirror theory:

$$\mathsf{E}_{K_2^i}(\Sigma_a^i) \oplus \mathsf{E}_{K_3^i}(\Theta_a^i) = T_a^i.$$

However, the non-triviality of the analysis lies in bounding the event $\Sigma_a^i = \Sigma_b^i, \Theta_a^i = \Theta_b^i$ for some user i. As usual, it is plausible to assume that an adversary might be well-informed about all the intermediate V values that define the event $\Sigma_a^i = \Sigma_b^i, \Theta_a^i = \Theta_b^i$ and hence in that case, we are no longer left with any randomness that will bound the above bad event. As before, the good news is that should the above situation hold, it must be the case that K_1^i collides with a chosen ideal-cipher key J^j which contributes to 2^{-k} probability to the event. Now, if one varies over all possible choices of (i, a, b, j), then the probability becomes $q^2 p/2^k$, which makes our bound worse. Now, if we apply the previous trick, i.e., if we restrict the choices of j to vary upto some parameter μ, then, we get the bound $\sum\limits_{i=1}^{u} q_i^2 \mu/2^k$. By choosing $\mu = 2^{k-n}k\ell$, we obtain the bound $2^{-n}(q_1^2 + \ldots + q_u^2)$. Since, a crude bound on the sum $(q_1^2 + \ldots + q_u^2)$ is q^2, we loose our target security bound. This triggers us to bound the sum in a careful way. We split the sum into two cases: (a) when $i \leq \sqrt{q}$, then we achieve the desired security bound $p\sqrt{q}/2^k$. On the other hand, (b) when $i \geq \sqrt{q}$, then by applying a combinatorial lemma (Lemma 2), we bound the sum $(q_1^2 + \ldots + q_u^2)$ to be at most $q^{3/2}$ and then by plugging-in the appropriate value of $\mu = 2^{k-n}k\ell$, we obtain the desired security bound. Summarizing above, we would like to mention that to achieve the security bounds of both constructions, our analysis has crucially relied on a combinatorial result stated in Lemma 2.

1.6 How Does Our Result Differ From Previous Works?

The works of Chatterjee et al. [14] and Andrew et al. [34] explore a generic reduction for Message Authentication Codes (MACs). By utilizing this reduction, the mu security of constructions in the DbHtS framework will be limited to the birthday bound or, even worse. For example, the best-known single-user security bound for the LightMAC_Plus construction is given by $q^{4/3}/2^n$ [26]. If we assume the number of users to be u, then according to the generic reduction outlined in [14] and [34], this bound becomes $uq^{4/3}/2^n$. Consequently, if the adversary issues only one query per user, the security bound reduces to $q^{7/3}/2^n$, which is well below the birthday bound. Two other recent works [44, 20] have addressed the multi-user security of DbHtS [19] type constructions. In [44], Shen et al. have analyzed the multi-user security of DbHtS construction and shown it to be secure roughly upto $2^{2n/3}$ construction queries and 2^k ideal-cipher queries. They have applied their generic security result to bound the multi-user security of different DbHtS type constructions that include SUM-ECBC [47], PMAC_Plus [48], 3kf9 [50], LightMAC_Plus [37] etc. However, as pointed out in [20], this application was not appropriate. Because, in the derivation of the multi-user security bound of DbHtS, the underlying hash function was assumed to be a keyed hash function (which may not be a block cipher based hash function), and thus their security proof has not analyzed the properties of the hash function in the ideal-cipher model. As a result, when the generic security bound was applied to bound the multi-user security of block cipher based DbHtS constructions, then authors have failed to consider the fact that the block cipher used in the hash function to be an ideal-cipher, where the adversary is allowed to make ideal-cipher queries. Therefore, to prove the multi-user security of the above block cipher based DbHtS constructions, one needs to do a dedicated security analysis without resorting to any generic security result. In [20], Datta et al. have shown a tight multi-user security bound on the two-keyed DbHtS construction with $2^{3n/4}$ queries and 2^k ideal-cipher queries. They have also instantiated the underlying double block hash function with an algebraic keyed hash function and shown its $3n/4$-bit multi-user security. In fact, extending their analysis to a block cipher based construction was posed as an open problem in [20].

Clearly, our result is different from the previous works in the sense that we have established the multi-user security bound on two particular constructions LightMAC and LightMAC_Plus using a dedicated security analysis. We have been able to show that multi-user security bound of LightMAC does not degrade much compared to its security bound in the single-user setting. On the other hand, we have been able to show that

LightMAC_Plus construction achieves $2n/3$-bit multi-user security bound when the number of ideal-cipher queries is restricted up to $2^{2k/3}$.

Table 1: Comparison of Single and Multi-user Security Analysis LightMAC and LightMAC_Plus. Here, q and p refers to the number of construction queries and ideal-cipher queries, respectively; n, ℓ, k refers to the block size, maximum message length and size of key, respectively. SM and ICM are shorthand of the Standard and Ideal Cipher Model, respectively.

Constructions	Single user	Multi user		
	(SM)	Generic red.	ICM	
			With ℓ	ℓ-free
LightMAC [31]	$\mathcal{O}\left(\frac{q^2}{2^n}\right)$	$\mathcal{O}\left(\frac{q^3}{2^n}\right)$	$\mathcal{O}\left(\frac{qp}{2^{n/2+k}} + \frac{q^2\ell k}{2^n}\right)$	$\mathcal{O}\left(\frac{qp}{2^{n/2+k}} + \frac{q^{3/2}}{2^{3n/4}}\right)$
LightMAC_Plus [26]	$\mathcal{O}\left(\frac{q^{4/3}}{2^n}\right)$	$\mathcal{O}\left(\frac{q^{7/3}}{2^n}\right)$	$\mathcal{O}\left(\frac{pq^{1/2}}{2^k} + \frac{q^{3/2}kl}{2^n}\right)$	$\mathcal{O}\left(\frac{pq^{1/2}}{2^k} + \frac{q^{3/2}}{2^{2n/3+k/4}}\right)$

Open Problems: This work has opened up several potential avenues for future research. Firstly, we have established an ℓ-free multi-user security bound of LightMAC, under the condition that the number of ideal-cipher queries is at most $2^{3k/4}$ and $\ell \leq 2^{n/4}/k$. It would be worthwhile to explore whether we can prove ℓ-free security bound by allowing the number of ideal-cipher queries up to 2^k and the bound on the maximum number of message blocks is at most $O(2^{n/2})$. Secondly, we have demonstrated a multi-user security bound of $2n/3$ bits for LightMAC_Plus, assuming only $k \geq n$ and the number of ideal-cipher queries is at most $2^{2k/3}$. Although this bound is not ℓ-free, the assumption $k \geq 4n/3$ enables us to establish an ℓ-free multi-user security bound of LightMAC_Plus, provided that $\ell \leq 2^{n/3}/k$. It would be interesting to investigate whether we can improve the multi-user security bound of LightMAC_Plus from $2^{2n/3}$ to $2^{3n/4}$ with the assumption that $k \geq n$, the number of ideal cipher queries is at most 2^k and the maximum number of message blocks is at most $2^{n/2}$.

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 $\{0,1\}^n$ as *block*. For any binary string $x \in \{0,1\}^*$, $|x|$ denotes the length of x, i.e., the number of bits in x. For $x, y \in \{0,1\}^n$, we write $z = x \oplus y$ to denote 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 $0 \leq |x_l| \leq n-1$. For any $n \in \mathbb{N}$, we define an injective function pad_n that takes an arbitrary string $x \in \{0,1\}^*$ as input, and returns $y \in (\{0,1\}^n)^*$ as output, which is defined as follows:

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

where d is the smallest integer such that $|\mathsf{pad}_n(x)|$ is a multiple of n. Typically, a tuple or a vector x over $\{0,1\}^n$ is denoted as $(x_i)_{i \in \mathcal{I}}$, where $\mathcal{I}$ is called the *index set* and each $x_i \in \{0,1\}^n$. However, when there are two index sets $\mathcal{I}, \mathcal{J}$, then we denote a tuple x over $\{0,1\}^n$ as $(x^i_j)_{i \in \mathcal{I}, j \in \mathcal{J}}$, where each x^i_j is an element of $\{0,1\}^n$. Extending it one step further, we denote a tuple x over $\{0,1\}^n$, when the number of index sets is three, i.e., $\mathcal{I}, \mathcal{J}$ and $\mathcal{B}$, as $x = (x^i_j[\alpha])_{i \in \mathcal{I}, j \in \mathcal{J}, \alpha \in \mathcal{B}}$.

For two positive integers i, s such that $i < 2^s$, we write $\langle i \rangle_s$ to denote the s-bit binary representation of integer i. We write $x \leftarrow y$ to denote the assignment of the variable y into

x. $\mathsf{X} \leftarrow\!\!\$\, \{0,1\}^n$ denotes that X is sampled uniformly at random from $\{0,1\}^n$. For a tuple of random variables $(X_1, \ldots, X_q)$, 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., $X_i \leftarrow\!\!\$\, \{0,1\}^n \setminus \{X_1, \ldots, X_{i-1}\}$. We denote the set of all functions from $\mathcal{X}$ to $\{0,1\}^n$ as $\mathsf{Func}_{\mathcal{X}}$. Sometimes, we omit the set $\mathcal{X}$ from $\mathsf{Func}_{\mathcal{X}}$ and simply write Func when the domain is clear from the context. The set of all permutations over $\{0,1\}^n$ is denoted as Perm. We write $\mathbf{P}(n,r)$ to denote $n(n-1)\ldots(n-r+1)$, where $(n)_0 = 1$ by convention, that represents the number of ways to arrange r different items from a set of n different items.

2.1 Pseudorandom 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 F with respect to a distinguisher A as follows:

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

We say that F is $(q, \ell, \sigma, \mathtt{t}, \epsilon)$ secure if the maximum pseudorandom function advantage of F is ϵ, where the maximum is taken over all distinguishers A that make q queries to its oracle such that the total number of message blocks queried across all q queries is σ with ℓ being the maximum number of message blocks among all q queries, and the adversary runs for time at most $\mathtt{t}$, i.e.,

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

where $\mathcal{C}$ is the class of all distinguishers A that makes at most q queries such that the total number of message blocks queried across all q queries is σ with ℓ being the maximum number of message blocks among all q queries with run time at most $\mathtt{t}$. Similarly, we define the notion of pseudorandom permutation advantage as follows:

Let $n, k \in \mathbb{N}$ be two natural numbers. Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of keyed functions from $\{0,1\}^n$ to $\{0,1\}^n$ such that for $K \in \{0,1\}^k$, the function $\mathsf{E}_K : \{0,1\}^n \to \{0,1\}^n$ is bijective. We define the pseudorandom permutation (prp) advantage of E with respect to a distinguisher A as follows:

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathsf{E}}(\mathsf{A}) \overset{\Delta}{=} \left|\mathsf{Pr}[K \leftarrow \{0,1\}^k : \mathsf{A}^{\mathsf{E}_K} = 1] - \mathsf{Pr}[\mathsf{P} \leftarrow \mathsf{Perm} : \mathsf{A}^{\mathsf{P}} = 1]\right|.$$

We call the family of keyed functions E a *block cipher* with the *block size* n-bits and the *key size* k-bits. We say that E is $(q, \mathtt{t}, \epsilon)$ secure if the maximum pesudorandom permutation advantage of E is ϵ, where the maximum is taken over all distinguishers A that make q queries to the respective oracle and run for time at most $\mathtt{t}$, i.e.,

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathsf{E}}(q, \mathtt{t}) \overset{\Delta}{=} \max_{\mathsf{A} \in \mathcal{C}} \mathbf{Adv}^{\mathrm{prp}}_{\mathsf{E}}(\mathsf{A}),$$

where $\mathcal{C}$ is the class of all distinguishers A that makes at most q queries with run time at most $\mathtt{t}$. We write $\mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ to denote the set of all block ciphers with key space $\mathcal{K}$ and block size n bits.

2.2 Expectation Method

The Expectation Method was introduced by Hoang and Tessaro [23] to derive a tight multi-user security bound of the key-alternating cipher. Subsequently, this technique has been used for bounding the distinguishing advantage of various cryptographic constructions [24, 11, 22]. The Expectation Method is a generalization of the H-Coefficient technique developed by Patarin [42], which serves as a "systematic" tool to upper bound the distinguishing advantage of any deterministic and computationally unbounded distinguisher A in distinguishing the real oracle $\mathcal{O}_1$ (construction of interest) from the ideal oracle $\mathcal{O}_0$ (idealized version). The collection of all the queries and responses that A made and received to and from the oracle, is called the *transcript* of A, denoted as τ. Sometimes, we allow the oracle to release more internal information to A only after A completes all its queries and responses, but before it outputs its decision bit. Note that, revealing extra informations will only increase the advantage of the distinguisher.

Let X_{re} and X_{id} denote the transcript random variable induced by the interaction of A with the real oracle and the ideal oracle respectively. The probability of realizing a transcript τ in the ideal oracle (i.e., $\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} = \tau]$) is called the *ideal interpolation probability*. Similarly, one can define the *real interpolation probability*. A transcript τ is said to be *attainable* with respect to A if the ideal interpolation probability is non-zero (i.e., $\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} = \tau] > 0$). We denote the set of all attainable transcripts by $\mathcal{V}$. Following these notations, we state the main result of the Expectation Method in Theorem 1. The proof of this theorem can be found in [23].

Theorem 1. *Let $\mathcal{V} = \mathsf{GoodT} \sqcup \mathsf{BadT}$ be a partition of the set of attainable transcripts. Let $\Phi : \mathcal{V} \to [0, \infty)$ be a non-negative real valued function. For any attainable good transcript $\tau \in \mathsf{GoodT}$, assume that*

$$\frac{\mathsf{Pr}[\mathsf{X}_{\mathrm{re}} = \tau]}{\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} = \tau]} \geq 1 - \Phi(\tau),$$

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

$$\mathbf{Adv}_{\mathcal{O}_1}^{\mathcal{O}_0}(\mathsf{A}) \leq \mathbf{E}[\Phi(\mathsf{X}_{\mathrm{id}})] + \epsilon_{\mathrm{bad}}. \tag{1}$$

If $\mathcal{O}_0$ is a random function, then Eqn. (1) gives the PRF advantage of A in distinguishing the real construction $\mathcal{O}_1$ from the random function and in that case, we write

$$\mathbf{Adv}_{\mathcal{O}_1}^{\mathrm{PRF}}(\mathsf{A}) \leq \mathbf{E}[\Phi(\mathsf{X}_{\mathrm{id}})] + \epsilon_{\mathrm{bad}}. \tag{2}$$

We would like to mention that if Φ is a constant function, then the Expectation method [23] boils down to the H-Coefficient technique [42].

2.3 Combinatorial Results

In this section, we state and prove the two results. The first one is from linear algebra that establishes an upper bound on the probability that a system of equations holds when the variables are wor samples. The second result is about maximizing a function, which will be useful in deriving the security bound of LightMAC and LightMAC_Plus constructions.

Lemma 1. *Let $(Z_1, \ldots, Z_q) \xleftarrow{\mathrm{wor}} \mathcal{X} \subseteq \{0,1\}^n$ 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*

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

Proof. The matrix A can be represented as $A = [A_1 A_2 \ldots A_q]$, where each A_i is a column vector of length k and $rank(A) = r$. W.l.o.g, we can assume $A_1, A_2, \ldots, A_r$ are linearly independent basis vectors. So, $A_{r+1}, \ldots, A_q$ are the non-basis vectors. Note that, for each choice of the tuple $(z_{r+1}, \ldots, z_q)$, with distinct z_i's, the remaining z_i values are uniquely determined. The total number of distinct choices of $(z_1, \ldots, z_q)$ is $\mathbf{P}(N, q)$, and the choices of $(z_{r+1}, \ldots, z_q)$ is $\mathbf{P}(N, q - r)$. Hence, the probability is at most $\frac{\mathbf{P}(N, q-r)}{\mathbf{P}(N, q)}$.

Lemma 2. *Let q be a positive non-zero integer and for all $i \in [q]$, $c_i, h_i \in \mathbb{Z}^+ \cup \{0\}$. Then the function*

$$c_1h_1^2 + c_2h_2^2 + \ldots + c_qh_q^2$$

subject to the constraint

$$c_1h_1 + c_2h_2 + \ldots + c_qh_q \leq q,$$

attains the maximum value $q^{3/2}$ when $c_1h_1 = q$, given that $h_i \leq \sqrt{q}$ for all $i \leq q$ and $h_1 \geq h_2 \geq \ldots \geq h_q$.

Proof. Let us consider z_i to denote c_ih_i, for all $i \in [q]$. Since, $c_i, h_i \in \mathbb{Z}^+ \cup \{0\}$, it holds that $z_i \in \mathbb{Z}^+ \cup \{0\}$, for all $i \in [q]$. Therefore, the objective function becomes

$$f(z_1, z_2, \ldots, z_q) \stackrel{\Delta}{=} z_1h_1 + z_2h_2 + \ldots + z_qh_q,$$

subject to the constraint

$$z_1 + z_2 + \ldots + z_q \leq q.$$

First of all, it is easy to see that the objective function will become maximized, when $z_1 + z_2 + \ldots z_q = q$. Therefore, we consider the constraint to be

$$z_1 + z_2 + \ldots z_q = q.$$

Now, our claim is $v^* \stackrel{\Delta}{=} (q, 0, 0, \ldots, 0)$ is the optimal solution for which the objective function will attain the maximum value. Let us consider some other arbitrary solution $v' \stackrel{\Delta}{=} (q', \alpha_1, \alpha_2, \ldots, \alpha_{q-1})$, where $q' < q$. Then, we have

$$A \stackrel{\Delta}{=} f(v^*) = qh_1, \; B \stackrel{\Delta}{=} f(v') = q'h_1 + \alpha_1h_2 + \alpha_2h_3 + \ldots + \alpha_{q-1}h_q.$$

Since, v' is a solution, we have $q' = q - (\alpha_1 + \alpha_2 + \ldots + \alpha_{q-1})$. Plugging-in the above equality in B yields

$$f(v') = qh_1 - (h_1 - h_2)\alpha_1 - (h_1 - h_3)\alpha_2 - \ldots - (h_1 - h_q)\alpha_{q-1}.$$

Since, $h_1 \geq h_i$, for all $i \in [2, q]$, it holds that $f(v') \leq f(v^*)$. Therefore, the maximum value obtained, is $qh_1 \leq q^{3/2}$, as $h_1 \leq \sqrt{q}$. □

2.4 Mirror Theory

Consider an undirected edge-labelled bipartite graph $\mathsf{G} = (\mathcal{V}_1 \sqcup \mathcal{V}_2, \mathcal{E}, \mathcal{L})$ with edge labelling function $\mathcal{L} : \mathcal{E} \to \{0,1\}^n$, where $\mathcal{V}_1 = \{Y_1, \ldots, Y_{s_\ell}\}$ and $\mathcal{V}_2 = \{Z_1, \ldots, Z_{s_\mathrm{r}}\}$, such that $s = s_\ell + s_\mathrm{r}$ is the total number of vertices in the graph. We denote an edge of $\mathcal{E}$ as $\{Y_i, Z_j\}$, and its label as $\mathcal{L}(\{Y_i, Z_j\}) = \lambda_{ij}$ (thus, $\lambda_{ij} = \lambda_{ji}$). For a path $\mathcal{P}$ in the graph G, we define the label of the path as $\mathcal{L}(\mathcal{P}) := \sum_{e \in \mathcal{P}} \mathcal{L}(e)$. Similarly, for a cycle $\mathcal{C}$ in the graph G, we define the label of the cycle as $\mathcal{L}(\mathcal{C}) := \sum_{e \in \mathcal{C}} \mathcal{L}(e)$. We say the graph G is **good** if it satisfies the following conditions:

1. G is acylic.

2. Maximum path length of G is two.

3. $\mathcal{L}(\mathcal{P}) \neq \mathbf{0}$, for all paths in G.

For such a good graph G, we associate a system of bivariate affine equations as follows:

$$\mathcal{E}_{\mathsf{G}}^{\mathtt{bi}} := \{Y_i \oplus Z_j = \lambda_{ij} \; \forall \; \{Y_i, Z_j\} \in \mathcal{E}\}.$$

In the above system of bivariate affine equations, the variables are the vertices of the associated graph G. 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 equation are the label of the corresponding edge. Therefore, for $\mathcal{E}_{\mathsf{G}}^{\mathtt{bi}}$, the variables are Y_i's and Z_i's. For a good graph G, two vertices are said to be adjacent to each other if and only if they are connected by an edge in $\mathcal{E}$. This induces a partition on $\mathcal{V}_1 \sqcup \mathcal{V}_2$, and each connected component is called a component. The size of a component refers to the number of elements (i.e., the number of vertices) in the partition, and the set of components is denoted by $\mathsf{comp}(\mathsf{G}) = (\mathsf{C}_1 \sqcup \cdots \sqcup \mathsf{C}_\alpha)$ where each component is of size at least 2.

Definition 1. Let $\mathcal{E}_{\mathsf{G}}$ be a system of equations corresponding to a good acyclic edge-labelled bipartite graph G (as defined above). An injective function $\Phi : \mathcal{V}_1 \sqcup \mathcal{V}_2 \rightarrow \{0,1\}^n$, is said to be an *injective solution* to $\mathcal{E}_{\mathsf{G}}$, if for all $\{Y_i, Z_j\} \in \mathcal{E}_{\mathsf{G}}$, it holds that $\Phi(Y_i) \oplus \Phi(Z_j) = \lambda_{ij}$.

In the following, we state a variant of mirror theory, which asserts that if G is a good, acyclic, edge-labelled bipartite graph that can be decomposed into finitely many components of size at least 2, then the number of solutions to $\mathcal{E}_{\mathsf{G}}$ chosen outside of the set $\mathcal{S}_1 \times \mathcal{S}_2 \subseteq \{0,1\}^n \times \{0,1\}^n$, where $\mathcal{S}_1, \mathcal{S}_2$ are two non-empty finite arbitrary subsets of $\{0,1\}^n$, is very close to the average number of solutions until the number of edges in $\mathcal{E}_{\mathsf{G}}$ is roughly $2^{2n/3}$. In the traditional mirror theory, solutions to $\mathcal{E}_{\mathsf{G}}$ is chosen from the set $\{0,1\}^n \times \{0,1\}^n$. However, in the current set up, we choose the solution from a non-empty subset of $\{0,1\}^n \times \{0,1\}^n$. We refer to this variant of mirror theory as *mirror theory over restricted set*. It is worth mentioning that Dutta and Nandi [21] have already established a similar security bound for the mirror theory over a restricted set when the graph G is an acylic good *general* graph. In other words, the authors of [21] have shown that the number of solutions to $\mathcal{E}_{\mathsf{G}}$, chosen from a non-empty subset of $\{0,1\}^n$, is close to the average number of solutions until the number of edges in $\mathcal{E}_{\mathsf{G}}$ is roughly $2^{2n/3}$. The following lemma gives a similar lower bound for the mirror theory over a restricted set when the graph G is a good, acyclic, edge-labelled bipartite graph, proof of which can be found in Theorem 1 of [16]. For completeness, we provide a independent proof of this lemma in Supplementary Section 7.

Lemma 3. *Let $\mathsf{G} = (\mathcal{V}_1 \sqcup \mathcal{V}_2, \mathcal{E}, \mathcal{L})$ be a good acyclic edge-labelled bipartite graph with s_ℓ many vertices in $\mathcal{V}_1$ and $s_{\mathtt{r}}$ many vertices in $\mathcal{V}_2$, such that $|\mathcal{E}| = q$ and $s = s_\ell + s_{\mathtt{r}}$, the total number of vertices of the graph G. Let the graph G have α components such that the i-th component has c_i vertices from $\mathcal{V}_1$ and d_i vertices from $\mathcal{V}_2$ such that $s_\ell = c_1 + \cdots + c_\alpha$ and $s_{\mathtt{r}} = d_1 + \cdots + d_\alpha$. Let $\rho_i[1] = (c_1 + c_2 + \cdots + c_i)$ and $\rho_i[2] = (d_1 + d_2 + \cdots + d_i)$. Then the total number of injective solutions to $\mathcal{E}_{\mathsf{G}}$ chosen from outside of the set $\mathcal{S}_1 \times \mathcal{S}_2 \subseteq \{0,1\}^n \times \{0,1\}^n$, is at least*

$$\frac{\mathbf{P}(2^n - \Delta_1, s_\ell).\mathbf{P}(2^n - \Delta_2, s_{\mathtt{r}})}{2^{nq}} \left(1 - \sum_{i=1}^{\alpha} \left(\frac{10\left(\binom{c_i+d_i}{2}(\Delta_1 + \Delta_2 + \rho_{i-1}[1] + \rho_{i-1}[2])^2\right)}{2^{2n}}\right)\right),$$

provided $(\Delta_1 + \rho_\alpha[1])c_{\max} \leq 2^{n-3}$ and $(\Delta_2 + \rho_\alpha[2])d_{\max} \leq 2^{n-3}$, where $c_{\max} = \max\{c_1, c_2, \cdots, c_\alpha\}$, $d_{\max} = \max\{d_1, d_2, \ldots, d_\alpha\}$, Δ_1 denotes the size of the set $\mathcal{S}_1$ and Δ_2 denotes the size of the set $\mathcal{S}_2$.

3 Security Results of LightMAC and LightMAC_Plus

In this section, we first state the existing security result of LightMAC and LightMAC_Plus. In FSE'16, Luykx et al. [31] have shown that LightMAC is secured against all information-theoretic distinguishers in the single user setting under the pseudorandom permutation assumption of the underlying block cipher of the construction that makes roughly up to $2^{n/2}$ queries such that the maximum length of the message is $2^s(n-s)$ bits, where n is the block size of the underlying block cipher and s is the size of the block counter. The following result establishes an upper bound on the PRF advantage of LightMAC construction against all information-theoretic adversaries in the single user setting.

Theorem 2 (**Security Result of LightMAC**)**.** *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,t) adversary against* LightMAC[E] *is given by,*

$$\begin{aligned}\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{LightMAC[E]}}(q,t) &\leq \left(1 + \frac{1}{2^{n/2}-1} + \frac{1}{2(2^{n/2}-1)^2}\right)\frac{q^2}{2^n} + \mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(q(2^s-1),t_1)\\ &+ \mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(q,t_2),\end{aligned}$$

provided the maximum number of message blocks $\ell \leq 2^{n/2}$ and $t_1 = t + O(q(2^s-1))$, and $t_2 = t + O(q)$.

In ASIACRYPT'17, Naito [37] has shown that LightMAC_Plus is secure against all information-theoretic distinguishers in the single user setting under the pseudorandom permutation assumption of the underlying block cipher of the construction that makes roughly up to $2^{2n/3}$ queries such that the maximum length of the message is $\min\{2^s(n-s),(n-s)2^{n-1}\}$ bits, where n is the block size of the underlying block cipher and s is the size of the block counter. The following result establishes an upper bound on the PRF advantage of LightMAC_Plus against all information-theoretic adversaries in the single user setting.

Theorem 3 (**Security Result of LightMAC_Plus**)**.** *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,t) adversary against* LightMAC_Plus[E] *is given by,*

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{LightMAC\_Plus[E]}}(q,t) \leq \frac{2q^2}{2^{2n}} + \frac{4q^3}{2^{2n}} + \mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(q(2^s-1),t_1) + 2\mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(q,t_2),$$

provided the maximum number of message blocks $\ell \leq 2^{n/2}$ and $t_1 = t + O(q(2^s-1))$, and $t_2 = t + O(q)$.

The bound has been later improved from $2n/3$ bits to $3n/4$ bits in [27].

3.1 Multi User Security Result of LightMAC

In this section, we state the security result of LightMAC in the multi-user setting. In particular, we state and prove that LightMAC is secure against all information-theoretic distinguishers in the multi-user setting under the assumption that the underlying block cipher is an ideal cipher that makes roughly up to $2^{n/2}$ message queries and roughly 2^k many ideal-cipher queries such that the maximum number of message blocks is at most $2^s(n-s)$ bits, where n is being the block size of the underlying block cipher and s is the size of the block counter. The following result establishes an upper bound on the multi-user PRF advantage of LightMAC against all information-theoretic adversaries.

Theorem 4 (**Multi-User Security Result of LightMAC**)**.** *Let $\mathcal{K}$ be a finite and non-empty set. Let $\mathsf{E} \leftarrow_{\$} \mathsf{BC}(\mathcal{K},\{0,1\}^n)$ be an ideal block cipher. Then any computationally unbounded distinguisher, making a total of q construction queries across all u users and a total of p ideal-cipher queries to the ideal block cipher* E*, can distinguish* LightMAC *from an n-bit uniform random function with prf advantage*

$$\mathbf{Adv}^{\mathrm{mu\text{-}PRF}}_{\mathsf{LightMAC[E]}}(u,q,p,\ell) \leq \frac{2q^2}{2^k} + \frac{2q^2}{2^n} + \frac{25p}{2^k} + \frac{3qp}{2^{n+k}} + \frac{pq\ell k}{2^{n+k}} + \frac{q^2\ell k}{2^n},$$

where ℓ is the maximum number of message blocks queried such that $\ell \leq 2^{n/2}$.

Note that the above security bound of LightMAC contains a factor of ℓ, whereas the single-user security of the LightMAC construction possesses an ℓ-free bound, provided $\ell \leq 2^{n/2}$. We show that if we restrict the number of ideal-cipher queries up to $2^{3k/4}$, then we can prove an ℓ-free birthday multi-user security bound of LightMAC, provided $\ell \leq 2^{n/4}/k$. Formally, we have the following:

Theorem 5 (**ℓ-Free Multi-User Security Result of LightMAC**). *Let $\mathcal{K}$ be a finite and non-empty set. Let $\mathsf{E} \leftarrow_{\$} \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ be an ideal block cipher. Then any computationally unbounded distinguisher, making a total of q construction queries across all u users and a total of p ideal-cipher queries to the ideal block cipher E, can distinguish* LightMAC *from an n-bit uniform random function with prf advantage*

$$\mathbf{Adv}^{\text{mu-PRF}}_{\mathsf{LightMAC[E]}}(u,q,p) \quad \leq \quad \frac{2q^2}{2^k} + \frac{2q^2}{2^n} + \frac{25p}{2^k} + \frac{3qp}{2^{n+k}} + \frac{pq}{2^{\frac{3n}{4}+k}} + \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}}{2^{3n/4}},$$

where ℓ is the maximum number of message blocks queried such that $\ell \leq 2^{n/4}/k$.

We would like to mention here that if the number of users $u \leq 2^{k/4}$, then also we obtain the desired ℓ-free bound provided $p \leq 2^{3k/4}$, and $\ell \leq 2^{n/2}$. Details can be found in Remark 3.

Implication of Theorem 4 and Theorem 5 in the Context of AES: LightMAC with AES-256 can be safely used in a protocol having $2^{32}/2^{16}/2^8$ users. When we instantiate LightMAC with AES-256, then Theorem 4 guarantees security up to $2^{16}/2^{24}$ construction queries for $2^{16}/2^8$ users respectively. Users can make construction queries with maximum allowable message length of 2^{56} blocks. However, Theorem 5, which ensures an ℓ-free security bound, provides security up to $2^{32}/2^{48}/2^{56}$ construction queries when there are $2^{32}/2^{16}/2^8$ users respectively. Moreover as we have $u \leq 2^{k/4}$ in our case, the result also guarantees $2^{160}/2^{176}/2^{184}$ ideal cipher queries respectively. Here, users can make construction queries with maximum allowable message length of 2^{64} blocks. It is important to note that Theorem 4 allows the processing of a greater number of data blocks in a query compared to what Theorem 5 offers. Nevertheless, the latter provides a superior security guarantee on the number of queries compared to the former.

3.2 Multi User Security Result of LightMAC_Plus

Now, we state the security result of LightMAC_Plus construction in the multi-user setting. In particular, we state and prove that LightMAC_Plus is secure against all information-theoretic distinguishers in the multi-user setting under the assumption that the underlying block cipher is an ideal cipher that makes roughly up to $2^{2n/3}$ many message queries and roughly $2^{2k/3}$ many ideal-cipher queries such that the maximum number of message blocks is at most $2^s(n-s)$ bits, where n is being the block size of the underlying block cipher and s is the size of the block counter. The following result establishes an upper bound on the multi-user PRF advantage of LightMAC_Plus construction against all information-theoretic adversaries.

Theorem 6 (**Multi-User Security Result of LightMAC_Plus**). *Let $\mathcal{K}$ be a finite and non-empty set. Let $\mathsf{E} \leftarrow_{\$} \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ be a ideal block cipher. Then any computationally unbounded distinguisher, making a total of q construction queries across all u users and a total of p ideal-cipher queries to the ideal block cipher E, can distinguish* LightMAC_Plus *from an n-bit uniform random function with prf advantage*

$$\mathbf{Adv}^{\text{mu-PRF}}_{\mathsf{LightMAC\_Plus[E]}}(u,q,p,\ell) \quad \leq \quad \frac{q^2}{2^{2k}} + \frac{q^3}{2^{2k}} + \frac{q^2p^2}{2^{3k}} + \frac{qp^2}{2^{2k}} + \frac{q}{2^k} + \frac{2q^2\ell}{2^{n+k}} + \frac{4q^2}{2^{2n}} + \frac{4q^2}{2^{n+k}}$$

$$
\begin{aligned}
&+ \frac{2q^3}{3.2^{2n}} + \frac{2q^{3/2}}{2^n} + \frac{4qp}{2^{n+k}} + \frac{2pq\ell k}{2^{n+k}} + \frac{48p}{2^k} + \frac{2pq^{1/2}}{2^k} + \frac{2q^{3/2}k\ell}{2^n} \\
&+ \frac{40p^2q^2}{2^{3n}} + \frac{320pq^3}{2^{3n}} + \frac{320q^4}{2^{3n}} + \frac{160p^2q}{2^{2n}} + \frac{1280pq^2}{2^{2n}} + \frac{1280q^3}{2^{2n}},
\end{aligned}
$$

where $q < 2^{n-2}$ and ℓ is the maximum number of message blocks queried such that $\ell \leq \min\{2^{n-1}, 2^s\}$.

Note that the above security bound of LightMAC_Plus contains a factor of ℓ, whereas the single-user security of the LightMAC_Plus construction possesses an ℓ-free bound, provided $\ell \leq 2^{n/2}$. We show that if we assume that $k \geq 4n/3$, then we can prove an ℓ-free multi-user security bound of the LightMAC_Plus construction, provided $\ell \leq 2^{n/3}/k$. Formally, we have the following:

Theorem 7 **(ℓ-free Multi-User Security Result of LightMAC_Plus).** *Let $\mathcal{K}$ be a finite and non-empty set. Let $\mathsf{E} \xleftarrow{\$} \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ be a ideal block cipher. Then any computationally unbounded distinguisher, making a total of q construction queries across all u users and a total of p ideal-cipher queries to the ideal block cipher E, can distinguish* LightMAC_Plus *from an n-bit uniform random function with prf advantage*

$$
\begin{aligned}
\mathbf{Adv}^{\text{mu-PRF}}_{\mathsf{LightMAC\_Plus[E]}}(u, q, p, \ell) \leq\ & \frac{q^2}{2^{2k}} + \frac{q^3}{2^{2k}} + \frac{q^2p^2}{2^{3k}} + \frac{qp^2}{2^{2k}} + \frac{q}{2^k} + \frac{2q^2}{2^{2n/3+k}} + \frac{4q^2}{2^{2n}} + \frac{4q^2}{2^{n+k}} \\
&+ \frac{2q^3}{3.2^{2n}} + \frac{2q^{3/2}}{2^n} + \frac{4qp}{2^{n+k}} + \frac{2pq}{2^{2n/3+k}} + \frac{36p}{2^{3k/4}} + \frac{2pq^{1/2}}{2^k} \\
&+ \frac{40p^2q^2}{2^{3n}} + \frac{320pq^3}{2^{3n}} + \frac{320q^4}{2^{3n}} + \frac{160p^2q}{2^{2n}} + \frac{1280pq^2}{2^{2n}} + \frac{1280q^3}{2^{2n}},
\end{aligned}
$$

where $q \leq 2^{n-2}$, $k \geq 4n/3$ and ℓ is the maximum number of message blocks queried such that $\ell \leq \min\{2^{n/3}/k, 2^s\}$.

Implication of Theorem 6 and Theorem 7 in the Context of AES: Here we again instantiate LightMAC_Plus with AES-256. Theorem 6 guarantees security up to $2^{20}/2^{36}/2^{44}$ construction queries for $2^{32}/2^{16}/2^8$ users respectively. Users can make construction queries with maximum allowable message length of 2^{40} blocks. However, Theorem 7, yields security up to $2^{66}/2^{82}/2^{90}$ construction queries when there are $2^{32}/2^{16}/2^8$ users respectively. Here, users can make construction queries with maximum allowable message length of 2^{34} blocks. Moreover, both the results guarantee $2^{138}/2^{154}/2^{162}$ ideal cipher queries respectively.

4 Proof of Theorem 4

We consider a computationally unbounded non-trivial deterministic distinghisher A that interacts with a pair of oracles in either the real world or the ideal world, described as follows: in the real world, A is given access to u independent instances of the LightMAC construction, i.e., to a tuple of u oracles $(\mathsf{LightMAC[E]}_{(K_1^i, K_2^i)})_{i \in [u]}$, where each (K_1^i, K_2^i) is independent of (K_1^j, K_2^j) and $\mathsf{E} \xleftarrow{\$} \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ is an ideal block cipher. Additionally, A has access to the oracle $\mathsf{E}^{\pm}$, underneath the construction LightMAC. In the ideal world, A is given access to (i) a tuple of u independent random functions $(\mathsf{RF}_1, \ldots, \mathsf{RF}_u)$, where each RF_i is the random function from $\{0,1\}^*$ to $\{0,1\}^n$ that can be equivalently described as a procedure that returns an n-bit uniform string on input of any arbitrary message, and (ii) the oracle $\mathsf{E}^{\pm}$, where $\mathsf{E} \xleftarrow{\$} \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ is an ideal block cipher, sampled independent of the distribution of the sequence of the u independent random functions. In both worlds, the first oracle is called the *construction oracle* and the latter, the *ideal cipher oracle*. Using the ideal cipher oracle, a distinguisher A can evaluate any query x under its chosen key J. A query to the construction oracle is called a *construction query* and to that of the ideal cipher oracle is called an *ideal cipher query*. Note that A can make either *forward* (i.e., it evaluates E with a chosen key and input), or *inverse* ideal cipher queries (i.e., it evaluates E^{-1} with a chosen key and input).

4.1 Attack Transcript

We summarize the interaction between the distinguisher and the challenger in a transcript $\tau_c = \tau_c^1 \cup \tau_c^2 \cup \ldots \cup \tau_c^u$, where $\tau_c^i = \{(M_1^i, T_1^i), \ldots, (M_{q_i}^i, T_{q_i}^i)\}$ denotes the query-response transcript generated from the i-th instance of the construction. Moreover, we assume that A has chosen g distinct ideal cipher keys $J^1, \ldots, J^g$ such that it makes p_j ideal cipher queries to the block cipher with the chosen key J^j. We summarize the ideal cipher queries in a transcript $\tau_p = \tau_p^1 \cup \tau_p^2 \cup \ldots \cup \tau_p^g$, where $\tau_p^j = \{(u_1^j, v_1^j), \ldots, (u_{p_j}^j, v_{p_j}^j), J^j\}$ denotes the transcript of the ideal cipher queries when the chosen ideal cipher key is J^j. We assume that A makes q_i construction queries for the i-th instance and p_j ideal cipher queries (including forward and inverse queries) with chosen ideal cipher key J^j. We also assume that the total number of construction queries across u instances is q, i.e., $q = (q_1 + \ldots + q_u)$ and the total number of ideal cipher queries is $p = (p_1 + \ldots + p_g)$. Since A is non-trivial, none of the transcripts contain any duplicate elements.

We modify the experiment by releasing internal informations to A after it has finished its interaction but has not yet output the decision bit. In the real world, we reveal all the keys (K_1^i, K_2^i) for all u users and also the $(V_a^i[\alpha])_{i\in[q],a\in[q_i],\alpha\in[\ell_a^i]}$ tuple, where ℓ_a^i is the maximum number of message blocks corresponding the a-th query of the i-th user and $V_a^i[\alpha] = \mathsf{E}_{K_1^i}(\langle\alpha\rangle_s \| M_a^i[\alpha])$. In the ideal world, the challenger samples the keys (K_1^i, K_2^i) uniformly at random from their respective key spaces for all u users and computes the $(V_a^i[\alpha])_{i\in[q],a\in[q_i],\alpha\in[\ell_a^i]}$ tuple as follows:

$$V_a^i[\alpha] = \mathsf{E}_{K_1^i}(\langle\alpha\rangle_s \| M_a^i[\alpha])$$

and reveal them to the distinguisher. Therefore, each transcript τ_i^c, where $i \in [u]$, is now modified to include the corresponding pair of keys and $V_a^i[\alpha]$ values for the i-th instance of the construction. Thus,

$$\tilde{\tau}_c^i = \{(M_1^i, T_1^i, \widetilde{V}_1^i), \ldots, (M_{q_i}^i, T_{q_i}^i, \widetilde{V}_{q_i}^i), K_1^i, K_2^i\},$$

where $\widetilde{V}_a^i := (V_a^i[\alpha])_{\alpha\in[\ell_a^i]}$. In all the following, the complete construction query transcript is

$$\tau_c = \bigcup_{i=1}^{u} \tilde{\tau}_c^i$$

and the overall transcript is $\tau = \tau_c \cup \tau_p$. The modified experiment only makes the distinguisher more powerful and hence the distinguishing advantage of A in this experiment is no less than its distinguishing advantage in the former.

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 find a lower bound for the ratio of the real to ideal interpolation probability for a good transcript. Therefore, it only remains to bound the probability of bad transcripts in the ideal world and provide a lower bound for the ratio of the real to ideal interpolation probability for a good transcript. It follows that for each $i \in [u]$, $\mathsf{LightMAC}[\mathsf{E}]_{(K_1^i,K_2^i)} \mapsto \tilde{\tau}_c^i$ denotes the following:

(a) $\Sigma_a^i = \bigoplus_{\alpha=1}^{\ell_a^i} V_a^i[\alpha]$, $a \in [q_i]$

(b) $\mathsf{E}_{K_2^i}(\Sigma_a^i) = T_a^i$, $a \in [q_i]$.

4.2 Definition and Bounding Probability of Bad Transcripts

In this section we define and bound the probability of bad transcripts in the ideal world. Note that, following (a), one can derive $\widetilde{\Sigma}^i := (\Sigma^i_1, \Sigma^i_2, \ldots, \Sigma^i_{q_i})$ tuple from the transcript $\tau = (\tau_c, \tau_p)$ for each user i. We denote the input to the α-th ideal-cipher query corresponding to the ideal-cipher key J^j as X^j_α and the corresponding response as Y^j_α. We say that an attainable transcript $\tau = (\tau_c, \tau_p)$ is a **bad** transcript if any one of the following events hold true

1. $\mathsf{BadK1}$: $\exists i_1 \neq i_2 \in [u]$ such that $K^{i_1}_2 = K^{i_2}_2$ or $K^{i_1}_1 = K^{i_2}_1$
2. $\mathsf{BadK2}$: $\exists i_1 \neq i_2 \in [u]$ such that $K^{i_1}_1 = K^{i_2}_2$
3. $\mathsf{BadCollT}$: $\exists i_1 \neq i_2 \in [u]$, $a \in [q_{i_1}]$, $b \in [q_{i_2}]$ such that $T^{i_1}_a = T^{i_2}_b$
4. $\mathsf{Bad1}$: $\exists i \in [u], a \in [q_i], j \in [g], \alpha \in [p_j]$ such that $K^i_2 = J^j, T^i_a = Y^j_\alpha$.
5. $\mathsf{Bad2}$: $\exists i \in [u], a \in [q_i], j \in [g], \alpha \in [p_j]$ such that $K^i_2 = J^j, \Sigma^i_a = X^j_\alpha$.
6. $\mathsf{Bad3}$: $\exists i \in [u], a \neq b \in [q_i]$ such that $\Sigma^i_a = \Sigma^i_b$.

Recall that $\mathsf{BadT} \subseteq \mathcal{V}$ is the set of all attainable bad transcripts and $\mathsf{GoodT} = \mathcal{V} \setminus \mathsf{BadT}$ is the set of all attainable good transcripts. Before we proceed for bounding the above events in the ideal world, we state the following lemma from [31, Proposition 1] that upper bounds the collision probability between two Σ 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 4 (**Collision of Σ**). *Let M_a and M_b be two distinct messages such that the maximum number of message blocks is ℓ. Then, for an arbitrary constant $c \in \{0,1\}^n$, we have*

$$(i)\ \Pr[\Sigma_a = \Sigma_b] \leq \frac{2}{2^n}, (ii)\ \Pr[\Sigma_a = c] \leq \frac{2}{2^n},$$

provided $\ell \leq 2^{n/2}$. [1]

The following lemma upper bounds the probability of realizing a bad transcript in the ideal world.

Lemma 5 (**Bad Lemma**). *Let $\tau = (\tau_c, \tau_p)$ be any attainable transcript. Let X_{id} and BadT be defined as above. Then*

$$\Pr[\mathsf{X}_{\mathrm{id}} \in \mathsf{BadT}] \quad \leq \quad \frac{2q^2}{2^k} + \frac{2q^2}{2^n} + \frac{25p}{2^k} + \frac{3qp}{2^{n+k}} + \frac{pq\ell k}{2^{n+k}} + \frac{q^2\ell k}{2^n},$$

where ℓ is the maximum number of message blocks queried such that $\ell \leq 2^{n/2}$.

Proof. Let us define the event $\mathsf{BadT} := \mathsf{BadK1} \vee \mathsf{BadK2} \vee \mathsf{BadCollT} \vee (\mathsf{Bad1} \mid \overline{\mathsf{BadCollT}}) \vee \mathsf{Bad2} \vee \mathsf{Bad3}$. 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.

I. Bounding $\mathsf{BadK1}$. Recall that the event $\mathsf{BadK1}$ holds if there exists two distinct users i_1 and i_2 such that $K^{i_1}_2$ collides with $K^{i_2}_2$ or $K^{i_1}_1$ collides with $K^{i_2}_1$. In the ideal world, since the block cipher keys of each user are drawn independently and uniformly at random, for a fixed choice of two users i_1 and i_2, the probability that $K^{i_1}_2 = K^{i_2}_2$ holds, is exactly

[1] The bound on the maximum message length in terms of the number of blocks is actually $\min\{2^{n-1}, 2^s\}$. However, as we choose $s = n/2$ for achieving rate $1/2$, the bound on ℓ is at most $2^{n/2}$.

2^{-k}. Similarly, for a fixed choice of two users i_1 and i_2, the probability that $K_1^{i_1} = K_1^{i_2}$ holds, is exactly 2^{-k}. Therefore, by varying over all possible choices of users, we have

$$\Pr[\mathsf{BadK1}] \leq \frac{2\binom{u}{2}}{2^k} \leq \frac{2\binom{q}{2}}{2^k} \leq \frac{q^2}{2^k}. \tag{3}$$

II. Bounding BadK2. Consider the event BadK2, defined as the presence of two distinct users, denoted as i_1 and i_2, such that their corresponding block cipher keys $K_1^{i_1}$ and $K_2^{i_2}$ collide. Since in the ideal world, the block cipher keys for each user are sampled independently and uniformly at random, the probability of $K_1^{i_1}$ being equal to $K_2^{i_2}$ for a fixed choices of i_1 and i_2 is precisely 2^{-k}. Consequently, by considering all possible combinations of users, the probability of the event BadK2 occurring is given by the inequality:

$$\Pr[\mathsf{BadK2}] \leq \frac{\binom{u}{2}}{2^k} \leq \frac{\binom{q}{2}}{2^k} \leq \frac{q^2}{2^{k+1}}. \tag{4}$$

III. Bounding BadCollT. Consider the event BadCollT holds if there exists a pair of users i_1, i_2 such that one of the T values of i_1 user $T_a^{i_1}$ collides with an another T values of i_2 user $T_b^{i_2}$. For a fixed choice of two users i_1 and i_2, the probability that $T_a^{i_1} = T_b^{i_2}$ holds, is exactly 2^{-n}. Therefore, by varying over all possible choices of users, we have

$$\Pr[\mathsf{BadCollT}] \leq \frac{\binom{u}{2}}{2^n} \leq \frac{\binom{q}{2}}{2^n} \leq \frac{q^2}{2^{n+1}}. \tag{5}$$

IV. Bounding Bad1 | $\overline{\text{BadCollT}}$. Note that the event Bad1 holds if there exists an user i such that its block cipher key K_2^i collides with some chosen ideal-cipher key J^j, for some $j \in [g]$, and one of its obtained response T_a^i collides with a Y_α^j value of the corresponding ideal-cipher query. Recall that, in the ideal world, the responses of the user's queries are sampled independently and uniformly at random from $\{0,1\}^n$, and the block cipher keys of every users are sampled from $\mathcal{K}$ uniformly and independent to the distribution of the responses. Also, due to $\overline{\mathsf{BadCollT}}$, all the responses of the user's construction queries are distinct. Now depending on the order of occurance of the construction queries and the ideal-cipher queries we have the following cases:

□ Case A: Construction query followed by ideal-cipher query:
For a fixed choice of $j \in [g]$ and a fixed choice of ideal-cipher query $\alpha \in [p_j]$, the probability that $K_2^i = J^j, T_a^i = Y_\alpha^j$ holds, becomes $2^{-(n+k)}$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\mathsf{Bad1} \mid \overline{\mathsf{BadCollT}}] \leq \sum_{i=1}^{u}\sum_{a=1}^{q_i}\sum_{j=1}^{g}\sum_{\alpha=1}^{p_j} \frac{1}{2^{n+k}} \leq \frac{pq}{2^{n+k}}. \tag{6}$$

□ Case B: Ideal-cipher query followed by construction query:
If the ideal-cipher query is a forward query, then the similar analysis as that of Case A follows. On the other hand, if the ideal-cipher query is a backward query , we can set Y_α^j to the tag value T_a^i. Therefore, we cannot use the randomness of T and the probability that $K_2^i = J^j, T_a^i = Y_\alpha^j$ holds, becomes 2^{-k}. However, due to $\overline{\mathsf{BadCollT}}$, there exists exactly one choice of (i, a) such that $T_a^i = Y_\alpha^j$. Therefore, by varying over all possible choices of indices, we have

$$\Pr[\mathsf{Bad1} \mid \overline{\mathsf{BadCollT}}] \leq \sum_{j=1}^{g}\sum_{\alpha=1}^{p_j} \frac{1}{2^k} \leq \frac{p}{2^k}. \tag{7}$$

By combining Eqn. (6) and Eqn. (7), we have

$$\Pr[\mathsf{Bad1} \mid \overline{\mathsf{BadCollT}}] \leq \frac{pq}{2^{n+k}} + \frac{p}{2^k}. \tag{8}$$

V. Bounding Bad2. The event $\mathsf{Bad2}$ holds if there exists an user i such that its block cipher key K_2^i collides with some chosen ideal-cipher key J^j, for some $j \in [g]$, and one of its Σ values Σ_a^i collides with a corresponding primitive query input X_α^j. To bound this event, for each $i \in [u]$, we define an auxiliary event as follows:

$$\mathsf{BadK1}_i := \exists j' \in [g] : K_1^i = J^{j'}.$$

Now, we write the probability of the event $\mathsf{Bad1}$ as follows:

$$\begin{aligned}\Pr[\mathsf{Bad2}] \quad \leq \quad & \sum_{i=1}^{u}\Bigg(\Pr[\underbrace{\exists a \in [q_i], j \in [g], \alpha \in [p_j] : K_2^i = J^j, \Sigma_a^i = X_\alpha^j, \mathsf{BadK1}_i}_{\mathsf{E.1}}]\Bigg) \\ + \quad & \sum_{i=1}^{u}\Bigg(\Pr[\underbrace{\exists a \in [q_i], j \in [g], \alpha \in [p_j] : K_2^i = J^j, \Sigma_a^i = X_\alpha^j, \overline{\mathsf{BadK1}_i}}_{\mathsf{E.2}}]\Bigg).\end{aligned}$$

A. Bounding Event E.1. The event $\mathsf{E.1}$ implies that the block cipher key K_1^i of the i-th user collides with some chosen ideal-cipher key $J^{j'}$. As a result, all the V values for computing Σ_a^i may be pre-determined, as the distinguisher can make appropriate ideal-cipher queries to determine all the V values. Hence, to upper bound the probability that $\Sigma_a^i = X_\alpha^j$, we cannot use the randomness of V variables, which in turn prohibits us to apply Lemma 4 to upper bound the probability of $\Sigma_a^i = X_\alpha^j$, for a fixed choice of i, a, j, and α. Therefore, we have to use the event that $K_1^i = J^{j'}$, for some $j' \in [g]$. Now, in a very crude way, one can bound the event $K_2^i = J^j, \Sigma_a^i = X_\alpha^j, K_1^i = J^{j'}$ to at most 2^{-2k} by using the independence of two random variables K_1^i and K_2^i. However, by varying the all possible choices of indices, we have roughly $qp^2/2^{2k}$ bound, which eventually worsen our target bound. This observation restricts us from allowing too many ideal-cipher queries to satisfy the above event.

To this end, for a fixed key J^j, we define a following function:

$$\Sigma_{J^j}(M) := \bigoplus_{i=1}^{\ell_i} \mathsf{E}_{J^j}(\langle i \rangle_s \| M[i]).$$

Now, for a fixed message M and for a fixed arbitrary constant $c \in \{0,1\}^n$, we define the following set:

$$\mathcal{S}_c := \{j \in [g] : \Sigma_{J^j}(M) = c\}.$$

In other words, $\mathcal{S}_c$ denotes the set of ideal-cipher keys J^j such that $\Sigma_{J^j}(M) = c$. Let $\mathcal{S}$ be the set $\mathcal{S}_c$ such that the size of $\mathcal{S}_c$ is maximum over all choices of $\mathcal{S}_{c'}, c' \in \{0,1\}^n$. Therefore, we can write

$$\sum_{i=1}^{u} \Pr[\mathsf{E.1}] \quad \leq \quad \sum_{i=1}^{u} \Pr[\mathsf{E.1}, |\mathcal{S}| < \mu] + \Pr[|\mathcal{S}| \geq \mu] \tag{9}$$

We write the first term of the right hand side of Eqn. (9) as follows:

$$\sum_{i=1}^{u} \Pr[\exists a \in [q_i], j \in [g], \alpha \in [p_j] : K_2^i = J^j, \Sigma_a^i = X_\alpha^j, |\mathcal{S}| < \mu, \mathsf{BadK1}_i].$$

For a fixed choice of i, a, j, j', α, the probability of the event is upper bounded by 2^{-2k} due to the randomness of $K_1^i = J^{j'}$ and $K_2^i = J^j$. However, the number of choices of (i, a)

is at most q, the number of choices of (j, α) is at most p and the number of choices of j' is at most μ. Therefore, we have

$$\sum_{i=1}^{u} \Pr[\mathsf{E}.1, |\mathcal{S}| < \mu] \leq \frac{qp\mu}{2^{2k}}. \tag{10}$$

Now, it remains to bound the last term of the right hand side of Eqn. (9). We would like to note first that the event $|\mathcal{S}| \geq \mu$ implies that at least μ many distinct ideal-cipher keys J^j are there such that all the $\Sigma_{J^j}(M)$ values collides at a fixed but an arbitrary value c. It is easy to see that for a message M and for an arbitrary but a fixed constant $c \in \{0,1\}^n$,

$$\Pr[\Sigma_{J^j}(M) = c] \leq \frac{2}{2^n}, \tag{11}$$

where the probability is defined over the randomness of $\mathsf{E} \leftarrow_{\$} \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$. The probability follows because there will be at least one input-output for which either the input (in case of inverse ideal-cipher query) or the output (in case of forward ideal-cipher query) will be random. We use that randomness to bound the probability of the above event. Due to the independence of the keys $J^{j_1}, J^{j_2}, \ldots, J^{j_\mu}$, varying all possible choices of c, and by following Eqn. (11), the probability of the above event is $2^n(\frac{2}{2^n})^{\mu-1}$. Moreover, the number of ways we can choose the keys $J^{j_1}, J^{j_2}, \ldots, J^{j_\mu}$, is exactly $\binom{p}{\mu}$. Recall that, $\mathcal{S}$ depends on the message M. Therefore, we vary all possible choices of message M, which is bounded by $\max\{p^\ell, 2^{(n-s)\ell}\}$. In the following, we consider two cases: (a) when the maximum number of message choices is p^ℓ and (b) when the maximum number of message choices is $2^{(n-s)\ell}$.

□ Case A: maximum number of message choices is p^ℓ:

$$\Pr[|\mathcal{S}| \geq \mu] \leq 2^n p^\ell \binom{p}{\mu} \left(\frac{2}{2^n}\right)^{\mu-1} \leq 2^n p^{\ell+\mu} \cdot \frac{1}{\mu!} \cdot \left(\frac{2}{2^n}\right)^{\mu-1}. \tag{12}$$

By applying the Stirling approximation, we have

$$\Pr[|\mathcal{S}| \geq \mu] \leq 2^{2n} \cdot p^\ell \cdot \left(\frac{6p}{2^n\mu}\right)^{\mu} \leq \left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}, \tag{13}$$

where the last inequality follows from the fact $2^{2n}p^\ell \leq (k\ell)^{2^{k-n}k\ell}$, for $\mu = 2^{k-n}k\ell$.

□ Case B: maximum number of message choices is $2^{(n-s)\ell}$:

$$\Pr[|\mathcal{S}| \geq \mu] \leq 2^n 2^{(n-s)\ell} \binom{p}{\mu} \left(\frac{2}{2^n}\right)^{\mu-1} \leq 2^n 2^{(n-s)\ell} \cdot p^\mu \cdot \frac{1}{\mu!} \cdot \left(\frac{2}{2^n}\right)^{\mu-1}. \tag{14}$$

By applying the Stirling approximation, we have

$$\Pr[|\mathcal{S}| \geq \mu] \leq 2^{2n+(n-s)\ell} \cdot \left(\frac{6p}{2^n\mu}\right)^{\mu} \leq \left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}, \tag{15}$$

where the last inequality follows from the simple algebraic calculation: $2^{2n+(n-s)\ell} \leq (k\ell)^{2^{k-n}k\ell}$, for any $k \geq 4, \ell \geq 1, s \geq 1$ and $\mu = 2^{k-n}k\ell$. Note that we make the standard assumption that $k \geq n$.

Combining Eqn. (9), Eqn. (10), Eqn. (13) and Eqn. (15) and putting $\mu = 2^{k-n}\ell k$, we have

$$\sum_{i=1}^{u} \Pr[\mathsf{E}.1] \leq \frac{pq\mu}{2^{2k}} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \leq \frac{pq\ell k}{2^{n+k}} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}. \tag{16}$$

Now, we upper bound the probability of the event $\mathsf{E.2}$.

B. Bounding Event $\mathsf{E.2}$. The event $\mathsf{E.2}$ implies that the block cipher key K_1^i of the i-th user does not collide with any chosen ideal-cipher keys. As a result, the V values for computing Σ_a^i, is not pre-determined. Hence, to upper bound the probability that $\Sigma_a^i = X_\alpha^j$, we are allowed to use the randomness of V variables, which in turn allows us to apply Lemma 4 to upper bound the probability of $\Sigma_a^i = X_\alpha^j$ for a fixed choice of i, a, j, and α. Moreover, the event $K_2^i = J^j$ is independent over $\Sigma_a^i = X_\alpha^j$ as the former event is based on the randomness of K_2^i and the latter one is based on the randomness of K_1^i. Therefore, for a fixed choice of indices, the probability that $K_2^i = J^j, \Sigma_a^i = X_\alpha^j$ is at most $2/2^{(n+k)}$. Therefore, by varying over all possible choices of indices, we have

$$\sum_{i=1}^{u} \Pr[\mathsf{E.2}] \leq \frac{2qp}{2^{n+k}}, \tag{17}$$

as the total number of choices of (i, a) is at most q and the total number of choices of (j, α) is at most p.

Finally, by combining Eqn. (16) and Eqn. (17), we obtain

$$\Pr[\mathsf{Bad2}] \leq \frac{2qp}{2^{n+k}} + \frac{pq\ell k}{2^{n+k}} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}. \tag{18}$$

VI. Bounding $\mathsf{Bad3}$. Bounding $\mathsf{Bad3}$ is similar to that of $\mathsf{Bad1}$. Recall that the event $\mathsf{Bad3}$ holds, if there exists an user i such that two of its Σ values have collided. To bound this event, for each $i \in [u]$, we define an auxiliary event as follows:

$$\mathsf{BadK1}_i := \exists j' \in [g] : K_1^i = J^{j'}.$$

Due to the theorem of total probability, we write $\mathsf{Bad3}$ as follows:

$$\begin{aligned} \Pr[\mathsf{Bad3}] \quad &\leq \quad \sum_{i=1}^{u} \left(\Pr[\underbrace{\exists a \neq b \in [q_i] : \Sigma_a^i = \Sigma_b^i, \mathsf{BadK1}_i}_{\mathsf{E.1}}] \right) \\ &+ \quad \sum_{i=1}^{u} \left(\Pr[\underbrace{\exists a \neq b \in [q_i] : \Sigma_a^i = \Sigma_b^i, \overline{\mathsf{BadK1}_i}}_{\mathsf{E.2}}] \right). \end{aligned} \tag{19}$$

A. Bounding Event $\mathsf{E.1}$. The event $\mathsf{E.1}$ implies that the block cipher key K_1^i of the i-th user collides with some chosen ideal-cipher key $J^{j'}$. As a result, all the V values for computing Σ_a^i and Σ_b^i may be pre-determined, as the distinguisher can make appropriate ideal-cipher queries to determine all the V values. Hence, to upper bound the probability that $\Sigma_a^i = \Sigma_b^i$, we cannot use the randomness of V variables, which in turn prohibits us to apply Lemma 4 to upper bound the probability of $\Sigma_a^i = \Sigma_b^i$, for a fixed choice of i, a, and b. Therefore, we have to use the event that $K^i = J^{j'}$, for some $j' \in [g]$. Now, in a very crude way, one can bound the event $\Sigma_a^i = \Sigma_b^i, K_1^i = J^{j'}$ to at most 2^{-k}, by using the randomness of the event $K_1^i = J^{j'}$. However, by varying the all possible choices of indices, we have roughly $q^2p/2^k$ bound, which eventually worsen our target bound. This observation restricts us from allowing too many ideal-cipher queries to satisfy the above event.

As before, it is easy to see that for two distinct messages,

$$\Pr[\Sigma_{J^j}(M) = \Sigma_{J^j}(M')] \leq \frac{2}{2^n}, \tag{20}$$

where the probability is defined over the randomness of $\mathsf{E} \leftarrow\!\!\$\, \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ and the probability follow because there will be at least one input-output for which either the input (in case of inverse ideal-cipher query) or the output (in case of forward ideal-cipher query) will be random. We use that randomness to bound the probability of the above event. Now, for a fixed pairs of messages M and M', we define the following set:

$$\mathcal{S} := \{j \in [g] : \Sigma_{J^j}(M) = \Sigma_{J^j}(M')\}.$$

Therefore, we can write

$$\sum_{i=1}^{u} \Pr[\mathsf{E.1}] \quad \leq \quad \sum_{i=1}^{u} \Pr[\mathsf{E.1}, |\mathcal{S}| < \mu] + \Pr[|\mathcal{S}| \geq \mu]. \tag{21}$$

We write the first term of the right hand side of Eqn. (21) as follows:

$$\sum_{i=1}^{u} \Pr[\exists a \neq b \in [q_i] : \Sigma_a^i = \Sigma_b^i, |\mathcal{S}| < \mu, \mathsf{BadK1}_i].$$

For a fixed choice of i, a, b, the probability of the event is upper bounded by 2^{-k} due to the randomness of $K_1^i = J^{j'}$. However, the number of choices of (i, a, b) is at most q^2 and the number of choices of j' is at most μ. Therefore, we have

$$\sum_{i=1}^{u} \Pr[\mathsf{E.1}, |\mathcal{S}| < \mu] \leq \frac{q^2 \mu}{2^k}. \tag{22}$$

Now, it remains to bound the last term of the right hand side of Eqn. (21). Using the similar technique, we have the following:

$$\Pr[|\mathcal{S}| \geq \mu] \leq 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}. \tag{23}$$

By combining Eqn. (21), Eqn. (22) and Eqn. (23), we have

$$\sum_{i=1}^{u} \Pr[\mathsf{E.1}] \leq \frac{q^2 \mu}{2^k} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \leq \frac{q^2 \ell k}{2^n} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}, \tag{24}$$

where the last inequality follows by pugging-in the value of $\mu = 2^{k-n}k\ell$. Now, we upper bound the probability of the event $\mathsf{E.2}$.

B. Bounding Event $\mathsf{E.2}$. The event $\mathsf{E.2}$ implies that the block cipher key K_1^i of the i-th user does not collide with any chosen ideal-cipher keys. As a result, the V values for computing Σ_a^i is not pre-determined. Hence, to upper bound the probability that $\Sigma_a^i = \Sigma_b^i$, we are allowed to use the randomness of V variables, which in turn allows us to apply Lemma 4 to upper bound the probability of $\Sigma_a^i = \Sigma_b^i$, for a fixed choice of i, a, and b. Therefore, for a fixed choice of indices, the probability that $\Sigma_a^i = \Sigma_b^i$ is at most $2/2^n$. Therefore, by varying over all possible choices of indices, we have

$$\sum_{i=1}^{u} \Pr[\mathsf{E.2}] \leq \frac{q^2}{2^n}, \tag{25}$$

as the total number of choices of (i, a, b) is at most $\binom{q}{2}$. Finally, combining Eqn. (24) and Eqn. (25), and putting $\mu = 2^{k-n}k\ell$, we obtain

$$\Pr[\mathsf{Bad3}] \leq \frac{q^2}{2^n} + \frac{q^2 \ell k}{2^n} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}. \tag{26}$$

Finally, by combining Eqn. (3), Eqn. (4), Eqn. (5), Eqn. (8), Eqn. (18), Eqn. (26), and the trivial inequality that

$$\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \leq \left(\frac{6p}{2^k}\right),$$

we obtain the bound of Lemma 5.

4.3 Analysis of Good Transcripts

In this section, we compute a lower bound for the ratio of the real to ideal interpolation probability for a good transcript τ. In particular, we show that for a good transcript $\tau = (\tau_c, \tau_p)$, realizing τ is almost as likely in the real world as in the ideal world.

Lemma 6 (Good Lemma). *Let $\tau = (\tau_c, \tau_p) \in \mathsf{GoodT}$ be a good transcript. Let X_{re} and X_{id} be defined as above. Then*

$$\frac{\Pr[\mathsf{X}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{X}_{\mathrm{id}} = \tau]} \geq 1.$$

Proof. For each $i \in [u]$, we first define the following tuple:

$$\widetilde{\Sigma}^i := (\Sigma^i_1, \Sigma^i_2, \ldots, \Sigma^i_{q_i}).$$

Note that, for each $i \in [u]$, all the elements in the tuple $\widetilde{\Sigma}^i$ are distinct by the virtue of $\overline{\mathsf{Bad3}}$. Moreover, as $\overline{\mathsf{BadK1}}$ holds true, we must have $K^i_2 \neq K^j_2$ and $K^i_1 \neq K^j_1$, for all $i \neq j \in [u]$. Let us assume that out of u distinct keys $(K^1_2, K^2_2, \ldots, K^u_2)$, β many keys have been collided with some chosen ideal-cipher keys, i.e.,

$$\mathcal{K}_{\mathsf{coll}} \overset{\Delta}{=} \{K^i_2 : \exists j \in [g], K^i_2 = J^j\}$$

and $\beta = |\mathcal{K}_{\mathsf{coll}}|$. Then, by the virtue of $\overline{\mathsf{Bad1}}$, for each $i \in [u]$ such that $K^i_2 \in \mathcal{K}_{\mathsf{coll}}$, none of the elements of the tuple $\widetilde{\Sigma}^i$ collides with any elements of $\mathsf{Dom}(\mathsf{E}_{J^j})$, for some $j \in [g]$ such that $K^i_2 = J^j$ holds, i.e., for all $a \in [q_i], \Sigma^i_a \neq X^j_\alpha$ for some $j \in [g]$ such that $K^i_2 = J^j$ and for all $\alpha \in [p_j]$. Similarly, for each $i \in [u]$ such that $K^i_2 \in \mathcal{K}_{\mathsf{coll}}$, by the virtue of $\overline{\mathsf{Bad2}}$, we have $T^i_a \neq Y^j_\alpha$, for all $a \in [q_i]$, for some $j \in [g]$ such that $K^i_2 \in \mathcal{K}_{\mathsf{coll}}$ and for all $\alpha \in [p_j]$. Let $\mathcal{J} = \{(j, i) \in [g] \times [u] : K^i_2 = J^j\}$. Note that, due to $\overline{\mathsf{BadK1}}$, we have $|\mathcal{J}| = |\mathcal{K}_{\mathsf{coll}}| = \beta$. We write $\mathcal{J}_1$ to denote the set of all $j \in [s]$ such that $(j, \star) \in \mathcal{J}$. Let $\sigma^i[\alpha]$ denotes the total number of distinct message blocks at the α-th position across all q_i queries, where $\alpha \in \ell^i$, and ℓ^i denotes the maximum number of message blocks queried across all q_i queries for the i-th user. Let

$$\sigma^i = \sum_{\alpha=1}^{\ell^i} \sigma^i[\alpha].$$

Now, we compute the ideal and real interpolation probability for a good transcript as follows.

<u>Ideal Interpolation Probability:</u> Note that, in the online phase of the game, the ideal world samples the response T^i_a independently and uniformly at random for each query M^i_a. Moreover, in the offline phase, it uniformly and independently samples u pairs of keys and also computes $V^i_a[\alpha]$ for all $i \in [u], a \in [q_i]$ and $\alpha \in [\ell^i_a]$. Therefore, we have

$$\Pr[\mathsf{X}_{\mathrm{id}} = \tau] = \prod_{i=1}^{u} \frac{1}{2^{nq_i}} \cdot \prod_{i=1}^{u} \frac{1}{2^{2k}} \cdot \prod_{j \in [g]} \frac{1}{\mathbf{P}(2^n, p_j)} \cdot \prod_{i=1}^{u} \frac{1}{\mathbf{P}(2^n, \sigma^i)}.$$

<u>Real Interpolation Probability:</u> To compute the real interpolation probability, first of all we count the total number of times the block cipher has been invoked with different keys to compute Σ values. It is easy to see that for the i-th user, total number of block ciphers called to compute $\widetilde{\Sigma}^i$ tuple is σ^i. Moreover, for each $(j, i) \in \mathcal{J}$, the block cipher used in the finalization phase is invoked for a total of $p_j + q_i$ times, and for all those $i \in [u]$ such that $K_2^i \notin \mathcal{K}_{\mathsf{coll}}$, the block cipher in the finalization phase is invoked for a total of q_i times with the user key K_2^i. Besides, as the transcript is good, all K^i keys are distinct. Therefore, we have

$$\begin{aligned}\Pr[\mathsf{X}_{\mathrm{re}} = \tau] \;&=\; \prod_{i=1}^{u} \frac{1}{2^{2k}} \cdot \prod_{(j,i)\in\mathcal{J}} \frac{1}{\mathbf{P}(2^n, p_j + q_i)} \cdot \prod_{j\in[g]\setminus\mathcal{J}_1} \frac{1}{\mathbf{P}(2^n, p_j)} \cdot \prod_{i\in[u]:K_2^i\notin\mathcal{K}_{\mathsf{coll}}} \frac{1}{\mathbf{P}(2^n, q_i)} \\ &\quad \cdot \prod_{i=1}^{u} \frac{1}{\mathbf{P}(2^n, \sigma^i)}.\end{aligned}$$

Note that, by rearranging terms, we have

$$\begin{aligned}\Pr[\mathsf{X}_{\mathrm{re}} = \tau] \;&=\; \prod_{i=1}^{u} \frac{1}{2^{2k}} \cdot \prod_{(j,i)\in\mathcal{J}} \frac{1}{\mathbf{P}(2^n, p_j)} \cdot \prod_{j\in[g]\setminus\mathcal{J}_1} \frac{1}{\mathbf{P}(2^n, p_j)} \\ &\quad \cdot \prod_{(j,i)\in\mathcal{J}} \frac{1}{\mathbf{P}(2^n - p_j, q_i)} \cdot \prod_{i\in[u]:K_2^i\notin\mathcal{K}_{\mathsf{coll}}} \frac{1}{\mathbf{P}(2^n, q_i)} \cdot \prod_{i=1}^{u} \frac{1}{\mathbf{P}(2^n, \sigma^i)} \\ &=\; \prod_{i=1}^{u} \frac{1}{2^{2k}} \cdot \prod_{j\in[g]} \frac{1}{\mathbf{P}(2^n, p_j)} \cdot \prod_{(j,i)\in\mathcal{J}} \frac{1}{\mathbf{P}(2^n - p_j, q_i)} \cdot \prod_{i\in[u]:K_2^i\notin\mathcal{K}_{\mathsf{coll}}} \frac{1}{\mathbf{P}(2^n, q_i)} \\ &\quad \cdot \prod_{i=1}^{u} \frac{1}{\mathbf{P}(2^n, \sigma^i)}.\end{aligned}$$

Now, by taking the ratio of the real to ideal interpolation probability, we have

$$\frac{\Pr[\mathsf{X}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{X}_{\mathrm{id}} = \tau]} = \prod_{i\in[u]:K_2^i\notin\mathcal{K}_{\mathsf{coll}}} \frac{2^{nq_i}}{\mathbf{P}(2^n, q_i)} \cdot \prod_{(j,i)\in\mathcal{J}} \frac{2^{nq_i}}{\mathbf{P}(2^n - p_j, q_i)} \geq 1,$$

which finally proves Lemma 6. Finally, by combining Lemma 5 and Lemma 6 in the H-Coefficient framework, we obtain the desired security bound of LightMAC construction in the multi-user setting.

4.4 Proof of Theorem 5

In the proof of Theorem 4, the term $q^2\ell k/2^n$ carries an ℓ factor. This term appears while bounding subcase E.1 under the bad event Bad3. To obtain an ℓ-free bound, we bound this subcase E.1 under the bad event Bad3 in a different way [2].

Bounding Subcase E.1 Under Bad Event Bad3: We first recall Eqn. (19) as follows:

$$\Pr[\mathsf{Bad3}] \;\leq\; \sum_{i=1}^{u} \Bigg(\Pr[\underbrace{\exists a \neq b \in [q_i] : \Sigma_a^i = \Sigma_b^i, \mathsf{BadK1}_i}_{\mathsf{E.1}}] \Bigg)$$

[2] We would like to note that the term $pq\ell k/2^{n+k}$ also carries an ℓ factor which arises while bounding subcase E.1 under the bad event Bad2. However, this term does not create any problem to achieve an ℓ-free bound if we appropriately set the bound on ℓ. Unfortunately, this is not the case for the term $q^2\ell k/2^n$ and thus, we need a separate treatment with this bound to achieve ℓ-freeness.

$$+ \sum_{i=1}^{u} \left(\Pr[\underbrace{\exists a \neq b \in [q_i] : \Sigma^i_a = \Sigma^i_b, \overline{\mathsf{BadK1}_i}}_{\mathsf{E.2}}] \right).$$

From Eqn. (25), we already have

$$\sum_{i=1}^{u} \Pr[\mathsf{E.2}] \leq \frac{q^2}{2^n}.$$

Therefore, to bound the subcase $\mathsf{E.1}$ under the event $\mathsf{Bad3}$, we consider two cases separately: (a) when $i < \sqrt{q}$ and (b) when $i \geq \sqrt{q}$, i.e., we write

$$\begin{aligned}
\sum_{i=1}^{u} \Pr[\mathsf{E.1}] &= \sum_{i=1}^{\sqrt{q}-1} \Pr[\mathsf{E.1}] + \sum_{i=\sqrt{q}}^{u} \Pr[\mathsf{E.1}] \\
&\leq \sum_{i=1}^{\sqrt{q}-1} \Pr[\exists j \in [g] : K_1^i = J^j] + \sum_{i=\sqrt{q}}^{u} \sum_{a,b=1}^{q_i} \Pr[\exists j \in [g] : \Sigma^i_a = \Sigma^i_b, K_1^i = J^j] \\
&\leq \frac{p\sqrt{q}}{2^k} + \sum_{i=\sqrt{q}}^{u} \sum_{a,b=1}^{q_i} \Pr[\underbrace{\exists j \in [g] : \Sigma^i_a = \Sigma^i_b, K_1^i = J^j}_{\mathsf{E}}], \qquad (27)
\end{aligned}$$

where recall that $\mathsf{BadK1}_i$ denotes the event that there exists an $j' \in [g]$ such that $K_1^i = J^{j'}$. Now, to bound the probability of the event E, we define the a set $\mathcal{S}$ for a fixed pair of messages M, M' as follows:

$$\mathcal{S} := \{j \in [g] : \Sigma_{J^j}(M) = \Sigma_{J^j}(M')\}.$$

Therefore, we can write

$$\sum_{i=\sqrt{q}}^{u} \sum_{a,b=1}^{q_i} \Pr[\mathsf{E}] = \sum_{i=\sqrt{q}}^{u} \sum_{a,b=1}^{q_i} \Pr[\mathsf{E}, |\mathcal{S}| < \mu] + \Pr[|\mathcal{S}| \geq \mu]. \qquad (28)$$

By combining Eqn. (27) and Eqn. (28), we have

$$\begin{aligned}
\sum_{i=1}^{u} \Pr[\mathsf{E.1}] &\leq \frac{p\sqrt{q}}{2^k} + \sum_{i=\sqrt{q}}^{u} \frac{q_i^2 \mu}{2^k} + \Pr[|\mathcal{S}| \geq \mu] \overset{(1)}{\leq} \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}\mu}{2^k} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \\
&\overset{(2)}{\leq} \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}k\ell}{2^n} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}, \qquad (29)
\end{aligned}$$

where inequality (1) follows as the summation q_i^2, for $i \in [\sqrt{q}, u]$, is bounded above by $q^{3/2}$ due to Lemma 2 and we inherit the bound of the probability of the event $|\mathcal{S}| \geq \mu$ from the previous analysis. Moreover, inequality (2) follows by choosing the value of $\mu = 2^{k-n}k\ell$. Therefore, by combining Eqn. (19), Eqn. (25), and Eqn. (29), we have

$$\Pr[\mathsf{Bad3}] \leq \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}k\ell}{2^n} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} + \frac{q^2}{2^n}.$$

By inheriting the bounds of the remaining bad events from the previous analysis, we obtain the probability of bad transcript as follows:

$$\Pr[\mathsf{X}_{\mathrm{id}} \in \mathsf{BadT}] \leq \frac{2q^2}{2^k} + \frac{2q^2}{2^n} + \frac{3qp}{2^{n+k}} + \frac{pq}{2^{3n/4+k}} + \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}}{2^{3n/4}} + \frac{25p}{2^k}. \qquad (30)$$

Finally, by combining Lemma 6 and Eqn. (30), we obtain the desired ℓ-free security bound of $\mathsf{LightMAC}$ construction in the multi-user setting, provided $\ell \leq 2^{n/4}/k$.

Remark 3. We would like to point out that one can get rid of the bound on the maximum message length $\ell \leq 2^{n/4}/k$, if the number of available users is less than $2^{k/4}$. In particular, if the number of available users is less than $2^{k/4}$, then we can trivially bound

$$\sum_{i=1}^{u} \Pr[\mathsf{E.1}] \leq \frac{p}{2^{3k/4}},$$

and obtain the desired ℓ-free bound, provided $\ell \leq 2^{n/2}$. This assumption on the number of users is realistic in most of the practical scenarios when we consider to instantiate LightMAC with block cipher having key size $k = 128$ and the number of queries is restricted upto 2^{32}.

5 Proof of Theorem 6

We consider a computationally unbounded non-trivial deterministic distinguisher A that is given access to u independent instances of the LightMAC_Plus construction, denoted as $(\mathsf{LightMAC\_Plus}[\mathsf{E}]_{(K_1^i,K_2^i,K_3^i)})_{i\in[u]}$ in the real world, where each (K_1^i, K_2^i, K_3^i) is independent of (K_1^j, K_2^j, K_3^j) and $\mathsf{E} \leftarrow\!\!\$\ \mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ is an ideal block cipher. In the ideal world, it has access to a tuple of u independent random functions $(\mathsf{RF}_1, \ldots, \mathsf{RF}_u)$. In both worlds, A is given additional access to the oracle $\mathsf{E}^{\pm}$. In the real world, E is the block cipher underneath the construction LightMAC_Plus and in the ideal world E is uniformly sampled from $\mathsf{BC}(\mathcal{K}, \{0,1\}^n)$ independent of the distribution of the sequence of u independent random functions.

The interaction between the distinguisher and the challenger is summarized in a transcript $\tau_c = \tau_c^1 \cup \tau_c^2 \cup \ldots \cup \tau_c^u$, where $\tau_c^i = \{(M_1^i, T_1^i), \ldots, (M_{q_i}^i, T_{q_i}^i)\}$ and the ideal-cipher queries are summarized in a transcript $\tau_p = \tau_p^1 \cup \tau_p^2 \cup \ldots \cup \tau_p^g$, where $\tau_p^j = \{(u_1^j, v_1^j), \ldots, (u_{p_j}^j, v_{p_j}^j), J^j\}$. As before, A makes q_i construction queries and p_j ideal cipher queries (including forward and inverse queries) with chosen ideal cipher key J^j. Let $q = (q_1 + \ldots + q_u)$ be the total number of construction queries $p = (p_1 + \ldots + p_g)$ be the total number of ideal cipher queries. We modify the experiment by releasing internal information to A after it has finished its interaction but has not yet output the decision bit. In the real world, we reveal all the keys (K_1^i, K_2^i, K_3^i) for all u users and also the $(V_a^i[\alpha])_{i\in[q],a\in[q_i],\alpha\in[\ell_a^i]}$ tuple, where ℓ_a^i is the maximum number of message blocks corresponding the a-th query of the i-th user and $V_a^i[\alpha] = \mathsf{E}_{K_1^i}(\langle\alpha\rangle_s \| M_a^i[\alpha])$. In the ideal world, the challenger sample the keys (K_1^i, K_2^i, K_3^i) uniformly at random from their respective key spaces for all u users and computes the tuple $(V_a^i)_{i\in[q],a\in[q_i]}$ tuple as follows:

$$V_a^i[\alpha] = \mathsf{E}_{K_1^i}(\langle\alpha\rangle_s \| M_a^i[\alpha])$$

and reveal them to the distinguisher. Therefore, each transcript τ_i^c, where $i \in [u]$, is now modified to include the corresponding triplet of keys and the $V_a^i[\alpha]$ values for the i-th instance of the construction. Thus, the modified transcript is

$$\tilde{\tau}_c^i = \{(M_1^i, T_1^i, \widetilde{V}_1^i), \ldots, (M_{q_i}^i, T_{q_i}^i, \widetilde{V}_{q_i}^i), (K_1^i, K_2^i, K_3^i)\},$$

where $\widetilde{V}_a^i := (V_a^i[\alpha])_{\alpha\in[\ell_a^i]}$. In all the following, the complete construction query transcript is $\tau_c = \bigcup_{i=1}^{u} \tilde{\tau}_c^i$ and the overall transcript is $\tau = \tau_c \cup \tau_p$. The modified experiment only makes the distinguisher more powerful and hence the distinguishing advantage of A in this experiment is no less than its distinguishing advantage in the former. Therefore, it follows that for each $i \in [u]$, $\mathsf{LightMAC\_Plus}[\mathsf{E}]_{(K_1^i,K_2^i,K_3^i)} \mapsto \tilde{\tau}_c^i$ denotes the following:

(a) $\Sigma^i_a = \bigoplus_{\alpha=1}^{\ell^i_a} V^i_a[\alpha]$, $a \in [q_i]$

(b) $\Theta^i_a = \bigoplus_{\alpha=1}^{\ell^i_a} 2^{\ell^i_a-\alpha} V^i_a[\alpha]$, $a \in [q_i]$

(b) $\mathsf{E}_{K^i_2}(\Sigma^i_a) \oplus \mathsf{E}_{K^i_3}(\Theta^i_a) = T^i_a$, $a \in [q_i]$.

5.1 Definition and Bounding Probability of Bad Transcripts

In this section, we define and bound the probability of bad transcripts in the ideal world. We denote the input to the α-th ideal-cipher query corresponding to the ideal-cipher key J^j as X^j_α and the corresponding response as Y^j_α. We say that an attainable transcript $\tau = (\tau_c, \tau_p)$ is a **bad** transcript if any one of the following events hold true:

`1. Bad Events Based on Key Collision:`

1. $\mathsf{BadK1}$: $\exists i_1 \neq i_2 \in [u]$ such that $K^{i_1}_1 = K^{i_2}_1, K^{i_1}_2 = K^{i_2}_2$.
2. $\mathsf{BadK2}$: $\exists i_1 \neq i_2 \in [u]$ such that $K^{i_1}_1 = K^{i_2}_1, K^{i_1}_3 = K^{i_2}_3$.
3. $\mathsf{BadK3}$: $\exists i_1 \neq i_2, i_3 \in [u]$ such that $K^{i_1}_2 = K^{i_2}_2, K^{i_1}_3 = K^{i_3}_3$.
4. $\mathsf{BadK4}$: $\exists i_1 \neq i_2 \in [u], j \in [g], j' \in [g], b \in \{2,3\}$ such that $K^{i_1}_b = K^{i_2}_b, K^{i_1}_1 = J^j, K^{i_2}_1 = J^{j'}$.
5. $\mathsf{BadK5}$: $\exists i \in [u], j, j' \in [g]$ such that $K^i_2 = J^j, K^i_3 = J^{j'}$.
6. $\mathsf{BadK6}$: $\exists i \in [u]$ such that $K^i_2 = K^i_3$.
7. $\mathsf{BadK7}$: $\exists i_1 \neq i_2 \in [u], a \in [q_{i_1}], b \in [q_{i_2}], m \in [l^{i_1}_a]$ such that $K^{i_1}_1 = K^{i_2}_2, \langle m \rangle \| M^{i_1}_a[m] = \Sigma^{i_2}_b$.
8. $\mathsf{BadK8}$: $\exists i_1 \neq i_2 \in [u], a \in [q_{i_1}], b \in [q_{i_2}], m \in [l^{i_1}_a]$ such that $K^{i_1}_1 = K^{i_2}_3, \langle m \rangle \| M^{i_1}_a[m] = \Theta^{i_2}_b$.

`2. Bad Events Based on Input and Key Collision:`

1. Bad1 : $\exists i \in [u], a \in [q_i], j \in [g], \alpha \in [p_j]$ such that $K_2^i = J^j, \Sigma_a^i = X_\alpha^j$.
2. Bad2 : $\exists i \in [u], a \in [q_i], j \in [g], \alpha \in [p_j]$ such that $K_3^i = J^j, \Theta_a^i = X_\alpha^j$.
3. Bad3 : $\exists i \in [u], a \neq b \in [q_i], j \in [g]$ such that $\Sigma_a^i = \Sigma_b^i, K_1^i = J^j$.
4. Bad4 : $\exists i \in [u], a \neq b \in [q_i], j \in [g]$ such that $\Theta_a^i = \Theta_b^i, K_1^i = J^j$.
5. Bad5 : $\exists i \in [u], a \neq b \in [q_i]$ such that $\Sigma_a^i = \Sigma_b^i, T_a^i = T_b^i$.
6. Bad6 : $\exists i \in [u], a \neq b \in [q_i]$ such that $\Theta_a^i = \Theta_b^i, T_a^i = T_b^i$.
7. Bad7 : $\exists i_1 \neq i_2 \in [u], a \in [q_{i_1}], b \in [q_{i_2}]$ such that $K_2^{i_1} = K_2^{i_2}, \Sigma_a^{i_1} = \Sigma_b^{i_2}$.
8. Bad8 : $\exists i_1 \neq i_2 \in [u], a \in [q_{i_1}], b \in [q_{i_2}]$ such that $K_2^{i_1} = K_2^{i_2}, \Theta_a^{i_1} = \Theta_b^{i_2}$.
9. Bad9 : $\exists i_1 \neq i_2 \in [u], a \in [q_{i_1}], b \in [q_{i_2}]$ such that $K_3^{i_1} = K_3^{i_2}, \Sigma_a^{i_1} = \Sigma_b^{i_2}$.
10. Bad10 : $\exists i_1 \neq i_2 \in [u], a \in [q_{i_1}], b \in [q_{i_2}]$ such that $K_3^{i_1} = K_3^{i_2}, \Theta_a^{i_1} = \Theta_b^{i_2}$.
11. Bad11 : $\exists i \in [u], a, b \in [q_i]$ such that $\Sigma_a^i = \Sigma_b^i, \Theta_a^i = \Theta_b^i$.
12. Bad12 : $\exists i \in [u], a, b, c \in [q_i]$ such that $\Sigma_a^i = \Sigma_b^i, \Theta_a^i = \Theta_c^i$.
13. Bad13 : $|\{(a,b) : \Sigma_a^i = \Sigma_b^i\}| \geq q_i^{1/2}$.
14. Bad14 : $|\{(a,b) : \Theta_a^i = \Theta_b^i\}| \geq q_i^{1/2}$.

Recall that $\mathsf{BadT} \subseteq \mathcal{V}$ is the set of all attainable bad transcripts and $\mathsf{GoodT} = \mathcal{V} \setminus \mathsf{BadT}$ is the set of all attainable good transcripts. Before we proceed for bounding the above events in the ideal world, we state the following lemma from [37, Lemma 1] that upper bounds the simultaneous collision probability between two Σ values and Θ values. We emphasize that the following results will be frequently used in upper bounding the probability of the above bad events.

Lemma 7 (**Collision of** (Σ, Θ))**.** *For three distinct messages M_a, M_b and M_c, we have*

$$\Pr[\Sigma_a = \Sigma_b, \Theta_a = \Theta_c] \leq \frac{4}{2^{2n}},$$

provided the maximum number of message blocks $\ell \leq 2^{n/2}$. [3]

For the subsequent analysis, we also require to bound the collision probability of Θ, which is formally captured in the following lemma.

Lemma 8 (**Collision of** Θ)**.** *Let M_a and M_b be two distinct messages such that the maximum number of message blocks is ℓ. Then, we have*

$$\Pr[\Theta_a = \Theta_b] \leq \frac{2}{2^n},$$

provided the maximum number of message blocks $\ell \leq 2^{n/2}$.

Proof of the above lemma is similar to that of Lemma 4 and thus can be followed from [31, Proposition 1]. The following lemma upper bounds the probability of realizing a bad transcript in the ideal world.

[3] The bound on the maximum message length in terms of the number of blocks is actually $\min\{2^{n-1}, 2^s\}$. However, as we choose $s = n/2$ for achieving rate 1/2, the bound on ℓ is at most $2^{n/2}$.

Lemma 9 (Bad Lemma). *Let $\tau = (\tau_c, \tau_p)$ be any attainable transcript. Let X_{id} and BadT be defined as above. Then*

$$\begin{aligned}\Pr[\mathsf{X}_{\text{id}} \in \mathsf{BadT}] \quad &\leq \quad \frac{q^2}{2^{2k}} + \frac{q^3}{2^{2k}} + \frac{q^2p^2}{2^{3k}} + \frac{qp^2}{2^{2k}} + \frac{q}{2^k} + \frac{2q^2l}{2^{n+k}} + \frac{4q^2}{2^{2n}} + \frac{4q^2}{2^{n+k}} + \frac{2q^3}{3 \cdot 2^{2n}} \\ &+ \quad \frac{2q^{3/2}}{2^n} + \frac{4qp}{2^{n+k}} + \frac{2pq\ell k}{2^{n+k}} + \frac{48p}{2^k} + \frac{2pq^{1/2}}{2^k} + \frac{2q^{3/2}k\ell}{2^n}.\end{aligned}$$

Proof. Let us define the event

$$\begin{aligned}\mathsf{BadT} \quad := \quad &\underbrace{\left(\vee_{i=1}^{8}\mathsf{BadKi}\right) \vee \left(\vee_{i=1}^{4} \mathsf{Badi} \right)}_{\mathsf{BadK}} \vee \left(\mathsf{Bad5} \mid \overline{\mathsf{Bad3}}\right) \vee \left(\mathsf{Bad6} \mid \overline{\mathsf{Bad4}}\right) \\ &\vee\left(\vee_{i=7}^{10} \mathsf{Badi} \mid \overline{\mathsf{BadK4}}\right) \vee \left(\vee_{i=11}^{12} (\mathsf{Badi} \mid \overline{\mathsf{Bad3}} \wedge \overline{\mathsf{Bad4}})\right) \vee \left(\mathsf{Bad13} \vee \mathsf{Bad14}\right).\end{aligned}$$

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.

I. Bounding $\mathsf{BadK1}, \mathsf{BadK2}$ and $\mathsf{BadK3}$. Recall that the event $\mathsf{BadK1}$ holds if there exists two distinct users i_1 and i_2 such that $K_1^{i_1}$ collides with $K_1^{i_2}$ and $K_2^{i_1}$ collides with $K_2^{i_2}$. In the ideal world, since the block cipher keys of each user are drawn independently and uniformly at random, for a fixed choice of two users i_1 and i_2, the probability that $K_1^{i_1} = K_1^{i_2}, K_2^{i_1} = K_2^{i_2}$ holds, is exactly 2^{-2k}. Therefore, by varying over all possible choices of users, we have

$$\Pr[\mathsf{BadK1}] \leq \frac{\binom{u}{2}}{2^{2k}} \leq \frac{\binom{q}{2}}{2^k} \leq \frac{q^2}{2^{2k+1}}. \tag{31}$$

Since, the events $\mathsf{BadK2}$ and $\mathsf{BadK3}$ are exactly similar to the event $\mathsf{BadK1}$, we bound these two events in a similar way, and hence, we have

$$\Pr[\mathsf{BadK2}] \leq \frac{q^2}{2^{2k+1}}, \ \Pr[\mathsf{BadK3}] \leq \frac{q^3}{2^{2k}}. \tag{32}$$

II. Bounding $\mathsf{BadK4}$. Recall that the event $\mathsf{BadK4}$ holds, if there exists two distinct users i_1 and i_2 such that $K_b^{i_1}$ collides with $K_b^{i_2}$, $K_1^{i_1}$ collides with J^j, and $K_1^{i_2}$ collides with $J^{j'}$ for some $j, j' \in [g]$ and $b \in \{2, 3\}$. In the ideal world, since the block cipher keys of each user are drawn independently and uniformly at random, for a fixed choice of two users i_1 and i_2, and for a fixed $b \in \{2, 3\}$, the probability that $K_b^{i_1} = K_b^{i_2}, K_1^{i_1} = J^j, K_1^{i_2} = J^{j'}$ holds, is exactly 2^{-3k} by using the randomness of $K_1^{i_1}, K_1^{i_2}$, and $K_b^{i_1}$. Therefore, by varying over all possible choices of users and $b \in \{2, 3\}$, we have

$$\Pr[\mathsf{BadK4}] \leq \frac{2\binom{u}{2}g^2}{2^{3k}} \leq \frac{2\binom{q}{2}p^2}{2^{3k}} \leq \frac{q^2p^2}{2^{3k}}. \tag{33}$$

III. Bounding $\mathsf{BadK5}$. Recall that the event $\mathsf{BadK5}$ holds, if there exists an user i such that K_2^i collides with a chosen ideal-cipher key J^j and K_3^i collides with an another chosen ideal-cipher key $J^{j'}$, for some $j, j' \in [g]$. In the ideal world, since the block cipher keys of each user are drawn independently and uniformly at random, for a fixed choice of user i and $j, j' \in [g]$, the probability that $K_2^i = J^j, K_3^i = J^{j'}$ holds, is exactly 2^{-2k} by using the randomness of K_2^i and K_3^i. Therefore, by varying over all possible choices of users $j, j' \in [g]$, we have

$$\Pr[\mathsf{BadK5}] \leq \frac{ug^2}{2^{2k}} \leq \frac{qp^2}{2^{2k}}. \tag{34}$$

IV. Bounding BadK6. Recall that the event BadK6 holds, if there exists an user i such that K_2^i collides with K_3^i. In the ideal world, since the block cipher keys of each user are drawn independently and uniformly at random, for a fixed choice of user i, the probability that $K_2^i = K_3^i$ holds, is exactly 2^{-k} using the randomness of K_2^i. Therefore, by varying over all possible choices of users, we have,

$$\Pr[\mathsf{BadK6}] \leq \frac{u}{2^k} \leq \frac{q}{2^k}. \tag{35}$$

V. Bounding BadK7. Recall that the event BadK7 holds, if there exists two distinct users i_1, i_2 and two construction queries of the users i_1 and i_2 such that $K_1^{i_1}$ collides with $K_2^{i_2}$ and $\langle m \rangle \| M_a^{i_1}[m] = \Sigma_b^{i_2}$. In the ideal world, the block cipher keys of each user are drawn independently and uniformly at random. Therefore, for a fixed choice of a query of users (i_1, a) and (i_2, b) and a fixed choice of $m \in [\ell_a^{i_1}]$ (given that ℓ is the maximum number of message blocks and so $\ell^{i_1} \leq \ell$), the probability that $K_1^{i_1} = K_2^{i_2}, \langle m \rangle \| M_a^{i_1}[m] = \Sigma_b^{i_2}$ holds, is exactly $2^{-(n+k)}$, where the bound on the probability of the event $\langle m \rangle \| M_a^{i_1}[m] = \Sigma_b^{i_2}$ follows from Lemma 4. Therefore, by varying over all possible choices of indices, we have,

$$\Pr[\mathsf{BadK7}] \leq \sum_{i_2=1}^{u} \sum_{b=1}^{q_{i_2}} \sum_{i_1=1}^{u} \sum_{a=1}^{q_{i_1}} \sum_{m=1}^{\ell_a^{i_1}} \frac{1}{2^{n+k}} \leq \frac{u^2\ell}{2^{n+k}} \leq \frac{q^2\ell}{2^{n+k}}. \tag{36}$$

VI. Bounding BadK8. The event BadK8 is similar to the event BadK7. So, we bound the event in a similar way, and we have

$$\Pr[\mathsf{BadK8}] \leq \frac{u^2\ell}{2^{n+k}} \leq \frac{q^2\ell}{2^{n+k}}. \tag{37}$$

VII. Bounding Bad1 and Bad2. Recall that the event Bad1 and Bad2 is identical to the event Bad2 of the LightMAC construction. Therefore, we bound these two events in exactly the same way, and hence, following the analysis of the Bad2 event of the LightMAC construction, we have

$$\begin{aligned}
\Pr[\mathsf{Bad1}] &\leq \frac{2qp}{2^{n+k}} + \frac{pq\ell k}{2^{n+k}} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \qquad (38)\\
\Pr[\mathsf{Bad2}] &\leq \frac{2qp}{2^{n+k}} + \frac{pq\ell k}{2^{n+k}} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}. \qquad (39)
\end{aligned}$$

VIII. Bounding Bad3 and Bad4. To bound the event Bad3, we consider two cases separately: (a) when $i < \sqrt{q}$ and (b) when $i \geq \sqrt{q}$. For the first case, we can easily bound the event by just considering the subevent $K^i = J^j$, which holds with probability $\sqrt{q}p/2^k$. On the other hand, when $i \geq \sqrt{q}$, then we need to consider both $\Sigma_a^i = \Sigma_b^i$ and $K_1^i = J^j$.

$$\begin{aligned}
\Pr[\mathsf{Bad3}] &\leq \sum_{i=1}^{\sqrt{q}-1} \Pr[\exists j \in [g] : K_1^i = J^j] + \sum_{i=\sqrt{q}}^{u} \sum_{a,b=1}^{q_i} \Pr[\exists j \in [g] : \Sigma_a^i = \Sigma_b^i, K_1^i = J^j] \\
&\leq \frac{p\sqrt{q}}{2^k} + \sum_{i=\sqrt{q}}^{u} \sum_{a,b=1}^{q_i} \Pr[\underbrace{\exists j \in [g] : \Sigma_a^i = \Sigma_b^i, K_1^i = J^j}_{\mathsf{E}}]. \qquad (40)
\end{aligned}$$

To bound the probability of the latter event E, we define the set

$$\mathcal{S} \overset{\Delta}{=} \{j \in [g] : \Sigma_{J^j}(M) = \Sigma_{J^j}(M')\}.$$

Therefore, we can write

$$\sum_{i=\sqrt{q}}^{u}\sum_{a,b=1}^{q_i}\Pr[\mathsf{E}] \;=\; \sum_{i=\sqrt{q}}^{u}\sum_{a,b=1}^{q_i}\Pr[\mathsf{E}, |\mathcal{S}| < \mu] + \Pr[|\mathcal{S}| \geq \mu]. \tag{41}$$

By combining Eqn. (40) and Eqn. (41), we have

$$\begin{aligned}\Pr[\mathsf{Bad3}] \;&\leq\; \frac{p\sqrt{q}}{2^k} + \sum_{i=\sqrt{q}}^{u}\frac{q_i^2\mu}{2^k} + \Pr[|\mathcal{S}| \geq \mu] \overset{(1)}{\leq} \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}\mu}{2^k} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \\ &\overset{(2)}{\leq}\; \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}k\ell}{2^n} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}, \end{aligned} \tag{42}$$

where inequality (1) follows as the summation q_i^2, for $i \in [\sqrt{q}, u]$ is bounded above by $q^{3/2}$ due to Lemma 2 and we inherit the bound of the probability of the event $|\mathcal{S}| \geq \mu$ from the previous analysis. Moreover, inequality (2) follows by choosing the value of $\mu = 2^{k-n}k\ell$.

Bounding the event Bad4, is exactly identical to that of Bad3 and hence, we bound the event Bad4 in exactly the same way as we did for Bad3, and hence, following the analysis of the Bad3, we have

$$\Pr[\mathsf{Bad4}] \leq \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}k\ell}{2^n} + 2\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell}. \tag{43}$$

IX. Bounding Bad5 | $\overline{\textbf{Bad3}}$. Recall that the event Bad5 holds, if there exists an user i such that one of its Σ values Σ_a^i collides with an another Σ values Σ_b^i and their corresponding tag collides. Since, we bound the event Bad5 holds conditioned that $\overline{\mathsf{Bad3}}$ holds, it holds that the underlying block cipher key K_1^i has not been collided with any chosen-ideal cipher key and hence, the V values are random. Therefore, by using the randomness of V values, and following Lemma 4, we bound the probability of $\Sigma_a^i = \Sigma_b^i$ to at most $2/2^n$. Moreover, the event $T_a^i = T_b^i$ is independent over $\Sigma_a^i = \Sigma_b^i$, which additionally contributes to the probability a factor 2^{-n}. Hence, by varying over all the possible choices of indices, we have

$$\Pr[\mathsf{Bad5} \mid \overline{\mathsf{Bad3}}] \leq \frac{q^2}{2^{2n}}. \tag{44}$$

X. Bounding Bad6 | $\overline{\textbf{Bad4}}$. Bounding the event Bad6 | $\overline{\mathsf{Bad4}}$, is exactly identical to that of Bad5 | $\overline{\mathsf{Bad3}}$ and hence, following the result of Lemma 8, we have

$$\Pr[\mathsf{Bad6} \mid \overline{\mathsf{Bad4}}] \leq \frac{q^2}{2^{2n}}. \tag{45}$$

XI. Bounding Bad7 | $\overline{\textbf{BadK4}}$. Recall that the event Bad7 holds, if there exists a pair of users i_1, i_2 such that one of the Σ values of i_1 user $\Sigma_a^{i_1}$ collides with an another Σ values of i_2 user $\Sigma_b^{i_2}$ and their corresponding key, i.e., $K_2^{i_1}$ collides with $K_2^{i_2}$. Since, we bound the event Bad7 holds conditioned that $\overline{\mathsf{BadK4}}$ holds, it holds that at least one of the block cipher keys $K_1^{i_1}$ or $K_1^{i_2}$ has not been collided with any chosen-ideal cipher key and hence, the corresponding V values are random. Without loss of generality, we assume that the V values of i_2 user are random. Therefore, by using the randomness of V values of i_2 user, and following Lemma 4, we bound the probability of $\Sigma_a^{i_1} = \Sigma_b^{i_2}$ to at most $2/2^n$. Moreover, the event $K_2^{i_1} = K_2^{i_2}$ is independent over $\Sigma_a^{i_1} = \Sigma_b^{i_2}$, which additionally contributes to the probability a factor 2^{-k}. Hence, by varying over all the possible choices of indices, we have

$$\Pr[\mathsf{Bad7} \mid \overline{\mathsf{BadK4}}] \leq \frac{q^2}{2^{n+k}}. \tag{46}$$

XII. Bounding $\mathsf{Bad8} \mid \overline{\mathsf{BadK4}}$. Bounding the event $\mathsf{Bad8} \mid \overline{\mathsf{BadK4}}$ is exactly identical to that of $\mathsf{Bad7} \mid \overline{\mathsf{BadK4}}$ and hence following the above analysis, we have

$$\Pr[\mathsf{Bad8} \mid \overline{\mathsf{BadK4}}] \leq \frac{q^2}{2^{n+k}}. \tag{47}$$

XIII. Bounding $\mathsf{Bad9} \mid \overline{\mathsf{BadK4}}$. Recall that the event $\mathsf{Bad9}$ holds, if there exists a pair of users i_1, i_2 such that one of the Θ values of i_1 user $\Theta_a^{i_1}$ collides with an another Θ values of i_2 user $\Theta_b^{i_2}$ and their corresponding key, i.e., $K_3^{i_1}$ collides with $K_3^{i_2}$. Since, we bound the event $\mathsf{Bad9}$ holds conditioned that $\overline{\mathsf{BadK4}}$ holds, it holds that at least one of the block cipher keys $K_1^{i_1}$ or $K_1^{i_2}$ has not been collided with any chosen-ideal cipher key and hence, the corresponding V values are random. Without loss of generality, we assume that the V values of i_2 user are random. Therefore, by using the randomness of V values of i_2 user, and following Lemma 8, we bound the probability of $\Theta_a^{i_1} = \Theta_b^{i_2}$ to at most $2/2^n$. Moreover, the event $K_3^{i_1} = K_3^{i_2}$ is independent over $\Theta_a^{i_1} = \Theta_b^{i_2}$, which additionally contributes to the probability a factor 2^{-k}. Hence, by varying over all the possible choices of indices, we have

$$\Pr[\mathsf{Bad9} \mid \overline{\mathsf{BadK4}}] \leq \frac{q^2}{2^{n+k}}. \tag{48}$$

XIV. Bounding $\mathsf{Bad10} \mid \overline{\mathsf{BadK4}}$. Bounding the event $\mathsf{Bad10} \mid \overline{\mathsf{BadK4}}$ is exactly identical to that of $\mathsf{Bad9} \mid \overline{\mathsf{BadK4}}$ and hence following the above analysis, we have

$$\Pr[\mathsf{Bad10} \mid \overline{\mathsf{BadK4}}] \leq \frac{q^2}{2^{n+k}}. \tag{49}$$

XV. Bounding $\mathsf{Bad11} \mid \overline{\mathsf{Bad3}} \wedge \overline{\mathsf{Bad4}}$. Recall that the event $\mathsf{Bad11}$ holds, if there exists an user i such that one of its (Σ, Θ) values (Σ_a^i, Θ_a^i) collides with an another (Σ, Θ) values (Σ_b^i, Θ_b^i). Since, we bound the event $\mathsf{Bad11}$ holds conditioned that $\overline{\mathsf{Bad3}}$ and $\overline{\mathsf{Bad4}}$ hold, it holds that the block cipher key K_1^i has not been collided with any chosen-ideal cipher key and hence, the corresponding V values are random. Therefore, by using the randomness of V values, and following Lemma 7, we bound the probability of $(\Sigma_a^i = \Sigma_b^i) \wedge (\Theta_a^i = \Theta_b^i)$ to at most $4/2^{2n}$. Hence, by varying over all the possible choices of indices, we have

$$\Pr[\mathsf{Bad11} \mid \overline{\mathsf{Bad3}} \wedge \overline{\mathsf{Bad4}}] \leq \frac{2q^2}{2^{2n}}. \tag{50}$$

XVI. Bounding $\mathsf{Bad12} \mid \overline{\mathsf{Bad3}} \wedge \overline{\mathsf{Bad4}}$. Recall that the event $\mathsf{Bad12}$ holds, if there exists an user i such that $\Sigma_a^i = \Sigma_b^i$ and $\Theta_a^i = \Theta_c^i$ hold, where $a, b, c \in [q_i]$. Since, we bound the event $\mathsf{Bad12}$ holds conditioned that $\overline{\mathsf{Bad3}}$ and $\overline{\mathsf{Bad4}}$ hold, it holds that the block cipher key K_1^i has not been collided with any chosen-ideal cipher key and hence, the corresponding V values are random. Therefore, by using the randomness of V values, and following Lemma 7, we bound the probability of $(\Sigma_a^i = \Sigma_b^i) \wedge (\Theta_a^i = \Theta_c^i)$ to at most $4/2^{2n}$. Hence, by varying over all the possible choices of indices, we have

$$\Pr[\mathsf{Bad12} \mid \overline{\mathsf{Bad3}} \wedge \overline{\mathsf{Bad4}}] \leq \frac{2q^3}{3 \cdot 2^{2n}}. \tag{51}$$

XVII. Bounding $\mathsf{Bad13}$ and $\mathsf{Bad14}$: For a fixed choice of indices, we define an indicator random variable $\mathbb{I}_{a,b}^i$ which takes the value 1, if $\Sigma_a^i = \Sigma_b^i$, and 0, otherwise. Let $\mathbb{I}^i = \sum_{a \neq b} \mathbb{I}_{a,b}^i$. By linearity of expectation,

$$\mathbf{E}[\mathbb{I}^i] = \sum_{a \neq b} \mathbf{E}[\mathbb{I}_{a,b}^i] = \sum_{a \neq b} \Pr[\Sigma_a^i = \Sigma_b^i] \overset{(1)}{\leq} \frac{q_i^2}{2^n},$$

where (1) holds from Lemma 4. Now,

$$\begin{aligned}\Pr[\mathsf{Bad13}] &\le \sum_{i\in[u]} \Pr[|\{(a,b)\in[q_i]^2 : \Sigma^i_a = \Sigma^i_b\}| \ge q_i^{1/2}] \\ &= \sum_{i=1}^{u} \Pr[\mathbb{I}^i \ge q_i^{1/2}] \overset{(2)}{\le} \sum_{i=1}^{u} \frac{q_i^2}{q_i^{1/2} 2^n} \le \frac{q^{3/2}}{2^n}, \qquad (52)\end{aligned}$$

where (2) holds due to the Markov inequality. Similar to $\mathsf{Bad13}$, we bound $\mathsf{Bad14}$ as follows:

$$\Pr[\mathsf{Bad14}] \le \frac{q^{3/2}}{2^n}, \qquad (53)$$

where the inequality follows from the result of Lemma 8. Finally, by combining Eqn. (31)-Eqn. (53), and the trivial inequality that

$$\left(\frac{6p}{2^k}\right)^{2^{k-n}k\ell} \le \frac{6p}{2^k},$$

we obtain the bound of Lemma 9.

5.2 Analysis of Good Transcripts

In this section, we compute a lower bound for the ratio of the real to ideal interpolation probability for a good transcript τ. Let us define the following sets for each $b \in \{2, 3\}$.

$$\mathcal{I}_b^{=} \overset{\Delta}{=} \{i \in [u] : \exists j \in [g], K_b^i = J^j\}.$$

We define an equivalence relation $\sim_b$ for $b \in \{2,3\}$, over $\mathcal{I}_b^{=}$ as follows: $i_1 \sim_b i_2$ if and only if $K_b^{i_1} = K_b^{i_2}$. As a result, $\sim_b$ induces a partition over the set $\mathcal{I}_b^{=}$ as follows:

$$\mathcal{I}_b^{=} = \mathcal{I}_b^{=}[1] \sqcup \ldots \sqcup \mathcal{I}_b^{=}[r_b].$$

In other words, $\mathcal{I}_b^{=}[j]$ is the set of all users i such that $K_b^i = J^j$. It is easy to see that due to $\overline{\mathsf{BadK5}}$, $\mathcal{I}_2^{=} \cap \mathcal{I}_3^{=} = \emptyset$. We define a set $\mathcal{U}^{=}$ as follows:

$$\mathcal{U}^{=} := \{i \in [u] : i \in \mathcal{I}_2^{=} \cup \mathcal{I}_3^{=}\}.$$

For each $j \in [r_b]$ and for each $i \in \mathcal{I}_b^{=}[j]$, we consider the sequences

$$\widetilde{\Sigma}^i := (\Sigma^i_1, \Sigma^i_2, \ldots, \Sigma^i_{q_i}), \widetilde{\Theta}^i := (\Theta^i_1, \Theta^i_2, \ldots, \Theta^i_{q_i}).$$

From these sequences, we construct a bipartite graph G_i^b, where the nodes in one partition represent Σ^i_a values and the nodes in the other represent Θ^i_a values, for $i \in \mathcal{I}_b^{=}$. We put an edge between the node corresponding to Σ^i_a and Θ^i_a with the label T^i_a if $\Sigma^i_a \oplus \Theta^i_a = T^i_a$ holds. For $i \in \mathcal{I}_b^{=}$, if $\Sigma^i_a = \Sigma^i_b$ or $\Theta^i_a = \Theta^i_b$, then we merge the corresponding nodes into a single node.

Note that, for each $i \in \mathcal{I}_b^{=}[j]$, if $\Sigma^i_a = \Sigma^i_b$ (resp. $\Theta^i_a = \Theta^i_b$), then all the elements in the tuple $\widetilde{\Theta}^i$ (resp. $\widetilde{\Sigma}^i$) are distinct (due to $\overline{\mathsf{Bad11}} \wedge \overline{\mathsf{Bad12}}$). Moreover, by the virtue of $\overline{\mathsf{Bad7}} \wedge \overline{\mathsf{Bad8}}$, we have $\widetilde{\Sigma}^{i_1} \cap \widetilde{\Sigma}^{i_2} = \emptyset$ and $\widetilde{\Theta}^{i_1} \cap \widetilde{\Theta}^{i_2} = \emptyset$ for $i_1, i_2 \in \mathcal{I}_2^{=}[j]$. In a similar way, by the virtue of $\overline{\mathsf{Bad9}} \wedge \overline{\mathsf{Bad10}}$, we have $\widetilde{\Sigma}^{i_1} \cap \widetilde{\Sigma}^{i_2} = \emptyset$ and $\widetilde{\Theta}^{i_1} \cap \widetilde{\Theta}^{i_2} = \emptyset$ for $i_1, i_2 \in \mathcal{I}_3^{=}[j]$.

As the transcript is good, it is easy to see that each component is acyclic and a star-graph. Due to $\overline{\mathsf{Bad13}} \wedge \overline{\mathsf{Bad14}}$, the component size is restricted up to $q^{1/2}$. Moreover, due to $\overline{\mathsf{Bad1}} \wedge \overline{\mathsf{Bad2}}$, each vertex of the graph, i.e., Σ^i_a or Θ^i_a does not collide with the input

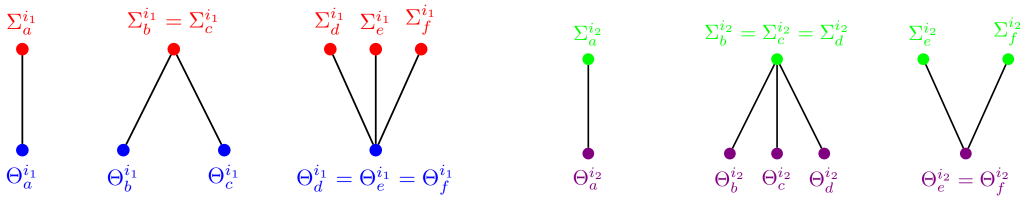

Figure 4: Distinct tuples for users i_1 and i_2 in $\mathcal{I}_b^{=}[j]$: Elements within $\widetilde{\Sigma}^{i_1}$ differ from those in $\widetilde{\Sigma}^{i_2}$, and likewise, elements within $\widetilde{\Theta}^{i_1}$ from $\widetilde{\Theta}^{i_2}$, due to conditions $\overline{\textsf{Bad7}}$ through $\overline{\textsf{Bad10}}$.

of any ideal-cipher query such that the ideal-cipher key collides with the i-th user key. Hence, each vertices of the graph G_i^b do not collide with the input of any ideal-cipher query. Note that, $\overline{\textsf{Bad5}}$ (resp. $\overline{\textsf{Bad6}}$) ensures the fact that if Σ_a^i collides with Σ_b^i (resp. Θ_a^i collides with Θ_b^i), then T_a^i must be distinct from T_b^i. On the other hand, $\overline{\textsf{Bad7-Bad10}}$ implies that there should not be any intersection between the equation variables corresponding to two different users whose keys have been collided.

We define the following set $\mathcal{U}^{\neq} := \{i \in [u] : i \notin \mathcal{U}^{=}\}$. Now, for any one of $b \in \{2, 3\}$, we define the equivalence relation $\sim$ over the set $\mathcal{U}^{\neq}$ as follows:

$$i \sim j \text{ if and only if } K_2^i = K_2^j \text{ or } K_3^i = K_3^j.$$

This equivalence relation induces a partition on the set $\mathcal{U}^{\neq}$. Therefore, we have

$$\mathcal{U}^{\neq} = (\mathcal{I}^{\neq}[1] \sqcup \ldots \sqcup \mathcal{I}^{\neq}[r']).$$

As before, for each $j \in [r']$, and for each $i \in \mathcal{I}^{\neq}[j]$, consider the sequences

$$\widetilde{\Sigma}^i := (\Sigma_1^i, \Sigma_2^i, \ldots, \Sigma_{q_i}^i), \widetilde{\Theta}^i := (\Theta_1^i, \Theta_2^i, \ldots, \Theta_{q_i}^i).$$

For each $i \in \mathcal{I}^{\neq}$, we construct a bipartite graph H_i, one of whose partitions represents the nodes corresponding to Σ_a^i values and the other one represents the nodes corresponding to Θ_a^i values. We put an edge between the node corresponding to Σ_a^i and Θ_a^i with the label T_a^i, if $\Sigma_a^i \oplus \Theta_a^i = T_a^i$ holds. However, if two nodes represent the same values, then we merge them into a single node. Note that, due to $\overline{\textsf{Bad7}}$- $\overline{\textsf{Bad10}}$, we have $\widetilde{\Sigma}^{i_1} \cap \widetilde{\Sigma}^{i_2} = \emptyset$ and $\widetilde{\Theta}^{i_1} \cap \widetilde{\Theta}^{i_2} = \emptyset$ for $i_1, i_2 \in \mathcal{I}^{\neq}[j]$. Let $\sigma^i[\alpha]$ denotes the total number of distinct message blocks at the α-th position across all q_i queries, where $\alpha \in [\ell^i]$, and ℓ^i denotes the maximum number of message blocks queried across all q_i queries for the i-th user. Let

$$\sigma^i = \sum_{\alpha=1}^{\ell^i} \sigma^i[\alpha].$$

Now, for a good transcript $\tau = (\tau_c, \tau_p)$, we show that realizing τ is almost as likely in the real world as in the ideal world. For calculating the ideal interpolation probability, each response to the construction query is sampled uniformly and independently. After the interaction is over, the ideal world samples three k-bit dummy keys uniformly and independently from $\{0, 1\}^k$. Therefore, we have

$$\Pr[\mathsf{X}_{\text{id}} = \tau] = \prod_{i=1}^{u} \frac{1}{2^{3k}} \cdot \prod_{j \in [g]} \frac{1}{\mathbf{P}(2^n, p_j)} \cdot \prod_{i=1}^{u} \frac{1}{2^{nq_i}} \cdot \prod_{i=1}^{u} \frac{1}{\mathbf{P}(2^n, \sigma^i)}. \tag{54}$$

For calculating the real interpolation probability, for each $j \in [r_2]$, let there are $\gamma_{2,j}$ be many vertices corresponding to all $\widetilde{\Sigma}^i$ values and $\delta_{2,j}$ be many vertices corresponding to all $\widetilde{\Theta}^i$ values in the graph $\cup_{i\in\mathcal{I}_2^{=}[j]}G_i^2$ for all $i\in\mathcal{I}_2^{=}[j]$. Similarly, for each $j\in[r_3]$, let there are $\gamma_{3,j}$ be many vertices corresponding to all $\widetilde{\Sigma}^i$ values and $\delta_{3,j}$ be many vertices corresponding to all $\widetilde{\Theta}^i$ values in the graph $\cup_{i\in\mathcal{I}_3^{=}[j]}G_i^3$ for all $i\in\mathcal{I}_3^{=}[j]$. Subsequently, for each $j\in[r']$, let there are η_j be many vertices corresponding to all $\widetilde{\Sigma}^i$ values and ξ_j be many vertices corresponding to all $\widetilde{\Theta}^i$ values in the graph $\cup_{i\in\mathcal{I}^{\neq}[j]}H_i$ for all $i\in\mathcal{I}^{\neq}[j]$. Thus, the real interpolation probability becomes

$$\begin{aligned}\Pr[\mathsf{X}_{\mathrm{re}}=\tau] &= \prod_{i=1}^{u}\frac{1}{2^{3k}}\cdot\prod_{j=1}^{g}\frac{1}{\mathbf{P}(2^n,p_j)}\cdot\prod_{i=1}^{u}\frac{1}{\mathbf{P}(2^n,\sigma^i)}\cdot\left(\prod_{j=1}^{r_2}\frac{h(\cup_{i\in\mathcal{I}_2^{=}[j]}G_i^2)}{\mathbf{P}(2^n-p_j,\gamma_{2,j})\cdot\mathbf{P}(2^n,\delta_{2,j})}\right)\\ &\cdot\left(\prod_{j=1}^{r_3}\frac{h(\cup_{i\in\mathcal{I}_3^{=}[j]}G_i^3)}{\mathbf{P}(2^n,\gamma_{3,j})\cdot\mathbf{P}(2^n-p_j,\delta_{3,j})}\right)\cdot\left(\prod_{j=1}^{r'}\frac{h(\cup_{i\in\mathcal{I}^{\neq}[j]}H_i)}{\mathbf{P}(2^n,\eta_j)\cdot\mathbf{P}(2^n,\xi_j)}\right)\end{aligned}\tag{55}$$

where $h(\cup_{i\in\mathcal{I}_b^{=}[j]}G_i^b)$ denotes the number of solutions to the graph $\cup_{i\in\mathcal{I}_b^{=}[j]}G_i^b$. Similarly, $h(\cup_{i\in\mathcal{I}^{\neq}[j]}H_i)$ denotes the number of solutions to the graph $\cup_{i\in\mathcal{I}^{\neq}[j]}H_i$. Due to the several bad conditions defined in Sect. 5.1, it is easy to see that both the graphs G_i^b for $i\in\mathcal{I}_b^{=}[j]$ and H_i for $i\in\mathcal{I}^{\neq}[j]$ are good.

For a fixed $j\in[r_b]$, let $\alpha_{b,j}$ denotes the number of components of the graph $\cup_{i\in\mathcal{I}_b^{=}[j]}G_i^b$. Let $c_{k,b,j}$ (resp. $d_{k,b,j}$) denotes the number of vertices corresponding to the Σ (resp. Θ) values in the k-th component of the graph $\cup_{i\in\mathcal{I}_b^{=}[j]}G_i^b$, where $k\in[\alpha_{b,j}]$. Therefore, we have

$$\gamma_{b,j}=\sum_{k=1}^{\alpha_{b,j}}c_{k,b,j},\ \delta_{b,j}=\sum_{k=1}^{\alpha_{b,j}}d_{k,b,j}.$$

Moreover, following the notations of Sect. 2.4, we write

$$\rho_{m,b,j}[1]=\sum_{k=1}^{m}c_{k,b,j},\ \rho_{m,b,j}[2]=\sum_{k=1}^{m}d_{k,b,j},$$

where $m\in[\alpha_{b,j}]$. Therefore, by applying Lemma 3, we have the following bound of $h(\cup_{i\in\mathcal{I}_b^{=}[j]}G_i^b)$ for a fixed j and $b\in\{2,3\}$:

$$\begin{aligned}h(\cup_{i\in\mathcal{I}_2^{=}[j]}G_i^2) &\geq \frac{\mathbf{P}(2^n-p_j,\gamma_{2,j})\cdot\mathbf{P}(2^n,\delta_{2,j})}{2^{n\sum\limits_{i\in\mathcal{I}_2^{=}[j]}q_i}}\left(1-\frac{1}{2^{2n}}\cdot\left(\sum_{k=1}^{\alpha_{2,j}}10\left(\binom{c_{k,2,j}+d_{k,2,j}}{2}\right.\right.\right.\\ &\qquad\left.\left.\left.\left(p_j+\rho_{k-1,2,j}[1]+\rho_{k-1,2,j}[2]\right)^2\right)\right)\right),\\ &\overset{(1)}{\geq}\frac{\mathbf{P}(2^n-p_j,\gamma_{2,j})\cdot\mathbf{P}(2^n,\delta_{2,j})}{2^{n\sum\limits_{i\in\mathcal{I}_2^{=}[j]}q_i}}\left(1-\frac{1}{2^{2n}}\cdot\left(\sum_{k=1}^{\alpha_{2,j}}10\left(\binom{c_{k,2,j}+d_{k,2,j}}{2}\left(p_j+4q_{2,j}\right)^2\right)\right)\right),\\ h(\cup_{i\in\mathcal{I}_3^{=}[j]}G_i^3) &\geq \frac{\mathbf{P}(2^n,\gamma_{3,j})\cdot\mathbf{P}(2^n-p_j,\delta_{3,j})}{2^{n\sum\limits_{i\in\mathcal{I}_3^{=}[j]}q_i}}\left(1-\frac{1}{2^{2n}}\cdot\left(\sum_{k=1}^{\alpha_{3,j}}10\left(\binom{c_{k,3,j}+d_{k,3,j}}{2}\right.\right.\right.\\ &\qquad\left.\left.\left.\left(p_j+\rho_{k-1,3,j}[1]+\rho_{k-1,3,j}[2]\right)^2\right)\right)\right),\\ &\overset{(2)}{\geq}\frac{\mathbf{P}(2^n,\gamma_{3,j})\cdot\mathbf{P}(2^n-p_j,\delta_{3,j})}{2^{n\sum\limits_{i\in\mathcal{I}_3^{=}[j]}q_i}}\left(1-\frac{1}{2^{2n}}\cdot\left(\sum_{k=1}^{\alpha_{3,j}}10\left(\binom{c_{k,3,j}+d_{k,3,j}}{2}\left(p_j+4q_{3,j}\right)^2\right)\right)\right),\end{aligned}$$

where (1) and (2) follows due to the fact that $\rho_{k-1,b,j}[1] \leq 2q_{b,j}$ and $\rho_{k-1,b,j}[2] \leq 2q_{b,j}$ for $b \in \{2,3\}$. Moreover, we have

$$q_{2,j} := \sum_{i \in \mathcal{I}_2^{=}[j]} q_i, \; q_{3,j} := \sum_{i \in \mathcal{I}_3^{=}[j]} q_i.$$

For a fixed $j \in [r']$, let β_j denotes the number of components of the graph $\cup_{i \in \mathcal{I}^{\neq}[j]} H_i$. Let $c'_{k,j}$ (resp. $d'_{k,j}$) denotes the number of vertices corresponding to the Σ (resp. Θ) values in the k-th component of the graph $\cup_{i \in \mathcal{I}^{\neq}[j]} H_i$, where $k \in [\beta_j]$. Therefore, we have

$$\eta_j = \sum_{k=1}^{\beta_j} c'_{k,j}, \; \xi_j = \sum_{k=1}^{\beta_j} d'_{k,j}.$$

Moreover, following the notations of Sect. 2.4, we write

$$\rho'_{m,j}[1] = \sum_{k=1}^{m} c'_{k,j}, \; \rho'_{m,j}[2] = \sum_{k=1}^{m} d'_{k,j},$$

where $m \in [\beta_j]$. Finally, for a fixed j, we have

$$\begin{aligned} h(\cup_{i \in \mathcal{I}^{\neq}[j]} H_i) \quad &\geq \quad \frac{\mathbf{P}(2^n, \eta_j) \cdot \mathbf{P}(2^n, \xi_j)}{2^{n \sum_{i \in \mathcal{I}^{\neq}[j]} q_i}} \Bigg(1 - \frac{1}{2^{2n}} \cdot \Bigg(\sum_{k=1}^{\beta_j} 10 \Bigg(\binom{c'_{k,j} + d'_{k,j}}{2} \\ &\qquad \Big(\rho'_{k-1,j}[1] + \rho'_{k-1,j}[2]\Big)^2\Bigg)\Bigg)\Bigg) \\ &\overset{(3)}{\geq} \quad \frac{\mathbf{P}(2^n, \eta_j) \cdot \mathbf{P}(2^n, \xi_j)}{2^{n \sum_{i \in \mathcal{I}^{\neq}[j]} q_i}} \Bigg(1 - \frac{1}{2^{2n}} \cdot \Bigg(\sum_{k=1}^{\beta_j} 160 q_j'^2 \Bigg(\binom{c'_{k,j} + d'_{k,j}}{2}\Bigg)\Bigg)\Bigg), \end{aligned}$$

where (3) follows due to the fact that $\rho'_{k-1,j}[1] \leq 2q_j$ and $\rho'_{k-1,j}[2] \leq 2q_j$. Moreover, we have

$$q'_j := \sum_{i \in \mathcal{I}^{\neq}[j]} q_i.$$

By plugging-in the inequality (1), (2), and (3) into Eqn. (55) and then by taking the ratio of real to ideal interpolation probability, we obtain

$$\begin{aligned} \frac{\Pr[\mathsf{X}_{\text{re}} = \tau]}{\Pr[\mathsf{X}_{\text{id}} = \tau]} \quad &\geq \quad \prod_{i=1}^{u} 2^{nq_i} \cdot \prod_{j=1}^{r_2} \frac{1}{2^{n \sum_{i \in \mathcal{I}_2^{=}[j]} q_i}} \Bigg(1 - \frac{1}{2^{2n}} \cdot \Bigg(\sum_{k=1}^{\alpha_{2,j}} 10 \Bigg(\binom{c_{k,2,j} + d_{k,2,j}}{2} \Big(p_j + 4q_{2,j}\Big)^2\Bigg)\Bigg)\Bigg) \\ &\cdot \quad \prod_{j=1}^{r_3} \frac{1}{2^{n \sum_{i \in \mathcal{I}_3^{=}[j]} q_i}} \Bigg(1 - \frac{1}{2^{2n}} \cdot \Bigg(\sum_{k=1}^{\alpha_{3,j}} 10 \Bigg(\binom{c_{k,3,j} + d_{k,3,j}}{2} + \Big(p_j + 4q_{3,j}\Big)^2\Bigg)\Bigg)\Bigg) \\ &\cdot \quad \prod_{j \in r'} \frac{1}{2^{n \sum_{i \in \mathcal{I}^{\neq}[j]} q_i}} \Bigg(1 - \frac{1}{2^{2n}} \cdot \Bigg(\sum_{k=1}^{\beta_j} 160 q_j'^2 \Bigg(\binom{c'_{k,j} + d'_{k,j}}{2}\Bigg)\Bigg)\Bigg) \\ &\geq \quad \Bigg(\prod_{j=1}^{r_2} \frac{2^{n \sum_{i \in \mathcal{I}_2^{=}[j]} q_i}}{2^{n \sum_{i \in \mathcal{I}_2^{=}[j]} q_i}}\Bigg) \cdot \Bigg(\prod_{j=1}^{r_3} \frac{2^{n \sum_{i \in \mathcal{I}_3^{=}[j]} q_i}}{2^{n \sum_{i \in \mathcal{I}_3^{=}[j]} q_i}}\Bigg) \cdot \Bigg(\prod_{j \in r'} \frac{2^{n \sum_{i \in \mathcal{I}^{\neq}[j]} q_i}}{2^{n \sum_{i \in \mathcal{I}^{\neq}[j]} q_i}}\Bigg) \\ &\cdot \quad \Bigg(1 - \sum_{j=1}^{r_2} \frac{1}{2^{2n}} \cdot \Bigg(\sum_{k=1}^{\alpha_{2,j}} 10 \Bigg(\binom{c_{k,2,j} + d_{k,2,j}}{2} \Big(p_j + 4q_{2,j}\Big)^2\Bigg)\Bigg)\Bigg) \end{aligned}$$

$$\begin{aligned}
&\cdot \quad \Bigg(1-\sum_{j=1}^{r_3}\frac{1}{2^{2n}}\cdot\Bigg(\sum_{k=1}^{\alpha_{3,j}}10\Bigg(\binom{c_{k,3,j}+d_{k,3,j}}{2}\Big(p_j+4q_{3,j}\Big)^2\Bigg)\Bigg)\Bigg)\\
&\cdot \quad \Bigg(1-\sum_{j=1}^{r'}\frac{1}{2^{2n}}\cdot\Bigg(\sum_{k=1}^{\beta_j}160q_j'^2\Bigg(\binom{c'_{k,j}+d'_{k,j}}{2}\Bigg)\Bigg)\Bigg). \qquad (56)
\end{aligned}$$

Let,

$$\begin{aligned}
\Phi_{2,j}(\tau) &:= \frac{1}{2^{2n}}\cdot\Bigg(\sum_{k=1}^{\alpha_{2,j}}10\Bigg(\binom{c_{k,2,j}+d_{k,2,j}}{2}\Big(p_j+4q_{2,j}\Big)^2\Bigg)\Bigg)\\
\Phi_{3,j}(\tau) &:= \frac{1}{2^{2n}}\cdot\Bigg(\sum_{k=1}^{\alpha_{3,j}}10\Bigg(\binom{c_{k,3,j}+d_{k,3,j}}{2}\Big(p_j+4q_{3,j}\Big)^2\Bigg)\Bigg)\\
\Phi'_j(\tau) &:= \frac{1}{2^{2n}}\cdot\Bigg(\sum_{k=1}^{\beta_j}160q_j'^2\Bigg(\binom{c'_{k,j}+d'_{k,j}}{2}\Bigg)\Bigg)
\end{aligned}$$

Therefore, we have

$$\frac{\Pr[\mathsf{X}_{\mathrm{re}}=\tau]}{\Pr[\mathsf{X}_{\mathrm{id}}=\tau]} \geq 1-\Bigg(\sum_{j=1}^{r_2}\Phi_{2,j}(\tau)+\sum_{j=1}^{r_3}\Phi_{3,j}(\tau)+\sum_{j=1}^{r'}\Phi'_j(\tau)\Bigg). \qquad (57)$$

<u>COMPUTING EXPECTATION.</u>

$$\begin{aligned}
\mathbf{E}[\Phi_{2,j}(\mathsf{X}_{\mathrm{id}})] &\overset{(4)}{=} \frac{1}{2^{2n}}\cdot\Bigg(10(p_j+4q_{2,j})^2\mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{2,j}}\binom{c_{k,2,j}+d_{k,2,j}}{2}\Bigg]\Bigg)\\
\mathbf{E}[\Phi_{3,j}(\mathsf{X}_{\mathrm{id}})] &\overset{(5)}{=} \frac{1}{2^{2n}}\cdot\Bigg(10(p_j+4q_{3,j})^2\mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{3,j}}\binom{c_{k,3,j}+d_{k,3,j}}{2}\Bigg]\Bigg)\\
\mathbf{E}[\Phi'_j(\mathsf{X}_{\mathrm{id}})] &\overset{(6)}{=} \frac{1}{2^{2n}}\cdot\Bigg(160q_j'^2\Bigg(\mathbf{E}\Bigg[\sum_{k=1}^{\beta_j}\binom{c'_{k,j}+d'_{k,j}}{2}\Bigg]\Bigg)\Bigg)
\end{aligned}$$

We first compute the right-hand side of (4). Let $\tilde{c}_{k,2,j} := c_{k,2,j}-1$ and $\tilde{d}_{k,2,j} := d_{k,2,j}-1$. Therefore, we have

$$\begin{aligned}
\mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{2,j}}\binom{c_{k,2,j}+d_{k,2,j}}{2}\Bigg] &= \mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{2,j}}\binom{\tilde{c}_{k,2,j}+\tilde{d}_{k,2,j}}{2}\Bigg]+2\mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{2,j}}(\tilde{c}_{k,2,j}+\tilde{d}_{k,2,j})\Bigg]\\
&\overset{(7)}{\leq} \mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{2,j}}\binom{\tilde{c}_{k,2,j}+\tilde{d}_{k,2,j}}{2}\Bigg]+8q_{2,j}. \qquad (58)
\end{aligned}$$

where the inequality (7) holds as $\tilde{c}_{k,2,j} \leq 2q_{2,j}$ and $\tilde{d}_{k,2,j} \leq 2q_{2,j}$. Let us define an indicator random variable $\mathbb{I}_{k,2,j}[ab]$ which takes the value 1 if $\Sigma_a^{i_1} = \Sigma_b^{i_2}$ or $\Theta_a^{i_1} = \Theta_b^{i_2}$, where $i_1, i_2 \in \mathcal{I}_2^{=}[j]$. Therefore, we have

$$\begin{aligned}
\mathbf{E}\Bigg[\sum_{k=1}^{\alpha_{2,j}}\binom{\tilde{c}_{k,2,j}+\tilde{d}_{k,2,j}}{2}\Bigg] &= \sum_{i\in\mathcal{I}_2^{=}[j]}\sum_{a\neq b}^{q_i}\mathbf{E}\Big[\mathbb{I}_{k,2,j}[ab]=1\Big]\\
&= \sum_{i\in\mathcal{I}_2^{=}[j]}\sum_{a\neq b}^{q_i}(\Pr[\Sigma_a^i=\Sigma_b^i]+\Pr[\Theta_a^i=\Theta_b^i])
\end{aligned}$$

$$\overset{(8)}{\leq} \quad \sum_{i \in \mathcal{I}_2^{=}[j]} 2q_i^2/2^n \leq 2q_{2,j}^2/2^n, \tag{59}$$

where (8) follows from Lemma 4 and Lemma 8. By plugging-in the bound of Eqn. (59) into Eqn. (58), we have

$$\mathbf{E}\left[\sum_{k=1}^{\alpha_{2,j}} \binom{c_{k,2,j} + d_{k,2,j}}{2}\right] \quad \leq \quad 2q_{2,j}^2/2^n + 8q_{2,j}, \tag{60}$$

In a similar way, we have

$$\mathbf{E}\left[\sum_{k=1}^{\alpha_{3,j}} \binom{c_{k,3,j} + d_{k,3,j}}{2}\right] \quad \leq \quad 2q_{3,j}^2/2^n + 8q_{3,j} \tag{61}$$

$$\mathbf{E}\left[\sum_{k=1}^{\beta_j} \binom{c'_{k,j} + d'_{k,j}}{2}\right] \quad \leq \quad 2q_j'^2/2^n + 8q'_j. \tag{62}$$

By plugging-in the bound of Eqn. (60), Eqn. (61), and Eqn. (62) into the right-hand side of Eqn. (4), Eqn. (5), and Eqn. (6) respectively, we have

$$\mathbf{E}[\Phi_{2,j}(\mathsf{X}_{\mathrm{id}})] \quad \leq \quad \frac{1}{2^{2n}} \cdot \Big(10(p_j + 4q_{2,j})^2 (2q_{2,j}^2/2^n + 8q_{2,j})\Big) \tag{63}$$

$$\mathbf{E}[\Phi_{3,j}(\mathsf{X}_{\mathrm{id}})] \quad \leq \quad \frac{1}{2^{2n}} \cdot \Big(10(p_j + 4q_{3,j})^2 (2q_{3,j}^2/2^n + 8q_{3,j})\Big) \tag{64}$$

$$\mathbf{E}[\Phi'_j(\mathsf{X}_{\mathrm{id}})] \quad \leq \quad 320q_j'^4/2^{3n} + 1280q_j'^3/2^{2n}. \tag{65}$$

By doing a simple algebra on Eqn. (63)-Eqn. (65) and by using Lemma 9 and equality

$$\sum_{j \in [r_2]} q_{2,j} + \sum_{j \in [r_3]} q_{3,j} + \sum_{j \in [r'} q'_j = q \text{ and } \sum_{j=1}^{g} p_j = p,$$

we derive the result.

5.3 Proof of Theorem 7

In the proof of Theorem 6, the only term that carries an ℓ factor, is $q^{3/2}\ell k/2^n$, which appears while bounding the probability of the joint event E and $|\mathcal{S}| < \mu$ under the bad events Bad3 and Bad4 in Eqn. (41). To obtain an ℓ-free bound, we bound the bad events Bad3 and Bad4 in a different way [4].

Bounding Bad3. We bound the event Bad3 in exactly the same way as we did for proving the security of LightMAC_Plus. However, in this case, when $k \geq 4n/3$, we choose the value of $\mu = 2^{3k/4-n}k\ell$. With this value of μ, we have

$$\begin{aligned}
\Pr[\mathsf{Bad3}] \quad &\leq \quad \frac{p\sqrt{q}}{2^k} + \sum_{i=\sqrt{q}}^{u} \frac{q_i^2 \mu}{2^k} + \Pr[|\mathcal{S}| \geq \mu] \overset{(1)}{\leq} \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}\mu}{2^k} + 2^{2n} \cdot p^{2\ell} \cdot \left(\frac{6p}{2^n \mu}\right)^{\mu} \\
&\overset{(2)}{\leq} \quad \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}}{2^n} \cdot \frac{\ell k}{2^{k/4}} + 2^{2n} \cdot p^{2\ell} \cdot \left(\frac{6p}{2^{3k/4}k\ell}\right)^{2^{3k/4-n}k\ell}
\end{aligned}$$

[4] We would like to note that the term $pq\ell k/2^{n+k}$ also carries an ℓ factor which arises while bounding subcase E.1 under the bad event Bad1 and Bad2. However, this term does not create any problem to achieve an ℓ-free bound if we appropriately set the bound on ℓ. Unfortunately, this is not the case for the term $q^{3/2}\ell k/2^n$ and thus, we need a separate treatment with this bound to achieve ℓ-freeness.

$$\overset{(3)}{\leq} \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}}{2^n} + \frac{6p}{2^{3k/4}}, \tag{66}$$

where inequality (1) follows as the summation q_i^2, for $i \in [\sqrt{q}, u]$ is bounded above by $q^{3/2}$ due to Lemma 2 and we inheriting the bound of the probability of the event $|\mathcal{S}| \geq \mu$ from the previous analysis. Moreover, inequality (2) follows by choosing the value of $\mu = 2^{3k/4-n}k\ell$.

Using the similar argument, we bound the probability of event $\mathsf{Bad4}$ as follows:

$$\Pr[\mathsf{Bad4}] \leq \frac{p\sqrt{q}}{2^k} + \frac{q^{3/2}}{2^n} + \frac{6p}{2^{3k/4}}. \tag{67}$$

By inheriting the bounds of the remaining bad events from the previous analysis, we obtain the probability of bad transcript as follows:

$$\begin{aligned}\Pr[\mathsf{X}_{\mathrm{id}} \in \mathsf{BadT}] \leq\ & \frac{q^2}{2^{2k}} + \frac{q^3}{2^{2k}} + \frac{q^2p^2}{2^{3k}} + \frac{qp^2}{2^{2k}} + \frac{q}{2^k} + \frac{2q^2}{2^{2n/3+k}} + \frac{4q^2}{2^{2n}} + \frac{4q^2}{2^{n+k}} + \frac{2q^3}{3 \cdot 2^{2n}} \\ & + \frac{2q^{3/2}}{2^n} + \frac{4qp}{2^{n+k}} + \frac{2pq}{2^{2n/3+k}} + \frac{36p}{2^{3k/4}} + \frac{2pq^{1/2}}{2^k}. \end{aligned} \tag{68}$$

Finally, by combining Eqn. (68) and following the analysis of lower bounding the ratio of real to ideal interpolation probability of a good transcript, we obtain the desired ℓ-free security bound of the LightMAC_Plus construction in the multi-user setting, provided $k \geq 4n/3$ and $\ell \leq 2^{n/3}/k$.

6 Conclusion

In this paper we have analyzed multi-user security of LightMAC and LightMAC_Plus construction. We have shown that likewise security of LightMAC construction in the single user model, it achieves birthday bound security in the multi-user security model. However, we have been able to show that LightMAC_Plus achieves $2n/3$-bit security in the multi-user setup, whereas it has $3n/4$-bit security in the single-user setting and the bound is tight. Thus, it remains open to improve the multi-user security bound of LightMAC_Plus from $2n/3$ bits to $3n/4$ bits.

References

[1] I.J.S 27. Information technology — lightweight cryptography — part 6: Message authentication codes (macs). iso/iec 29192-6, international organization for standardization (2019), 2019.

[2] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 259–274. Springer, 2000.

[3] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, 2000.

[4] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In *EUROCRYPT '98, Proceeding.*, pages 266–280, 1998.

[5] Mihir Bellare and Björn Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 247–276. Springer, 2016.

[6] Mihir Bellare and Björn Tackmann. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 247–276, 2016.

[7] Eli Biham. How to decrypt or even substitute des-encrypted messages in 2^{28} steps. *Inf. Process. Lett.*, 84(3):117–124, 2002.

[8] Alex Biryukov, Sourav Mukhopadhyay, and Palash Sarkar. Improved time-memory trade-offs with multiple data. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*, pages 110–127. Springer, 2005.

[9] John Black and Phillip Rogaway. CBC macs for arbitrary-length messages: The three-key constructions. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 197–215. Springer, 2000.

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

[11] Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 468–499, 2018.

[12] A. Bosselaers. *Integrity Primitives for Secure Information Systems: Final RIPE Report of RACE Integrity Primitives Evaluation.* Lecture Notes in Computer Science. Springer, 1995.

[13] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, 2014. http://competitions.cr.yp.to/caesar.html.

[14] Sanjit Chatterjee, Alfred Menezes, and Palash Sarkar. Another look at tightness. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 293–319. Springer, 2011.

[15] Soumya Chattopadhyay, Ashwin Jha, and Mridul Nandi. Fine-tuning the ISO/IEC standard lightmac. *IACR Cryptol. ePrint Arch.*, page 1166, 2021.

[16] Yu Long Chen. A modular approach to the security analysis of two-permutation constructions. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 379–409, Cham, 2022. Springer Nature Switzerland.

[17] Nilanjan Datta, Avijit Dutta, and Samir Kundu. Tight security bound of 2k-lightmac plus. *IACR Cryptol. ePrint Arch.*, page 1422, 2023.

[18] Nilanjan Datta, Avijit Dutta, and Cuauhtemoc Mancillas Lopez. LightMAC: Fork it and make it faster. *Advances in Mathematics of Communications*, pages 0–0, 2023.

[19] 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.

[20] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Tight multi-user security bound of dbhts. *IACR Trans. Symmetric Cryptol.*, 2023(1):192–223, 2023.

[21] Avijit Dutta and Mridul Nandi. BBB secure nonce based MAC using public permutations. In Abderrahmane Nitaj and Amr M. Youssef, editors, *Progress in Cryptology - AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020, Proceedings*, volume 12174 of *Lecture Notes in Computer Science*, pages 172–191. Springer, 2020.

[22] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, pages 437–466, 2019.

[23] Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 3–32, 2016.

[24] Viet Tung Hoang and Stefano Tessaro. The multi-user security of double encryption. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, pages 381–411, 2017.

[25] Tetsu Iwata and Kaoru Kurosawa. OMAC: one-key CBC MAC. In *Fast Software Encryption, 2003*, pages 129–153, 2003.

[26] Hwigyeom Kim, Yeongmin Lee, and Jooyoung Lee. Forking tweakable even-mansour ciphers. *IACR Trans. Symmetric Cryptol.*, 2020(4):71–87, 2020.

[27] 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.

[28] Kaoru Kurosawa and Tetsu Iwata. Tmac: Two-key cbc mac. In Marc Joye, editor, *Topics in Cryptology — CT-RSA 2003*, pages 33–49, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[29] 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.

[30] Atul Luykx, Bart Mennink, and Kenneth G. Paterson. Analyzing multi-key security degradation. 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 II, volume 10625 of *Lecture Notes in Computer Science*, pages 575–605. Springer, 2017.

[31] 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.

[32] David A. McGrew and John Viega. The security and performance of the galois/counter mode (GCM) of operation. In Anne Canteaut and Kapalee Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355. Springer, 2004.

[33] M.Dworkin. Recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac, 2007.

[34] Andrew Morgan, Rafael Pass, and Elaine Shi. On the adaptive security of macs and prfs. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 724–753. Springer, 2020.

[35] Nicky Mouha. Chaskey: a MAC algorithm for microcontrollers - status update and proposal of chaskey-12 -. *IACR Cryptol. ePrint Arch.*, page 1182, 2015.

[36] Nicky Mouha and Atul Luykx. Multi-key security: The even-mansour construction revisited. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 209–223. Springer, 2015.

[37] 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.

[38] 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.

[39] Yusuke Naito. The exact security of PMAC with two powering-up masks. *IACR Trans. Symmetric Cryptol.*, 2019(2):125–145, 2019.

[40] Yusuke Naito. The multi-user security of macs via universal hashing in the ideal cipher model. In Elisabeth Oswald, editor, *Topics in Cryptology – CT-RSA 2024*, pages 51–77, Cham, 2024. Springer Nature Switzerland.

[41] NIST. Lightweight cryptography, 2018. Online: https://csrc.nist.gov/Projects/Lightweight-Cryptography. Accessed: August 01, 2019.

[42] 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.

[43] Yaobin Shen, Lei Wang, and Dawu Gu. Ledmac: More efficient variants of lightmac. *IACR Cryptol. ePrint Arch.*, page 1210, 2021.

[44] Yaobin Shen, Lei Wang, Dawu Gu, and Jian Weng. Revisiting the security of dbhts macs: Beyond-birthday-bound in the multi-user setting. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 309–336. Springer, 2021.

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

[46] Gene Tsudik. Message authentication with one-way hash functions. In *Proceedings IEEE INFOCOM '92, The Conference on Computer Communications, Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, One World through Communications, Florence, Italy, May 4-8, 1992*, pages 2055–2059. IEEE Computer Society, 1992.

[47] Kan Yasuda. The sum of CBC macs is a secure PRF. In *CT-RSA 2010*, pages 366–381, 2010.

[48] Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In *CRYPTO 2011*, pages 596–609, 2011.

[49] Kan Yasuda. PMAC with parity: Minimizing the query-length influence. In Orr Dunkelman, editor, *Topics in Cryptology - CT-RSA 2012 - The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 - March 2, 2012. Proceedings*, volume 7178 of *Lecture Notes in Computer Science*, pages 203–214. Springer, 2012.

[50] Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In *ASIACRYPT 2012*, pages 296–312, 2012.

Supplementary Section

7 Proof of Lemma 3

Consider the first component C_1 of the graph G. Let $Y_{i_1} \in \mathcal{V}_1$ be any arbitrary vertex of C_1. There are $2^n - \Delta_1$ choices for assigning values to the variable Y_{i_1}. Let the assigned value to Y_{i_1} be y_{i_1}. Now, for any other variable Y_{i_2} of C_1, we consider the path $\mathcal{P}$ from Y_{i_1} to Y_{i_2} and assign the value $y_{i_1} \oplus \mathcal{L}(\mathcal{P})$ to the variable Y_{i_2}. Let this value be y_{i_2}. Note that the path is unique as the graph is acyclic and $\mathcal{L}(\mathcal{P}) \neq 0^n$ and hence $y_{i_1} \neq y_{i_2}$. However, we require $y_{i_2} \notin \mathcal{S}_1$. Similarly, for any other variable Z_{i_2} of C_1, we consider the path $\mathcal{P}$ from Y_{i_1} to Z_{i_2} and assign the value $y_{i_1} \oplus \mathcal{L}(\mathcal{P})$ to the variable Z_{i_2}. Let this value be z_{i_2}. Note that $z_{i_1} \neq z_{i_2}$. However, we require $z_{i_2} \notin \mathcal{S}_2$. Thus, the number of valid choices for assigning values to Y_{i_1} is at least $2^n - (c_1\Delta_1 + d_1\Delta_2)$. In general, for the i-th component, the number of ways we assign a value to a vertex in $\mathcal{V}_1$ of component C_i is at least

$$2^n - \big((c_1 + \ldots + c_{i-1} + \Delta_1)c_i + (d_1 + \ldots + d_{i-1} + \Delta_2)d_i\big).$$

This is because, to assign a value in a vertex in $\mathcal{V}_1$ of C_i, we need to ensure that the assignment should not create any collision between the assigned values and all the previously assigned values in all vertices of $\mathcal{V}_1$ of component $\mathsf{C}_1, \ldots, \mathsf{C}_{i-1}$. Similarly, the assigned values should not create any collision between the assigned values in the vertices $\mathcal{V}_2$ of C_i and all the previously assigned values in all vertices of $\mathcal{V}_2$ of component $\mathsf{C}_1, \ldots, \mathsf{C}_{i-1}$. Additionally, the assigned vertex should not collide with any element of Δ_1 or Δ_2. Let $h(\alpha)$ denotes the number of solutions chosen outside of $\mathcal{S}_1$ and $\mathcal{S}_2$ to $\mathcal{E}_{\mathsf{G}}$. Therefore, we have

$$\begin{aligned} h(\alpha) &\geq \prod_{i=1}^{\alpha} (2^n - ((c_1 + \ldots + c_{i-1} + \Delta_1)c_i + (d_1 + \ldots + d_{i-1} + \Delta_2)d_i)) \\ &= \prod_{i=1}^{\alpha} (2^n - ((\rho_{i-1}[1] + \Delta_1)c_i + (\rho_{i-1}[2] + \Delta_2)d_i)). \qquad (69) \end{aligned}$$

We would like to note that since the graph G is good, for each component i, at least one of c_i or d_i must be 1. By multiplying $2^{nq}/\mathbf{P}(2^n - \Delta_1, s_\ell)\mathbf{P}(2^n - \Delta_2, s_{\mathtt{r}})$ in both side of Eqn. (69), we have

$$\begin{aligned} h(\alpha) &\cdot \frac{2^{nq}}{\mathbf{P}\left(2^n - \Delta_1, s_\ell\right)\mathbf{P}\left(2^n - \Delta_2, s_{\mathtt{r}}\right)} \\ &\geq \prod_{i=1}^{\alpha} \frac{\left(2^n - \left(\left(\rho_{i-1}[1] + \Delta_1\right)c_i + \left(\rho_{i-1}[2] + \Delta_2\right)d_i\right)\right)2^{n(c_i+d_i-1)}}{\mathbf{P}\left(2^n - \left(\Delta_1 + \rho_{i-1}[1]\right), c_i\right)\mathbf{P}\left(2^n - \left(\Delta_2 + \rho_{i-1}[2]\right), d_i\right)} \\ &= \prod_{i=1}^{\alpha} \frac{2^{n(c_i+d_i)} - 2^{n(c_i+d_i-1)}\left(\left(\rho_{i-1}[1] + \Delta_1\right)c_i + \left(\rho_{i-1}[2] + \Delta_2\right)d_i\right)}{\mathbf{P}\left(2^n - \left(\Delta_1 + \rho_{i-1}[1]\right), c_i\right)\mathbf{P}\left(2^n - \left(\Delta_2 + \rho_{i-1}[2]\right), d_i\right)}. \end{aligned}$$

Now, we note that

$$\begin{aligned} \underbrace{\mathbf{P}\left(2^n - \left(\Delta_1 + \rho_{i-1}[1]\right), c_i\right)}_{A_i} &\leq 2^{nc_i} - 2^{n(c_i-1)}\left(\left(\Delta_1 + \rho_{i-1}[1]\right)c_i + \binom{c_i}{2}\right) \\ &+ 2^{n(c_i-2)}\left(\binom{c_i}{2}(\Delta_1 + \rho_{i-1}[1])^2 + \binom{c_i}{2}(c_i - 1)(\Delta_1 + \rho_{i-1}[1])\right. \\ &+ \left.\binom{c_i}{2}\frac{(c_i-2)(3c_i-1)}{12}\right). \qquad (70) \end{aligned}$$

Similarly, we have

$$\begin{aligned} \underbrace{\mathbf{P}(2^n - (\Delta_2 + \rho_{i-1}[2]), d_i)}_{B_i} &\leq 2^{nd_i} - 2^{n(d_i-1)}\left((\Delta_2 + \rho_{i-1}[2])d_i + \binom{d_i}{2}\right) \\ &+ 2^{n(d_i-2)}\left(\binom{d_i}{2}(\Delta_2 + \rho_{i-1}[2])^2 + \binom{d_i}{2}(d_i - 1)(\Delta_2 + \rho_{i-1}[2])\right. \\ &+ \left.\binom{d_i}{2}\frac{(d_i-2)(3d_i-1)}{12}\right). \qquad (71) \end{aligned}$$

Let us define the following:

$$\begin{aligned} C_i &:= \left(\binom{c_i}{2}(\Delta_1 + \rho_{i-1}[1])^2 + \binom{c_i}{2}(c_i - 1)(\Delta_1 + \rho_{i-1}[1]) + \binom{c_i}{2}\frac{(c_i-2)(3c_i-1)}{12}\right), \\ D_i &:= \left(\binom{d_i}{2}(\Delta_2 + \rho_{i-1}[2])^2 + \binom{d_i}{2}(d_i - 1)(\Delta_2 + \rho_{i-1}[2]) + \binom{d_i}{2}\frac{(d_i-2)(3d_i-1)}{12}\right). \end{aligned}$$

Combining Eqn. (70) and Eqn. (71), and by assuming $\big(\Delta_1 + \rho_\alpha[1]\big)c_{\max} \leq 2^{n-3}$, we have

$$A_i B_i \leq 2^{n(c_i+d_i)} - 2^{n(c_i+d_i-1)} \underbrace{\left(c_i(\Delta_1 + \rho_{i-1}[1]) + d_i(\Delta_2 + \rho_{i-1}[2]) + \binom{c_i}{2} + \binom{d_i}{2}\right)}_{Y_i}$$

$$+ \quad 2^{n(c_i+d_i-2)} \underbrace{\left(C_i + D_i + \left(c_i(\Delta_1 + \rho_{i-1}[1]) + \binom{c_i}{2}\right)\left(d_i(\Delta_2 + \rho_{i-1}[2]) + \binom{d_i}{2}\right)\right)}_{X_i} (72)$$

where we use the fact that, $2^n[D_i\big(c_i(\Delta_1+\rho_{i-1}[1])+\binom{c_i}{2}\big)+C_i\big(d_i(\Delta_2+\rho_{i-1}[2])+\binom{d_i}{2}\big)]-C_iD_i \geq 0$. By using Eqn. (72), we have

$$\begin{aligned} h(\alpha)\cdot\frac{2^{nq}}{\mathbf{P}(2^n-\Delta_1,s_\ell)\mathbf{P}(2^n-\Delta_2,s_{\mathtt{r}})} &\geq \prod_{i=1}^{\alpha} 1+\frac{2^{n(c_i+d_i-1)}\left(\binom{c_i}{2}+\binom{d_i}{2}\right)-2^{n(c_i+d_i-2)}X_i}{2^{n(c_i+d_i)}-2^{n(c_i+d_i-1)}Y_i+2^{n(c_i+d_i-2)}X_i} \\ &= \prod_{i=1}^{\alpha} 1+\frac{2^n\left(\binom{c_i}{2}+\binom{d_i}{2}\right)-X_i}{2^{2n}-2^nY_i+X_i} \overset{(2)}{\geq} \prod_{i=1}^{\alpha}\left(1-\frac{2X_i}{2^{2n}}\right). \end{aligned}$$

Thus, we have

$$h(\alpha) \overset{(3)}{\geq} \frac{\mathbf{P}(2^n-\Delta_1,s_\ell)\mathbf{P}(2^n-\Delta_2,s_{\mathtt{r}})}{2^{nq}}\left(1-\sum_{i=1}^{\alpha}\frac{10\left(\binom{c_i+d_i}{2}\left(\Delta_1+\Delta_2+\rho_{i-1}[1]+\rho_{i-1}[2]\right)^2\right)}{2^{2n}}\right),$$

where (2) follows from the fact that, $2^nY_i - X_i \leq 2^{2n-1}$ which holds true by assuming $(\Delta_1+\rho_\alpha[1])c_{\max} \leq 2^{n-3}$ and $(\Delta_2+\rho_\alpha[2])d_{\max} \leq 2^{n-3}$. Moreover, inequality (3) holds as it can be easily seen that each term of X_i is at most $\binom{c_i+d_i}{2}(\Delta_1+\Delta_2+\rho_{i-1}[1]+\rho_{i-1}[2])^2$. □