Building Single-Key Beyond Birthday Bound Message Authentication Code

Nilanjan Datta[1], Avijit Dutta[1], Mridul Nandi[1], Goutam Paul[1], Liting Zhang[2,3]

[1] Indian Statistical Institute, Kolkata
[2] State Key Laboratory of Computer Science
Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences
[3] Nanyang Technological University .
nilanjan_isi_jrf@yahoo.com, avirocks.dutta13@gmail.com, mridul.nandi@gmail.com, goutam.paul@isical.ac.in, liting.zhang@hotmail.com

Abstract. MACs (Message Authentication Codes) are widely adopted in communication systems to ensure data integrity and data origin authentication, e.g. CBC-MACs in the ISO standard 9797-1. However, all the current designs based on block cipher either suffer from birthday attacks or require long key sizes. In this paper, we focus on designing *single keyed block cipher based MAC achieving beyond-birthday-bound (BBB) security (in terms of number of queries) in the standard model.* Here, we develop several tools on sampling distributions which would be quite useful in the analysis of mode of operations. In this paper, we also show that the sum of two dependent pseudorandom permutation with some loss of randomness is still PRF with BBB security. Then, we demonstrate a generic composition (including the single keyed) achieving BBB security provided that the underlying internal construction satisfies some variants of cover-free (we call them *extended cover-free* and *pseudo-cover-free*) and block-wise universal properties. By applying this result, we finally provide two concrete single keyed constructions which achieve BBB security. These two constructions, called 1kf9 and 1k_PMAC+, are basically simple one key variants of 3kf9 and PMAC_Plus respectively. Thus, we solve a long-standing open problem in designing single-keyed BBB-secure MAC.

Keywords: 1kf9, 1k_PMAC+, Beyond Birthday Bound, Cover-free, PRF, Sum of PRP.

1 Introduction

Message Authentication Code (MAC) is one of the important primitives in symmetric key cryptography to preserve the integrity of the message being transmitted. A MAC algorithm produces a fixed-length message digest, called a tag, from a variable-length message. For a secure MAC, it will be hard to forge a

tag for a completely new message for which tag has not been observed. In this paper we focus on a stronger requirement of a MAC, namely pseudorandom function (PRF). Throughout the paper we fix a positive integer n. A **random function** $\mathtt{F}$ is a function which is chosen from the set of all functions following some distribution, not necessarily uniform. In particular, **uniform random function**, denoted Γ_n, (or **uniform random permutation** Π_n) is chosen uniformly from the set of all functions (or permutations respectively) from a specified finite domain $\mathcal{D}$ to $\{0,1\}^n$. We define **distinguishing advantage** of an oracle algorithm $\mathcal{A}$ for distinguishing two random functions $\mathtt{F}$ from $\mathtt{G}$ as $\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathtt{G}) := \mathsf{Pr}[\mathcal{A}^{\mathtt{F}} = 1] - \mathsf{Pr}[\mathcal{A}^{\mathtt{G}} = 1]$. We define PRF-advantage and PRP-advantage of $\mathcal{A}$ for an n-bit construction $\mathtt{F}$ respectively by

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathtt{F}}(\mathcal{A}) := \mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \Gamma_n), \quad \mathbf{Adv}^{\mathrm{prp}}_{\mathtt{F}}(\mathcal{A}) = \mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \Pi_n).$$

Beyond Birthday Bound (BBB) Security. If $\mathcal{A}$ makes at most q queries (query-complexity) with at most ℓ-blocks (a block contains n-bits) in each query (data-complexity) and runs in time at most t (time-complexity) we also call it a (q,ℓ,t)-distinguisher. We write $\mathbf{Adv}^{\mathrm{xxx}}_{\mathtt{F}}(q,\ell,t) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{xxx}}_{\mathtt{F}}(\mathcal{A})$ where maximum is taken over all (q,ℓ,t)-distinguisher $\mathcal{A}$ and xxx is either PRF or PRP. In an information theoretic situation, we also ignore the time parameter t. We call a keyed construction $\mathtt{F}$ is (q,ℓ,ϵ)-PRF if $\mathbf{Adv}^{\mathrm{prf}}_{\mathtt{F}}(q,\ell) \leq \epsilon$. We say that $\mathtt{F}$ achieves beyond-birthday bound security if for some reasonable choice of ℓ, ϵ is negligible even if $q = 2^{n/2}$. Note that, in this paper we mean BBB security in terms of q, unlike Zhang [36] where BBB security is implied in terms of ℓ. Moreover, our security bound drops down to the birthday-bound if we consider large values of ℓ. Since long messages are not popular in practical communications and lightweight applications, as observed in [20], in most practical protocols typical messages are relatively short. Therefore, in such settings, the BBB security in terms of ℓ does not benefit much, and lower bound on q is more in desire. Thus, our BBB security notion is relevant in lightweight application where l is small.

Beyond Birthday Secure Constructions. In cryptographic community, designing a PRP-secure block cipher got more attention than designing PRF-secure compression functions. The performance of a block cipher based MAC construction is balanced in both software and hardware. Thus, block-cipher (assumed to be PRP) based PRF constructions would be practically useful. Examples of popular block-cipher based MACs are CBC-MAC [6], OMAC [12], PMAC [8], TMAC [15] etc. However, for each of them, the so far best PRF-security advantage is $O(\ell q^2/2^n)$. For example, if PMAC is being implemented based on PRINCE [9] (a 64-bit lightweight block cipher, i.e., $n = 64$) in some small device and if we allow to process up to 2^{10} message-blocks per query then after 2^{25} message-tag queries, one may be able to distinguish it from random function with about $1/16$ probability. But when the PRF-security advantage is $O(\ell^4 q^3/2^{2n})$ then using the same block-cipher PRINCE with block length 64 bits and the maximum number of message blocks 2^{10}, one may be able to distinguish it from random function with the same probability after 2^{28} message-tag queries.

The difference becomes more visible when we consider the same setting (i.e $\ell = 2^{10}$) for AES block-cipher: If the PRF-advantage is $O(\ell q^2/2^n)$ then at least 2^{56} message-tag queries are required to distinguish it from a random function with probability 1/64 whereas $O(\ell^4 q^3/2^{2n})$ PRF-advantage requires at least 2^{70} message-tag queries.

Related Works on Beyond-Birthday Secure MACs. Among the block cipher based MACs that are beyond-birthday secure, two rate-1 (efficient) constructions[4] are PMAC_Plus [34] and 3kf9 [35]. In CRYPTO 2011, Yasuda proposed PMAC_Plus, a simple three key variant of parallelizable and efficient PMAC. In ASIACRYPT 2012, Zhang et al. proposed 3kf9 that improves the $f9$ MAC mode adopted in the 3rd Generation Partnership Project (3GPP). 3kf9 also requires three independent keys to lift its security beyond birthday-bound. In both the papers, it is mentioned that constructing 1-key rate 1 MAC is challenging.

There is also another deterministic MAC mode provides security beyond the birthday bound. As Dodis et al. [10] have shown, MD$[f, g]$ reaches $O(\epsilon q \text{poly}(n))$ MAC security. However, this design requires even longer keys and more block cipher invocations. By parity method, Bellare et al. present MACRX [4] with BBB security, conditioned on the input parameters are random and distinct. In [13], Jaulmes et al. proposed a randomized MAC that provides BBB security based on the ideal model (or possibly based on tweakable block cipher). Another BBB secure randomized construction called generic enhanced hash then MAC has been proposed in [23] by Minematsu. In [33] Yasuda proved that the sum of two independent ECBC has beyond birthday bound. However, it requires four keys and it is rate 1/2 construction as it requires two block cipher calls for processing each message block.

Key-size Reduction in Block Cipher Based MACs. While beyond birthday bound block cipher modes are especially useful for small-size block ciphers, their large key sizes prevent themselves from practical usages. This is more serious when implementing it in hardware, where registers to store key materials are expensive or otherwise injecting keys from outside brings security risks and slows down its overall efficiency. Furthermore, using three block cipher keys(as an example) imply three block cipher key scheduling algorithms (even though the keys are generated from a master key like many practical protocols [1]), and this means, for most block ciphers (e.g. AES), three more block cipher invocation time and energy consumption. Moreover, the results of [34, 35], can not be applied where three keys are generated from a single master key.

A more technical method is to use tweakable block ciphers [18], which are expected to be independently random permutations with a single secret key and distinct-and-public tweaks. However, there are still some problems. If we adopt dedicated tweakable block ciphers, (e.g. [14]) in PMAC_Plus and 3kf9, we benefit from optimized efficiency but can hardly get provable security on normal block ciphers (PRP assumption); if we adopt birthday-bound tweakable block ciphers, e.g. [30, 11, 24], we in fact loose the beyond-birthday bound in PMAC_Plus and

[4] By rate, we mean the no. of blocks processed per block-cipher invocation

3kf9. Then we have to adopt the provably secure tweakable block ciphers with beyond-birthday-bound security, e.g. [22, 17, 16, 21]. As far as we know, current solutions provide no good efficiency in our setting, because they need at least two normal block cipher invocations to build a tweakable block cipher, and their key sizes are not small either.

The Open Problem. Up to now, how to construct a BBB MAC mode under a single key and reduce its security to the PRP assumption of its underlying block ciphers is still technically hard and remains as an open problem.

1.1 Our Contributions

With a view to solving the above problem, first we review the techniques used in 3kf9 and PMAC_Plus. Despite their specific mechanisms to process message blocks, they both have double internal state-sizes and then encrypt their last internal states by the well-known "Sum of PRPs" technique [19, 5]. In proofs, cover-freeness of the final internal states is strictly necessary, and then by the previous results on "Sum of PRPs", the modes can reach a bound beyond the birthday paradox. With respect to the usages of key materials, the final "Sum of PRPs" needs two keys, and one more individual key is required by the message blocks processing phase. So, if we just adopt a single key in these modes, we encounter the following two problems:

(i) The first problem is that the "Sum of PRPs" may not work properly, since the outputs of the last two PRP calls do not have full entropy due to some previous assignments of output values of the internal structure. So we need some general results for sum of PRP which allows some loss of randomness in the output of PRPs and still achieves beyond birthday bound security.

(ii) The second problem is, the $O(q\ell)$ block cipher inputs within internal structures may collide with the last two inputs ($2q$ blocks in total) to "Sum of PRPs". So we need to extend the definition of cover-freeness. In other words, more bad cases are involved and one has to incorporate all these bad events carefully.

Obviously, designing a single-key such mode requires more techniques and its corresponding formal proof would be even harder and complex.

Contribution 1. Generalized Result on Sum of PRP: To solve the first problem, we revisit the proofs for "Sum of PRPs", and propose a generalized but even simpler proof. Our basic observation is that the original provable security results hold even when the output space is restricted to a subset instead of the full set $\{0,1\}^n$. That is, *over restricted domain and range, the sum of two same PRPs remains a PRF*. We examine this by considering the appropriate popular sampling model, namely WOR (without replacement). We show that the sum of (dependent) WOR samples is a very good approximation of the uniform distribution. We believe that this result could have its own interest and could be applicable in other settings.

Contribution 2. (Single Keyed) Generic Composition: To solve the second problem, we first define several notions, e.g. extended-cover-free, pseudo-

cover-free, and block-wise universal, which are in fact abstracted from our analysis on one-key constructions. Taking advantages of this, we propose and prove our main theorem that can upper bound any one-key construction following "hash-then-sum" paradigm by these items.

Contributions 3. Two BBB-secure Single Keyed Constructions: Finally, we propose two BBB-secure single keyed constructions namely 1kf9 and 1k_PMAC+, which are single-key variants of 3kf9 and PMAC_Plus respectively - solving the long-standing open problem of designing single-keyed BBB secure MAC. Taking advantage of our main theorem and upper bounding the three items, i.e., extended-cover-free, pseudo-cover-free, and block-wise universal, we prove the BBB security of our single-keyed constructions. Though the proofs are more involved, interestingly, our bounds $O(\frac{q^3\ell^4}{2^{2n}})$ for 1kf9 and 1k_PMAC+ essentially have the similar PRF advantage. Proving such a result for single key almost rate-1 is not done before, (may be done for nonce based AE) which is beyond our scope, but not in PRF without nonce. Our proof technique highly depends on sum of PRP with loss of randomness.

We would like to remark that a direct one-key substitution of 3kf9 and PMAC_Plus can be easily shown to be insecure. This is why we need simple variants of one-key version.

2 Preliminaries

Notation. We denote $X \xleftarrow{\$} S$ to mean that X is chosen uniformly from S and independently to all other random variables defined so far. We write $X \perp Y$ for independent random variables X and Y. Let $[a..b] := \{a, a+1, \ldots, b\}$, $[a] = [1..a]$. By a q-set or q-tuple, we mean a set or a tuple of size q. Given a q-tuple $x = (x_i : i \in I)$, where I is the index set, we abuse the notation x also to mean the set $\{x_i : i \in I\}$. When all elements x_i's are distinct we simply write $x \in \mathsf{dist}_q$ or $x \in \mathsf{dist}$ and we call x *element-wise distinct*. For a subset $J \subseteq I$, the sub-tuple $x_J := (x_j)_{j \in J}$. Fix a positive integer n. Let $\mathbb{P}$ denote the set of all permutations over $\{0,1\}^n$. For any function f, and two tuples x, y over same set of indices I, we write $x \xmapsto{f} y$ to mean that $f(x_i) = y_i,\ \forall i \in I$. Let $\mathbb{P}_{x \to y} := \{\pi \in \mathbb{P} : x \xmapsto{\pi} y\}$. For two tuples x and y over a same index set, we write $x \longrightarrow y$ (or $x \longleftrightarrow y$) if there exists a function (or permutation respectively) π such that $x \xmapsto{\pi} y$. In this case, we call (x, y) function-compatible or (permutation-compatible respectively).

2.1 Oracle Algorithm and Its Transcript

An oracle algorithm $\mathcal{A}$ (e.g., distinguisher or some block cipher based constructions in which block ciphers are viewed as oracles) interacting with one or more oracles $\mathcal{O}$ makes queries depending on the previous query responses. We denote the oracle interaction by $\mathcal{A}^{\mathcal{O}}(m)$ or $\mathcal{A}(m) \to \mathcal{O}$ where m is an initial input of $\mathcal{A}$. During the interaction $\mathcal{A}^{\mathcal{O}}(m)$, let $X_1 := (X_{1,1}, \ldots, X_{1,r})$ be the tuple of all

queries to $\mathcal{O}$ and $Y_1 := (Y_{1,1}, \ldots, Y_{1,r})$ be the tuple of corresponding responses. The transcript (X_1, Y_1) is denoted as $\tau(\mathcal{A}(m) \to \mathcal{O})$. In case of a deterministic algorithm $\mathcal{A}$, $X_{1,i}$ is some function of $Y_{1,1}, \ldots, Y_{1,i-1}$ and m. Finally, it returns some output c which must be a function of Y and m.[5] Let $\mathcal{A}$ be a deterministic oracle algorithm and $m = (m_1, \ldots, m_q)$ be a q-tuple. For any function f, we write the q-transcript of all query-responses $(X := (X_1, \ldots, X_q), Y := (Y_1, \ldots, Y_q))$ as $\tau(\mathcal{A}(m) \to_q f)$ or simply as $\tau(\mathcal{A}(m) \to f)$ (whenever q is understood from the context) where $(X_i, Y_i) = \tau(\mathcal{A}(m_i) \to f)$.

Definition 1. *A pair of tuples (x, y) is called $\mathcal{A}(m)$-**realizable** for a q-tuple m, if there exists a function f such that $\tau(\mathcal{A}(m) \to_q f) = (x, y)$.*

The following simple observation is very useful which abstracts a feature of query-responses for an interaction of a deterministic algorithm with a random function. We skip the proof as it is straight forward.

Lemma 1. *Let $\mathcal{A}$ be a deterministic oracle algorithm. For any $\mathcal{A}(m)$-realizable pair (x, y), we have $x \xmapsto{f} y$ if and only if $\tau(\mathcal{A}(m) \to f) = (x, y)$. Thus, for any event E and for any random function $\mathtt{F}$,*

$$\mathsf{Pr}_{\mathtt{F}}[E \mid \tau(\mathcal{A}(m) \to \mathtt{F}) = (x, y)] = \mathsf{Pr}_{\mathtt{F}}[E \mid x \xmapsto{\mathtt{F}} y].$$

Note that the right hand side of the probability does not depend on any choice of adversary. This would be useful while we compute the interpolation probability.

Interpolation Probability. For any tuples x, y with the same index set and a random function $\mathtt{F}$, we call $\mathsf{Pr}[x \overset{\mathtt{F}}{\mapsto} y]$ *interpolation probability*. Let x and y be a tuple of elements from the domain and range of Γ_n (or Π_n) over a same set of indices. Moreover, let s be the number of distinct elements in x. It is easy to see that the interpolation probability $\mathsf{Pr}[x \overset{\Gamma_n}{\mapsto} y]$ is positive and equals to 2^{-ns} if and only if (x, y) is function-compatible. Similarly, $\mathsf{Pr}[x \overset{\Pi}{\mapsto} y]$ is positive and equals to $1/P_s^{2^n}$ if and only if (x, y) is permutation-compatible where $P_s^N := N(N-1)\cdots(N-s+1)$. This observation can be extended to the conditional probability for the uniform random permutation.

Lemma 2. *Let $((x, a), (y, b))$ be a permutation-compatible pair such that $a \cap x = \emptyset$ and $a \in \mathsf{dist}_s$ then*

$$\mathsf{Pr}[a \overset{\Pi_n}{\mapsto} b \mid x \overset{\Pi_n}{\mapsto} y] \geq 2^{-ns}. \tag{1}$$

2.2 Coefficient H-Technique

In this section we briefly discuss Patarain's Coefficient-H Technique [27]. It was also known as Decorrelation Theorem due to Vaudenay [32].

[5] We ignore the previous queries X in the query computations and in the final output, as these are eventually defined recursively in terms of Y and m.

Definition 2 (statistical distance). *Let X and Y two random variables over a set S. We define the* **statistical distance** *between X and Y as*

$$\Delta(X\ ;\ Y) = \max_{T \subseteq S} \mathsf{Pr}[X \in T] - \mathsf{Pr}[Y \in T].$$

We state some tools which would be used to bound the statistical distance between two random variables. The coefficient H-technique is the generalized version of this result for bounding distinguishing advantage of two random functions. We write $X \succ_\epsilon Y$ if $\mathsf{Pr}[X = s] \geq (1 - \epsilon) \times \mathsf{Pr}[Y = s], \forall s$ and we say that $X \succ_\epsilon Y$ over E, if this holds only for all $s \in E$.

Lemma 3 (coefficient H-technique for random variables). *Let X, Y be two random variables over S such that $X \succ_\epsilon Y$ over $\mathcal{V}_{\text{good}} \subseteq S$ then,*

$$\Delta(X\ ;\ Y) \leq \epsilon + \mathsf{Pr}[Y \notin \mathcal{V}_{\text{good}}].$$

Proof of this lemma is given in Appendix A.

Theorem 1 (coefficient H-technique for random functions). *Let $\mathtt{F}$ and $\mathtt{G}$ be two random functions. Let $\mathcal{V}_{good} \subseteq \mathcal{X}^q \times \mathcal{Y}^q$. If (i) $\forall\ m = (m_1, \ldots, m_q) \in \mathsf{dist}_q$, $(\mathtt{F}(m_i))_i \succ_{\epsilon_1} (\mathtt{G}(m_i))_i$ over $\mathcal{V}_{good}$ and (ii) $\mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{G}) \notin \mathcal{V}_{good}] \leq \epsilon_2$, then $\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathtt{G}) \leq \epsilon_1 + \epsilon_2$.*

We give the proof of this theorem in Appendix A.

3 Some Results on Sampling Distributions

In this section, we discuss some general results on sampling distribution with replacement and without replacement.

3.1 With (out) replacement sampling

Let $(Y_1, \ldots, Y_r) \xleftarrow{\text{wor}} S$ be a set of r samples drawn without replacement from a set S. In other words, we sample the conditional distribution as $Y_i \mid (Y_1, \ldots, Y_{i-1}) \xleftarrow{\$} S \setminus \{Y_1, \ldots, Y_{i-1}\}$. Similarly, for the with replacement sampling, we write $U := (U_1, \ldots, U_r) \xleftarrow{\text{wr}} S$ which is same as drawing U_i's uniformly and independently from the set S. Let us consider the following question.

How close the sum of two WOR sampling to WR ?

More precisely, let $U := (U_1, \ldots, U_q) \xleftarrow{\text{wr}} \{0,1\}^n$. We would like to obtain an upper bound of the statistical distance $\Delta((Z_1, \ldots, Z_q)\ ;\ (U_1, \ldots, U_q))$ where $Z_i = Y_{1,i} \oplus Y_{2,i}$, $1 \leq i \leq q$, and the joint distributions of Y's are any one of the followings cases.

- **Case-1**: (sum of two independent WOR samples over two equal sized subsets of $\{0,1\}^n$): $Y_1 = (Y_{1,1}, \ldots, Y_{1,q}) \xleftarrow{\text{wor}} S$ and $Y_2 = (Y_{2,1}, \ldots, Y_{2,q}) \xleftarrow{\text{wor}} T$ and $Y_1 \perp Y_2$ where (a) $|S| = |T| = 2^n - s$, (b) $S = T = \{0,1\}^n$.

- **Case-2**: (sum of two dependent WOR samples over a subset of $\{0,1\}^n$): $(Y_{1,1}, Y_{2,1}, \ldots, Y_{1,q}, Y_{2,q}) \xleftarrow{\text{wor}} S \subseteq \{0,1\}^n$ for a set S with size (a) $2^n - s$, $s \geq 0$, (b) $S = \{0,1\}^n$.

Existing Results. For the first two cases (i.e. case 1(a) and case 1(b)), Bellare et.al [5] had shown that $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + O(n \times (\frac{q}{2^n})^{1.5})$. Their analysis uses some advanced results of probability theory (e.g., Azuma's inequality and Chernoff theorem). For case 1(b), later Lucks [19] provided an elementary proof with the upper bound $O(q^3/2^{2n})$ and Patarin [29] provides a much involved complex proof with the upper bound $O(q/2^n)$.

Our Results. We have two main results, one for each of Case-1 and Case-2, as stated below.

Theorem 2 (Case-1(a)). *Let $X \xleftarrow{\text{wor}} S$ and $Y \xleftarrow{\text{wor}} T$ be two independent q-samples such that $S, T \subseteq \{0,1\}^n$ of size $2^n - s$. If $s \leq 2^{n-1} - q$ then*

$$\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{4qs^2 + 4sq^2 + 4q^3/3}{2^{2n}}.$$

*In particular, for **Case-1(b)** we have $S = T = \{0,1\}^n$ (i.e., $s = 0$) and so $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{4q^3/3}{2^{2n}}$.*

Theorem 3 (Case-2(a)). *Let $(X_1, Y_1, \ldots, X_q, Y_q) \xleftarrow{\text{wor}} S \subseteq \{0,1\}^n$ such that $|S^c| := s \leq 2^{n-1} - 2q$. Then*

$$\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{4qs^2 + 8sq^2 + 6q^3}{2^{2n}}.$$

*When $q \leq s$, we have $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{18s^3}{2^{2n}}$. In particular, for **Case-2(b)**, we additionally have $s = 0$, leading to $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{6q^3}{2^{2n}}$.*

Our Approach. In this paper, we only prove for Case-1(a) and Case-2(a). Our result is a generalization of that of Lucks [19], albeit with a much simpler analysis. Later, we will show the application of these results for analyzing one-key constructions of a specific form.

We start our proof with Lemma 4 which bounds the interpolation probability of sum of two WOR samples drawn from arbitrary subset of $\{0,1\}^n$. Then we extend Lemma 4 in Lemma 5 for $2q$ many samples over an arbitrary subset of $\{0,1\}^n$. Then in Corollary 1 we consider the interpolation probability of sum of two independent WOR samples drawn from two arbitrary equal-sized subsets of $\{0,1\}^n$. Similarly, Corollary 2 is a natural extension of Corollary 1 for $2q$ many samples over two arbitrary equal-sized subsets of $\{0,1\}^n$. Then we resume the proof of Theorem 2 and 3.

High Interpolation Probability for Sum of Dependent WOR Samples. We now state the key lemma which would be used to bound the statistical distance between sum of WOR sampling and WR sampling.

Lemma 4 (1-interpolation probability of sum of WOR samples). *Let $S' \subseteq \{0,1\}^n$ be a subset of size $(2^n - s')$ and $U_n \xleftarrow{\$} \{0,1\}^n$. Let $(V,W) \xleftarrow{\text{wor}} S'$ be a WOR sample of size 2 drawn from S'. Then, $V \oplus W \succ_\epsilon U_n$ over $\mathbb{F}^*_{2^n} := \mathbb{F}_{2^n} \setminus \{0^n\}$ where $\epsilon := \frac{s'^2}{(2^n - s')^2}$.*

Proof. Let $t \in \mathbb{F}^*_{2^n}$. For $i = 1, 2$, let $A_i = \{(a_1, a_2) : a_1 \oplus a_2 = t, a_i \notin S'\}$. Clearly, $|A_i| \leq s'$. Note that $\{(x,y) \in S^{'} \times S^{'} : x \oplus y = t\} = \{(x, t \oplus x) : x \in \{0,1\}^n\} \setminus (A_1 \cup A_2)$. So,

$$\begin{aligned}\mathsf{Pr}[V \oplus W = t] &= \frac{2^n - |A_1 \cup A_2|}{(2^n - s')(2^n - s' - 1)} \\ &\geq \frac{2^n - 2s'}{(2^n - s')^2} = 2^{-n}(1 - \frac{s'^2}{(2^n - s')^2}). \quad \square\end{aligned}$$

Corollary 1. *Let $S' \subseteq \{0,1\}^n$ and $T' \subseteq \{0,1\}^n$ be two subsets of equal size $(2^n - s')$. Let $(V,W) \xleftarrow{\$} S' \times T' \ni V \perp W$. Then $V \oplus W \succ_\epsilon U_n$ over $\mathbb{F}^*_{2^n}$. When $s' \leq 2^{n-1}$, $\epsilon \leq 4s'^2/2^{2n}$.*

We now state and prove the extension of Lemma 4 for $2q$ many samples.

Lemma 5 (q-interpolation probability of sum of dependent WOR samples over S). *Let $S \subseteq \{0,1\}^n$ of size $2^n - s$, $(Y_{1,1}, Y_{2,1}, \ldots, Y_{1,q}, Y_{2,q}) \xleftarrow{\text{wor}} S$ and let $Z = (Z_1 := (Y_{1,1} \oplus Y_{2,1}), \ldots, Z_q := (Y_{1,q} \oplus Y_{2,q}))$. Then,*

$$Z \succ_\epsilon U \text{ over } \mathbb{F}^*_{2^n} \text{ where } \epsilon := \frac{qs^2 + 2sq^2 + 4q^3/3}{(2^n - s - 2q)^2}.$$

Proof. Let $S^c = \{a_0, a_{-1}, \ldots, a_{-s+1}\}$. Let us fix $i \geq 1$, $t = (t_1, \ldots, t_q) \in (\mathbb{F}^*_{2^n})^q$ and $a_1, a_2, \ldots, a_{2i-3}, a_{2i-2}$ be distinct elements from S such that $a_{2j-1} \oplus a_{2j} = t_j$, $1 \leq j < i$. By using Lemma 4 with $S' = \{0,1\}^n \setminus \{a_j : -s < j \leq 2i-2\}$ and $s' = s + 2(i-1)$, we have

$$\mathsf{Pr}[Z_i = t_i \mid Y_{1,1} = a_1, Y_{2,1} = a_2, \ldots, Y_{1,i-1} = a_{2i-3}, Y_{2,i-1} = a_{2i-2}] \geq \tfrac{1}{2^n}(1 - \epsilon_i)$$

where $\epsilon_i = \frac{(s+2(i-1))^2}{(2^n - s - 2(i-1))^2}$. Since this bound holds for any a_i's, we can conclude that $\mathsf{Pr}[Z_i = t_i \mid Z_1 = t_1, \ldots, Z_{i-1} = t_{i-1}] \geq \frac{1}{2^n}(1 - \epsilon_i)$. After applying chain rule for these conditional probabilities, we obtain that

$$\mathsf{Pr}[Z = t] \geq 2^{-nq}(1 - \sum_i \epsilon_i) \geq 2^{-nq}(1 - \frac{qs^2 + 2sq^2 + 4q^3/3}{(2^n - s - 2q)^2}). \tag{2}$$

$\square$

It is to be noted that in both the lemmas the samples are chosen from S without replacement and as a result the sum of q-many samples becomes non-zero which justifies $Z \succ_\epsilon U$ over $\mathbb{F}^*_{2^n}$.

Corollary 2. *Let* $Y_1 := (Y_{1,1}, Y_{1,2} \ldots, Y_{1,q}) \overset{\text{wor}}{\leftarrow} S$ *and* $Y_2 := (Y_{2,1}, Y_{2,2}, \ldots, Y_{2,q}) \overset{\text{wor}}{\leftarrow} T$ *are two* q*-samples and* $Y_1 \perp Y_2$ *where* S *and* T *are two equal-sized subsets of* $\{0,1\}^n$ *of size* $2^n - s$*. Let* $Z := (Z_1, Z_2, \ldots, Z_q)$ *where each* $Z_i = Y_{1,i} \oplus Y_{2,i}$*. Then* $Z \succ_\epsilon U$ *where* $\epsilon \leq \frac{4qs^2+4sq^2+4q^3/3}{2^{2n}}$ *provided* $s + q \leq 2^{n-1}$*.*

Proof. On the calculation of the conditional probability of Z_i, we set $S' = \{0,1\}^n \setminus (S^c \cup \{a_1, a_3, \ldots, a_{2i-3}\})$ and $T' = \{0,1\}^n \setminus (T^c \cup \{a_2, a_4, \ldots, a_{2i-2}\})$ and so we set $s'_i = s + (i-1)$. Then using Corollary 1, the Equation (2) holds with $\epsilon_i = s'^2_i/(2^n - s'_i)^2$. After simplifying $\sum_i \epsilon_i$, we obtain the result. □

Now we have all the required materials to prove Theorem 2 and Theorem 3.

Proof of Theorem 2.

Let us consider a view $\mathbb{V} := (C_1, C_2, \ldots, C_q)$ consisting of q samples, where $C_i = X_i \oplus Y_i$ such that $X_i \overset{\text{wor}}{\leftarrow} S$ and $Y_i \overset{\text{wor}}{\leftarrow} T$, $X_i \perp Y_i, i \in [1,q]$ and $S, T \subseteq \{0,1\}^n$. We say a view $\mathbb{V}$ is *bad* if $\exists C_i = 0$. Let $\mathcal{V}_b$ be the set of all bad-views and $\mathcal{V}_g$ be the set of all good views. Now, it is easy to see that $\mathsf{Pr}[\, U \notin \mathcal{V}_g] \leq \frac{q}{2^n}$ and from Corollary 2 we have, $Z \succ_\epsilon U$ over $\mathcal{V}_g$ where $\epsilon \leq \frac{4qs^2+4sq^2+4q^3/3}{2^{2n}}$ as $s + q \leq 2^{n-1}$. Thus, using Lemma 3 we have, $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{4qs^2+4sq^2+4q^3/3}{2^{2n}}$.

In particular, when $|S| = |T| = \{0,1\}^n$, putting $s = 0$ we obtain $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{4q^3/3}{2^{2n}}$, which is actually the bound that Lucks had shown in [19]. □

Proof of Theorem 3.

Let us consider a view $\mathbb{V} := (C_1, C_2, \ldots, C_q)$ consisting of q samples, where $C_i = X_i \oplus Y_i$ such that $X_i, Y_i \overset{\text{wor}}{\leftarrow} S$, $S \subseteq \{0,1\}^n$. We say a view $\mathbb{V}$ is *bad* if $\exists C_i = 0$. Let $\mathcal{V}_b$ be the set of all bad-views and $\mathcal{V}_g$ be the set of all good views. Now, it is easy to see that $\mathsf{Pr}[\, U \notin \mathcal{V}_g] \leq \frac{q}{2^n}$ and from Lemma 5 we have, $Z \succ_\epsilon U$ over $\mathcal{V}_g$ where $\epsilon \leq \frac{4qs^2+8sq^2+6q^3}{2^{2n}}$ provided $s + 2q \leq 2^{n-1}$. Thus, using Lemma 3 we have, $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{4qs^2+8sq^2+6q^3}{2^{2n}}$.

It is easy to see that (i) when $q \leq s$ then $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{18s^3}{2^{2n}}$. (ii) when $|S| = |T| = \{0,1\}^n$, putting $s = 0$ we obtain $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \frac{6q^3}{2^{2n}}$. □

3.2 Applications to PRF Security of Sum of URP(Uniform Random Permutation)

Let Π be a uniform random permutation on $\{0,1\}^n$. Then, for any distinct $x_1, \ldots, x_q$, it is easy to see that $\Pi^{(q)}(x) := (\Pi(x_1), \ldots, \Pi(x_q)) \overset{\text{wor}}{\leftarrow} \{0,1\}^n$. So when Π_1 and Π_2 are two independent uniform random permutations then, $\Pi_1^{(q)}(x) \overset{\text{wor}}{\leftarrow} \{0,1\}^n$, $\Pi_2^{(q)}(x) \overset{\text{wor}}{\leftarrow} \{0,1\}^n$ and $\Pi_1^{(q)}(x) \perp \Pi_2^{(q)}(x)$ where $x \in \mathsf{dist}$.

- **Case-1(b)** actually talks about the pseudorandomness of sum of two independent random permutations. More precisely, let $\mathsf{SUM}_1^{\Pi_1,\Pi_2}(x) = \Pi_1(x) \oplus \Pi_2(x)$ where Π_1 and Π_2 are two independent random permutations. Then, using Theorem 2, we have

$$\mathbf{Adv}^{\text{prf}}_{\mathsf{SUM}_1^{\Pi_1,\Pi_2}}(q) \leq \frac{q}{2^n} + \frac{4q^3/3}{2^{2n}}.$$

The above construction has been analyzed in [19].

- **Case-2(b)** talks about the pseudorandomness of $(\Pi(x_1)\oplus\Pi(x_2), \ldots, \Pi(x_{2q-2}) \oplus \Pi(x_{2q}))$ where $x = (x_1, \ldots, x_{2q})$ is element wise distinct. We can define a function $\mathsf{SUM}_2^{\Pi} : \{0,1\}^{n-1} \to \{0,1\}^n$ mapping an $(n-1)$ bit string y to $\Pi(0\|y) \oplus \Pi(1\|y)$. So using Theorem 3 we have,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{SUM}_2^{\Pi}}(q) \leq \frac{q}{2^n} + \frac{6q^3}{2^{2n}}.$$

The above construction has been analyzed in [5].

- **Case-2(a)** talks about the more general case that deals with the pseudorandomness of $(\Pi^*(x_1) \oplus \Pi^*(x_2), \ldots, \Pi^*(x_{2q-2}) \oplus \Pi^*(x_{2q}))$ where $\Pi^* \xleftarrow{\$} \mathbb{P}_{a\to b}$ for two element wise distinct s-tuples a, b, and $x \cap a = \phi$. Suppose we restrict the domain of $\mathsf{SUM}_2^{\Pi^*}$ (as defined above) to $D := \{y \in \{0,1\}^{n-1} : 0\|y, 1\|y \notin a\}$. Then, according to Theorem 3, for all $q \leq s$, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{SUM}_2^{\Pi^*}}(q) \leq \frac{q}{2^n} + \frac{18s^3}{2^{2n}}.$$

We also state a theorem involving interpolation probability which would be used later for PRF security analysis of sum-based construction. The proof of the theorem is obvious from Theorem 3. We define sum function over two blocks as follows: $\mathsf{sum}^{\pi}(x, y) = \pi(x) \oplus \pi(y)$ and $\mathsf{sum}^{\pi_1,\pi_2}(x, y) = \pi_1(x) \oplus \pi_2(y)$. It is easy to see that the two block sum function can not be PRF. However, we have some lower bounds on interpolation probability provided that inputs are in special form. More formally we have the following theorem.

Theorem 4. *Let (x, y) be a permutation compatible pair of s-tuples. Let $\sigma_1, \theta_1, \ldots, \sigma_q, \theta_q$ be $2q$ distinct elements from the set $\{0,1\}^n \setminus x$. If $s + 2q \leq 2^{n-1}$ then, for any non-zero $t_1, \ldots, t_q \in \{0,1\}^n$,*

$$\frac{1}{(2^n - s)^q} \geq \mathsf{Pr}[(\sigma_i, \theta_i)_i \overset{\mathsf{sum}^{\Pi}}{\longmapsto} t \mid x \overset{\Pi}{\longmapsto} y] \geq 2^{-nq}(1 - \epsilon),$$

where $\epsilon = \frac{4qs^2+8sq^2+6q^3}{2^{2n}}$.

Proof. Set $Y_{1,i} = \Pi_{x\to y}(\sigma_i)$, $Y_{2,i} = \Pi_{x\to y}(\theta_i)$ then $(Y_1, Y_2) \overset{\mathrm{wor}}{\leftarrow} S := \{0,1\}^n \setminus y$. Hence we can apply Lemma 5 to conclude our theorem. □

A simpler version of the above theorem when we consider sum of two uniform random permutations, we have the following result. The proof is again straightforward from Corollary 2.

Theorem 5. *Let (x, y) and (x', y') be two permutation compatible pair of s-tuples. Let $\sigma_1, \ldots \sigma_q$ be q distinct elements from the set $\{0,1\}^n \setminus x$ and $\theta_1, \ldots \theta_q$ be q distinct elements from the set $\{0,1\}^n \setminus x'$. If $s + q \leq 2^{n-1}$ then, for any non-zero $t_1, \ldots, t_q \in \{0,1\}^n$,*

$$\frac{1}{(2^n - s)^q} \geq \mathsf{Pr}[(\sigma_i, \theta_i)_i \overset{\mathsf{sum}^{\Pi_1,\Pi_2}}{\longmapsto} t \mid x \overset{\Pi_2}{\longmapsto} y,\ x' \overset{\Pi_1}{\longmapsto} y'] \geq 2^{-nq}(1 - \epsilon),$$

where $\epsilon = \frac{4qs^2+4sq^2+4q^3/3}{2^{2n}}$.

4 A Generic Hash-then-Sum Construction for Building BBB Secure MAC

Road Map. In this section, we describe a generic method to build a BBB secure MAC. We start with a well known result of composition theorem to compose a universal hash function with a PRF. Now to achieve BBB security for this composed construction, one can consider a $2n$ bit output universal hash function composing with a BBB secure PRF. But obtaining double block BBB secure PRF based on a single key block cipher would not be easy and efficient.

Then we consider three types of hash-then-sum paradigm of constructions based on three, two and one key. We also build various cover-free notions and using those notions, we first find the sufficient condition for three key and two key versions of such constructions to achieve BBB security. Finally, using the similar idea, we provide the suffcient condition for single keyed hash-then-sum construction to achieve BBB security.

A Composition Theorem: PRF(U) $\equiv$ PRF. It is well known [31] that composition of ϵ universal hash function $\mathcal{H}$ and a PRF g is a PRF which has been proved using game-playing technique. For the sake of completeness, we formally define universal hash function and prove the theorem using Patarin's Coefficient-H Technique. Let $\mathcal{H}_K$ be an n-bit random function then

$$\mathbf{Adv}^{\mathrm{univ}}_{\mathcal{H}}(\ell) = \max_{m_1 \neq m_2 \in \{0,1\}^{\leq \ell}} \mathsf{Pr}_K[\mathcal{H}_K(m_1) = \mathcal{H}_K(m_2)].$$

We say that a construction $\mathtt{F}$ is (ℓ, ϵ)-universal if $\mathbf{Adv}^{\mathrm{univ}}_{\mathtt{F}}(\ell) \leq \epsilon$.

Theorem 6 ([31]). *Let $F_{K_1,K_2} := g_{K_2} \circ \mathcal{H}_{K_1} : \{0,1\}^* \to \{0,1\}^n$. Then,*

$$\mathbf{Adv}^{\mathrm{prf}}_{F}(q,\ell,t) \leq \mathbf{Adv}^{\mathrm{prf}}_{g}(q,\ell,t') + \binom{q}{2} \times \mathbf{Adv}^{\mathrm{univ}}_{\mathcal{H}}(\ell),$$

where $t' = t + \mathcal{O}(qT_\ell)$ and T_ℓ denotes the maximum time for computing $\mathcal{H}(m)$ for any m with maximum number of blocks ℓ.

Proof of this lemma is given in Appendix C.

Beyond Birthday Security. To achieve the beyond birthday security, one can consider $\mathcal{H}_{K_1} : \{0,1\}^* \to \{0,1\}^{2n}$ and $g_{K_2} : \{0,1\}^{2n} \to \{0,1\}^n$. So if $\mathbf{Adv}^{\mathrm{univ}}_{\mathcal{H}}(\ell) = O(2^{-2n})$ and g has beyond birthday PRF-security then we can achieve beyond birthday PRF-security for the composition function [6] . However, obtaining a double-block beyond birthday secure PRF based on a (single-keyed) block cipher would not be easy and efficient. One may try some variants of 6 rounds Luby-Rackoff [26] or Benes-Butterfly construction [28]. However, no such single key efficient construction is known.

Block-Separated Double Block Construction. Let $\mathcal{H}^\pi : \{0,1\}^* \to R$ be a

[6] This could be feasible as it is a collision probability for double-block construction. However, a term ℓ denoting the maximum message size may appear.

permutation-based deterministic construction. When e is a block cipher then for any key K, e_K is an n-bit permutation. Thus, a block cipher based construction $\mathcal{H}^{e_K}$ can be viewed as a permutation-based construction $\mathcal{H}^{\pi}$. When $R = \{0,1\}^{2n}$, it is called a double block construction and we write the two output blocks as $\mathcal{H}^{\pi}(m) = (\Sigma, \Theta)$. We say that $\mathcal{H}$ is **block-separated** if the range of possible values of Σ and Θ are disjoint. More formally, for all $m_1 \neq m_2$, and for all permutation π if

$$\mathcal{H}^{\pi}(m_1) = (\Sigma_1, \Theta_1), \mathcal{H}^{\pi}(m_2) = (\Sigma_2, \Theta_2) \;\Rightarrow\; \Sigma_i \neq \Theta_j, i, j \in \{1,2\}.$$

For any double construction (Σ', Θ'), with a minor modification, one can make it block-separated. For example, let $\mathsf{fix0} : \{0,1\}^n \to \{0,1\}^n$ be a function mapping $x_1 x_2 \cdots x_n$ to $0 x_2 \cdots x_n$. Similarly, we define $\mathsf{fix1}$ which fixes the first bits to 1. Now, the double block construction defined as $\mathcal{H} = (\Sigma, \Theta)$ is block-separated where $\Sigma = \mathsf{fix0}(\Sigma')$ and $\Theta = \mathsf{fix1}(\Theta')$. We use this to define block-separated constructions. Later we see that PRF analysis of block separated cases are easier as it does not need to handle bad events dealing collision between Σ and Θ values.

In the subsequent sections by double block construction we mean the block-separated double-block construction.

4.1 Hash-Then-Sum Construction

In this paper, we consider a special and very simple form of g function, namely the **sum function** over two blocks, which is considered in [5, 19]. We define

$$\mathsf{sum}^{\pi_1}(x,y) = \pi_1(x) \oplus \pi_1(y), \text{ and } \mathsf{sum}^{\pi_1,\pi_2}(x,y) = \pi_1(x) \oplus \pi_2(y)$$

where π_1 and π_2 are two independent n-bit functions (possibly permutations). Given a double-block construction $\mathcal{H}_K$, let's consider the following three composition rules depending on key reuse.

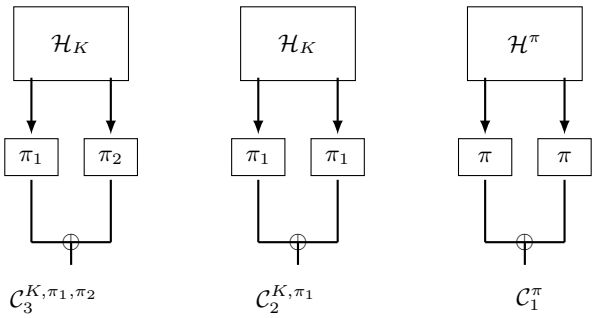

Fig. 4.1. Three different types of Hash-then-Sum constructions: (1) three-key construction $\mathcal{C}_3^{K,\pi_1,\pi_2} := \mathsf{sum}^{\pi_1,\pi_2} \circ \mathcal{H}_K$. (2) two-key construction $\mathcal{C}_2^{K,\pi_1} := \mathsf{sum}^{\pi_1} \circ \mathcal{H}_K$. (3) one-key construction $\mathcal{C}_1^{\pi} := \mathsf{sum}^{\pi} \circ \mathcal{H}^{\pi}$.

Note that we can not apply the above composition result as the sum construction is clearly not a PRF over two blocks. So we need a different type of composition result for sum-based construction. In [10], it has been proved that $\mathsf{sum}^{f_{K_1},f_{K_2}} \circ \mathcal{H}_K$ is unforgeable whenever $\mathcal{H}$ is cover-free and f is unforgeable. The same can be proved for PRF security instead of unforgeable. To do so, we formally define cover-free which would be used to analyze hash-then-sum constructions.

Let $\mathcal{H}_K := (\Sigma, \Theta)$ be a random function which outputs two blocks. For a q-tuple of distinct messages $m = (m_1, \ldots, m_q)$, we write $\mathcal{H}_K(m_i) = (\Sigma_i, \Theta_i)$. For a q-tuple of pairs $(\sigma_i, \theta_i)_i$, we say that

1. σ_i (or θ_i) is **fresh** [7] if it is not same as σ_j (or θ_j respectively) for some $j \neq i$.
2. We say that a tuple $(\sigma_i, \theta_i)_i$ is **cover-free** if for all i, either σ_i or θ_i is fresh.

We define (q, ℓ)-*cover-free advantage* of $\mathcal{H}$ as

$$\mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(q, \ell) = \max_{m \in \mathsf{dist}_q} \mathsf{Pr}[(\Sigma_i, \Theta_i)_i \text{ is not cover-free}],$$

where maximum is taken over all q-tuple of distinct messages having at most ℓ blocks. We say that a construction $\mathtt{F}$ is (q, ℓ, ϵ)-cover-free if $\mathbf{Adv}^{\mathrm{cf}}_{\mathtt{F}}(q, \ell) \leq \epsilon$.

4.1.1 Hash-then-sum based on PRF.

Lemma 6. *For any q, ℓ, the three-key construction $\mathcal{C}_3 := \mathsf{sum}^{f_{K_1},f_{K_2}} \circ \mathcal{H}_K$ satisfies the following:*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{C}_3}(t, q, \ell) \leq \mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(q, \ell) + 2\mathbf{Adv}^{\mathrm{prf}}_{f}(t', q, \ell).$$

Proof. Fix a cover-free tuple $(\sigma_i, \theta_i)_{i \in [q]}$. We denote the event $E(\sigma, \theta) \equiv \big((\mathcal{H}_K(m_i))_{i \in [q]} = (\sigma_i, \theta_i)_{i \in [q]}\big)$. Therefore, $\mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t \mid E] = \mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t] = \mathsf{Pr}[\Gamma_1(\sigma_i) \oplus \Gamma_2(\theta_i) = t_i, \forall i] = 2^{-nq}$ where $m = (m_1, \ldots, m_q)$ be the distinct q-tuple of messages and $t = (t_1, \ldots, t_q)$ be a q-tuple response such that t_i be the response of $\mathcal{C}_3$ for the corresponding message m_i. The first equation follows from the argument that the randomness for $\mathcal{H}$ is independent of Γ_1's and Γ_2's. The last equality follows from the following argument. Let ψ_i denote the one of the fresh blocks from σ_i and θ_i and ψ'_i denotes the other. Then, by conditioning on the output of ψ'_i's the above probability becomes the interpolation probability of a uniform random function for q distinct inputs which equals to 2^{-nq}. As the conditional probability is same for all condition events, the unconditional probability is also equal to 2^{-nq}. So $\mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t] \geq \frac{(1-\epsilon)}{2^{nq}}$ where $\epsilon := \mathsf{Pr}[E^c]$ which is at most $\mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(q, \ell)$. The above analysis is done for uniform random functions. The rest follows by applying standard reduction. □

[7] Some paper considers the definition when $j < i$, but here we consider the definition for all $j \neq i$ to simplify our analysis as in terms of order the security bound does not change.

Remark 1 *The above three-key construction is a potential candidate for having beyond birthday security. Note that from definition of cover-free,* $\mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(q,\ell) \leq \binom{q}{3}\mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(3,\ell)$*. So, for any three messages* m_1, m_2, m_3 *with* $m_1 \neq m_2, m_3$*, if*

$$Pr[\Sigma_1 = \Sigma_2, \Theta_1 = \Theta_3] = \mathcal{O}(\ell^c 2^{-2n})$$

for some small constant c then we have the beyond birthday security for small ℓ*. Intuitively, the event* $\Sigma_1 = \Sigma_2, \Theta_1 = \Theta_3$ *deals two (possibly linear independent) equations and it may be feasible to have such a bound.*

4.1.2 Hash-then-Sum based on Pseudorandom Permutation.

Block cipher (which is assumed to be PRP) based three key Hash-then-Sum constructions ($\mathcal{C}_3$) are well known from PMAC_Plus [34] and 3kf9 [35]. After modeling a block cipher to be a PRF, one can apply the above Lemma 6. However, *block cipher can ensure PRF with a maximum birthday bound security.* So we need to treat it differently to have beyond birthday analysis. In the following, let Π, Π_1, Π_2 be random permutations over the domain $\{0,1\}^n$ and range $\{0,1\}^n$. We state the results for the constructions using uniform random permutations instead of pseudorandom permutation as the standard reduction can be applied for the later constructions.
Let $\mathcal{H}_K$ be a block separated double block construction, we write $\mathcal{H}_K = (\mathcal{H}_{K,1}, \mathcal{H}_{K,2})$ where $\mathcal{H}_{K,1}, \mathcal{H}_{K,2}$ are single block functions.

4.2 PRF-security of Hash-then-Sum Construction based on Two and Three Key Constructions.

Theorem 7. *Let* $\mathcal{H}_K$ *be a* (q,ℓ,ϵ_{cf})*-cover-free function and for all* $i = 1,2$*,* $\mathcal{H}_{K,i}$ *are* (ℓ,ϵ_{univ})*-universal hash functions. Then,* $\mathcal{C}_2 := \mathsf{sum}^{\Pi} \circ \mathcal{H}_K$ *is* (q,ℓ,ϵ_2)*-PRF and* $\mathcal{C}_3 := \mathsf{sum}^{\Pi_1,\Pi_2} \circ \mathcal{H}_K$ *is* (q,ℓ,ϵ_3)*-PRF, where*

1. $\epsilon_2 = \epsilon_{\mathrm{cf}} + (2q + \frac{2q^3}{2^n-1})\epsilon_{\mathrm{univ}} + \frac{38q^3\ell^3}{2^{2n}} + \rho_{bad}$.
2. $\epsilon_3 = \epsilon_{cf} + (q + \frac{q^3}{2^n-1})\epsilon_{\mathrm{univ}} + \frac{10q^3\ell^3}{2^{2n}} + \rho_{bad}$.

The proofs for both constructions are similar except that we have to analyze sum of two independent or dependent uniform random random permutations. As the later involves more dependency, we only prove for $\mathcal{C}_2$. We provide the proof by using coefficient H-technique for which it would be sufficient to obtain a lower bound of interpolation probability.

Proof Sketch. Informally, given that we obtain cover-free outputs $(\sigma_i, \theta_i)_i$ from $\mathcal{H}$, for all i at least one block is fresh. *If both are fresh then we call i free.* For all non-free indices i, exactly one, denoted ψ_i, of σ_i and θ_i is not fresh and the other denoted by ψ_i', is fresh. We sample the output $\Pi(\psi_i')$ which will be forced as the sum of these values are fixed. Note that in the interpolation probability calculation, we fix some values for sum beforehand. Now, we will have high interpolation probability due to low collision probability of $\mathcal{H}_{K,i}$'s and independence

of sampling Π. In this way, we obtain high interpolation probability except for free i. Now we can apply sum of a uniform random permutation sampled from a restricted class of permutation (as analyzed in section 4) to complete the interpolation probability for free indices.

Formal Proof. As we mentioned above, we provide the formal proof of this theorem using Coefficient-H Technique. For that, we proceed in three streps: (A) Bound the probability of obtaining a bad view in ideal world, (B) Show high interpolation probability for the good view, and (C) Combine these two.

(A) Bounding the probability of Bad view. We first define the Bad view.

Definition 3 (Bad view). *A tuple $t := (t_1, \ldots, t_q)$ is said to have a r-collision if there exists an r-set I such that $t_i = t_j$ for all $i, j \in I$. Let*

$$\mathcal{V}_{bad} = \{t : \exists i, \quad t_i = 0\} \cup \{t : t \text{ has 3-collision}\}. \tag{3}$$

A view t is said to be a bad view if $t \in \mathcal{V}_{bad}$.

Let $\mathcal{V}_{good}$ be the complement of $\mathcal{V}_{bad}$. *Any element $t \in \mathcal{V}_{good}$ is called a good view.* Note that this view is observable by the adversary. For a random function Γ and for any adversary $\mathcal{A}$,

$$\rho_{bad} := \mathsf{Pr}[\tau(\mathcal{A}^{\Gamma}) \in \mathcal{V}_{bad}] \leq \frac{q}{2^n} + \frac{q^3}{2^{2n}}. \tag{4}$$

Now, we fix any $t \in \mathcal{V}_{good}$ and a q-tuple m of distinct messages. We write $\mathcal{H}_K(m_i) = (\Sigma_i, \Theta_i)$, $1 \leq i \leq q$.

(B) High Interpolation Probability for the Good view. In order to show the high interpolation probability for the good view, we will define a good internal transcript corresponding to the fixed good view. Then we will calculate the interpolation probability for good internal transcript followed by providing the bound for the probability for bad internal transcripts.

(B.1) Identify Good Internal Transcript. We first define some notations and definitions for defining good internal transcript. Let $(\sigma_i, \theta_i)_{i \in [q]}$ be any tuple. It is easy to see that for any i exactly one of the these will happen: (i) i is free, (ii) σ_i is fresh and θ_i is not, (iii) θ_i is fresh and σ_i is not and (iv) both σ_i and θ_i are not fresh. We call the tuple **cover-free** if the item (iv) does not happen for all i. Now let $I_\Sigma = \{i : \sigma_i \text{ is not fresh } \}$ and similarly we define I_Θ. We define

$$(\psi_i, \psi_i') = \begin{cases} (\sigma_i, \theta_i), & \text{if } i \in I_\Sigma \\ (\theta_i, \sigma_i), & \text{if } i \in I_\Theta \end{cases}$$

Note that ψ_i''s are always fresh and ψ_i's are not. We write $I = I_\Sigma \cup I_\Theta$. For all $i \in I$, we again choose a tuple $(w_j)_{j \in I}$ which is permutation compatible with $(\psi_j)_{j \in I}$. Let $\mathcal{T} = \{((\sigma_i, \theta_i)_{i \in [q]}, (w_j)_{j \in I}) : w_I \longleftrightarrow \psi_I\}$ be the set of all internal transcripts. Given any such tuple from $\mathcal{T}$, we define $w_i' = w_i + t_i$, $i \in I$. Now we define goodness of internal transcripts.

Definition 4. *A tuple* $((\sigma_i,\theta_i)_{i\in[q]},(w_j)_{j\in I})\in\mathcal{T}$ *is called* **good** *w.r.t.* t *if all of the followings happen:*

1. $E_1\equiv$: $((\sigma_i,\theta_i)_{i\in[q]}$ *is a cover-free tuple,*
2. $E_2\equiv$: *whenever* $t_i=t_j$, $\sigma_i\neq\sigma_j$ *and* $\theta_i\neq\theta_j$,
3. $E_3\equiv$: *for* $w'_i=w_i+t_i$, $i\in I$, *the tuple* $w'_I\in\mathsf{dist}$ *and*
4. $E_4\equiv$: $w'_I\cap w_I=\phi$.

Note, due to the choice of the q-tuple t, at most for $q/2$ pairs (i,j), $t_i=t_j$ can happen. Now we see why we call this internal transcript good. Informally, for a good internal transcript, we can have permutation-compatible input outputs and so we have high interpolation probability (otherwise, the interpolation probability would be zero).

Claim. If $((\sigma_i,\theta_i)_{i\in[q]},(w_j)_{j\in I})\in\mathcal{T}$ is **good** then $(\psi'_I,\psi_I)\longleftrightarrow(w'_I,w_I)$, $\psi'_I\in\mathsf{dist}_s$, and $\psi\cap\psi'=\phi$ where $s=|I|$.

Proof of the claim. Due to the definition of good tuple, $w'_I\in\mathsf{dist}_s$, $w'_I\cap w_I=\phi$. Whenever $t_i=t_j$, we have $w_i\neq w_j$ as $w'_i\neq w'_j$. At the same time, by definition of good tuple we know that $\sigma_i\neq\sigma_j$ and $\theta_i\neq\theta_j$. So, $(\psi'_I,\psi_I)\longleftrightarrow(w'_I,w_I)$.

(B.2) High Interpolation probability for Good Internal Transcript. Let us fix a good tuple as defined above. We denote the event

$$E(\sigma,\theta,w)\ \equiv\ \big((\mathcal{H}_K(m_i))_{i\in[q]}=(\sigma_i,\theta_i)_{i\in[q]},\Pi(\psi_j)=w_j\forall j\in I\big).$$

It is easy to see that given E, the interpolation event $m_I\overset{\mathcal{C}_2}{\longmapsto}t_I$ is same as $\psi'_I\overset{\Pi}{\longmapsto}w'_I$. Also, we have observed that, $\psi'_I\in\mathsf{dist}_s$ and $\psi\cap\psi'=\phi$ where $s=|I|$. So, we can use the lemma 2 given in section 2. More precisely, we have

$$\begin{aligned}\mathsf{Pr}[m_I\overset{\mathcal{C}_2}{\longmapsto}t_I\mid E]&=\mathsf{Pr}[\psi'_I\overset{\Pi}{\longmapsto}w'_I\mid E]\\&=\mathsf{Pr}[\psi'_I\overset{\Pi}{\longmapsto}w'_I\mid\psi_I\overset{\Pi}{\longmapsto}w_I]\quad\text{(As }K\text{ and }\Pi\text{ are independent)}\\&\geq\frac{1}{2^{ns}}\quad\text{(As }(\psi'_I,\psi_I)\longleftrightarrow(w'_I,w_I),\ \psi'_I\cap\psi_I=\phi\text{ and }\psi'_I\in\mathsf{dist}_s\ )\end{aligned}$$

Using the above result, we find the following conditional probability

$$\begin{aligned}\mathsf{Pr}[m\overset{\mathcal{C}_2}{\longmapsto}t\mid E]&=\mathsf{Pr}[m_{I^c}\overset{\mathcal{C}_2}{\longmapsto}t_{I^c}\mid E\wedge m_I\overset{\mathcal{C}_2}{\longmapsto}t_I]\times\mathsf{Pr}[m_I\overset{\mathcal{C}_2}{\longmapsto}t_I\mid E]\\&\geq\mathsf{Pr}[(\sigma_i,\theta_i)_{i\in I^c}\overset{\mathsf{sum}^{\Pi}}{\longmapsto}t_{I^c}\mid(\psi_I,\psi'_I)\overset{\Pi}{\longmapsto}(w_I,w'_I)]\times\frac{1}{2^{ns}}\geq\frac{(1-38s^3/2^{2n})}{2^{nq}}\end{aligned}$$

The last inequality follows from theorem 4. For the first statement of the theorem, we can apply Theorem 5 instead of Theorem 4 as we have two independent PRP. In this case the lower bound becomes $\frac{(1-10s^3/2^{2n})}{2^{nq}}$.

Now, we find our desired interpolation probability as we sum over all good tuples for $\epsilon=\mathsf{Pr}[(\Sigma_i,\Theta_i)_{i\in[q]},(\Psi_i,\Pi(\Psi_i))_{i\in I}$ is not good $]$:

$$\mathsf{Pr}[m\overset{\mathcal{C}_2}{\longmapsto}t]\geq\sum_E\mathsf{Pr}[m\overset{\mathcal{C}_2}{\longmapsto}t\mid E]\times\mathsf{Pr}[E]\geq\frac{(1-38s^3/2^{2n})}{2^{nq}}\times(1-\epsilon).\qquad(5)$$

(B.3) Find ϵ : Bounding Probability of Bad Internal Transcript. Now, we are left with bounding ϵ. By using the definition of good tuple and using the union bound, we have $\epsilon = \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4$ where $\epsilon_i = \mathsf{Pr}[E_i^c]$, $1 \le i \le 4$. Now we bound each ϵ_i as follows:

(a) $\epsilon_1 = \mathsf{Pr}[(\Sigma_i, \Theta_i)_i \text{ is not cover-free}] \le \epsilon_{\text{cf}}$.

(b) $\epsilon_2 = \sum_{i \neq j : t_i = t_j} (\mathsf{Pr}[\Sigma_i = \Sigma_j] + \mathsf{Pr}[\Theta_i = \Theta_j]) \le 2q\epsilon_{\text{univ}}$.

(c) $\epsilon_3 = \mathsf{Pr}[w'_I \in \mathsf{dist}] \le \frac{q^3}{2^n}\epsilon_{\text{univ}}$. The proof is given below:

$$
\begin{aligned}
\epsilon_3 &= \sum_{i \neq j : t_i \neq t_j} \mathsf{Pr}[i, j \in I, \Pi(\Psi_i) \oplus \Pi(\Psi_j) = t_i \oplus t_j] \\
&\le \sum_{i,j,k,\psi_i,\psi_j : i \neq j, t_i \neq t_j} \mathsf{Pr}[\Pi(\Psi_i) \oplus \Pi(\Psi_j) = t_i \oplus t_j \mid H \equiv (\Psi_i = \Psi_k = \psi_i, \Psi_j = \psi_j)] \times \mathsf{Pr}[H] \\
&\le \sum_{i,j,k,\psi_i,\psi_j : i \neq j, t_i \neq t_j} \mathsf{Pr}[\Pi(\psi_i) \oplus \Pi(\psi_j) = t_i \oplus t_j] \times \mathsf{Pr}[H] \\
&\le \sum_{i \neq j,k} \frac{1}{2^n - 1} \times \mathsf{Pr}[\Psi_i = \Psi_k] \le \frac{q^3}{2^n - 1}\epsilon_{\text{univ}}.
\end{aligned}
$$

The last two inequalities follows from the two fact: (i) K is independent of Π and (ii) for any $a, b, \mathsf{Pr}[\Pi(a) \oplus \Pi(b) = c] \le 1/(2^n - 1)$

(d) $\epsilon_4 = \mathsf{Pr}[w'_I \cap w_I = \phi] = \sum_{i \neq j : t_i \neq t_j} \mathsf{Pr}[i, j \in I, \Pi(\Psi_i) \oplus \Pi(\Psi_j) = t_i] \le \frac{q^3}{2^n - 1}\epsilon_{\text{univ}}$. This proof is identical to case (c).

Summing these four error terms, we obtain an upper bound of $\epsilon \le \epsilon_{cf} + (2q + \frac{2q^3}{2^n - 1})\epsilon_{univ}$. Now, plugging it in Equation (5) we obtain,

$$
\mathsf{Pr}[m \xmapsto{\mathcal{C}_2} t] \ge \epsilon_{cf} + (2q + \frac{2q^3}{2^n - 1})\epsilon_{univ} + \frac{38q^3l^3}{2^{2n}} \tag{6}
$$

(C) Combining the Results:. The proof completes as we apply Patarin's Coefficient Technique by putting Eqn. 4 and Eqn. 6 in Theorem 1.

4.3 PRF-security of Hash-then-Sum Construction based on Single keyed PRP

In this paper, we show a PRF-security bound for one-key hash-then-sum constructions $\mathcal{C}_1 := \mathsf{sum}^{\Pi} \circ \mathcal{H}^{\Pi}$. Note that the hash function is also permutation based and uses same permutation Π used in the outer layer sum function. The PRF security analysis is similar to that of Theorem 7. However, it requires to handle more bad cases.

Notation. Given any permutation π, let $\tau(\mathcal{H}(m) \to_q \pi) = (x, y)$, the pair of inputs and outputs of π during the computations of $\mathcal{H}^{\pi}(m_i) = (\sigma_i, \theta_i)$ for all $i \in [q]$. We also write $x = (x_{i,j} : i \in [q], j \in [\ell_i])$ and similarly y for the same index set. Note that $(\sigma_i, \theta_i)_i$ is uniquely determined by (x, y).

Definition 5. *For any i, we say that σ_i is x-***fresh** *if it is not same as σ_j for some $j \neq i$ or $x_{r,s}$ for any $r \in [q], s \in [\ell_r]$. Similarly, we define for x-freshness of θ_i. We say that a tuple $(\sigma_i, \theta_i)_i$ is x-***cover-free** *(or (x, y)* **is extended-cover-free***) if for all i, either σ_i or θ_i (or both) is x-***fresh**[8]*. If both σ_i and θ_i are x-fresh we call i to be free.*

We denote $I_\Sigma = \{i : \sigma_i \text{ is not } x\text{-fresh } \}$ and similarly I_Θ and let $I = I_\Sigma \cup I_\Theta$. For all $i \in I_\Sigma$, we define $(\psi_i, \psi_i') = (\sigma_i, \theta_i)$ and similarly, for all $i \in I_\Theta$, we define $(\psi_i', \psi_i) = (\sigma_i, \theta_i)$ and so ψ_i's are always non-fresh and ψ_i''s are fresh. We say that ψ_i is **old** if there exists $x_{r,s}$ such that $\psi_i = x_{r,s}$, otherwise ψ_i is called **new**. We define $I_{old} = \{i : \psi_i \text{ is old}\}$ and similarly $I_{new} = \{i : \psi_i \text{ is new}\}$. Clearly, $I = I_{old} \cup I_{new}$.

(x, y) is extended Covered	(L_{11}) $\sigma_i = \sigma_j, \theta_i = \theta_k$ (L_{12}) $\sigma_i = x_{j,a}, \theta_i = \theta_k$ (L_{13}) $\sigma_i = \sigma_j, \theta_i = x_{k,b}$ (L_{14}) $\sigma_i = x_{j,a}, \theta_i = x_{k,b}$
(x, y) is Pseudo Covered (type-1)	(L_{21}) $\sigma_i = x_{j,a}, y_{j,a} \oplus t_i = y_{k,s}$ (L_{22}) $\theta_i = x_{j,a}, y_{j,a} \oplus t_i = y_{k,s}$
(x, y) is Pseudo Covered (type-2)	(L_{31}) $\sigma_i = x_{k,a}, \sigma_j = x_{l,b}, y_{k,a} \oplus y_{l,b} = t_i \oplus t_j$ (L_{32}) $\theta_i = x_{k,a}, \theta_j = x_{l,b}, y_{k,a} \oplus y_{l,b} = t_i \oplus t_j$ (L_{33}) $\sigma_i = x_{k,a}, \theta_j = x_{l,b}, y_{k,a} \oplus y_{l,b} = t_i \oplus t_j$
$(x, y, w_{I_{new}})$ Mixed Covered	(L_{41}) $\sigma_i = x_{j,a}, y_{j,a} \oplus t_i = w_k$ (L_{42}) $\theta_i = x_{j,a}, y_{j,a} \oplus t_i = w_k$ (L_{43}) $\sigma_i = \sigma_j, w_i + t_i = w_j + t_j$ (L_{44}) $\sigma_i = \sigma_j, w_i + t_i = w_j$ (L_{45}) $\theta_j = x_{l,b}, y_{k,a} \oplus y_{l,b} = t_i \oplus t_j$
universal-collision	(L_{51}) $x_{j,a} = \sigma_i / \theta_i$ (L_{52}) $\theta_i = \theta_j$ / $\sigma_i = \sigma_j$
t-collision	(L_{61}) $\sigma_i = \sigma_j$ for some $t_i = t_j$ (L_{62}) $\theta_i = \theta_j$ for some $t_i = t_j$

Table 1. Table representing bad equations for fully covered, pseudo-covered and mix-covered cases. Moreover we also consider collision for extended universal hash.

Definition 6. *1. A double block construction $\mathcal{H}^\Pi$ is called (q, ℓ, ϵ)-***extended-cover-free** *if for all q-tuple $m = (m_1, \ldots, m_q)$ of distinct messages of size at most ℓ,*

$$\mathsf{Pr}_\Pi[(\mathcal{H}^\Pi(m_i))_i)_{i\in[q]} \text{ is extended-covered }] \leq \epsilon.$$

*2. $\mathcal{H}^\Pi$ is called (q, ℓ, ϵ)-***pseudo-cover-free** *w.r.t. t if for all q-tuple m of distinct messages of size at most ℓ, if*

$$\mathsf{Pr}_\Pi[(\mathcal{H}^\Pi(m_i))_i)_{i\in[q]} \text{ is pseudo-covered }] \leq \epsilon.$$

[8] Here we consider the definition for all i, r such that $r \neq i$. Defining x-fresh, assuming $r < i$ would give a better bound but as the order of the bound does not change, for simplification of the analysis, we keep this definition

3. *It is called* ϵ**-extended universal** *if* $\mathcal{H}_i^{\Pi}$*'s are* ϵ*-universal, i.e., for all pairs* $m = (m_1, m_2)$ *of distinct messages* $\mathsf{Pr}_{\Pi}[\Sigma_1 = X_{i,j}], \mathsf{Pr}[\Theta_1 = X_{i,j}] \leq \epsilon$ *for all* $i = 1, 2$ *and* $j \in [\ell_i]$.

Now, we state our main theorem which provides PRF security for hash-then-sum construction based on a single PRP.

Theorem 8. *If* $\mathcal{H}$ *is block-separated,* $(q, \ell, \epsilon_{ecf})$*-extended-cover-free,* $(q, \ell, \epsilon_{pcf})$*-pseudo-cover-free for any* q*-tuple* $t \in \mathcal{V}_{good}$ *and* ϵ_{euniv}*-extended universal then* $\mathcal{C}_1 := \mathsf{sum}^{\Pi} \circ \mathcal{H}^{\Pi}$ *is* (q, ϵ)*-PRF where*

$$\epsilon = \epsilon_{ecf} + \epsilon_{pcf} + (2q + q^3/2^n)\epsilon_{euniv} + \frac{18(\ell+2)^3 q^3}{2^{2n}} + \rho_{bad}.$$

Proof. We again prove the theorem using Coefficient-H Technique. Likewise the proof of Theorem 7, we identify three steps of the technique and combine them altogether to obtain the result.

(A) Bound the probability of Bad view. We will use the same defintion of Bad view as used in Definition 3. Recall that the set of bad views $\mathcal{V}_{bad} = \{t : \exists i, \ \ t_i = 0\} \cup \{t : t \text{ has 3-collision}\}$ observed by $\mathcal{A}$ and for any random function Γ, $\rho_{bad} := \mathsf{Pr}[\tau(\mathcal{A}^{\Gamma}) \in \mathcal{V}_{bad}] \leq \frac{q}{2^n} + \frac{q^3}{2^{2n}}$ (from Eqn. 4)

(B) High Interpolation Probability for Good View. We fix any $t \in \mathcal{V}_{good}$ and a q-tuple m of distinct messages. We write $\mathcal{H}^{\pi}(m_i) = (\Sigma_i, \Theta_i)$, $1 \leq i \leq q$.

(B.1) Identify Good Internal Transcript. Similar to proof of Theorem 7 (the two keyed constructions), we define $\mathcal{T} = \{((\sigma_i, \theta_i)_{i \in [q]}, (w_j)_{j \in I_{new}}) : w_{I_{new}} \longleftrightarrow \psi_{I_{new}}\}$ be the set of all internal transcripts. Given any such tuple from $\mathcal{T}$, we first define $w_i = y_{j,a}$ for all $i \in I_{old}$ with $\psi_i = x_{j,a}$. So we have defined w_I. Now we define $w'_i = w_i + t_i$, for all $i \in I$.

Definition 7. *We say that a tuple* $((x, y), w_{I_{new}}) \in \mathcal{T}$ ***good*** *if followings happen:*

1. $E_1 \equiv (x, y)$ *is extended-cover-free,*
2. $E_2 \equiv$ *whenever* $t_i = t_j$, $\sigma_i \neq \sigma_j$ *and* $\theta_i \neq \theta_j$,
3. $E_3 \equiv (x, \psi_I, \psi'_I) \longleftrightarrow (y, w_I, w'_I)$.

Thus, for a good tuple all permutation compatible input output values arise. Now we categorize different possibilities of not being good. We have already defined extended cover-free of (x, y). Now we define two more possibilities.

Definition 8. 1. *We say that a tuple* (x, y) *is* **pseudo-covered** *if it satisfies either type-1 or type-2 pseudo-covered equations given in the Table 1.*
2. *We say that a tuple* $((x, y), w_{I_{new}}) \in \mathcal{T}$ *is mix-covered if one of equations of mixed-covered in Table 2 satisfies.*

Now state that these newly defined bad events are actually equivalent to not being good tuple as defined before. The verification of this statement is more or less straightforward. We basically, need to consider all possible collisions of inputs and outputs.

Lemma 7. *A tuple* $((x,y),w_{I_{new}}) \in \mathcal{T}$ *is bad if and only if* (x,y) *is extended covered or pseudo-covered or t-collision or* $((x,y),w_{I_{new}})$ *is mix-covered.*

Let us fix a good tuple $((x,y),w_{I_{new}})$ as defined in Definition 7. We denote the event

$$E(x,y,w) \;\equiv\; \tau(\mathcal{A}\rightarrow\mathcal{H}^{\Pi})=(x,y), \Pi(\Psi_i)=w_i \forall i \in I_{new}).$$

It is easy to see that given E the interpolation event $m_I \xmapsto{\mathcal{C}_1} t_I$ is same as $\psi'_I \xmapsto{\Pi} w'_I$. Also observe that $\psi'_I \in \mathsf{dist}$ and (ii) $\psi'_I \cap (x,\psi_I)=\phi$ where $s=|I|$. So we can proceed exactly similar to the proof of the Theorem 7.

(B.2) High Interpolation Probability for good Internal Transcript. We have

$$\begin{aligned}\mathsf{Pr}[m_I \xmapsto{\mathcal{C}_1} t_I \mid E] &= \mathsf{Pr}[\psi'_I \xmapsto{\Pi} w'_I \mid E]\\ &= \mathsf{Pr}[\psi'_I \xmapsto{\Pi} w'_I \mid (x,\psi_I) \xmapsto{\Pi} (y,w_I)].\\ &\geq \frac{1}{2^{ns}} \quad \text{As, } (\psi'_I,\psi_I) \longleftrightarrow (w'_I,w_I), \psi'_I \cap (x,\psi_I)=\phi, \psi'_I \in \mathsf{dist}.\end{aligned}$$

Using the above result, we find the following conditional probability

$$\begin{aligned}\mathsf{Pr}[m \xmapsto{\mathcal{C}_1} t \mid E] &= \mathsf{Pr}[m_{I^c} \xmapsto{\mathcal{C}_2} t_{I^c} \mid E \wedge m_I \xmapsto{\mathcal{C}_1} t_I] \times \mathsf{Pr}[m_I \xmapsto{\mathcal{C}_1} t_I \mid E]\\ &\geq \mathsf{Pr}[(\sigma_i,\theta_i)_{i\in I^c} \xmapsto{\mathsf{sum}^{\Pi}} t_{I^c} \mid (x,\psi_I,\psi'_I) \xmapsto{\Pi} (y,w_I,w'_I)] \times \frac{1}{2^{ns}}\\ &\geq 2^{-nq} \times (1-18(\ell+2)^3q^3/2^{2n}) \quad \text{[From Theorem 4 with } q \leq s \text{].}\end{aligned}$$

Now, we find our desired interpolation probability as we sum over all good tuples for $\epsilon = \mathsf{Pr}[(X,Y)_{i\in[q]}, (\Pi(\Psi_j))_{j\in I}$ is not good]:

$$\mathsf{Pr}[m \xmapsto{\mathcal{C}_1} t] \;\geq\; \sum_E \mathsf{Pr}[m \xmapsto{\mathcal{C}_1} t \mid E] \times \mathsf{Pr}[E] \;\geq\; \frac{(1-18(\ell+2)^3q^3/2^{2n})}{2^{nq}} \times (1-\epsilon) \tag{7}$$

(B.3) Bounding ϵ : Probability of Bad Internal Transcript. By using the equivalent definition of good tuple (as described in lemma 7) and using the union bound, we have $\epsilon = \epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4$ where ϵ_i's are described and bounded as below.

(a) $\epsilon_1 = \mathsf{Pr}[(x,y)$ is extended-covered$] \leq \epsilon_{\text{ecf}}$.
(b) $\epsilon_2 = \sum_{i\neq j: t_i=t_j} (\mathsf{Pr}[\Sigma_i=\Sigma_j] + \mathsf{Pr}[\Theta_i=\Theta_j]) \leq 2q\epsilon_{\text{univ}}$.
(c) $\epsilon_3 = \mathsf{Pr}[(x,y)$ is pseudo-covered$] \leq \epsilon_{\text{pcf}}$.
(d) $\epsilon_4 = \mathsf{Pr}[(x,y)$ is mix-covered$] \leq \frac{q^3}{2^n} \times \epsilon_{\text{univ}}$.

To bound ϵ_4 we use the similar observation that the bad equations are combination of an event defined by (X,Y) only and an event related to the output of $\Pi(\psi')$ where ψ' is new.

Summing these four error terms, we obtain an upper bound of $\epsilon \leq \epsilon_{ecf}+\epsilon_{pcf}+(2q+\frac{q^3}{2^n})\epsilon_{univ}$. Plugging it in into Equation (7), we obtain

$$\mathsf{Pr}[m \xmapsto{\mathcal{C}_1} t] \;\geq\; \epsilon_{ecf}+\epsilon_{pcf}+(2q+\frac{q^3}{2^n})\epsilon_{univ}+\frac{18(\ell+2)^3q^3}{2^{2n}} \tag{8}$$

(C) Summing up all the Results. The proof completes as we apply Patarin's Coefficient Technique by putting Eqn. 4 and Eqn. 8 in Theorem 1.

5 A Generic Bound for ϵ_{ecf}, ϵ_{pcf} and ϵ_{univ} using Rank and Accident

Road Map. We consider block cipher-based constructions in affine mode and show that all intermediate outputs of the computation of one or more messages can be viewed as a conditional WOR sampling, that are not independent. To analyze these samples, we introduce the notion of *almost independent sampling*. All the bad cases can then be viewed as restrictions on these linear equations obtained from the affine mode analysis, thereby forming a reduced set of equations. We also use the idea of accidents as in [7, 25] and represent the total rank of the linear system as the sum of accidents and the rank of the reduced system. This formulation gives a tool to bound the different types of cover-free advantage corresponding to the bad cases described in the last section.

5.1 Almost Independent Sampling

WR sampling is an independent sampling, but WOR is not. But they share common features in terms of conditional entropy. In particular, the conditional distribution of i^{th} sample has high entropy when i is not very close to total population size. We formally define it by almost-independence.

Definition 9. *$(X_1, \ldots, X_q)$ is called* **ϵ-almost-independent** *if for all $t_1, \ldots, t_q$, and i, the conditional probability $\mathsf{Pr}[X_i = t_i \mid X_1 = t_1, \ldots, X_{i-1} = t_{i-1}] \leq \epsilon$.*

If $(X_1, \ldots, X_q) \xleftarrow{\text{wr}} S$ then $(X_1, \ldots, X_q)$ is also $|S|^{-1}$-almost-independent. Similarly, if $(X_1, \ldots, X_q) \xleftarrow{\text{wor}} S$ then $(X_1, \ldots, X_q)$ is also $(|S|-q)^{-1}$-almost-independent. Now we consider a different example of almost-independent random variables obtained by conditioning WR samples.

Lemma 8. *Let $X_1, \ldots, X_q$ is ϵ-almost-independent over $GF(2^n)$, and let L_1, ..., L_r be r linearly independent equations with q variables over the finite field $GF(2^n)$. Then, for any constants $c_1, \ldots, c_r \in GF(2^n)$, we have*

$$\mathsf{Pr}[L_i(X_1, \ldots, X_q) = c_i, 1 \leq i \leq q] \leq \epsilon^r. \tag{9}$$

5.1.1 Conditional WOR Sampling. We consider a variant of WOR sampling, called **conditional WOR sampling**. This sampling scheme is motivated from the affine mode. Let A_i be an affine equation over $GF(2^n)$ with $i-1$ variables, $1 \leq i \leq \ell$. The samples $Y = (Y_1, \ldots, Y_\ell)$ and $X = (X_1, \ldots, X_\ell)$ are defined recursively as follows:

- $X_i = A_i(Y_1, \ldots, Y_{i-1})$ and

- $Y_i = \begin{cases} Y_j & \text{if for some } j < i, X_i = X_j; \\ \xleftarrow{\$} \{0,1\}^n \setminus \{Y_j : 1 \le j < i\} & \text{otherwise.} \end{cases}$

Definitely Y_i's are not almost-independent as $Y_i = Y_j$ for some conditional choices of $Y_1, \ldots, Y_{i-1}$. So we now identify a set of (random) indices I for which Y_i's behave almost-independently for all $i \in I$. But, this I is a random set and so we will consider the conditional distribution of $Y_I := (Y_i)_{i \in I}$ given I (more precisely given an equivalence relation $\sim$ which uniquely determines I). Then, this conditional distribution would behave almost-independently.

Definition 10. *Let $Y = (Y_1, \ldots, Y_\ell)$ be an A-conditional WOR ℓ-sample. We define an (induced) equivalence relation $\sim_Y$ on $[\ell]$ as $i \sim j$ if and only if $A_i(Y) = A_j(Y)$ (and hence $Y_i = Y_j$). We say that an equivalence relation $\sim$ is* **realizable** *if $\mathsf{Pr}[\sim_Y = \sim] > 0$.*

Proposition 1. *Let $\sim$ be a realizable equivalence relation and let I be the corresponding indices as defined above. Then, the conditional distribution of $Y_I \mid \sim_Y = \sim$ is $(2^n - \ell^2)^{-1}$-almost-independence.*

5.2 Conditional WOR sample vs. Block cipher based Construction

Let $\mathcal{C}$ be an affine construction meaning that the intermediate inputs X (the inputs of the block cipher) is an affine function of previous intermediate outputs Y and message blocks. Then, all intermediate outputs of the computation of one or more messages can be viewed as a conditional WOR sampling for a suitable choices of affine functions. We can similarly define accident of a permutation for a tuple of messages.

For any pair (m, π) of q-tuple of distinct messages and a permutation, we associate the following objects:

1. equivalence relation $\sim$ (which is same as the **structure graph** in case of CBC construction) [7] on intermediate outputs Y with s many classes,
2. accident $a := \mathsf{acc}^m(\pi)$, as defined in [7, 25], representing the number of linearly independent restrictions and
3. and a set of indices $I \subset \{J_1, \ldots, J_s\}$ be the set of free variables of size $s - a$ such that Y_I is $(2^n - (\sigma')^2)$-almost-independent where σ' is the total number of message blocks.

For a detailed discussion on affine system and the above notions, please refer to Appendix D.

Lemma 9 ([25]). *For any realizable equivalence relation $\sim$ with accident a $\mathsf{Pr}[\sim_Y = \sim] \le \frac{1}{(2^n - \ell)^a}$. The number of realizable equivalence relation with accident a is at most $\binom{s}{2}^a$.*

We skip the proof of bounding the number of realizable equivalence relations with accident a. Informally, to each an a accident realizable relation, we would be able to uniquely identify a basis of a linear equations (there are several choices of basis, but a special way of selecting basis will ensure the uniqueness of the choice). Since each equation can be chosen at most $\binom{s}{2}$ ways, the number of ways we can choose a special basis is at most $\binom{s}{2}^a$.

Definition 11. *A permutation is* **not allowed** *or* **bad** *w.r.t. a q-tuple of distinct messages $m := (m_1, \ldots, m_q)$, if*

1. *for all i, $\mathsf{acc}^{m_i}(\pi) \geq 1$,*
2. *for all i, j, k, $\mathsf{acc}^{m_i,m_j,m_k}(\pi) \geq 2$ and*
3. *for all i, j, k, l, $\mathsf{acc}^{m_i,m_j,m_k,m_l}(\pi) \geq 3$.*

Lemma 10. *Probability that a random permutation is bad for a tuple of q messages is at most*

$$\frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}} + \frac{q^3\ell^6}{2^{3n}}.$$

Now onwards, we make our analysis for allowed permutation. Note that a permutation is allowed for a q-tuple of messages if and only if for all distinct i, j, k; π is also allowed for (m_i, m_j, m_k).

5.3 PRF Bound of Single-Key Hash-then-Sum Construction through rank analysis

Lemma 11. *If $\mathcal{C}$ is $(\epsilon, 3)$-extended-cover-free, then $\mathcal{C}$ is $(\binom{q}{3}\epsilon, q)$-cover-free; if $\mathcal{C}$ is $(\epsilon, 3)$-pseudo-cover-free-1, then $\mathcal{C}$ is $(\binom{q}{3}\epsilon, q)$-pseudo-cover-free-1; and if if $\mathcal{C}$ is $(\epsilon, 4)$-pseudo-cover-free-2, then $\mathcal{C}$ is $(\binom{q}{4}\epsilon, q)$-pseudo-cover-free-2.*

Applying this result to Theorem 8, it would be sufficient to bound, extended-cover-free for three messages and pseudo-cover-free advantages for three and four messages. However, for some constructions, we may not be able to obtain desired bound. So **we need to consider allowed or good permutations**.

Given, a set of affine equations $\mathcal{L}$ and an equivalence relation $\sim$, we define the extended-rank of the pair $(\mathcal{L}(Y), \sim)$ as $\mathsf{acc}(\sim) + rank(\mathcal{L}'(Y_I))$, where rank of a linear system means the rank of the corresponding coefficient matrix and $\mathcal{L}'(Y_I)$ is the reduced form of the equation $\mathcal{L}(Y)$ after applying equivalence relation and the a many restrictions induced by the accidents. Let $\{\mathcal{L}_{ij}\}$ be a set of systems of linear equations. Note that, $\mathcal{L}_{ij}$ is a system of linear equations. Now we identify the set of systems of linear equations which are actually obtained from different bad cases for three messages $m := (m_1, m_2, m_3)$ as shown in Table 1.

Let N_{ij}^r denote the number of pairs of the form $(\sim, \mathcal{L}_{ij})$ such that $\sim$ is allowed and the extended-rank of the pair is r. Then, we have the following general bound for any sum-based construction.

Theorem 9. *For the construction $\mathcal{C}_1$,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathcal{C}_1}(q,\ell) \leq \frac{18(\ell+2)^3q^3}{2^{2n}} + q^3(\epsilon'_{ecf} + \epsilon'_{pcf1}) + q^4\epsilon'_{pcf2} + \left(2q + \frac{q^3}{2^n}\right)\epsilon^g_{euniv} + \left(\frac{q}{2^n} + \frac{q^3}{2^{2n}}\right) + (\frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}} + \frac{q^3\ell^6}{2^{3n}}).$$

where $\epsilon'_{ecf} := \sum_{j=1}^{4}\sum_{r=0}^{4}\frac{N^r_{1j}}{2^{nr}}, \epsilon'_{pcf1} := \sum_{j=1}^{2}\sum_{r=0}^{4}\frac{N^r_{2j}}{2^{nr}}, \epsilon'_{pcf2} := \sum_{j=1}^{3}\sum_{r=0}^{5}\frac{N^r_{3j}}{2^{nr}}$ *and* $\epsilon^g_{euniv} := \sum_{j=1}^{5}\sum_{r=0}^{2}\frac{N^r_{5j}}{2^{nr}}$.

Proof. Let $m = (m_1, m_2, m_3)$ be a 3-tuple of distinct messages and $t = (t_1, t_2, t_3) \notin \mathcal{V}_{bad}$. Let us consider A denotes the event $[(x, y)$ is extended-covered]. Similarly B, C and D denote the event $[\mathcal{H}^{\Pi}_i$'s are ϵ-universal], $[(x, y)$ is pseudo-covered] and $[(x, y)$ is mix-covered] respectively.
Now, recall the proof of Theorem 8 in which $\epsilon = \epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4$ where $\epsilon_1 = \mathsf{Pr}[A]$, $\epsilon_2 = \mathsf{Pr}[B]$, $\epsilon_3 = \mathsf{Pr}[C]$ and $\epsilon_4 = \mathsf{Pr}[D]$. Therefore, $\epsilon_1 \leq \mathsf{Pr}[A|\Pi$ is good] + $\mathsf{Pr}[\Pi$ is bad $], \epsilon_2 \leq \mathsf{Pr}[B|\Pi$ is good] + $\mathsf{Pr}[\Pi$ is bad $], \epsilon_3 \leq \mathsf{Pr}[C|\Pi$ is good] + $\mathsf{Pr}[\Pi$ is bad $], \epsilon_4 \leq \mathsf{Pr}[D|\Pi$ is good] + $\mathsf{Pr}[\Pi$ is bad].
Now we define ϵ^g_{ecf} to be the maximum *extended-cover free* advantage when Π is randomly sampled from set of good permutations. Similalrly, we define ϵ^g_{pcf} to be the maximum *pseudo-cover-free* advantage and ϵ^g_{euniv} to be the maximum *extended-universal* advantage when Π is randomly sampled from set of good permutations. Moreover, $\epsilon^g_{pcf} = \epsilon^g_{pcf1} + \epsilon^g_{pcf2}$. Therefore, $\epsilon \leq \epsilon^g_{ecf} + \epsilon^g_{pcf1} + \epsilon^g_{pcf2} + (2q + \frac{q^3}{2^n})\epsilon^g_{euniv} + \mathsf{Pr}[\Pi$ is bad]. Thus,

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathcal{C}_1}(q,\ell) \leq \epsilon^g_{ecf} + \epsilon^g_{pcf1} + \epsilon^g_{pcf2} + (2q + q\frac{q^3}{2^n})\epsilon^g_{euniv} + \mathsf{Pr}[\Pi \text{ is bad }] + \frac{18(\ell+2)^3q^3}{2^{2n}} + (\frac{q}{2^n} + \frac{q^3}{2^{2n}}). \quad (10)$$

Now, $\mathsf{Pr}[\Pi$ is bad] can be upper-bounded by Lemma 10. By Lemma 11, $\epsilon^g_{ecf} \leq q^3\epsilon'_{ecf}$, $\epsilon^g_{pcf1} \leq q^3\epsilon'_{pcf1}$, $\epsilon^g_{pcf2} \leq q^4\epsilon'_{pcf2}$ where, according to the Definition 6, Lemma 11 and Table 1, it is easy to check that the following holds:
(a) $\epsilon'_{ecf} \leq \sum_{j=1}^{4}\sum_{r=0}^{4}\frac{N^r_{1j}}{2^{nr}}$, (b) $\epsilon'_{pcf1} \leq \sum_{j=1}^{2}\sum_{r=0}^{4}\frac{N^r_{2j}}{2^{nr}}$, (c) $\epsilon^g_{euniv} \leq \sum_{j=1}^{2}\sum_{r=0}^{2}\frac{N^r_{5j}}{2^{nr}}$.
Moreover, if $m = (m_1, m_2, m_3, m_4)$ be a 4-tuple of distinct messages and $t = (t_1, t_2, t_3, t_4) \notin \mathcal{V}_{bad}$ then from Definition 6, Lemma 11 and from Table 1, one can easily check that $\epsilon_{pcf2} \leq \sum_{j=1}^{3}\sum_{r=0}^{5}\frac{N^r_{3j}}{2^{nr}}$. Therefore plugging the bound of $\epsilon'_{ecf}, \epsilon'_{pcf1}, \epsilon'_{pcf2}$ and ϵ^g_{euniv} in Equation (10) we obtain the result. □

6 New Proposals for BBB Secure One Key MAC

We introduce here the construction of two separate MACs. One is 1kf9 MAC and another is 1k_PMAC+, both of the constructions require a single key K. For simplicity we assume that all messages have size multiple of n. Otherwise, we

can apply an injective padding rule to make it multiple of n. For example, we define the padded message $\overline{M} \leftarrow M\|10^d$ where d is the smallest non-negative integer such that $|M| + 1 + d$ is multiple of n. Note that the PRF advantage of the construction after applying any injective function does not change. So we implicitly assume this padding rule and we denote message M by $(M_1, \ldots, M_l)$ where $M_i \in \{0,1\}^n$ for all $1 \leq i \leq l$. We propose two constructions 1kf9 and 1k_PMAC+ (see Fig. 6.1) which are simple variants of one key versions of 3kf9 and PMAC_Plus respectively.

Algorithm 1kf9(K, M)	**Algorithm** 1k_PMAC+(K, M)
1. $Z \leftarrow Y_0 \leftarrow E_K(0^n)$	1. $\Delta_i \leftarrow E_K(\mathrm{Cst}_i)$ for $i = 1, 2$
2. for $j = 1$ to l	2. for $j = 1$ to l
3. $\quad X_j = Y_{j-1} \oplus M_j$	3. $\quad X_j = M_j \oplus 2^{j-1}\Delta_1 \oplus 2^{2(j-1)}\Delta_2$
4. $\quad Y_j = E_K(X_j)$	4. $\quad Y_j = E_K(X_j)$
5. $\quad Z = (Z \oplus Y_j)$	5. $\Sigma^{'} = Y_1 \oplus Y_2 \oplus \ldots \oplus Y_l$;
6. $\Sigma^{'} = 2Y_l$, $\Theta^{'} = 2Z$;	6. $\Theta^{'} = 2^l \cdot Y_1 \oplus 2^{l-1} \cdot Y_2 \oplus \ldots \oplus 2 \cdot Y_l$;
7. $\Sigma = \mathsf{fix0}(\Sigma^{'})$; $\Theta = \mathsf{fix1}(\Theta^{'})$	7. $\Sigma = \mathsf{fix0}(\Sigma^{'})$, $\Theta = \mathsf{fix1}(\Theta^{'})$;
8. $T \leftarrow E_K(\Sigma) \oplus E_K(\Theta)$	8. $T \leftarrow E_K(\Sigma) \oplus E_K(\Theta)$
9. **return** T	9. **return** T

Fig. 6.1. Algorithm of our proposed 1-key block cipher based BBB Secure MAC.

6.1 PRF Security Analysis of 1kf9 and 1k_PMAC+

In this section we analyze the security of our proposed construction 1kf9 and 1k_PMAC+. Mainly we prove the following theorem.

Theorem 10. *For any q-tuple of message $m := (m_1, m_2, \ldots, m_q)$ such that the maximum number of message blocks is ℓ. Then*

$$\mathbf{Adv}^{\mathrm{prf}}_{1kf9}(q, \ell, t) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(q, \ell, t') + O(q^3\ell^3/2^{2n} + q^3\ell^4/2^{2n} + q^4\ell^4/2^{3n} + q^4\ell^6/2^{4n}) + \left(2q + \frac{q^3}{2^n}\right)\frac{\ell^3}{2^n} + \left(\frac{q}{2^n} + \frac{q^3}{2^{2n}}\right) + \left(\frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}} + \frac{q^3\ell^6}{2^{3n}}\right).$$

where $t' = t + O(q\ell)$.

Proof. Proof of this theorem directly follows from Theorem 9 and Table 2. Note that, from Table 2 we obtain $\epsilon_{ecf} = O(\frac{q^3\ell^4}{2^{2n}})$, $\epsilon_{pcf1} = O(\frac{q^3\ell^4}{2^{2n}})$, $\epsilon_{pcf2} = O(\frac{q^4\ell^4}{2^{3n}} + \frac{q^4\ell^6}{2^{4n}})$, $\epsilon_{euniv} \leq \frac{\ell^3}{2^n}$. Similarly one can see the rest of the terms. Moreover, according to Lemma 10, probability of not allowed permutation is $\frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}} + \frac{q^3\ell^6}{2^{3n}}$. Therefore combining altogether, we obtain the result. □

$\mathcal{L}_{ij}$		$\#acc(\sim)$	N^r_{ij}	r	$N^r_{ij}/2^{nr}$
Extended Cover	$\Sigma_i = \Sigma_j, \Theta_i = \Theta_k$	0	2	2	
		1	l^2	2	$\frac{l^2}{2^{2n}}$
	$\Sigma_i = \Sigma_j, \Theta_i = X_k$	0	l	2	
		1	l^3	2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = \Theta_k$	0	l	2	
		1	l^3	2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = X_k$	0	l^2	2	
		1	l^4	2	$\frac{l^4}{2^{2n}}$
Extended Universal Hash	$\Sigma_i = \Sigma_j$	0	2	1	
		1	l^2	1	$\frac{l^2}{2^n}$
	$\Sigma_i = X_j$	0	l	1	
		1	l^3	1	$\frac{l^3}{2^n}$
	$\Theta_i = X_k$	0	l	1	
		1	l^3	1	$\frac{l^3}{2^n}$
	$\Theta_i = \Theta_k$	0	2	1	
		1	l^2	1	$\frac{l^2}{2^n}$
Pseudo Cover Type-I	$\Sigma_i = X_j, Y_j + t_i = Y_k$	0	$9l^2$	2	
		1	l^4	2	$\frac{l^4}{2^{2n}}$
	$\Theta_i = X_j, Y_j + t_i = Y_k$	0	$9l^2$	2	
		1	l^4	2	$\frac{l^4}{2^{2n}}$
Pseudo Cover Type-II	$\Sigma_i = X_e, \Sigma_j = X_f, Y_e + Y_f = t_i + t_j$	0	l^2	3	
		1	l^4	3	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$
		2	l^6	4	
	$\Sigma_i = X_e, \Theta_j = X_f, Y_e + Y_f = t_i + t_j$	0	l^2	3	
		1	l^4	3	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$
		2	l^6	4	
	$\Theta_i = X_e, \Theta_j = X_f, Y_e + Y_f = t_i + t_j$	0	l^2	3	
		1	l^4	3	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$
		2	l^6	4	

Table 2. Table of bad equations of 1kf9 with no. of choice and ranks corresponding to accidents 0, 1 and 2 of Extended Cover, Extended-Universal Hash, Pseudo-Cover Type-I and Pseudo-Cover Type-II. Details of the calculations can be found in Appendix E.

Theorem 11. *For any q-tuple of message $m := (m_1, m_2, \ldots, m_q)$ such that the maximum number of message blocks is ℓ. Then*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathit{1k\_PMAC+}}(q, \ell, t) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(q, \ell, t') + O(q^3\ell^3/2^{2n} + q^3\ell^4/2^{2n} + q^4\ell^4/2^{3n}) + \left(2q + \frac{q^3}{2^n}\right)\frac{\ell^3}{2^n} + \left(\frac{q}{2^n} + \frac{q^3}{2^{2n}}\right) + \left(\frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}\right).$$

where $t' = t + O(q\ell)$.

Proof. Proof of the theorem goes in the same line as that of Theorem 10 except that (i) probability of not allowed permutation is $\frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}$ as (a) we do not allow any accident within a single message and (b) number of accident at least 2 in a pair of messages and (ii) we refer to Table 3. for proving the theorem. □

6.2 Comparison wih Existing Constructions

Here we compare our results with the existing related constructions.

$\mathcal{L}_{ij}$		$\#acc(\sim)$	N_{ij}^r	r	$N_{ij}^r/2^{nr}$
Extended Cover	$\Sigma_i = \Sigma_j, \Theta_i = \Theta_k$	0	2	2	
		1	l^2	2	$\frac{l^2}{2^{2n}}$
	$\Sigma_i = \Sigma_j, \Theta_i = X_k$	0	l	2	
		1	l^3	2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = \Sigma_j, \Theta_i = \mathrm{Cst}_{j2}$	0	l	2	
		1	l^2	2	$\frac{l^2}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = \Theta_k$	0	l	2	
		1	l^3	2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = X_k$	0	l^2	2	
		1	l^4	2	$\frac{l^4}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = \mathrm{Cst}_{j2}$	0	l^2	2	
		1	l^3	2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = \mathrm{Cst}_{j1}, \Theta_i = \Theta_k$	0	l	2	
		1	l^2	2	$\frac{l^2}{2^{2n}}$
	$\Sigma_i = \mathrm{Cst}_{j1}, \Theta_i = X_k$	0	l^2	2	
		1	l^3	2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = \mathrm{Cst}_{j1}, \Theta_i = \mathrm{Cst}_{j2}$	0	l^2	2	
		1	l^2	2	$\frac{l^2}{2^{2n}}$
Extended Universal Hash	$\Sigma_i = \Sigma_j \;/\; \Theta_i = \Theta_k$	0	2	1	
		1	l^2	1	$\frac{l^2}{2^n}$
	$\Sigma_i = X_j \;/\; \Theta_i = X_k$	0	l	1	
		1	l^3	1	$\frac{l^3}{2^n}$
	$\Sigma_i = \mathrm{Cst}_a \;/\; \Theta_i = \mathrm{Cst}_b$	0	1	1	
		1	l^2	1	$\frac{l^2}{2^n}$
Pseudo Cover Type-I	$\Sigma_i = X_j, Y_j + t_i = Y_k$	0	l^2	2	
		1	l^4	2	$\frac{l^4}{2^{2n}}$
	$\Theta_i = X_j, Y_j + t_i = Y_k$	0	l^2	2	
		1	l^4	2	$\frac{l^4}{2^{2n}}$

$\mathcal{L}_{ij}$	$\#acc(\sim)$	N_{ij}^r	r	$N_{ij}^r/2^{nr}$
$\Sigma_i = X_{k,a}, \Sigma_j = X_{l,b}$, $Y_{k,a} + Y_{l,b} = t_i + t_j$	0	l^2	3	
	1	l^4	3	$\frac{l^4}{2^{3n}}$
$\Sigma_i = \mathrm{Cst}_a, \Sigma_j = X_{l,b}$, $\Delta_a + Y_{l,b} = t_i + t_j$	0	l	3	
	1	l^3	3	$\frac{l^3}{2^{3n}}$
$\Sigma_i = \mathrm{Cst}_a, \Sigma_j = \mathrm{Cst}_b$, $\Delta_a + \Delta_b = t_i + t_j$	0	1	3	
	1	l^2	3	$\frac{l^2}{2^{3n}}$
$\Theta_i = X_{k,a}, \Theta_j = X_{l,b}$, $Y_{k,a} + Y_{l,b} = t_i + t_j$	0	l^2	3	
	1	l^4	3	$\frac{l^4}{2^{3n}}$
$\Theta_i = \mathrm{Cst}_a, \Theta_j = X_{l,b}$, $\Delta_a + Y_{l,b} = t_i + t_j$	0	l	3	
	1	l^3	3	$\frac{l^3}{2^{3n}}$
$\Theta_i = \mathrm{Cst}_a, \Theta_j = \mathrm{Cst}_b$, $\Delta_a + \Delta_b = t_i + t_j$	0	1	3	
	1	l^2	3	$\frac{l^2}{2^{3n}}$
$\Sigma_i = X_{k,a}, \Theta_j = X_{l,b}$, $Y_{k,a} + Y_{l,b} = t_i + t_j$	0	l^2	3	
	1	l^4	3	$\frac{l^4}{2^{3n}}$
$\Sigma_i = \mathrm{Cst}_a, \Theta_j = X_{l,b}$, $\Delta_a + Y_{l,b} = t_i + t_j$	0	l	3	
	1	l^3	3	$\frac{l^3}{2^{3n}}$
$\Sigma_i = X_{k,a}, \Theta_j = \mathrm{Cst}_b$, $Y_{k,a} + \Delta_b = t_i + t_j$	0	l	3	
	1	l^3	3	$\frac{l^3}{2^{3n}}$
$\Sigma_i = \mathrm{Cst}_a, \Theta_j = \mathrm{Cst}_b$, $\Delta_a + \Delta_b = t_i + t_j$	0	1	3	
	1	l^2	3	$\frac{l^2}{2^{3n}}$

Table 3. Table of bad equations of 1k_PMAC+ with no. of choice and ranks corresponding to (a) accidents 0, 1 of Extended Cover, Extended-Universal Hash and Pseudo-Cover Type-I [left] and (b) accidents 0, 1 and 2 of Pseudo-Cover Type-II [right]. Details of the calculations can be found in Appendix F.

Construction	Reference	No. Keys	Security Bound
Sum of ECBC	[33]	4-Keys	$O(l^3q^3/2^{2n})$
PMAC_Plus	[34]	3-keys	$O(l^3q^3/2^{2n} + lq/2^n)$
3kf9	[35]	3-keys	$O(l^3q^3/2^{2n} + lq/2^n)$
1kf9	This Paper	1-key	$O(ql^2/2^n + q^3l^4/2^{2n} + q^4l^4/2^{3n} + q^4l^6/2^{4n})$
1k_PMAC+	This Paper	1-key	$O(ql^2/2^n + q^3l^4/2^{2n} + q^4l^4/2^{3n})$

7 Conclusion

With the fast developments of computing power, birthday attacks gradually become practical threats to cryptographic algorithms, and this is especially serious for modes of operation on small-size block ciphers. Compared with the passive ways that just enlarge the sizes of internal states and outputs, designing beyond-birthday-bound schemes is active and promising.

We successfully unify the three independent keys in the current beyond-birthday-bound MAC modes in this paper, by developing several theorems that

can reduce the security of three/two/one-key such constructions to some properties on internal structures and PRP assumption on block ciphers. Our developed tools are also useful to simplify the analysis for other modes of operations, which is of independent interests.

References

1. TS 35.206, 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification.
2. *FSE 2010, Revised Selected Papers*, volume 6147 of *LNCS*. Springer, 2010.
3. *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *LNCS*. Springer, 2012.
4. Mihir Bellare, Oded Goldreich, and Hugo Krawczyk. Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier. In *CRYPTO '99*, volume 1666 of *LNCS*, pages 270–287. Springer, 1999.
5. Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. *IACR Cryptology ePrint Archive*, 1999:24, 1999.
6. 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.
7. Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC macs. In *CRYPTO 2005*, volume 3621 of *LNCS*, pages 527–545. Springer, 2005.
8. John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 384–397. Springer, 2002.
9. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings* [3], pages 208–225.
10. Yevgeniy Dodis and John P. Steinberger. Domain extension for macs beyond the birthday barrier. In *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 323–342. Springer, 2011.
11. David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu. On tweaking luby-rackoff blockciphers. In *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 342–356. Springer, 2007.
12. Tetsu Iwata and Kaoru Kurosawa. OMAC: one-key CBC MAC. In *Fast Software Encryption, 2003*, volume 2887 of *LNCS*, pages 129–153. Springer, 2003.
13. Éliane Jaulmes, Antoine Joux, and Frédéric Valette. On the security of randomized CBC-MAC beyond the birthday paradox limit: A new construction. In *Fast Software Encryption, 2002*, volume 2365 of *LNCS*, pages 237–251. Springer, 2002.
14. Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In *ASIACRYPT 2014*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.

15. Kaoru Kurosawa and Tetsu Iwata. TMAC: two-key CBC MAC. *IEICE Transactions*, 87-A(1):46–52, 2004.
16. Rodolphe Lampe and Yannick Seurin. Tweakable blockciphers with asymptotically optimal security. In *FSE 2013*, volume 8424 of *LNCS*, pages 133–151. Springer, 2013.
17. Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In *CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.
18. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In *CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.
19. Stefan Lucks. The sum of prps is a secure PRF. In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 470–484. Springer, 2000.
20. David McGrew. Authenticated encryption in practice. Invited talkl at DIAC, 2012. http://hyperelliptic.org/DIAC/.
21. Bart Mennink. Optimally secure tweakable blockciphers. Cryptology ePrint Archive, Report 2015/363, 2015. http://eprint.iacr.org/.
22. Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In *FSE*, volume 5665 of *LNCS*, pages 308–326. Springer, 2009.
23. Kazuhiko Minematsu. How to thwart birthday attacks against macs via small randomness. In *Fast Software Encryption, 2010* [2], pages 230–249.
24. Atsushi Mitsuda and Tetsu Iwata. Tweakable pseudorandom permutation from generalized feistel structure. In *ProvSec 2008*, volume 5324 of *LNCS*, pages 22–37. Springer, 2008.
25. Mridul Nandi. A unified method for improving PRF bounds for a class of blockcipher based macs. In *Fast Software Encryption* [2], pages 212–229.
26. Jacques Patarin. About feistel schemes with six (or more) rounds. In *Fast Software Encryption*, volume 1372 of *LNCS*, pages 103–121. Springer, 1998.
27. Jacques Patarin. The "coefficients h" technique. In *Selected Areas in Cryptography, 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.
28. Jacques Patarin. A proof of security in $o(2^n)$ for the benes scheme. In *AFRICACRYPT*, volume 5023 of *LNCS*, pages 209–220. Springer, 2008.
29. Jacques Patarin. A proof of security in $o(2^n)$ for the xor of two random permutations. In *ICITS 2008*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008.
30. Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.
31. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.
32. Serge Vaudenay. Decorrelation: A theory for block cipher security. *J. Cryptology*, 16(4):249–286, 2003.
33. Kan Yasuda. The sum of CBC macs is a secure PRF. In *CT-RSA 2010*, volume 5985 of *LNCS*, pages 366–381. Springer, 2010.
34. Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In *CRYPTO 2011*, volume 6841 of *LNCS*, pages 596–609. Springer, 2011.
35. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In *ASIACRYPT 2012* [3], pages 296–312.
36. Yusi Zhang. Using an error-correction code for fast, beyond-birthday-bound authentication. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 291–307. Springer, 2015.

Supplementary Materials

Appendix A: Coefficient H Techniques

Lemma 3 (coefficient H-technique for random variables) Let X, Y be two random variables over S such that $X \succ_\epsilon Y$ over $\mathcal{V}_{\text{good}} \subseteq S$ then,

$$\Delta(X\ ;\ Y) \leq \epsilon + \mathsf{Pr}[Y \notin \mathcal{V}_{\text{good}}].$$

Proof. Let $T \subseteq S$. Then, $X \succ_\epsilon Y$ over $\mathcal{V}_{\text{good}}$ implies that

$$\mathsf{Pr}[Y \in \mathcal{V}_{\text{good}} \cap T] - \mathsf{Pr}[X \in \mathcal{V}_{\text{good}} \cap T] \leq \epsilon \times \mathsf{Pr}[Y \in \mathcal{V}_{\text{good}} \cap T] \leq \epsilon.$$

So,

$$\begin{aligned}\mathsf{Pr}[Y \in T] - \mathsf{Pr}[X \in T] &\leq \epsilon + (\mathsf{Pr}[Y \in T \setminus \mathcal{V}_{\text{good}}] - \mathsf{Pr}[X \in T \setminus \mathcal{V}_{\text{good}}]) \\ &\leq \epsilon + \mathsf{Pr}[Y \notin \mathcal{V}_{\text{good}}]\end{aligned}$$

Hence the result follows. □

Theorem 1 (coefficient H-technique for random functions) Let $\mathtt{F}$ and $\mathtt{G}$ be two random functions. Let $\mathcal{V}_{good} \subseteq \mathcal{X}^q \times \mathcal{Y}^q$. If

1. $\forall\ m = (m_1, \ldots, m_q) \in \mathsf{dist}_q$, $(\mathtt{F}(m_i))_i \succ_{\epsilon_1} (\mathtt{G}(m_i))_i$ over $\mathcal{V}_{good}$ and
2. $\mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{G}) \notin \mathcal{V}_{good}] \leq \epsilon_2$,

then $\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathtt{G}) \leq \epsilon_1 + \epsilon_2$.

Proof. W.l.o.g. we can assume that $\mathcal{A}$ is deterministic. Let V denote the set of all views for which $\mathcal{A}$ returns 1. Condition (i) says that, for all $v \in V_{good}$, $\mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{G}) = v] - \mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{F}) = v] \leq \epsilon_1.\mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{F}) = v]$ and hence $\sum_{v \in V_{good}} (\mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{G}) = v] - \mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{F}) = v]) \leq \epsilon_1$. Now,

$$\begin{aligned}\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathtt{G}) = \mathsf{Pr}[\mathcal{A}^{\mathtt{G}} = 1] - \mathsf{Pr}[\mathcal{A}^{\mathtt{F}} = 1] &= \sum_{v \in V} (\mathsf{Pr}[\tau(\mathcal{A}^{\mathtt{G}}) = v] - \mathsf{Pr}[\tau(\mathcal{A}^{\mathtt{F}}) = v]) \\ &\leq \sum_{v \in V \bigcap V_{good}} (\mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{G}) = v] - \mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{F}) = v]) \\ &\quad + \sum_{v \notin V_{good}} \mathsf{Pr}[\tau(\mathcal{A} \to \mathtt{G}) = v] \leq\ \epsilon_1 + \epsilon_2 \qquad \square\end{aligned}$$

Appendix B: Figures of Our Constructions

Appendix C: Proof of Theorem 6

Theorem 6 Let $F_{K_1,K_2} := g_{K_2} \circ \mathcal{H}_{K_1} : \{0,1\}^* \to \{0,1\}^n$. Then,

$$\mathbf{Adv}^{\text{prf}}_{F}(q, \ell, t) \leq \mathbf{Adv}^{\text{prf}}_{g}(q, \ell, t') + \binom{q}{2} \times \mathbf{Adv}^{\text{univ}}_{\mathcal{H}}(\ell),$$

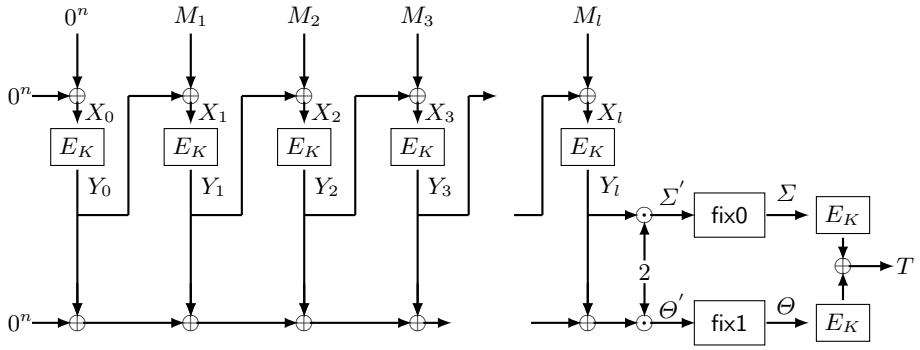

Fig. 7.1. Construction of 1kf9-MAC

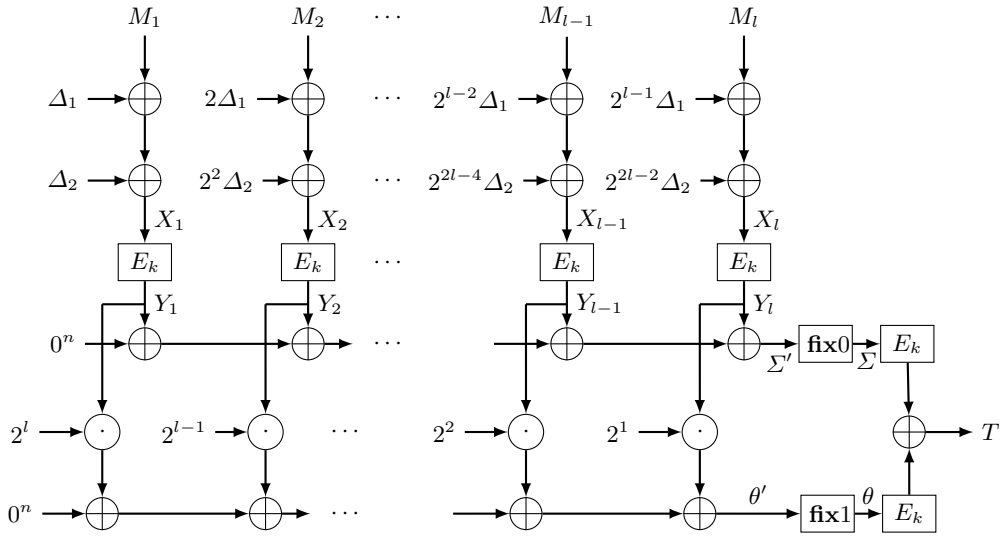

Fig. 7.2. Construction of 1Key PMAC+

where $t' = t + \mathcal{O}(qT_\ell)$ and T_ℓ denotes the maximum time for computing $\mathcal{H}(m)$ for any m with maximum number of blocks ℓ.

Proof. By using standard reduction argument, we can consider the composition function $\mathit{\Gamma}_n \circ \mathcal{H}_{K_1}$ at the cost of $\mathbf{Adv}_g^{\mathrm{prf}}(q, \ell, t')$. Now, for any q-tuple $m = (m_1, \ldots, m_q)$ of distinct messages, we denote $\mathcal{H}_{K_1}(m_i) = X_i$. For all $t = (t_1, \ldots, t_q) \in (\{0,1\}^n)^q$, the interpolation probability

$$\begin{aligned}
\mathsf{Pr}_{\mathit{\Gamma}_n, K_1}[m \overset{\mathit{\Gamma}_n \circ \mathcal{H}_{K_1}}{\longmapsto} t] &\geq \sum_{x \in \mathsf{dist}_q} \mathsf{Pr}[x \overset{\mathit{\Gamma}_n}{\longmapsto} t \mid X = x] \times \mathsf{Pr}[X = x] \\
&= 2^{-nq} \times \mathsf{Pr}[X \in \mathsf{dist}_q] \;\; (\mathsf{Pr}[x \overset{\mathit{\Gamma}_n}{\longmapsto} t \mid X = x] = 2^{-nq}) \\
&\geq 2^{-nq} \times (1 - \sum_{1 \leq i < j \leq q} \mathsf{Pr}[X_i = X_j]) \\
&\geq 2^{-nq} \times (1 - \binom{q}{2} \mathbf{Adv}_{\mathcal{H}}^{\mathrm{univ}}(\ell)). \qquad \square
\end{aligned}$$

Appendix D: Block Cipher in Affine Mode, Rank and Accident

Linear Equations and Rank. A linear equation $L_1(X_1, \ldots, X_s) := L_{1,1} \cdot X_1 + \cdots + L_{1,s} \cdot X_s$ over the finite field $\mathbb{F}_{2^n}$[9] of size 2^n with s variables can be identified as an s-tuple $(L_{1,1}, \ldots, L_{1,s})$. Let $\mathcal{L} = \{L_1, \ldots, L_q\}$ be a q-set of linear equations with s-variable, then $\mathcal{L}$ can be viewed as an $q \times s$ matrix $\mathbf{L} := ((L_{i,j}))_{i,j}$ where $L_{i,j}$ is the j^{th} coefficient of L_i. $\mathsf{rank}(\mathcal{L})$ denotes the rank of the matrix $\mathbf{L}$.

Reducing Linear Equations By Eliminating Dependent Variables. Let L be a s-variable linear equation over $\mathbb{F}_{2^n}$. Then, given any equivalence relation $\sim$ over $[s]$ one can reduce the equation L by eliminating dependent variables assuming that the variables induces the collision relation $\sim$. For example let $L = X_1 + aX_2 + X_3 + bX_4 + cX_5$ for some constant a, b, c and let $\sim$ be an equivalence relation on [5] corresponding to the partition $\{\{1,3,4\},\{2,5\}\}$. If $X := (X_1, X_2, X_3, X_4, X_5)$ induces $\sim$ then $X_1 = X_3 = X_4$ and $X_2 = X_5$. So, by eliminating X_3, X_4, X_5, the equation $L(X)$ can be simplified to $bX_1 + (a+c)X_2$. Note that the choice of free and determined variables are not unique and as a matter of fact we keep the minimum indexed variables (w.r.t some natural order). Let $\sim$ have c classes and $I = \{i_1, \ldots, i_c\}$ be the set consisting of all minimum elements from each c classes. The X_I is a tuple of **free** variables and the rest of the variables can be uniquely determined from X_I. After eliminating the determined variables, the simplified (also called reduced) equation would be denoted by $L^{\sim}(X_I)$. Note that

$$\text{for all } x, \quad \sim_x = \sim \;\; \Rightarrow \;\; L^{\sim}(x_I) = L(x). \tag{11}$$

[9] We implicitly fixed a primitive polynomial through which the multiplication is defined. In this paper, the whole analysis is independent of the choice of the polynomial and so we do not explicitly specify it.

In addition to these equalities, we also have some inequalities since x_I should be element-wise distinct. We can also reduce when the restrictions among variables are some general linear equations instead of equality or collision relation (which is also a special form of linear equations). Let $\mathcal{R}$ be a set of linear equations over s-tuple of variables X and $L(X)$ be the target linear equation which is going to be reduced by applying the restriction $\mathcal{R}$. We can then similarly reduce the equation L by eliminating the dependent variables with free variables of $\mathcal{R}$ after applying the linear restrictions $\mathcal{R}$. Let X_I be the free variables in $\mathcal{R}$ which determine the rest of the variables.[10] Note that $|I| = s - \mathsf{rank}(\mathcal{R})$. Then by applying the linear dependencies of X_{I^c} on X_I, we can reduce $L(X)$ to an equation of the form $L^{\mathcal{R}}(X_I)$. We similarly have, $\forall L' \in \mathcal{R}, L'(x) = 0 \Rightarrow L^{\mathcal{R}}(x_I) = L(x)$.

Conditional WOR Sampling in Affine Mode. During the computation of permutation based affine mode, the intermediate outputs forms a conditional WOR sample. Informally, depending on the previous sample values, a conditional WOR sampling scheme either makes a fresh WOR sample or it choose one of the specific previous values. Clearly, it can not be almost-independent as the sample values can be same as the previous values. Later we identify a (random) subset of the sample which would constitute an almost independent random variables.

Let A_i be an affine equation over $GF(2^n)$ with $i-1$ variables, $1 \le i \le \ell$. The samples $Y = (Y_1, \ldots, Y_\ell)$ and $X = (X_1, \ldots, X_\ell)$ are defined recursively as follows:

- $X_i = A_i(Y_1, \ldots, Y_{i-1})$ and
- $Y_i = \begin{cases} Y_j & \text{if for some } j < i, X_i = X_j; \\ \xleftarrow{\$} \{0,1\}^n \setminus \{Y_j : 1 \le j < i\} & \text{otherwise.} \end{cases}$

Clearly Y_i's are not almost-independent as $Y_i = Y_j$ for some conditional choices of $Y_1, \ldots, Y_{i-1}$. So we now identify a set of (random) indices I for which Y_i's behave almost-independently for all $i \in I$. But, this I is a random set and so we will consider the conditional distribution of $Y_I := (Y_i)_{i \in I}$ given I (more precisely given an equivalence relation $\sim$ which uniquely determines I). Then, this conditional distribution would behave almost-independently. The details are given below.

Let $Y = (Y_1, \ldots, Y_\ell)$ be an A-conditional WOR ℓ-sample. We define an (induced) equivalence relation $\sim_Y$ on $[\ell]$ as $i \sim j$ if and only if $A_i(Y) = A_j(Y)$ (and hence $Y_i = Y_j$. We say that an equivalence relation $\sim$ is **realizable** if $\mathsf{Pr}[\sim_Y = \sim] > 0$.

Let $J := (J_1, \ldots, J_s)$ be the first indices at which X_i-values (i.e., A_i values) are fresh. In other words, these are the minimum value for the equivalence classes and hence J_i's are uniquely determined from $\sim$. Note that $J_1 = 1$. Moreover, X_i can be expressed as some affine function, denoted $\overline{A}_i$, over Y_{J_i}'s. In other words, $\overline{A}_i(Y_J) = A_i(Y)$ for all i. Now, consider the following set of linear equations

$$\overline{A}_i(Y_{J_1}, \ldots, Y_{J_s}) = \overline{A}_j(Y_{J_1}, \ldots, Y_{J_s}), \quad \forall i \sim j.$$

[10] Like collision relation, choice of I is not unique. However, we implicitly fix a choice.

These conditions restrict the values of Y_{J_i}'s.

Definition 12 (accident [7, 25]). *Let $\sim$ be a realizable equivalence relation. We define accident of $\sim$, denoted $\mathsf{acc}(\sim)$, the rank of the set of linear equations:*

$$\overline{A}_i(Y_{J_1}, \ldots, Y_{J_s}) = \overline{A}_j(Y_{J_1}, \ldots, Y_{J_s}), \quad \forall i \sim j.$$

Let $I \subset \{J_1, \ldots, J_s\}$ be the set of free variables of size $s - a$, which appear first, such that Y_{I_j}'s will determine rest of the Y values. We call I to be the set of free indices associated with $\sim$.

Appendix E: Rank Analysis of 1kf9

Revisiting Structure Graph [7]

In this section we revisit the structure graph introduced by Bellare et.al in [7]. We recall that given a q-tuple of distinct messages m and a permutation π, the transcript $\tau(\mathcal{H} \to \pi) = (x, y)$ represents the set of all inputs and outputs of π. Here the function $\mathcal{H}$ is nothing but CBC^{π}. We write $x = (x_{i,j})_{(i,j)\in\mathcal{I}}$ and similarly for y where $\mathcal{I} := \{(i, j) : i \in [q], j \in [L_i]\}$. We have defined an equivalence relation $\sim_y$ over $\mathcal{I}$. Let us assume that the permutation π does not map to 0, i.e., $y_{i,j} \neq 0$ for all i, j. Let $\{V_1, \ldots, V_s\}$ be the set of all partitions of $\mathcal{I}$ induced by $\sim_y$. So V_i is a subset of $\mathcal{I}$ whose elements are related to each other by the relation $\sim$. We define a vertex set $V = \{V_0, V_1, \ldots, V_s\}$. We give an edge from V_0 to V_b if there exists $(i, 1) \in V_b$. We also put an edge label $m_{i,1}$, the first block of the i^{th} message. Similarly, we give an edge from V_a to V_b if there exists $(i, j) \in V_a$ and $(i, j + 1) \in V_b$ and we put an edge label $m_{i,j+1}$. We write a labeled edge as $V \xrightarrow{m} V'$. It is straightforward to see that the graph is well defined. We call this labeled graph **structure graph** and denoted $G^{\pi}(m)$. For each message m_i, we can consider the walk starting from V_0 to V_a for some a, following the edge labels $m_{i,1}, \ldots, m_{i,\ell_i}$ one by one. We denote the walk by W_i^{π} or simply W_i. Note that the structure graph G would be the union of all walks W_i, $1 \leq i \leq q$.

A node V is said to be a collision node (or true collision) in a structure graph G if the in-degree of the node is at least two. The number of true collision is defined to be the the sum $TC(G) := \sum_{i=1}^{s}(indeg(V_i) - 1)$.

Definition 13. *A collection of edges $C = \{V_{i_1} \to V_{i_2}, V_{i_3} \to V_{i_2}, \ldots, V_{i_{2k}} \to V_{i_1}\}$ in a structure graph G is called an* **alternating cycle** *(AC) where $k \geq 2$.*

We provide an equivalent definition of the number of accidents of a structure graph as defined in [7].

Definition 14. *Let $G_0 := G$ be a structure graph. Now we do the following steps until we find an alternating cycle. For $i \geq 1$, we define $G_i = G_{i-1} \setminus e$ where e is a labeled edge of an alternating cycle in G_{i-1}. Let G_t be the final graph (may not be unique as it depends on the choice of the edges from the AC which are removed. The number of accidents of the graph G_0 is defined to be the number of true collision of G_t.*

One can check that this definition is well defined. In other words, the number of true collision for the final graphs is independent of the choice of the edges removed. We denote the number of accidents and true collision of a structure graph $G^{\pi}(m)$ by $acc^{\pi}(m)$ and $TC^{\pi}(m)$ respectively.

Characterization of Valid Structure Graphs with 3 and 4 Messages

Definition 15. *A Structure Graph G is said to be a Valid Structure Graph, if it meets the following three conditions : (i) $|Acc(G)| \leq 2$, (ii) No accident within a message m_i, (iii) At most one accident within three messages m_i, m_j, m_k.*

Important Properties of Valid Structure Graphs for 3 Messages

Lemma 12. *A valid structure graph with* 3 *messages cannot contain an alternating cycle of length* 4*.*

Proof. Let us consider an alternating cycle $Cycl$ of length at least 4. Let $E_{alt} := \{(AB), (AD), (CD), (CB)\}$ be the set of edges of $Cycl$ as shown in Fig. 7.3. Now we make the following two important observations :

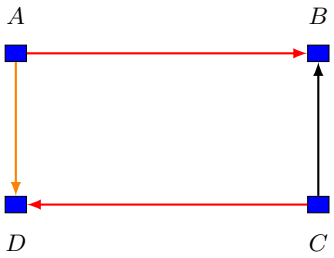

Fig. 7.3. Alternating cycle of length 4

(i) As we have three messages, at least one message covers two edges from E_{alt}.

Without loss of generality let m_i be the message that covers two edges.

(ii) The covered edges will be parallel, otherwise there will be an accident within the walk of m_i.

W.l.o.g, let the covered edges of m_i be (AB) and (CD). Let m_j covers consider the message which covers the edge (CB). W.l.o.g, let it be m_j. Now to cover that edge, m_j could come to node C in either of the two ways :

(a) m_j follows the walk of m_i and reaches to C

(b) m_j does not follow the walk of m_i.

For case (a) when m_j covers the edge (CB), then there will be an accident within the walk of m_j. For case (b) when m_j covers the edge (CB) then m_i, m_j will collide twice and hence the number of accident in (m_i, m_j) pair will be 2. As, in both the cases the condition for a valid structure graph is violated, the result follows. □

Lemma 13. *A valid structure graph with* 3 *messages cannot contain an alternating cycle of length* 6*.*

Proof. Let $Cycl_6$ be an alternating cycle of length 6 in the valid structure graph G with 3 messages. Let m_1 be the message taking part in two collision points say C_1 and C_2. Now consider other messages (say m_2 and m_3) taking part in these collisions, i.e. $C_1 = coll(m_1, m_2)$, $C_2 = coll(m_1, m_3)$. Now it is easy to see that there are 2 accidents in m_1, m_2 and m_3 that violates the validity of a structure graph. Hence no valid graph is possible with 6-alternating cycle. □

Important Properties of Valid Structure Graphs for 4 Messages

Claim 1 *For any* 4*-length alternating cycle in a valid structure graph with* 4 *messages, the 4 edges must come from distinct messages*

Proof. If not, then 3 distinct messages cover 4 edges of the 4-length alternating cycle. But according to Lemma 12, a valid structure graph with 3 messages cannot contain a 4-length alternating cycle. □

Lemma 14. *A valid structure graph with* 4 *messages cannot contain a* 4*-length alternating cycle with number of accidents* 2*.*

Proof. Due to Claim 1 without loss of generality, we can assume that the edges AB, AD, CB and CD of an alternating cycle belong to messages m_1, m_2, m_3, m_4 respectively, where m_1 and m_3 have an accident at B and m_2 and m_4 meet at B to close the alt-cycle with an induced collision. Now, if there is a second accident, it cannot involve any one of m_1 or m_3, otherwise it will violate condition 2 (#acc at most one with any 3 messages). Thus, the second accident, if any, must involve m_2 and m_4. But again this is not allowed, since m_2 and m_4 has already collided at B. □

Lemma 15. *A valid structure graph with* 4 *messages cannot contain multiple alternating cycle of length* 4*.*

Proof. Due to Claim 1, without loss of generality, we can assume that the edges AB, AD, CB and CD of an alternating cycle belong to messages m_1, m_2, m_3, m_4 respectively. Now, if another 4-alternating cycle exists, Claim 1 must hold for this second cycle as well. This implies that two edges (from two different messages) must be shared between the two cycles.The shared edges may be any one of the 4 pairs from AB, AD, CB and CD. Case a) Pairs that do not have a common node from A, B, C, D, i.e., pair (AB, CD) or pair (AD, BC): Then the other two edges of the second cycle will add two more accidents, one in node B and

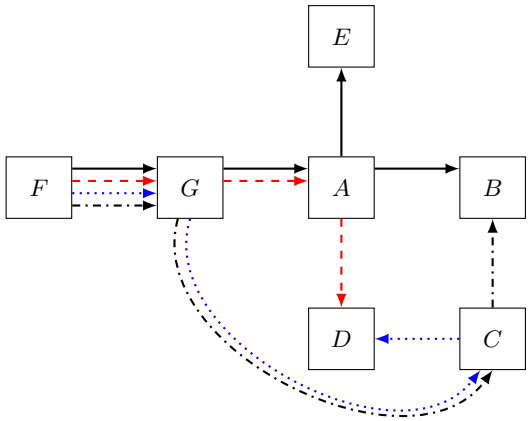

Fig. 7.4. Multiple Alternating Cycle with 4 messages.

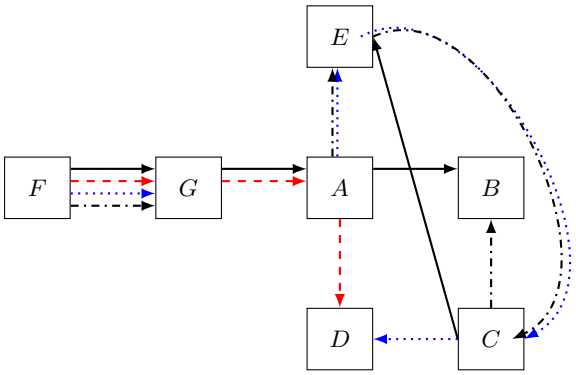

Fig. 7.5. Multiple Alternating Cycle with 4 messages.

Msg contain AE	Conclusion
m_1	loop in m_1 at node A
m_2	loop in m_2 at node A
m_3	$\#acc = 2$ in m_1 and m_3
m_4	$\#acc = 2$ in m_2 and m_4

Table 4. Impossibilities of any message covers edge AE corresponding to Fig. 7.4.

another in node C, violating condition 3. Case b) Pairs that have a common node. In this case, two possible graphs are possible, as shown in the Fig. 7.4 and Fig. 7.5 Note that, the other two edges must meet at a fifth node E which cannot be realized with distinct 4 messages (refer to Table 5 and 6). □

Msg contain CE	Conclusion
m_1	$\#acc = 2$ in m_1 and m_3
m_2	$\#acc = 2$ in m_1 and m_4
m_3	loop in m_1 at node C
m_4	loop in m_4 at node A

Table 5. Impossibilities of any message covers edge CE corresponding to Fig. 7.5.

Lemma 16. *A valid structure graph with* 4 *messages cannot contain an alternating cycle of length* 6*.*

Proof. Let $Cycl_6$ be the alternating cycle of length 6 in the valid structure graph G with 4 messages. As there are 3 accident points C_1, C_2, C_3 in $Cycl_6$, there will be at least one message say m_1 taking part in two collision points say C_1 and C_2. Now consider other messages (say m_2 and m_3) taking part in these collisions, i.e. $C_1 = coll(m_1, m_2)$, $C_2 = coll(m_1, m_3)$. Now it is easy to see that there are 2 accidents in m_1, m_2 and m_3 that violates the validity of a structure graph. Hence no valid graph is possible with 6-length alternating cycle. □

List of Valid Structure Graphs with 3 and 4 messages Given all the properties, now we list down all the possible structure graphs with 3 and 4 messages as follows:

(I) Acc = 0 for 3 **messages**: As no accident is present, the only possible structure graph has the following structure depicted in Fig. 7.6:

(II) Acc = 1 for 3 **messages**: From Lemma 12, we observe that, there can be no valid graph 4-length alternating cycles. So we consider structure graphs where number of true-collision is 1 and the graph is shown in Fig 7.7.

(III) Acc = 0 for 4 **messages** As no accident is present, the only possible

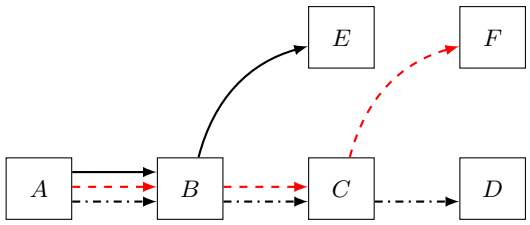

Fig. 7.6. Structure graph of 3 messages with $Acc = 0$

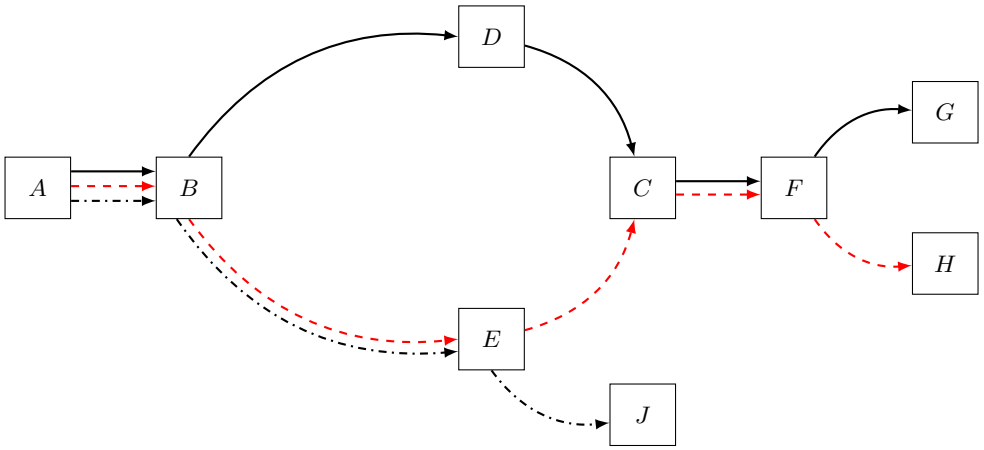

Fig. 7.7. Structure graph of 3 messages with $Acc = 1$ (at node C)

structure graph has the following structure depicted in Fig. 7.8:

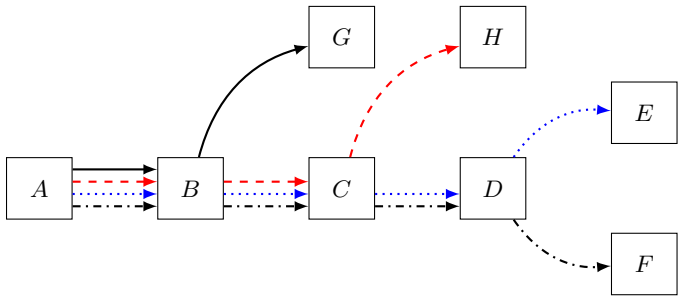

Fig. 7.8. Structure graph of 4 messages with $Acc = 0$

(IV) Acc = 1 for 4 **messages**: We can have two types of graph in this case:

- 1 accident with 1 collision point: This graph is shown in Fig. 7.9 .
- Graph with 1-alternating cycle: This graph is shown in Fig. 7.10 .

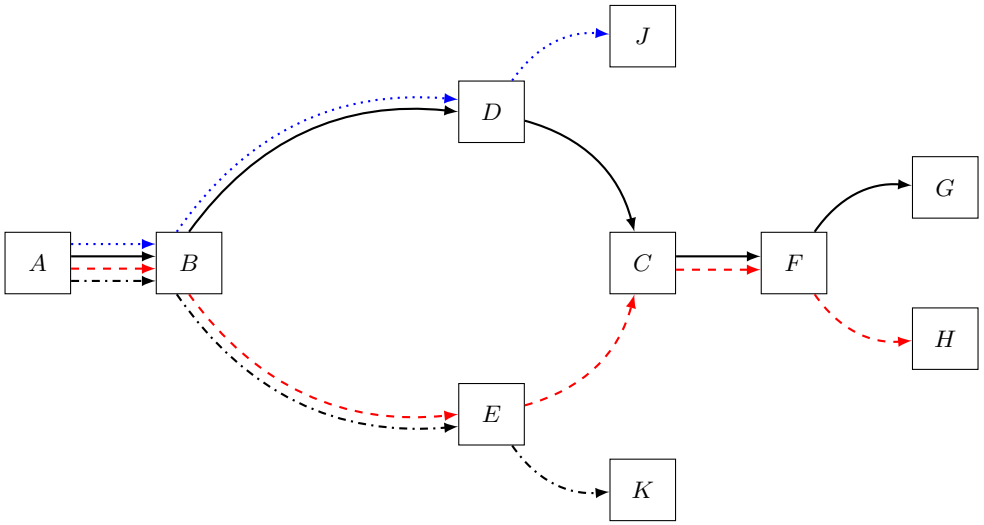

Fig. 7.9. Structure graph of 4 messages with $Acc = 1$ (at node C)

(V) Acc = 2 for 4 **messages**: From Lemma 14 and 16, we observe that, there can be no valid graphs with alternating 4-cycle or alternating 6 cycle.

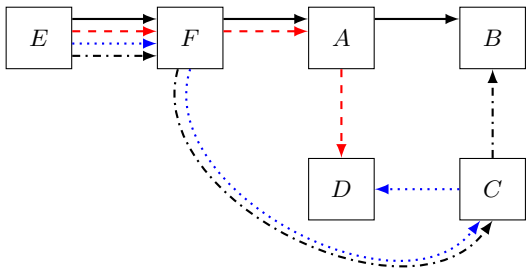

Fig. 7.10. Structure graph of 4 messages with $Acc = 1$ (at node B) and an induced collision (at node D)

Hence there is only one possible structure graph - with one accident C_1 occuring between two messages (say m_1 and m_2) and the other accident C_2 occuring for the remaining messages (here m_3 and m_4). This graph also satisfy the condition: (m_1, m_2) and (m_3, m_4) doesn't meet after collision C_1 and C_2 respectively as depicted in Fig. 7.11.

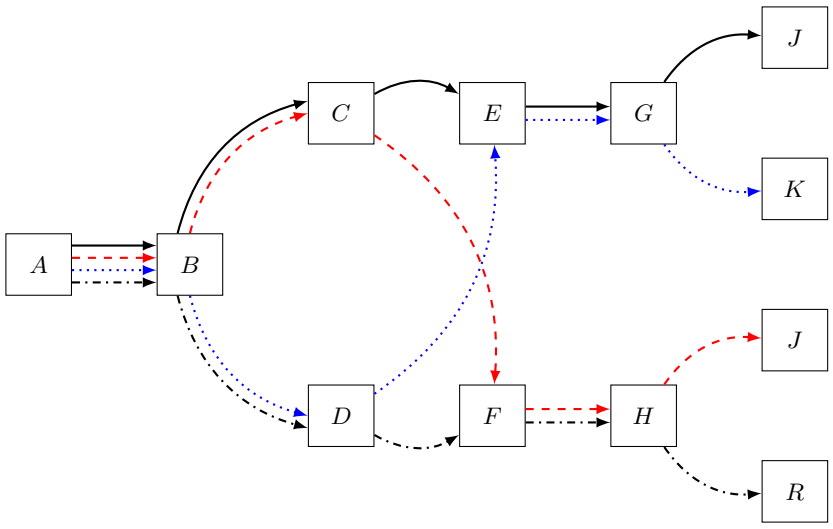

Fig. 7.11. Structure graph of 4 messages with $Acc = 2$ (at nodes E and F)

Rank Analysis of Systems of Equations for Bad Cases

Case (A) : Rank Analysis of Extended Covered Bad Equations

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = \Sigma_j, \Theta_i = \Theta_k)$ for $Acc = 0$ and $Acc = 1$.
Case (a) When $Acc = 0$, then $\Sigma_i = \Sigma_j$ implies $\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = O^{n-1}1$. Let us aussme that p is the length of the longest common prefix of M_i and M_k and wihput loss of generality $l_i > l_k$. Therefore, we have following equations:

$$\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = 0^{n-1}1 \tag{12}$$
$$Y_{i,p+1} + \ldots Y_{i,l_i} + Y_{k,p+1} + \ldots Y_{k,l_j} = 0 \tag{13}$$

Now it is to be noted that, if m_k is a prefix of m_i, then $Y_{i,p+1} + \ldots Y_{i,l_i}$ contains at least 3 variables. Therefore, Y_{j,l_j} could be equal to one of these three variables, and other two variables will remain free. In that case we will identify one such variable $Y_{i,s}$ which is not equal to Y_{j,l_j} and choose Y_{i,l_i}. If m_k is not a prefix of m_i then $Y_{i,p+1} + \ldots Y_{i,l_i} + Y_{k,p+1} + \ldots Y_{k,l_j}$ conatins at least 3 variables and therefore, Y_{j,l_j} could be equal to one of these three variables; we will identify one of the remaining free variable $Y_{i,s}$ which is not equal to Y_{j,l_j} and choose Y_{i,l_i}. Therefore we identify two such variables, one in each equation, giving us rank 2.
Case (b) When $Acc = 1$, we argue that rank of $\mathcal{L}(Y)$ will be 2. For $Acc = 1$, we introduce one more equation

$$Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau} \tag{14}$$

along with Equation (12) and (13). Note that if $Acc = 1$, then $\Sigma_i = \Sigma_j$ implies eiher of the following two cases: (i) $\alpha Y_{i,l_i} = \alpha Y_{j,l_j}$. or (ii) $\alpha Y_{i,l_i} \neq \alpha Y_{j,l_j}$ but $\mathsf{fix0}(\alpha Y_{i,l_i}) = \mathsf{fix0}(\alpha Y_{j,l_j})$. Note that, considering case (i), this is equivalent to considering the equation $Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau}$. According to our assumption p be the last index where m_i and m_k is identical. Therefore, as argued before, $Y_{i,p+1} + \ldots Y_{i,l_i} + Y_{k,p+1} + \ldots Y_{k,l_j}$ contains at least three variables. Now $Y_{j,\gamma}$ could be equal to any one of the three variables; thus we will be left with at least two variable which are free . Let us consider $Y_{i,s} \neq Y_{j,\gamma}$. Therefore we identify two free variables $Y_{i,\beta}$ and $Y_{i,s}$, one in each equation, giving us rank 2. If case (ii) occurs then we consider the Equation (12). In that case $Y_{j,\gamma}$ and Y_{j,l_j} could be equal to any two of the three variables. Then also we will be left with at least one variable $Y_{i,s}$. Therefore, we identify two free variables $Y_{i,\beta}$ and $Y_{i,s}$, one in each equation, such that the rank becomes 2.

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = X_{j,r}, \Theta_i = \Theta_k)$ for $Acc = 0$ and $Acc = 1$.
Case (a): When $\#Acc = 0$, then we argue that rank of $\mathcal{L}(Y)$ is 2. We have the following two equations:

$$\alpha Y_{i,l_i} + Y_{j,r-1} + m_{j,r} = 0 \tag{15}$$
$$Y_{i,p+1} + \ldots Y_{i,l_i} + Y_{k,p+1} + \ldots Y_{k,l_k} = 0 \tag{16}$$

where p is the length of the longest common prefix of m_i and m_k. It is to be noted that there are at least three distinct variables in Equation (16). Now,

we identify Y_{i,l_i} and one of the remaining free variable $Y_{i,s}$ out of above three variables which is distinct from Y_{i,l_i} and $Y_{j,r-1}$, giving us rank 2.

Case (b): When $Acc = 1$, then one additional equation

$$Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau} \tag{17}$$

is introduced. Now if $Y_{i,\beta} \neq Y_{i,l_i}$ and $Y_{j,\gamma} \neq Y_{i,l_i}$, then we identify two variables $Y_{i,\beta}$ and Y_{i,l_i} such that rank of $\mathcal{L}(Y)$ with $Acc = 1$ is 2. If this is not the case, we identify $Y_{i,\beta}$ and $Y_{i,s}$ which is one of the out of three variables in Equation (16), such that the rank becoms 2 again.

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = \Sigma_j, \Theta_i = X_{k,r})$ for $Acc = 0$ and $Acc = 1$

Case (a): Let us first consider that $Acc = 0$. Now we have the following two equations:

$$\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = 0^{n-1}1 \tag{18}$$

$$\alpha(Y_{i,0} + Y_{i,1} + \ldots Y_{i,l_i}) = Y_{k,r-1} + m_{k,r} \tag{19}$$

From Equation (18) and (19), we identify two free variables Y_{i,l_i} and $Y_{i,0}$, giving us rank 2.

Case(b): When $Acc = 1$, then along with Equation (18) and (19), we have an additional equation

$$Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau}.$$

Now, $\Sigma_i = \Sigma_j$ can occur in either of the following ways: (i) $\alpha Y_{i,l_i} = \alpha Y_{j,l_j}$ or (ii) $\alpha Y_{i,l_i} \neq \alpha Y_{j,l_j}$ but $\mathsf{fix0}(\alpha Y_{i,l_i}) = \mathsf{fix0}(\alpha Y_{j,l_j})$. Note that, considering case (i) is equivalent to considering the equation $Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau}$. Therefore we identify two free variables $Y_{i,0}$ and $Y_{i,\beta}$, such that the rank becomes 2. Considering case (ii) is boiling down to considering Equation (18). Therefore, we identify Y_{i,l_i} and $Y_{i,0}$, such that the rank becomes 2 again.

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = X_{j,s}, \Theta_i = X_{k,r})$ for $Acc = 0$ and $Acc = 1$.

Case (a): Let us consider $Acc = 0$. We have the following equations:

$$\alpha Y_{i,l_i} + Y_{j,s-1} = m_{*\mathrm{J},s} \tag{20}$$

$$\alpha(Y_{i,0} + Y_{i,1} + \ldots Y_{i,l_i}) = Y_{k,r-1} + m_{k,r} \tag{21}$$

In this case we identify two free variables $Y_{i,0}$ and Y_{i,l_i}.

Case (b): When $Acc = 1$, we have an additional equation

$$Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau}.$$

Thus, again we can identify two free variables $Y_{i,0}$ and Y_{i,l_i} and the rank does not decrease.

Case (B) : Rank Analysis of Extended-Universal Hash Equations

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = \Sigma_j)$ for $Acc = 0$ and $Acc = 1$.
Case (a): For $Acc = 0$, $\Sigma_i = \Sigma_j$ implies $\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = 0^{n-1}1$. Since Y_{i,l_i} is not trivially equal to Y_{j,l_j}, $\mathcal{L}(Y)$ will have rank 1 for choosing variable Y_{i,l_i}.

Case (b): For $Acc = 1$, $\Sigma_i = \Sigma_j$ implies either (i) $\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = 0^{n-1}1$ or (ii) $\alpha Y_{i,l_i} = \alpha Y_{j,l_j}$ but $\mathsf{fix0}(\alpha Y_{i,l_i}) = \mathsf{fix0}(\alpha Y_{j,l_j})$. Therefore, considering case (ii) boils down to considering the Equation (22) which is induced by the accident.

$$Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau}. \tag{22}$$

Therefore, choosing $Y_{i,\beta}$ gives the rank of $\mathcal{L}(Y)$ to be 1.

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = X_{j,r})$ for $Acc = 0$ and $Acc = 1$.
Case (a): For $Acc = 0$, we choose Y_{i,l_i} such that rank of $\mathcal{L}(Y)$ is 1 as equality of Σ_i and $X_{j,r}$ is not trivial equality.

Case (b): For $Acc = 1$, we introduce the collision relation $Y_{i,\beta} + Y_{j,\gamma} = m_{\delta,\tau}$. Since any accident gives a linearly indpendent equation, therefore we choose $Y_{i,\beta}$ to show the rank of $\mathcal{L}(Y)$ with $Acc = 1$ is 1.

Calculating the rank of $\mathcal{L}(Y) = (\Theta_i = X_{k,r})$ for $Acc = 0$ and $Acc = 1$.
Case (a): For $Acc = 0$, we choose $Y_{i,0}$ such that rank of $\mathcal{L}(Y)$ is 1 as equality of Θ_i and $X_{k,r}$ is not trivial equality.

Case (b): For $Acc = 1$, we introduce the collision relation $Y_{i,\beta} + Y_{k,\gamma} = m_{\delta,\tau}$. Since any accident gives a linearly indpendent equation, therefore we choose $Y_{i,\beta}$ to show the rank of $\mathcal{L}(Y)$ with $Acc = 1$ is 1.

Calculating the rank of $\mathcal{L}(Y) = (\Theta_i = \Theta_k)$ for $Acc = 0$ and $Acc = 1$.
Case (a): Let p be the longest common prefix of m_i and m_j. Therefore, $\Theta_i = \Theta_k$ gives the following equation

$$Y_{i,p+1} + \ldots Y_{i,l_i} + Y_{j,p+1} + \ldots Y_{j,l_j} = 0 \tag{23}$$

Note that there must be at least three distinct variables in Equation (23). Therefore, for $Acc = 0$, we choose any of the three variables $Y_{i,s}$ such that rank of $\mathcal{L}(Y)$ is 1.

Case (b): For $Acc = 1$, we introduce the collision relation $Y_{i,\beta} + Y_{k,\gamma} = m_{\delta,\tau}$. Since any accident gives a linearly indpendent equation, therefore we choose $Y_{i,\beta}$ to show the rank of $\mathcal{L}(Y)$ with $Acc = 1$ is 1.

Case (C) : Rank Analysis of Pseudo Cover-I Bad Equations

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = X_{j,r}, Y_{j,r} + Y_* = t_i)$ for $Acc = 0$ and $Acc = 1$.
Case (a): Let us consider $Acc = 0$. We have the following Equations:

$$\alpha Y_{i,l_i} + Y_{j,r-1} = m_{j,r} \tag{24}$$
$$Y_{j,r} + Y_* = t_i \tag{25}$$

We identify two variables $Y_{j,r}$ and $Y_{j,r-1}$ such that the contribution matrix E becomes non-singular. It is easy to note that $Y_{j,r}$ can never be equal to $Y_{j,r-1}$ as we are not allowing any loop in the structure graph.

Case (b): When $Acc = 1$, we additionally introduce one more equation

$$Y_{i,s} + Y_{j,t} = m_{\delta,\tau}$$

We identify the same two variables $Y_{j,r}$ and $Y_{j,r-1}$ such that one can show the rank of $\mathcal{L}(Y)$ with $Acc = 1$ is 2.

Calculating the rank of $\mathcal{L}(Y) = (\Theta_i = X_{j,r}, Y_{j,r} + Y_* = t_i)$ for $Acc = 0$ and $Acc = 1$.
One can argue the rank of $\mathcal{L}(Y)$ for $Acc = 0$ and $Acc = 1$ is 2 in the same line of argument for the rank analysis of the previous case.

Case (D) : Rank Analysis of Pseudo Cover-II Bad Equations

Calculating the rank of $\mathcal{L}(Y) = (\Sigma_i = X_{k,e}, \Sigma_j = X_{l,f}, Y_{k,e} + Y_{l,f} = t_i + t_j$ for $Acc = 0, 1$ and 2).
Case (a): Let us consider $Acc = 0$. We have the following equations:

$$\alpha Y_{i,l_i} + Y_{k,e-1} = m_{k,e} \tag{26}$$
$$\alpha Y_{j,l_j} + Y_{l,f-1} = m_{l,f} \tag{27}$$
$$Y_{k,e} + Y_{l,f} = t_i + t_j \tag{28}$$

Now we analyse the rank in three cases. Case (i) when $Y_{k,e} \neq Y_{i,l_i}$ and $Y_{k,e} \neq Y_{j,l_j}$ then we identify three variables Y_{i,l_i}, Y_{j,l_j} and $Y_{k,e}$ such that the rank of $\mathcal{L}(Y)$ is 3.

Case (ii) when $Y_{l,f} \neq Y_{i,l_i}$ and $Y_{l,f} \neq Y_{j,l_j}$ then we can identify the variables Y_{i,l_i}, Y_{j,l_j} and $Y_{l,f}$ such that the rank will become 3.

Case (iii) If none of the above two cases occur (i.e., $Y_{i,l_i} = Y_{k,e}$, $Y_{j,l_j} = Y_{l,f}$) then we identify three variables Y_{i,l_i}, Y_{j,l_j} and $Y_{k,e-1}$ such that the rank becomes 3.
Case (b): When $Acc = 1$ we introduce Equation (39) along with the previous three equations.

$$Y_{i,s} + Y_{j,t} = m_{\delta,\tau}. \tag{29}$$

Even if $Y_{i,s}$ or $Y_{j,t}$ is equal to any of the previously chosen free variables, the rank does not decrease.

Case (c): When $Acc = 2$, we introduce an additional equation, namely, Equation (40) as below.

$$Y_{k,s'} + Y_{l,t'} = m_{\delta',\tau'}. \tag{30}$$

According to our assumptions, the second accident must occur between two other messages that were not involved in the first accident. Hence, we can choose an additional free variable and hence the rank becomes 4.

Calculating the rank of $\mathcal{L}(Y) = (\boldsymbol{\Sigma_i = X_{k,e}, \Theta_j = X_{l,f}, Y_{k,e} + Y_{l,f} = t_i + t_j}$ for $\boldsymbol{Acc = 0, 1}$ and 2).

Case (a): Let us consider $Acc = 0$. We have the following Equations:

$$\alpha Y_{i,l_i} + Y_{k,e-1} = m_{k,e} \tag{31}$$

$$\alpha(Y_{j,0} + Y_{j,1} + \ldots + Y_{j,l_j}) + Y_{l,f-1} = m_{l,f} \tag{32}$$

$$Y_{k,e} + Y_{l,f} = t_i + t_j \tag{33}$$

Now we analyse the rank in three cases. Case (i) when $Y_{k,e} \neq Y_{i,l_i}$ and $Y_{k,e} \neq Y_{j,0}$ then we identify three variables $Y_{i,l_i}, Y_{j,0}$ and $Y_{k,e}$ such that the rank of $\mathcal{L}(Y)$ is 3.

Case (ii) when $Y_{l,f} \neq Y_{i,l_i}$ and $Y_{l,f} \neq Y_{j,0}$ then we can identify the variables $Y_{i,l_i}, Y_{j,0}$ and $Y_{l,f}$ such that the rank will become 3.

Case (iii) If none of the above two cases occur (i.e., $Y_{i,l_i} = Y_{k,e}$, $Y_{j,0} = Y_{l,f}$) then we identify three variables $Y_{i,l_i}, Y_{j,0}$ and $Y_{k,e-1}$ such that the rank becomes 3.

Case (b): When $Acc = 1$ we introduce Equation (39) along with the previous three equations.

$$Y_{i,s} + Y_{j,t} = m_{\delta,\tau}. \tag{34}$$

Even if $Y_{i,s}$ or $Y_{j,t}$ is equal to any of the previously chosen free variables, the rank does not decrease.

Case (c): When $Acc = 2$, we introduce an additional equation, namely, Equation (40) as below.

$$Y_{k,s'} + Y_{l,t'} = m_{\delta',\tau'}. \tag{35}$$

According to our assumptions, the second accident must occur between two other messages that were not involved in the first accident. Hence, we can choose an additional free variable and hence the rank becomes 4.

Calculating the rank of $\mathcal{L}(Y) = (\boldsymbol{\Theta_i = X_{k,e}, \Theta_j = X_{l,f}, Y_{k,e} + Y_{l,f} = t_i + t_j}$ for $\boldsymbol{Acc = 0, 1}$ and 2).

Case (a): Let us consider $Acc = 0$. We have the following Equations:

$$\alpha(Y_{i,0} + Y_{i,1} + \ldots + Y_{i,l_i}) + Y_{k,e-1} = m_{k,e} \tag{36}$$

$$\alpha(Y_{j,0} + Y_{j,1} + \ldots + Y_{j,l_j}) + Y_{l,f-1} = m_{l,f} \tag{37}$$

$$Y_{k,e} + Y_{l,f} = t_i + t_j \tag{38}$$

Now we analyse the rank in three cases. Case (i) when $Y_{k,e} \neq Y_{i,l_i}$ and $Y_{k,e} \neq Y_{j,0}$ then we identify three variables $Y_{i,l_i}, Y_{j,0}$ and $Y_{k,e}$ such that the rank of $\mathcal{L}(Y)$ is 3.

Case (ii) when $Y_{l,f} \neq Y_{i,l_i}$ and $Y_{l,f} \neq Y_{j,0}$ then we can identify the variables $Y_{i,l_i}, Y_{j,0}$ and $Y_{l,f}$ such that the rank will become 3.

Case (iii) If none of the above two cases occur (i.e., $Y_{i,l_i} = Y_{k,e}$, $Y_{j,0} = Y_{l,f}$) then we identify three variables $Y_{i,l_i}, Y_{j,0}$ and $Y_{k,e-1}$ such that the rank becomes 3.

Case (b): When $Acc = 1$ we introduce Equation (39) along with the previous three equations.

$$Y_{i,s} + Y_{j,t} = m_{\delta,\tau}. \tag{39}$$

Even if $Y_{i,s}$ or $Y_{j,t}$ is equal to any of the previously chosen free variables, the rank does not decrease.

Case (c): When $Acc = 2$, we introduce an additional equation, namely, Equation (40) as below.

$$Y_{k,s'} + Y_{l,t'} = m_{\delta',\tau'}. \tag{40}$$

According to assumptions, the second accident must occur between two other messages that were not involved in the first accident. Hence, we can choose an additional free variable and hence the rank becomes 4.

Appendix F: Rank Analysis of 1k_PMAC+

Preparation

Taking advantage of Theorem 8, to prove the PRF security of 1k-PMAC_Plus, we need to upper bound its three items, extended-cover-free ϵ_{ecf}, pseudo-cover-free ϵ_{pcf}, and extended universal ϵ_{euniv}. To show they are sufficiently small, we would define some bad cases on inputs to block ciphers. Each bad case is equivalent to a equation set over block cipher outputs as variables. By solving the equations we get an upper bound of permutations over $\{0,1\}^n$ that can induce the bad cases. Then notice that there are totally $2^n!$ permutations, we get the occurrence probability for each bad case.

1. $\exists X_{i,l} \in \{\mathrm{Cst}_1, \mathrm{Cst}_2\}$, for some $i \in [q]$ and $l \in [\ell_i]$. This implies no more than $\sum_{j=1}^{2}\sum_{i=1}^{q}\sum_{l=1}^{\ell_i}$ equations of the form,

$$X_{i,l} = M_{i,l} \oplus 2^{l-1}\Delta_1 \oplus 2^{2l-2}\Delta_2 = \mathrm{Cst}_j.$$

Notice that $\Delta_1 = \pi(\mathrm{Cst}_1)$ and $\Delta_2 = \pi(\mathrm{Cst}_2)$, we have no more than $(2^n-1)!$ permutations satisfying each equation, and totally we have at most $\varsigma_{-1} = \sum_{j=1}^{2}\sum_{i=1}^{q}\sum_{l=1}^{\ell_i}((2^n-1)!)$ permutations over $\{0,1\}^n$. Then, the non-occurrence of this event ensures the Δ_1, Δ_2 values are independent of $Y_{i,l}$ values.

2. $\exists X_{i1,l1} = X_{i2,l2} = X_{i3,l3}$ for some $i1, i2, i3 \in [q]$ and distinct $l1, l2, l3 \in [\ell]$. This implies no more than $\binom{q\ell}{3}$ equations of the form,

$$\begin{bmatrix} 2^{l1-1} \oplus 2^{l2-1}, 2^{2(l1-1)} \oplus 2^{2(l2-1)} \\ 2^{l1-1} \oplus 2^{l3-1}, 2^{2(l1-1)} \oplus 2^{2(l3-1)} \end{bmatrix} \times \begin{bmatrix} \Delta_1 \\ \Delta_2 \end{bmatrix} = \begin{bmatrix} M_{i1,l1} \oplus M_{i2,l2} \\ M_{i1,l1} \oplus M_{i3,l3} \end{bmatrix}.$$

The determinant of its coefficient matrix is $(2^{l1-1} \oplus 2^{l2-1})(2^{l1-1} \oplus 2^{l3-1})$ $(2^{l2-1} \oplus 2^{l3-1}) \neq 0^n$ for any distinct $l1, l2, l3$, so this matrix has rank=2 and we have $(2^n - 2)!$ solutions on Δ_1 and Δ_2 for each equation. Then by this we get at most $\varsigma_0 = \binom{q\ell}{3}((2^n - 2)!) \leq q^3\ell^3/6((2^n - 2)!)$ permutations from $\mathrm{Perm}(n)$.

Based on the above, let us formally upper bound the three items. In each case, we show how to find a rank=2 coefficients matrix.

Upper Bounding extended-cover-free ϵ_{ecf}

According to the definition of extended-cover-freeness, we need to upper bound the probabilities for four linear equations (L_{11}), (L_{12}), (L_{13}), (L_{14}) to occur. By 1kPMAC_Plus definition, we in fact have 9 cases with respect to this, because in the previous inputs to block ciphers, we have both $\Delta_1 = \pi(\mathrm{Cst}_1)$, $\Delta_2 = \pi(\mathrm{Cst}_2)$, and $Y_{i,l} = \pi(X_{i,l})$, as listed in Table. 6.

Table 6. 9 Bad Cases in Upper Bounding ϵ_{ecf}.

$\Sigma_i =$ \ $\Theta_i =$	Cst_{j2}	$X_{j2,l}$	Θ_{j2}
Cst_{j1}	1	2	5
$X_{j1,l}$	3	4	7
Σ_{j1}	6	8	9

1. $\exists \Sigma_i = \mathrm{Cst}_{j1}$ for some $j1 \in [2]$ and $\Theta_i = \mathrm{Cst}_{j2}$ for some $j2 \in [2]$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1 \end{bmatrix} \times [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}]^T = \begin{bmatrix} \mathrm{Cst}_{j1} \\ \mathrm{Cst}_{j2} \end{bmatrix}.$$

Let us analyze in more detail.

(a) If $\ell_i = 1$ and $\mathrm{Cst}_{j2} = 2\mathrm{Cst}_{j1}$. We get only one equation $Y_{i,1} = \mathrm{Cst}_{j1}$, and for q messages, we have at most $\sum_{i=1}^{q}((2^n - 1)!)$ permutations.

(b) Else if $\ell_i = 1$ and $\mathrm{Cst}_{j2} \neq 2\mathrm{Cst}_{j1}$. There is no solution.

(c) Else if $\ell_i \geq 2$, and $\nexists Y_{i,l1} = Y_{i,l2}$ for any distinct $l1, l2 \in [\ell_i]$. Then we have a non-singular submatrix $[1, 1; 2^2, 2^1]$ on the left side. For any values of $Y_{i,l}$ $(l \geq 3)$, we have a unique solution for Y_1^i and Y_2^i. For q messages, we have at most $\sum_{i=1}^{q}\sum_{j1=1}^{2}\sum_{j2=1}^{2}((2^n - 2)!)$ permutations in total.

(d) Else $\ell_i \geq 2$, and $\exists Y_{i,l1} = Y_{i,l2}$ for distinct $l1, l2 \in [\ell_i]$. We have an equation $(2^{l1-1} \oplus 2^{l2-1})\Delta_1 \oplus (2^{2(l1-1)} \oplus 2^{2(l2-1)})\Delta_2 = M^i_{l1} \oplus M^i_{l2}$, and an equation set of the form

$$\begin{bmatrix} 1 \oplus 1, & \cdots \\ 2^{\ell_i - l1+1} \oplus 2^{\ell_i - l2+1}, & \cdots \end{bmatrix} \times [Y_{i,l1}, \cdots]^T = \begin{bmatrix} \mathrm{Cst}_{j1} \\ \mathrm{Cst}_{j2} \end{bmatrix}.$$

Since $2^{\ell_i - l1+1} \oplus 2^{\ell_i - l2+1} \neq 0^n$, for any values of $Y_{i,l}$ ($l \neq l1, l2$), we have at most one value for $Y_{i,l1}$. By the independence of Δ_1, Δ_2 and $Y_{i,l}$. In total we have at most $\sum_{i=1}^{q} \binom{\ell_i}{2} \sum_{j2=1}^{2}((2^n-2)!)$ permutations.

To summarize Case 1, we have at most $\varsigma_1 = (q\ell^2 + q(2^n-1))((2^n-2)!)$ permutations.

2. $\exists \Sigma_i = \mathrm{Cst}_j$ for some $j \in [2]$ and $\Theta_i = X_{u,v}$ for some $u \in [q]$, $v \in [\ell_u]$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 0, & 0 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 2^{v-1}, & 2^{2(v-1)} \end{bmatrix} \times [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, \Delta_1, \Delta_2]^T = \begin{bmatrix} \mathrm{Cst}_j \\ M_{u,v} \end{bmatrix}.$$

By the independence of Δ_1, Δ_2 and $Y_{i,l}$, let us analyze in detail.

(a) If $\nexists Y_{i,l1} = Y_{i,l2}$ for any distinct $l1, l2 \in [\ell_i]$. The coefficient matrix on the left side has a non-singular submatrix $[1, 0; 2^1, 2^{v-1}]$. For q messages, we have at most $\sum_{i=1}^{q}\sum_{l=1}^{\ell_i}\sum_{u=1}^{q}\sum_{v=1}^{\ell_u}\sum_{j=1}^{2}((2^n-2)!)$ permutations.

(b) Else $\exists Y_{i,l1} = Y_{i,l2}$ for distinct $l1, l2 \in [\ell_i]$. Then, we have one equation over Δ_1 and Δ_2 by the 2-collision, and another equation over $Y_{i,l1}$ (with coefficient $2^{\ell_i - l1+1} \oplus 2^{\ell_i - l2+1} \neq 0$), Δ_1 and Δ_2. By their independence, we have at most $\sum_{i=1}^{q} \binom{\ell_i}{2} \sum_{u=1}^{q} \sum_{v=1}^{\ell_u}((2^n-2)!)$ permutations.

To summarize Case 2, we have at most $\varsigma_2 = (2q^2\ell^2 + q^2\ell^3/2)((2^n-2)!)$ permutations.

3. $\exists \Sigma_i = X_{u,v}$ for some $u \in [q]$, $v \in [\ell_u]$ and $\Theta_i = \mathrm{Cst}_j$ for some $j \in [2]$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 2^{v-1}, & 2^{2(v-1)} \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 0 & 0 \end{bmatrix} \times [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, \Delta_1, \Delta_2]^T = \begin{bmatrix} M_{u,v} \\ \mathrm{Cst}_j \end{bmatrix}.$$

The analysis is similar with Case 2, and we have at most $\varsigma_3 = (2q^2\ell^2 + q^3\ell^3)((2^n-2)!)$ permutations.

4. $\exists \Sigma_i = X_{u1,v1}$ and $\Theta_i = X_{u2,v2}$ for some $i, u1, u2 \in [q]$, $v1 \in [\ell_{u1}]$, $v2 \in [\ell_{u2}]$. Then we have an equation set

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 2^{v1-1}, & 2^{2(v1-1)} \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 2^{v2-1}, & 2^{2(v2-1)} \end{bmatrix} \times [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, \Delta_1, \Delta_2]^T = \begin{bmatrix} M_{u1,v1} \\ M_{u2,v2} \end{bmatrix}.$$

(a) If $v1 \neq v2$. On the left side we get a non-singular submatrix $[2^{v1-1}, 2^{2(v1-1)}; 2^{v2-1}, 2^{2(v2-1)}]$. So by this we have at most $\sum_{i=1}^{q}\sum_{u1=1}^{q}\sum_{v1=1}^{\ell_{u1}}\sum_{u2=1}^{q}\sum_{v2=1}^{\ell_{u2}}((2^n-2)!)$ permutations.

(b) Else if $v1 = v2 = v \in [\min\{\ell_{u1}, \ell_{u2}\}]$ and $\nexists Y_{i,l1} = Y_{i,l2}$ for any distinct $l1, l2 \in [\ell_i]$. We get a non-singular submatrix $[1, 2^{v-1}; 2^1, 2^{v-1}]$. By this we have at most $\sum_{i=1}^{q} \sum_{l=1}^{\ell_i} \sum_{u1=1}^{q} \sum_{u2=1}^{q} \sum_{v=1}^{\min\{\ell_{u1}, \ell_{u2}\}} ((2^n - 2)!)$ permutations.

(c) Else $v1 = v2 = v \in [\min\{\ell_{u1}, \ell_{u2}\}]$, and $\exists Y_{i,l1} = Y_{i,l2}$ for distinct $l1, l2 \in [\ell_i]$, we get a non-singular submatrix $[0^n, 2^{v-1}; 2^{\ell_i - l1+1} \oplus 2^{\ell_i - l2+1}, 2^{v-1}]$, by combing the columns for $Y_{i,l1}$ and $Y_{i,l2}$. So by this we have at most $\sum_{i=1}^{q} \binom{\ell_i}{2} \sum_{u1=1}^{q} \sum_{u2=1}^{q} \sum_{v=1}^{\min\{\ell_{u1}, \ell_{u2}\}} ((2^n - 2)!)$ permutations.

Totally, we have at most $\varsigma_4 = (2q^3\ell^2 + q^3\ell^3/2)((2^n - 2)!)$ permutations can induce this.

5. $\exists \Sigma_i = \mathrm{Cst}_j$ for some $j \in [2]$ and $\Theta_i = \Theta_u$ for some $u \neq i$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 0, & 0, & \cdots, & 0 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 2^{\ell_u}, & 2^{\ell_u - 1}, & \cdots, & 2^1 \end{bmatrix} \times \overrightarrow{Y[i,u]} = \begin{bmatrix} \mathrm{Cst}_j \\ 0^n \end{bmatrix}, \tag{41}$$

where $\overrightarrow{Y[i,u]} = [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, Y_{u,1}, Y_{u,2}, \cdots, Y_{u,\ell_u}]^T$, $\mathrm{Set}Y[i,u] = \{Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, Y_{u,1}, Y_{u,2}, \cdots, Y_{u,\ell_u}\}$.

(a) If $\nexists Y'_{l1}, Y''_{l2} \in \mathrm{Set}Y[i,u]$ s.t. $Y'_{l1} = Y''_{l2}$ with any distinct $l1, l2 \in [\max\{\ell_i, \ell_u\}]$.

i. If $\ell_i = \ell_u$, notice that $M_i \neq M_u$, so $\exists l \in [\ell_i]$ s.t. $M_{i,l} \neq M_{u,l}$. Then, we get a non-singular submatrix $[1, 0; 2^{\ell_i - l+1}, 2^{\ell_u - l+1}]$.

ii. Else if $\ell_i = \ell_u + 1$, then we focus on the coefficients of Y_{i,ℓ_i}, $Y_{i,\ell_i - 1}$ and Y_{u,ℓ_u}, and get a non-singular submatrix $[1, 1; 2^1, 2^2 \oplus 2^1]$ (when $Y_{i,\ell_i - 1} = Y_{u,\ell_u}$ is a trivial collision) or $[1, 1; 2^1, 2^2]$ (when $Y_{i,\ell_i - 1} \neq Y_{u,\ell_u}$).

iii. Else if $\ell_i \geq \ell_u + 2$, let us focus on the coefficients of Y_{i,ℓ_i} and $Y_{i,\ell_i - 1}$, and we get a non-singular submatrix $[1, 1; 2^2, 2^1]$.

iv. Else $\ell_u \geq \ell_i + 1$, let us focus on the coefficients of Y_{u,ℓ_u}, $Y_{u,\ell_u - 1}$ and Y_{i,ℓ_i}, and get a non-singular submatrix $[1, 0; 2^1 \oplus 2^2, 2^1]$ (when $Y_{u,\ell_u - 1} = Y_{i,\ell_i}$ is a trivial collision) or $[1, 0; 2^1, 2^1]$ (when $Y_{u,\ell_u - 1} \neq Y_{i,\ell_i}$).

To summarize this subcase, each case in the above presents us a non-singular coefficients matrix on the left side, and by this we get at most $\sum_{i=1}^{q} \sum_{u=1, u \neq i}^{q} \sum_{j=1}^{2} ((2^n - 2)!)$ permutations.

(b) Else $\exists Y'_{l1}, Y''_{l2} \in \mathrm{Set}Y[i,u]$ s.t. $Y'_{l1} = Y''_{l2}$ with distinct $l1, l2 \in [\max\{\ell_i, \ell_u\}]$.

i. If $\ell_i \neq \ell_u$, then $\bigoplus_{l=1}^{\ell_i} 2^l \oplus \bigoplus_{l=1}^{\ell_u} 2^l \neq 0$. On one side, the 2-collision $Y'_{l1} = Y''_{l2}$ implies $(2^{l1-1} \oplus 2^{l2-1})\Delta_1 \oplus (2^{2(l1-1)} \oplus 2^{2(l2-1)})\Delta_2 = M'_{l1} \oplus M''_{l2}$, which is over Δ_1 and Δ_2. On the other side, some coefficients of Eq. (41) should be combined, if their corresponding variables belong to 2-collisions or trivial collisions. This makes the final coefficients matrix of Eq. (41) complex. However, notice in this final coefficients matrix that, there is at least one element in its second row should not be 0, otherwise the sum of all coefficients in the second row should be 0, and this contradicts with the fact that $\bigoplus_{l=1}^{\ell_i} 2^l \oplus \bigoplus_{l=1}^{\ell_u} 1 = (2^1 \oplus 2^{\ell_i + 1})/3$ or $(2^1 \oplus 2^{\ell_i + 1})/3 \oplus 1$, neither of which is 0 when $1 \leq \ell_i \leq 2^{2n/3}$. By this we get an equation over $Y_{i,l}$ with $l \in [\ell_i]$, whose coefficient is not 0. Then, according to the independence of

$Y_{i,l}$, Δ_1 and Δ_2, we have two independent equations and get at most $\sum_{i=1}^{q}\sum_{u=1,u\neq i}^{q}\binom{\max\{\ell_i,\ell_u\}}{2}\sum_{j=1}^{2}((2^n-2)!)$ permutations.

ii. Else $\ell_i = \ell_u$, on one side by the 2-collision $Y'_{l1} = Y''_{l2}$ we have an equation over Δ_1 and Δ_2. On the other side, let us find another equation independent of Δ_1 and Δ_2. Notice that $M_i \neq M_u$, so $\exists l \in [\ell_i]$ s.t. $M_{i,l} \neq M_{u,l}$, and this implies $X_{i,l} \neq X_{u,l}$ and $Y_{i,l} \neq Y_{u,l}$. For $Y'_{l'} \in \mathrm{Set}Y[i,u] \setminus \{Y_{i,l}\}$, if $\nexists Y'_{l'} = Y_{i,l}$, then we get an equation over $Y_{i,l}$, whose coefficient is $2^{\ell_i-l+1} \neq 0$. Else $\exists Y'_{l'} = Y_{i,l}$, obviously we have $l' \neq l$. Then we get an equation over $Y_{i,l}$, whose coefficient is either $2^{\ell_i-l+1} \oplus 2^{\ell_i-l'+1} \neq 0$ (when $Y_{i,l'} \neq Y_{u,l'}$) or $2^{\ell_i-l+1} \neq 0$ (when $Y_{i,l'} = Y_{u,l'}$).

To summarize this subcase, we get at most $\sum_{i=1}^{q}\sum_{u=1,u\neq i}^{q}\binom{\max\{\ell_i,\ell_u\}}{2}\sum_{j=1}^{2}((2^n-2)!)$ permutations.

To summarize Case 5, we get at most $\varsigma_5 = (2q^2 + q^2\ell^2)((2^n-2)!)$ permutations.

6. $\exists \Sigma_i = \Sigma_u$ for some $u \neq i$ and $\Theta_i = \mathrm{Cst}_j$ for some $j \in [2]$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 1, 1, \cdots, 1 \\ 2^{\ell_i}, & 2^{\ell_i-1}, & \cdots, & 2^1, & 0, 0, \cdots, 0 \end{bmatrix} \times \overrightarrow{Y[i,u]} = \begin{bmatrix} 0^n \\ \mathrm{Cst}_j \end{bmatrix}.$$

(a) If $\nexists Y'_{l1}, Y''_{l2} \in \mathrm{Set}Y[i,u]$ s.t. $Y'_{l1} = Y''_{l2}$ with any distinct $l1, l2 \in [\max\{\ell_i,\ell_u\}]$.

i. If $\ell_i = \ell_u$, notice that $M_i \neq M_u$, so $\exists l \in [\ell_i]$ s.t. $M_{i,l} \neq M_{u,l}$. Then, we get a non-singular submatrix $[1, 1; 2^{\ell_i-l+1}, 0]$.

ii. Else if $\ell_i = \ell_u + 1$, then we focus on the coefficients of Y_{i,ℓ_i}, Y_{i,ℓ_i-1} and Y_{u,ℓ_u}, and get a non-singular submatrix $[0, 1; 2^2, 2^1]$ (when $Y_{i,\ell_i-1} = Y_{u,\ell_u}$ is a trivial collision) or $[1, 1; 2^2, 2^1]$ (when $Y_{i,\ell_i-1} \neq Y_{u,\ell_u}$).

iii. Else if $\ell_i \geq \ell_u + 2$, let us focus on the coefficients of Y_{i,ℓ_i} and Y_{i,ℓ_i-1}, and we get a non-singular submatrix $[1, 1; 2^2, 2^1]$.

iv. Else $\ell_u \geq \ell_i + 1$, let us focus on the coefficients of Y_{u,ℓ_u}, Y_{u,ℓ_u-1} and Y_{i,ℓ_i}, and get a non-singular submatrix $[1, 0; 0, 2^1]$ (when $Y_{u,\ell_u-1} = Y_{i,\ell_i}$ is a trivial collision) or $[1, 1; 0, 2^1]$ (when $Y_{u,\ell_u-1} \neq Y_{i,\ell_i}$).

Each case in the above presents us a non-singular coefficients matrix on the left side, and by this we can get at most $\sum_{i=1}^{q}\sum_{u=1,u\neq i}^{q}\sum_{j=1}^{2}((2^n-2)!)$ permutations.

(b) Else $\exists Y'_{l1}, Y''_{l2} \in \mathrm{Set}Y[i,u]$ s.t. $Y'_{l1} = Y''_{l2}$ with distinct $l1, l2 \in [\max\{\ell_i,\ell_u\}]$. Notice that $\bigoplus_{l=1}^{\ell_i} 2^l \neq 0$, and then the analysis is similar with Case (5.bi). To summarize, we can get at most $\sum_{i=1}^{q}\sum_{u=1,u\neq i}^{q}\binom{\max\{\ell_i,\ell_u\}}{2}\sum_{j=1}^{2}((2^n-2)!)$ permutations.

To summarize Case 6, we can get at most $\varsigma_6 = (2q^2 + q^2\ell^2)((2^n-2)!)$ permutations.

7. $\exists \Sigma_i = X_{u,v}$ for some $u \in [q]$, $v \in [\ell_u]$ and $\Theta_i = \Theta_j$ for some $j \neq i$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 0, & 0, & \cdots, & 0, & 2^{v-1}, & 2^{2(v-1)} \\ 2^{\ell_i}, & 2^{\ell_i-1}, & \cdots, & 2^1, & 2^{\ell_j}, & 2^{\ell_j-1}, & \cdots, & 2^1, & 0, & 0 \end{bmatrix} \times \overrightarrow{Y[i,j,\Delta]} = \begin{bmatrix} M_{u,v} \\ 0^n \end{bmatrix},$$

where $\overrightarrow{Y[i,j,\Delta]} = [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, Y_{j,1}, Y_{j,2}, \cdots, Y_{j,\ell_j}, \Delta_1, \Delta_2]^T$, The analysis is similar with that in Case 5, and their only difference is that, here we have two more variables Δ_1 and Δ_2. Specially, their coefficients matrix is exactly the same, except for the coefficients for Δ_1 and Δ_2. Then, we can apply the same analysis, and we can either get a non-singular submatrix on the left side, or get one equation over Δ_1 and Δ_2, and another equation over $Y_{i,l}$, Δ_1 and Δ_2. Finally, in this case we can get at most $\varsigma_7 = (q^3\ell + q^3\ell^3/2)((2^n - 2)!)$ permutations.

8. $\exists \Sigma_i = \Sigma_j$ for some $j \neq i$ and $\Theta_i = X_{u,v}$ for some $u \in [q]$, $v \in [\ell_u]$. This implies

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 1, 1, \cdots, 1, & 0, & 0 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 0, 0, \cdots, 0, & 2^{v-1}, & 2^{2(v-1)} \end{bmatrix} \times \overrightarrow{Y[i,j,\Delta]} = \begin{bmatrix} 0^n \\ M_{u,v} \end{bmatrix}.$$

The analysis is similar with that in Case 7, and in this case we get at most $\varsigma_8 = (q^3\ell + q^3\ell^3/2)((2^n - 2)!)$ permutations.

9. $\Sigma_i = \Sigma_j$ for some $j \neq i$ and $\Theta_i = \Theta_u$ for some $u \neq i$, and we have

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 1, 1, \cdots, 1, & 0, & 0, & \cdots, & 0 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 0, 0, \cdots, 0, & 2^{\ell_u}, & 2^{\ell_u - 1}, & \cdots, & 2^1 \end{bmatrix} \times \overrightarrow{Y[i,j,u]} = \begin{bmatrix} 0^n \\ 0^n \end{bmatrix},$$

where $\overrightarrow{Y[i,j,u]} = [Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, Y_{j,1}, Y_{j,2}, \cdots, Y_{j,\ell_j}, Y_{u,1}, Y_{u,2}, \cdots, Y_{u,\ell_u}]^T$.

(a) If $j = u \wedge \nexists Y'_{l'}, Y''_{l''} \in \mathrm{Set}Y[i,u]$ s.t. $Y'_{l'} = Y''_{l''}$ with any distinct $l', l'' \in [\max\{\ell_i, \ell_u\}]$. The equation set turns to be

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 1, & 1, & \cdots, & 1 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 2^{\ell_u}, & 2^{\ell_u - 1}, & \cdots, & 2^1 \end{bmatrix} \times \overrightarrow{Y[i,u]} = \begin{bmatrix} 0^n \\ 0^n \end{bmatrix}. \quad (42)$$

i. If $\ell_i = \ell_u$, let us denote $Y_{*,l} = Y_{i,l} \oplus Y_{u,l}$, then Eq. (42) becomes

$$\begin{bmatrix} 1, & 1, & \cdots, & 1 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1 \end{bmatrix} \times [Y_{*,1}, Y_{*,2}, \cdots, Y_{*,\ell_i}]^T = \begin{bmatrix} 0^n \\ 0^n \end{bmatrix}.$$

On the left side the coefficients matrix is an MDS matrix, and on the right side we have two 0^n, so by the property of MDS matrix and the fact $M_i \neq M_u$, we have at least 3 non-zero $Y_{*,l}$. This means in Eq. (42) we have distinct $l1, l2, l3 \in [\ell_i]$ s.t. $Y_{i,l1} \neq Y_{u,l1}$, $Y_{i,l2} \neq Y_{u,l2}$ and $Y_{i,l3} \neq Y_{u,l3}$. Then in Eq. (42) we find a non-singular submatrix $[1, 1; 2^{\ell_i - l1 + 1}, 2^{\ell_i - l2 + 1}]$.

ii. Else if $\ell_i = \ell_u + 1$, then we focus on the coefficients of Y_{i,ℓ_i}, $Y_{i,\ell_i - 1}$ and Y_{u,ℓ_u}, and get a non-singular submatrix $[1, 0; 2^1, 2^2 \oplus 2^1]$ (when $Y_{i,\ell_i - 1} = Y_{u,\ell_u}$ is a trivial collision) or $[1, 1; 2^1, 2^2]$ (when $Y_{i,\ell_i - 1} \neq Y_{u,\ell_u}$).

iii. Else if $\ell_i \geq \ell_u + 2$, let us focus on the coefficients of Y_{i,ℓ_i} and $Y_{i,\ell_i - 1}$, and we get a non-singular submatrix $[1, 1; 2^2, 2^1]$.

iv. Else $\ell_u \geq \ell_i + 1$, the analysis is the same as (ii) and (iii).

(b) Else if $j = u \wedge \exists Y'_{l'}, Y'''_{l''} \in \mathrm{Set}Y[i,u]$ s.t. $Y'_{l'} = Y'''_{l''}$ with distinct $l', l'' \in [\max\{\ell_i, \ell_u\}]$. On one side by the 2-collision $Y'_{l'} = Y'''_{l''}$ we have an equation over Δ_1 and Δ_2. On the other side, let us find another equation independent of Δ_1 and Δ_2.
   i. If $\ell_i \neq \ell_u$, then $\bigoplus_{l=1}^{\ell_i} 2^l \oplus \bigoplus_{l=1}^{\ell_u} 2^l \neq 0$, we get an equation over $Y_{i,l}$, and the analysis is similar with (5.b).
   ii. Else $\ell_i = \ell_u$, notice that $M_i \neq M_u$, so $\exists l \in [\ell_i]$ s.t. $M_{i,l} \neq M_{u,l}$, and this implies $Y_{i,l} \neq Y_{u,l}$. For $Y'_{l'} \in \mathrm{Set}Y[i,u] \setminus \{Y_{i,l}\}$, if $\nexists Y'_{l'} = Y_{i,l}$, then we get an equation over $Y_{i,l}$, whose coefficient is $2^{\ell_i - l + 1} \neq 0$. Else $\exists Y'_{l'} = Y_{i,l}$, obviously we have $l' \neq l$. Then we get an equation over $Y_{i,l}$, whose coefficient is either $2^{\ell_i - l + 1} \oplus 2^{\ell_i - l' + 1} \neq 0$ (when $Y_{i,l'} \neq Y_{u,l'}$) or $2^{\ell_i - l + 1} \neq 0$ (when $Y_{i,l'} = Y_{u,l'}$).

(c) Else if $j \neq u \wedge \nexists Y'_{l'}, Y'''_{l''} \in \mathrm{Set}Y[i,j,u]$ s.t. $Y'_{l'} = Y'''_{l''}$ with any distinct $l', l'' \in [\max\{\ell_i, \ell_j, \ell_u\}]$. By $M_i \neq M_j$ we know $\exists l1 \in [\max\{\ell_i, \ell_j\}]$ s.t. $Y_{i,l1} \neq Y_{j,l1}$. Here $Y_{i,l1} = 0^n$ if $l1 > \ell_i$ and $Y_{j,l1} = 0^n$ if $l1 > \ell_j$. Notice that $Y_{i,l1} \oplus Y_{j,l1} \neq 0^n$ can be seen as a new variable. We ignore $Y_{u,l1}$ here because its coefficient is 0^n in the first row of coefficients matrix. Similarly, by $M_i \neq M_u$ we know $\exists l2 \in [\max\{\ell_i, \ell_u\}]$ s.t. $Y_{i,l2} \neq Y_{u,l2}$. Here $Y_{i,l2} = 0^n$ if $l2 > \ell_i$ and $Y_{u,l2} = 0^n$ if $l2 > \ell_u$. Then $2^{\ell_i - l2 + 1} Y_{i,l2} \oplus Y_{u,l2}$ is a new variable. We ignore $Y_{j,l2}$ here because its coefficient is 0^n in the second row of coefficients matrix. Also by $M_j \neq M_u$ we have $\exists l3 \in [\max\{\ell_j, \ell_u\}]$ s.t. $Y_{j,l3} \neq Y_{u,l3}$. Here $Y_{j,l3} = 0^n$ if $l3 > \ell_j$ and $Y_{u,l3} = 0^n$ if $l3 > \ell_u$.
If $l1 \neq l2$, it is easy to see that $Y_{i,l1} \oplus Y_{j,l1}$ and $2^{\ell_i - l2 + 1} Y_{i,l2} \oplus 2^{\ell_u - l2 + 1} Y_{u,l2}$ are independent of each other, because we have $Y'_{l'} \neq Y'''_{l''}$ with any distinct $l', l'' \in [\max\{\ell_i, \ell_j, \ell_u\}]$. If $l1 = l2$ and $Y_{j,l1} \neq Y_{u,l2}$, then $Y_{i,l1} \oplus Y_{j,l1}$ and $2^{\ell_i - l2 + 1} Y_{i,l2} \oplus 2^{\ell_u - l2 + 1} Y_{u,l2}$ are also independent. If $l1 = l2$ and $Y_{j,l1} = Y_{u,l2}$, notice that $Y_{j,l3} \neq Y_{u,l3}$ and $l2 \neq l3$, we have variables $Y_{i,l1} \oplus Y_{j,l1} \oplus Y_{j,l3}$ and $2^{\ell_i - l2 + 1} Y_{i,l2} \oplus 2^{\ell_u - l2 + 1} Y_{u,l2} \oplus 2^{\ell_u - l3 + 1} Y_{u,l3}$ are independent.
Then we find a non-singular submatrix in the above coefficients matrix, i.e. $[1, 0; 0, 1]$ for independent variables $Y_{i,l1} \oplus Y_{j,l1}$ and $2^{\ell_i - l2 + 1} Y_{i,l2} \oplus 2^{\ell_u - l2 + 1} Y_{u,l2}$ or $Y_{i,l1} \oplus Y_{j,l1} \oplus Y_{j,l3}$ and $2^{\ell_i - l2 + 1} Y_{i,l2} \oplus 2^{\ell_u - l2 + 1} Y_{u,l2} \oplus 2^{\ell_u - l3 + 1} Y_{u,l3}$.

(d) Else $j \neq u \wedge \exists Y'_{l'}, Y'''_{l''} \in \mathrm{Set}Y[i,j,u]$ s.t. $Y'_{l'} = Y'''_{l''}$ with distinct $l', l'' \in [\max\{\ell_i, \ell_j, \ell_u\}]$. On one side by the 2-collision $Y'_{l'} = Y'''_{l''}$ we have an equation over Δ_1 and Δ_2. On the other side, let us find another equation independent of Δ_1 and Δ_2.
   i. If $\ell_i \neq \ell_u$, we have $\bigoplus_{l=1}^{\ell_i} 2^l \oplus \bigoplus_{l=1}^{\ell_u} 2^l \neq 0$, so we get an equation over $Y_{i,l}$ for some $l \in [\ell_i]$.
   ii. Else $\ell_i = \ell_u$, notice that $M_i \neq M_u$, so $\exists l \in [\ell_i]$ s.t. $M_{i,l} \neq M_{u,l}$, and this implies $Y_{i,l} \neq Y_{u,l}$. For $Y'_{l'} \in \mathrm{Set}Y[i,j,u] \setminus \{Y_{i,l}\}$, if $\nexists Y'_{l'} = Y_{i,l}$, then we get an equation over $Y_{i,l}$, whose coefficient is $2^{\ell_i - l + 1} \neq 0$. Else $\exists Y'_{l'} = Y_{i,l}$, let us focus on the second row of the coefficients matrix. By this we can ignore the influence from M_j, then we have $Y'_{l'} = Y_{i,l'}$ or $Y'_{l'} = Y_{u,l'}$, so it is obvious that $l' \neq l$. Then we get an

equation over $Y_{i,l}$, whose coefficient is either $2^{\ell_i-l+1} \oplus 2^{\ell_i-l'+1} \neq 0$ (when $Y_{i,l'} \neq Y_{u,l'}$) or $2^{\ell_i-l+1} \neq 0$ (when $Y_{i,l'} = Y_{u,l'}$).

To summarize, we can get at most $\varsigma_9 = (\sum_{i=1}^{q}\sum_{j=1,j\neq i}^{q}(1+\binom{\max\{\ell_i,\ell_j\}}{2})) + \sum_{i=1}^{q}\sum_{j=1,j\neq i}^{q}\sum_{u=1,u\neq i,j}^{q}(1+\binom{\max\{\ell_i,\ell_j,\ell_u\}}{2})))((2^n-2)!) \leq (q^2+q^2\ell_{\max}^2/2+q^3+q^3\ell_{\max}^2/2)((2^n-2)!)$ permutations.

Finally, we can get

$$\epsilon_{ecf} \leq \frac{\sum_{i=-1}^{9}\varsigma_i}{2^n!} \leq \frac{3q\ell((2^n-1)!)+20q^3\ell^3((2^n-2)!)}{2^n!} \leq \frac{3q\ell}{2^n}+\frac{5q^3\ell^3}{2^{2n-3}}.$$

Upper Bounding pseudo-cover-free ϵ_{pcf}

pseudo-cover-1 ϵ_1 This is defined by two equation sets, (L_{21}) and (L_{22}), and we further turn them into two bad events respectively, according to our 1kPMAC_Plus specification.

For (L_{21}) $\Sigma_i = X_{j,a}, Y_{j,a} \oplus t_i = Y_{k,s}$, we have

1. $\Sigma_i = \mathrm{Cst}_j$ for some $j \in [2]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_j$, i.e. an equation over variables $Y_{i,l}$. On the other side, notice that by $\Sigma_i = \mathrm{Cst}_j$ we have $Y_{j,a} = \pi(\Sigma_i) = \pi(\mathrm{Cst}_j) = \Delta_j$. This means, $Y_{j,a} \oplus t_i = \Delta_j \oplus t_i$. Then, the equation $Y_{j,a} \oplus t_i = Y_{k,s}$ depends on random variable Δ_j. Notice that we have restrict $t_i \neq 0^n$ for all $i \in [q]$, so the equation can't trivially hold. Then, we find two equations independent of each other.
2. $\Sigma_i = X_{j,a}$ for some $j \neq i$, $a \in [\ell_j]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-2)}\Delta_2 \oplus M_{j,a}$, i.e. an equation over variables $Y_{i,l}$, Δ_1 and Δ_2. When $Y_{j,a} \oplus t_i = \Delta_s$, we get a non-singular submatrix $[1,1;1,0]$ or $[1,1;0,1]$ with variables Δ_1 and Δ_2. When $Y_{j,a} \oplus t_i = Y_{k,s}$, this equation depends only on Y variables, where $t_i \neq 0^n$ excludes trivial collisions $Y_s = Y'_s$. Then we get two independent equations.

For (L_{22}) $\Theta_i = X_{j,a}, Y_{j,a} \oplus t_i = Y_{k,s}$, we have

1. $\Theta_i = \mathrm{Cst}_j$ for some $j \in [2]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} 2^{\ell_i-l+1} Y_{i,l} = \mathrm{Cst}_j$, i.e. an equation over variables $Y_{i,l}$. On the other side, notice that by $\Theta_i = \mathrm{Cst}_j$ we have $Y_{j,a} = \pi(\Theta_i) = \pi(\mathrm{Cst}_j) = \Delta_j$. This means, $Y_{j,a} \oplus t_i = \Delta_j \oplus t_i$. So, $Y_{j,a} \oplus t_i = Y_{k,s}$ depend on random variable Δ_j. Notice that we have restrict $t_i \neq 0^n$ for all $i \in [q]$, so the equation can't trivially hold. Then, we find two independent equations.
2. $\Theta_i = X_{j,a}$ for some $j \neq i$, $a \in [\ell_j]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} 2^{\ell_i-l+1} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-2)}\Delta_2 \oplus M_{j,a}$, i.e. an equation over variables $Y_{i,l}$, Δ_1 and Δ_2. When $\pi(\Theta_i) \oplus t_i = \Delta_s$, we get a non-singular submatrix $[2^{a-1}, 2^{2(a-2)}; 1, 0]$ or $[2^{a-1}, 2^{2(a-2)}; 0, 1]$ with variables Δ_1 and Δ_2. When $\pi(\Theta_i) \oplus t_i = Y_{k,s}$ depends only on Y variables, where $t_i \neq 0^n$ excludes trivial collisions $Y_s = Y'_s$. Then we get two independent equations.

By this, we can get $\epsilon_1 \leq \frac{4\sum_{i=1}^{q}\sum_{j=1}^{q}\sum_{a=1}^{\ell_j}\sum_{k=1}^{q}\sum_{s=1}^{\ell_k}}{(2^n-q\ell-2-2q)^2} \leq \frac{q^3\ell^2}{2^{2n-3}}$.

pseudo-cover-2 ϵ_2 According to the definition of pseudo-cover-2, we need to upper bound the occurrence probability of (L_{31}), (L_{32}) and (L_{33}).

For L_{23}, we have the following four equation sets

1. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a} \\ \bigoplus_{l=1}^{\ell_j} Y_{j,l} = 2^{b-1}\Delta_1 \oplus 2^{2(b-1)}\Delta_2 \oplus M_{l,b} \\ Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j, \end{cases}$
2. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_a \\ \bigoplus_{l=1}^{\ell_j} Y_{j,l} = 2^{b-1}\Delta_1 \oplus 2^{2(b-1)}\Delta_2 \oplus M_{l,b} \\ \Delta_a \oplus Y_{l,b} = t_i \oplus t_j, \end{cases}$
3. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a} \\ \bigoplus_{l=1}^{\ell_j} Y_{j,l} = \mathrm{Cst}_b \\ Y_{k,a} \oplus \Delta_b = t_i \oplus t_j, \end{cases}$
4. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_a \\ \bigoplus_{l=1}^{\ell_j} Y_{j,l} = \mathrm{Cst}_b \\ \Delta_a \oplus \Delta_b = t_i \oplus t_j, \end{cases}$

For the first subcase, if $a \neq b$, it is easy to see that its coefficients matrix has rank 3. If $a = b$, then we get one equation over Δ_1 and Δ_2, and the other two independent equations over variables Y. They are independent because they are defined on four distinct messages, and if there exists collisions among Y values, we get one more equation over Δ_1 and Δ_2. So, we still get a rank=3 coefficients matrix. For the rest three subcases, there are also rank=3 coefficients matrices, and their message queries (w.r.t. i, j, k, l) and lengths (w.r.t. a, b) are even smaller.

For L_{24}, we have the following four equation sets

1. $\begin{cases} \bigoplus_{l=1}^{\ell_i} 2^{\ell_i-l+1} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a} \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j-l+1} Y_{j,l} = 2^{b-1}\Delta_1 \oplus 2^{2(b-1)}\Delta_2 \oplus M_{l,b} \\ Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j, \end{cases}$
2. $\begin{cases} \bigoplus_{l=1}^{\ell_i} 2^{\ell_i-l+1} Y_{i,l} = \mathrm{Cst}_a \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j-l+1} Y_{j,l} = 2^{b-1}\Delta_1 \oplus 2^{2(b-1)}\Delta_2 \oplus M_{l,b} \\ \Delta_a \oplus Y_{l,b} = t_i \oplus t_j, \end{cases}$
3. $\begin{cases} \bigoplus_{l=1}^{\ell_i} 2^{\ell_i-l+1} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a} \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j-l+1} Y_{j,l} = \mathrm{Cst}_b \\ Y_{k,a} \oplus \Delta_b = t_i \oplus t_j, \end{cases}$
4. $\begin{cases} \bigoplus_{l=1}^{\ell_i} 2^{\ell_i-l+1} Y_{i,l} = \mathrm{Cst}_a \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j-l+1} Y_{j,l} = \mathrm{Cst}_b \\ \Delta_a \oplus \Delta_b = t_i \oplus t_j, \end{cases}$

For L_{25}, we have the following four equation sets

1. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a} \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j-l+1} Y_{j,l} = 2^{b-1}\Delta_1 \oplus 2^{2(b-1)}\Delta_2 \oplus M_{l,b} \\ Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j, \end{cases}$

2. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_a \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j - l + 1} Y_{j,l} = 2^{b-1}\Delta_1 \oplus 2^{2(b-1)}\Delta_2 \oplus M_{l,b} \\ \Delta_a \oplus Y_{l,b} = t_i \oplus t_j, \end{cases}$
3. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a} \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j - l + 1} Y_{j,l} = \mathrm{Cst}_b \\ Y_{k,a} \oplus \Delta_b = t_i \oplus t_j, \end{cases}$
4. $\begin{cases} \bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_a \\ \bigoplus_{l=1}^{\ell_j} 2^{\ell_j - l + 1} Y_{j,l} = \mathrm{Cst}_b \\ \Delta_a \oplus \Delta_b = t_i \oplus t_j, \end{cases}$

By similar analysis as for L_{23}, we always get rank=3 coefficients matrices. Then, for pseudo-cover-2 we have

$$\epsilon_2 \leq 3 \sum_{i=1}^{q} \sum_{j=1}^{q} \sum_{k=1}^{q} \sum_{l=1}^{q} \sum_{a=1}^{\ell_k} \sum_{b=1}^{\ell_l} \frac{1}{(2^n - ql - 2 - 2q)^3} \leq \frac{3q^4\ell^2}{2^{3n-1}},$$

and together with ϵ_1 we conclude

$$\epsilon_{pcf} \leq \epsilon_1 + \epsilon_2 \leq \frac{q^3\ell^2}{2^{2n-3}} + \frac{3q^4\ell^2}{2^{3n-1}}.$$

Upper Bounding extended universal ϵ_{euniv}

By its definition, we have six cases.

1. $\Sigma_i = \Sigma_j$ for some $j \neq i$. This implies an equation

$$\bigoplus_{l=1}^{\ell_i} Y_{i,l} = \bigoplus_{l=1}^{\ell_j} Y_{j,l}.$$

Notice that $M_i \neq M_j$, so there exists $l' \in [\max\{\ell_i, \ell_j\}]$ s.t. $Y_{i,l'} \neq Y_{j,l'}$, where $Y_{i,l'} = 0^n$ if $l' > \ell_i$ and $Y_{j,l'} = 0^n$ if $l' > \ell_j$. Then, the variable $Y_{i,l'} \oplus Y_{j,l'}$ has a non-zero coefficient, so we have

$$\Pr[\Sigma_i = \Sigma_j] \leq \frac{1}{2^n - (q\ell - 2 - 2q)} \leq \frac{1}{2^{n-1}}.$$

2. $\Theta_i = \Theta_j$ for some $j \neq i$. This implies an equation

$$\bigoplus_{l=1}^{\ell_i} 2^{\ell_i - l + 1} Y_{i,l} = \bigoplus_{l=1}^{\ell_j} 2^{\ell_j - l + 1} Y_{j,l}.$$

Notice that $M_i \neq M_j$, so there exists $l' \in [\max\{\ell_i, \ell_j\}]$ s.t. $Y_{i,l'} \neq Y_{j,l'}$, where $Y_{i,l'} = 0^n$ if $l' > \ell_i$ and $Y_{j,l'} = 0^n$ if $l' > \ell_j$. Then, the variable $2^{\ell_i - l' + 1} Y_{i,l'} \oplus 2^{\ell_j - l' + 1} Y_{j,l'}$ has a non-zero coefficient, so we have

$$\Pr[\Sigma_i = \Sigma_j] \leq \frac{1}{2^n - (q\ell - 2 - 2q)} \leq \frac{1}{2^{n-1}}.$$

3. $\Sigma_i = X_{k,a}$, this is equivalent to

$$\bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a}.$$

   By the randomness of Δ_1, we have $\Pr[\Sigma_i = X_{k,a}] \leq 1/2^{n-1}$.
4. $\Sigma_i = \mathrm{Cst}_a$, this is equivalent to

$$\bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_a.$$

   If there exists no 2-collision among $Y_{i,l}$, we have $\Pr[\Sigma_i = \mathrm{Cst}_a] \leq 1/2^{n-1}$ by the randomness of $Y_{i,l}$; otherwise we have another equation over Δ_1 and Δ_2, and get the same upper bound.
5. $\Theta_i = X_{k,a}$, this is equivalent to

$$\bigoplus_{l=1}^{\ell_i} 2^{\ell_i - l + 1} Y_{i,l} = 2^{a-1}\Delta_1 \oplus 2^{2(a-1)}\Delta_2 \oplus M_{k,a}.$$

   By the randomness of Δ_1, we have $\Pr[\Theta_i = X_{k,a}] \leq 1/2^{n-1}$.
6. $\Theta_i = \mathrm{Cst}_a$, this is equivalent to

$$\bigoplus_{l=1}^{\ell_i} 2^{\ell_i - l + 1} Y_{i,l} = \mathrm{Cst}_a$$

   Notice that we have excluded 3-collision among $Y_{i,l}$, so we always have the coefficients of $Y_{i,l}$ are non-zero. By their randomness, we have $\Pr[\Theta_i = \mathrm{Cst}_a] \leq 1/2^{n-1}$.

In conclusion, we have $\epsilon_{euniv} \leq 2^{1-n}$.