One-key Double-Sum MAC with Beyond-Birthday Security

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

[1] Indian Statistical Institute, Kolkata
[2] Institute of Information Engineering, Chinese Academy of Sciences.
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 either suffer from birthday attacks or require long key sizes. In this paper, we focus on designing beyond-birthday-bound MAC modes with a single key, and investigate their design principles. First, we review the current proposals, e.g. 3kf9 and PMAC_Plus, and identify that the security primarily comes from the construction of a cover-free function and the advantage of the sum of PRPs. The main challenge in reducing their key size is to find a mechanism to carefully separate the block cipher inputs to the cover-free construction and the sum of PRPs that work in cascade with such a construction. Secondly, we develop several tools on sampling distributions that are quite useful in analysis of the MAC mode of operations and by which we unify the proofs for three/two-key beyond-birthday-bound MACs. Thirdly, we establish our main theorem that upper-bounds the PRF security of the one-key constructions by extended-cover-free, pseudo-cover-free, block-wise universal and the normal PRP assumption on block ciphers. Finally, we apply our main theorem to 3kf9 and PMAC_Plus, and successfully reduce their key sizes to the minimum possible. Thus, we solve a long-standing open problem in designing beyond-birthday-bound MAC with a single key.

Keywords: Beyond Birthday, 3kf9, PMAC_Plus, MAC, Sum of PRP, Cover-free, Rank, Strucutre Graph

1 Introduction

MAC. 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 would be hard to forge a tag for a completely new message for which tag has not been observed. A stronger requirement of a MAC is pseudo-random function (PRF) which informally says that the distribution of the tags be indistinguishable from uniform random distribution for any "efficient" adversary. The commonly used prf-advantage of a keyed construction F against an adversary $\mathcal{A}$ is defined as follows:

$$\mathbf{Adv}_{\mathbf{F}}^{\mathbf{prf}}(\mathcal{A}) = \mathsf{Pr}\left[\mathcal{A}^{F} = 1\right] - \Pr\left[\mathcal{A}^{\Gamma} = 1\right]$$

where Γ denotes the random function over the same domain and range as F. In practical applications, in addition to security, the issue of efficiency of MAC computation and the key-size are also very important.

Designing MAC/PRF. There are mainly three different approaches for designing a MAC: (a) universal hash function based, (b) compression function based, and (c) block cipher based. The drawback of universal hash based MAC design is that the performance of the MAC depends on the platform; some universal hash based MAC performs well in software, whereas the performance of others is noticeable only in hardware. In case of a compression function based MAC, the security of the MAC is established in terms of the prf-security of the underlying compression function. But designing a provably secure compression function got less attention than designing collision and (2nd) preimage compression function. On the other hand, analyzing block cipher becomes more popular.

Block Cipher Based MAC. Constructions that are based on block ciphers overcome the above difficulties. Performance of block cipher based MAC construction is balanced in both software and hardware. Examples of popular block cipher based MACs are CBC-MAC [3], OMAC [8], PMAC [5], TMAC [10] etc. However, for each of them, the so far best prf-security advantage is $O(Lq^2/2^n)$ where q is the maximum number of queries, L is maximum allowed message size and n is the block-length of the underlying block cipher. For example, if PMAC is being implemented by PRINCE [5] (a 64-bit lightweight block cipher) in some small device and if we allow to encrypt up to 1MB ($= 2^{20}$) messages then after 1 Million ($\approx 2^{20}$) encryption, one may be able to distinguish it from random function with about 1/16 probability. Thus, when n is small (e.g., $<= 64$ bits), as in lightweight cryptographic applications like RFIDs and smart cards, the birthday-bound security is no longer practical and so we need to seek for the construction achieving beyond birthday security.

Beyond-Birthday Secure MACs and Challenges. Among the block cipher based MACs that are beyond-birthday secure, two efficient (rate-1) constructions are PMAC_Plus and 3kf9.

1. In CRYPTO 2011, Yasuda proposed PMAC_Plus, a simple three key variant of parallelizable and efficient PMAC. The author mentioned that – "This raises a challenge to come up with a 1-key rate-1 MAC construction which is secure beyond the birthday bound."
2. 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. Zhang et al. mentioned in their conclusion that, "However, its key size seems to be too large in some particular environments, requiring further improvements therefore."

There is also another deterministic MAC mode provides security beyond the birthday bound. As Dodis and Steinberger have shown, MD$[f, g]$ reaches $O(\epsilon q \mathrm{poly}(n))$ MAC security. However, this design requires even longer keys and more block cipher invocations.

1.1 Motivation for 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, three block cipher keys imply three block cipher key schedulings, and this means, for most block ciphers (e.g. AES), three more block cipher invocation time and energy consumption.

A trivial way to reduce the key size, as commonly adopted in many practical protocols [1], is using a subkey generation algorithm f. Given a master key and some intermediate values, f can derive several subkeys for each invocation on block ciphers. Despite of inconvenience, implementing and running f requires extra memory and computation load, and its outputs pseudo-randomness is also a potential security risk, because to secure `PMAC_Plus` and 3kf9 we need three *independently random* keys.

A more technical method is to use tweakable block ciphers [13], 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. [9]) 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. [23, 7, 17], we in fact lose the beyond-birthday bound in `PMAC_Plus` and 3kf9. Then we have to adopt the provably secure tweakable block ciphers with beyond-birthday-bound security, e.g. [16, 12, 11, 15]. 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 beyond-birthday-bound 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.

1.2 Our Contributions

With a view to solving the above problem, first we review the techniques used in3kf9 and PMAC_Plus. Despite their specific mechanisms to process message blocks, they both have doubled internal states sizes and then "encrypt" their last internal state by the well-known "Sum of PRPs". 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. Then, if we just adopt a single key in these modes, we encounter two problems.

1. The first problem is "Sum of PRPs" may not work properly, because it will always output an all zero block once its two inputs collide.
2. The second problem is, the qL block cipher inputs within internal structures may collide with the last two inputs ($2q$ in total) to "Sum of PRPs", and this seems to happen with a birthday bound probability. Once occurred, even though a specific attack is hard to present, a proof is however easily ruined because we can get no new randomness for the final output.

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

Contribution 1. 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 input domain is restricted. That is, *over restricted domain and range, the sum of two same PRPs remains a PRF.* Then we examine it by deriving "1-interpolation probability of sum of WOR (WithOut Replacement) samples", and generalize it to the q-interpolation case. As applications, we apply them to three/two-key sum constructions, and get successful proofs.

Contribution 2. 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 such construction by these items and an additional value.

Contributions 3 and 4. Finally, we turn to reduce the key size for 3kf9 and PMAC_Plus. Taking advantage of our main theorem, in both proofs we just need to upper bound three items, i.e., extended-cover-free, pseudo-cover-free, and block-wise universal, for the corresponding CBC-like and PMAC-like structures. Though the proofs are more involved, interestingly, our obtained bounds for the one-key versions are only slightly larger than those for 3kf9 and PMAC_Plus, and they essentially have the same form $O(qL_{\max}/2^n + q^3L_{\max}^3/2^{2n})$.

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 $x_J := (x_j)_{j \in J}$. In this paper, **we fix a positive integer** n and all block ciphers considered in this paper have the block size n and L denotes the number of message blocks and ℓ denotes the length of the message it bits. 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

$$x \xmapsto{f} y \text{ to mean that } f(x_i) = y_i,\ \forall i \in I \text{ and}$$

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 $\mathcal{A}(m) \to \mathcal{O}$. 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.[3] Let $\mathcal{A}$ be a deterministic oracle algorithm and a q-tuple $m = (m_1, \ldots, m_q)$. 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) by abusing notation 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 useful feature of query-responses for an interaction of a deterministic algorithm with a random function.

[3] 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.

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

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

Proof. Clearly, if $\tau(\mathcal{A}(m) \longrightarrow f) = (x, y)$ then $x \xmapsto{f} y$. Conversely, let $(X, Y) = \tau(\mathcal{A}(m) \to f)$ then we can prove $X_i = x_i, Y_i = y_i$ by induction on the query index i. When $i = 1$, $X_1 = x_1$ since otherwise (x, y) can not be realizable and so $Y_1 = y_1$. Now suppose $X_j = x_j$, $Y_j = y_j$ for all $j < i$. As $\mathcal{A}$ is a deterministic algorithm $X_i = x_i$ (otherwise (x, y) can not be realizable). So $Y_i = y_i$. □

Random Functions. A **random function** is a function which is chosen from the set of all functions following some distribution. In particular, **uniform random function**, denoted $\mathit{\Gamma}_n$, (or **uniform random permutation** $\mathit{\Pi}_n$) is chosen uniformly from the set of all functions (or permutations respectively) from a specified finite domain to $\{0, 1\}^n$.

Interpolation Probability. For any tuples x, y with 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 $\mathit{\Gamma}_n$ (or $\mathit{\Pi}_n$) 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 $\mathsf{Pr}[x \overset{\mathit{\Gamma}_n}{\mapsto} y]$ is positive and equals to 2^{-ns} if and only if (x, y) function compatible. Similarly, $\mathsf{Pr}[x \overset{\mathit{\Pi}}{\mapsto} y]$ 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. Let $((x, a), (y, b))$ be a permutation-compatible pair such that $a \cap x = \phi$ and $a \in \mathsf{dist}_s$ then

$$\mathsf{Pr}[a \overset{\mathit{\Pi}_n}{\mapsto} b \mid x \overset{\mathit{\Pi}_n}{\mapsto} y] \geq 2^{-ns}.$$

2.2 Security Definitions

Pseudorandom Function and Permutation. We define **distinguishing advantage** of an oracle algorithm $\mathcal{A}$ for distinguishing two random functions $\mathtt{F}$ from $\mathtt{G}$ as

$$\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathtt{G}) := \mathsf{Pr}[\mathcal{A}^{\mathsf{F}} = 1] - \mathsf{Pr}[\mathcal{A}^{\mathsf{G}} = 1]. \quad (1)$$

We define prf-advantage and prp-advantage of $\mathcal{A}$ for an n-bit construction $\mathtt{F}$ respectively by

$$\mathbf{Adv}_{\mathtt{F}}^{\mathrm{prf}}(\mathcal{A}) := \mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathit{\Gamma}_n), \quad \mathbf{Adv}_{\mathtt{F}}^{\mathrm{prp}}(\mathcal{A}) = \mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathit{\Pi}_n)$$

. By a (q, ℓ, t)-distinguisher $\mathcal{A}$ we mean, $\mathcal{A}$ makes at most q queries (query-complexity) with at most ℓ-bits in each query (data-complexity) and runs in time at most t (time-complexity). One may include some other complexities, e.g., memory complexity. We write $\mathbf{Adv}_{\mathtt{F}}^{\mathrm{xxx}}(q,\ell,t) = \max_{\mathcal{A}} \mathbf{Adv}_{\mathtt{F}}^{\mathrm{xxx}}(\mathcal{A})$ where maximum is taken over all (q,ℓ,t)-distinguishers $\mathcal{A}$ and xxx denotes either prf or prp. A non-adaptive adversary fixes all its queries before it sees the responses.

Universal and Cover-Free. Now we define some other information-theoretic security advantages (in which there is no presence of an adversary). Let $\mathtt{F}$ be an n-bit random function then

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

Let $\mathtt{F}$ be a random function which outputs two blocks, denoted $(\Sigma, \Theta) \in (\{0,1\}^n)^2$. For a q-tuple of distinct messages $m = (m_1, \ldots, m_q)$, we write $\mathtt{F}(m_i) = (\Sigma_i, \Theta_i)$. For a q-tuple of pairs $(\sigma_i, \theta_i)_i$, we say that

1. σ_i (or θ_i) is **fresh** 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.

Definition 2. *We define* (q, L)-cover-free advantage *as*

$$\mathbf{Adv}_{\mathtt{F}}^{\mathrm{cf}}(q,L) = \max_{m \in \mathit{dist}_q} \mathit{Pr}[(\Sigma_i, \Theta_i)_i \text{ is not cover-free}].$$

Clearly, $\mathbf{Adv}_{\mathtt{F}}^{\mathrm{cf}}(q,L) \leq q^3 \mathbf{Adv}_{\mathtt{F}}^{\mathrm{cf}}(3,L)$. So it would be sufficient to concentrate on a triple of messages while bounding cover-free advantages. We say that a construction F is (q,L,t,ϵ)-xxx if $\mathbf{Adv}_{\mathtt{F}}^{\mathrm{xxx}}(q,L,t) \leq \epsilon$ where xxx denotes either univ or cf.

2.3 Coefficient H-Technique

In this section we discuss briefly Coefficient-H Tehcnique [20] which is also known as Decorrelation Theorem due to Vaudenay [25].

Definition 3 (statistical distance). *Let X and Y two random variables over a set S. We define the* **statistical distance** *between X and Y as*

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

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 $s \in E$. We state a tool 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 systems or probabilistic oracles.

Lemma 2 (coefficient H-technique for random variables). *Let X, Y be two random variables over S such that $X \succ_\epsilon Y$ over $\mathcal{V}_{\mathrm{good}} \subseteq S$ then,*

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

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

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

So,

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

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 (i) for all q-distinct messages* $m = (m_1, \ldots, m_q)$, $(\mathtt{F}(m_i))_i \succ_{\epsilon_1} (\mathtt{G}(m_i))_i$ *over* $\mathcal{V}_{good}$ *(ii)* $\mathsf{Pr}[\tau(\mathcal{A}^{\mathtt{G}}) \notin \mathcal{V}_{good}] \le \epsilon_2$ *then* $\mathbf{Adv}_{\mathcal{A}}(\mathtt{F}\ ;\ \mathtt{G}) \le \epsilon_1 + \epsilon_2$.

Proof. Condition (i) says that, for all $v \in V_{good}$, $\mathsf{Pr}[\tau(\mathcal{A}^{\mathtt{G}}) = v] - \mathsf{Pr}[\tau(\mathcal{A}^{\mathtt{F}}) = v] \le \epsilon_1.\mathsf{Pr}[\tau(\mathcal{A}^{\mathtt{F}}) = v]$. Now,

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

3 New Proposals for Beyond-Birthday 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.

3.1 1kf9-MAC

In this section we present the algorithm for 1kf9 MAC followed by its schematic diagram. For any message $M \in \{0,1\}^*$, 1kf9 Algorithm first prepends a all zero block to the message and pads it to make the length multiple of the block length n. Then M is iteratively processed through block cipher E_K as shown in Fig. 3.1 and the final tag T is obtained by XOR-ing $E_K(\Sigma)$ and $E_K(\Theta)$.

Input: $K \xleftarrow{\$} \mathcal{K}$, $M \leftarrow \{0,1\}^*$
Output: $T \in \{0,1\}^n$
$M \leftarrow 0^n||M||10^{n-1-len(M) \mod n}$;
$M_1, M_2, \ldots, M_l \leftarrow$ **Partition**(M);
$Y_0 \leftarrow E_K(0^n)$;
$Z \leftarrow Y_0$;
for $j = 1$ *to* l **do**
  $X_j = Y_{j-1} \oplus M_j$;
  $Y_j = E_K(X_j)$;
  $Z = (Z \oplus Y_j)$;
end
$\Theta^{'} = 2Z$;
$\Sigma^{'} = 2Y_l$;
$\Sigma = fix0(\Sigma^{'})$;
$\Theta = fix1(\Theta^{'})$;
$T \leftarrow E_K(\Sigma) \oplus E_K(\Theta)$;
Return T;

Algorithm 1: Algorithm of 1kf9-MAC

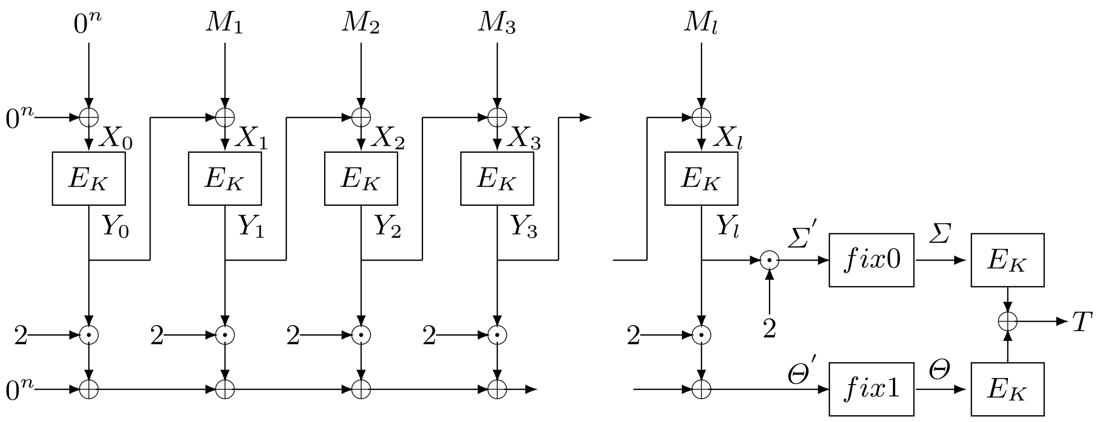

Fig. 3.1. Construction of 1kf9-MAC

3.2 1k-PMAC+

In this section we present the algorithm for 1k-PMAC+ followed by its schematic diagram. Δ_i is the encryption of field element Cst_i for $i = 1, 2$. After suitable

Input: $K \xleftarrow{\$} \mathcal{K}$, $M \leftarrow \{0,1\}^*$
Output: $T \in \{0,1\}^n$
$\Delta_i \leftarrow E_K(\mathrm{Cst}_i)$ for $i = 1, 2$;
$M \leftarrow M || 10^{n-1-len(M) \mod n}$;
$M_1, M_2, \ldots, M_l \leftarrow$ **Partition**(M);
for $j = 1$ *to* l **do**
  $X_j = M_j \oplus 2^{j-1} \cdot \Delta_1 \oplus 2^{2(j-1)} \cdot \Delta_2$;
  $Y_j = E_K(X_j)$;
end
$\Sigma^{'} = Y_1 \oplus Y_2 \oplus \ldots \oplus Y_l$;
$\Theta^{'} = 2^l \cdot Y_1 \oplus 2^{l-1} \cdot Y_2 \oplus \ldots \oplus 2 \cdot Y_l$;
$\Sigma = \mathsf{fix0}(\Sigma^{'})$;
$\Theta = \mathsf{fix1}(\Theta^{'})$;
$T \leftarrow E_K(\Sigma) \oplus E_K(\Theta)$;
Return T;

Algorithm 2: Algorithm of 1-Key PMAC+

padding of the message M, each block is processed in parallel fashion as shown in Fig. 3.2. $\Sigma^{'}$ is obtained by sum of the all the intermediate outputs and $\Theta^{'}$ is obtained by a linear combination of the intermediate outputs. Σ is obtained by fix0 on $\Sigma^{'}$ and Θ is obtained by fix1 on $\Theta^{'}$. Then the xor of $E_K(\Sigma)$ and $E_K(\Theta)$ is returned as the tag T of message M.

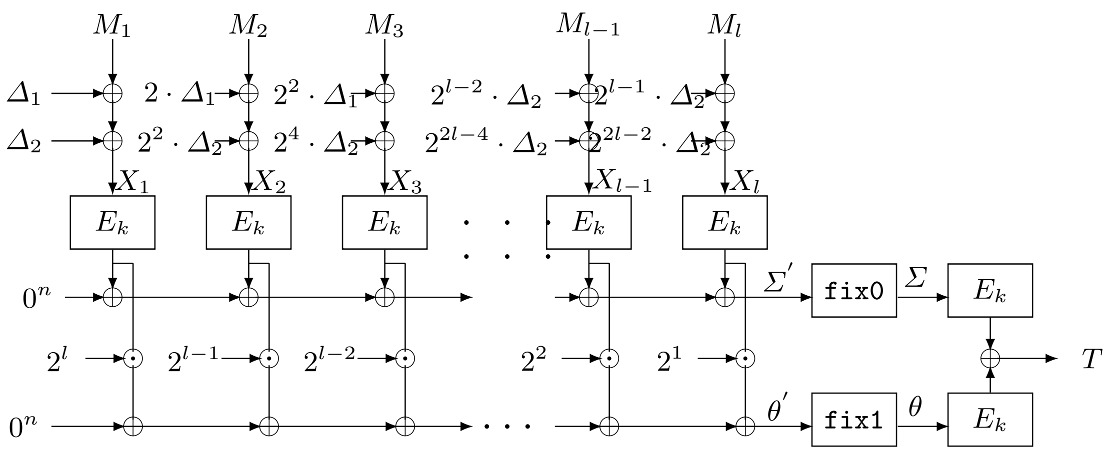

Fig. 3.2. Construction of 1Key PMAC+

3.3 Comparison Chart of Our Construction with 3kf9 and PMAC+

Construction	Reference	No.of Keys Required	Security Bound
Sum of CBC	[26]	4-Keys	$O(l^4q^3/2^{2n})/O(l^3q^3/2^{2n})$
PMAC+	[27]	3-keys	$O(l^3q^3/2^{2n} + lq/2^n)$
3kf9	[28]	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	$O(ql^2/2^n + q^3l^4/2^{2n} + q^4l^4/2^{3n} + q^4l^6/2^{4n})$

3.4 Design Rationale

In 1kf9, we prepend a 0 block message to ensure that $\Sigma, \Theta \neq 0$. Moreover, in order to ensure that $\Sigma \neq \Theta$, we fix the last bit of $\Sigma^{'}$ to 0 and that of $\Theta^{'}$ to 1.To ensure the deired rank as described in Section 9, we multiply the intermediate output with 2 and add them.

In 1k-PMAC+ we use a double mask that ensures the rank of bad equations described in Section 9 is at least 2 and we use `fix0` and `fix1` to ensure $\Sigma \neq \Theta$.

4 Some Results on Sampling Distributions

4.1 With (out) replacement sampling

Let $(Y_1, \ldots, Y_r) \stackrel{\text{wor}}{\leftarrow} S$ be a set of r samples drawn without replacement from a set S. In other words, the conditional distribution

$$Y_i \mid (Y_1, \ldots, Y_{i-1}) \stackrel{\$}{\leftarrow} S \setminus \{Y_1, \ldots, Y_{i-1}\}.$$

Similarly, for the with replacement sampling, we write $U := (U_1, \ldots, U_r) \stackrel{\text{wr}}{\leftarrow} S$ 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 $U := (U_1, \ldots, U_q) \stackrel{\text{wr}}{\leftarrow} \{0,1\}^n$. 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 over $\{0,1\}^n$): $Y_1 = (Y_{1,1}, \ldots, Y_{1,q}) \stackrel{\text{wor}}{\leftarrow} \{0,1\}^n$ and $Y_2 = (Y_{2,1}, \ldots, Y_{2,q}) \stackrel{\text{wor}}{\leftarrow} \{0,1\}^n$ and $Y_1 \perp Y_2$.

Case-2 (sum of two dependent WOR over $\{0,1\}^n$): $(Y_{1,1}, Y_{2,1}, \ldots, Y_{1,q}, Y_{2,q}) \stackrel{\text{wor}}{\leftarrow} \{0,1\}^n$.

Case-3 (sum of two dependent WOR over S): $(Y_{1,1}, Y_{2,1}, \ldots, Y_{1,q}, Y_{2,q}) \stackrel{\text{wor}}{\leftarrow} S \subseteq \{0,1\}^n$ for a set S with size $2^n - \sigma$, $\sigma \geq 0$.

For the first two cases, Bellare et.al [2] had shown that $\Delta(Z\ ;\ U) \leq \frac{q}{2^n} + \mathcal{O}(n \times (\frac{q}{2^n})^{1.5})$. Their analysis uses some advanced results of probability theory (e.g., Azuma's inequality and Chernoff theorem). For the first case, later Lucks [14] provided an elementary proof with the upper bound $\mathcal{O}(q^3/2^{2n})$ and Patarin [22] provides a much involved complex proof with the upper bound $\mathcal{O}(q/2^n)$.

In this paper, we consider the third case which also generalizes case 2 when $S = \{0,1\}^n$. Our analysis is similar to that of Lucks [14] but much more simplified and can be similarly applicable to the first case. In the next section, we see the application of this result for analyzing one-key constructions of a specific form. We now state the key lemma which would be used to bound the statistical distance between sum of WOR sampling and WR sampling.

Lemma 3 (1-interpolation probability of sum of WOR samples). *Let $S' \subseteq \{0,1\}^n$ be a subset of size $(2^n - s')$ and $U_n \stackrel{\$}{\leftarrow} \{0,1\}^n$. Let $(V, W) \stackrel{\text{wor}}{\leftarrow} S'$ 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,

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

Observation 1. The above result is also valid if $(V, W) \stackrel{\$}{\leftarrow} S' \times T'$ such that $|S'| = |T'| = 2^n - s'$. Then, exactly same argument and hence result holds (i.e., $V \oplus W \succ_\epsilon U_n$ over $\mathbb{F}_{2^n}^*$. When $s' \leq 2^{n-1}$, $\epsilon \leq 4s'^2/2^{2n}$.

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

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

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 3 with $S' = \{0,1\}^n \setminus \{a_j : -s < j \leq 2i-2\}$ and $s' = s + 2(i-1)$, we have

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

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

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

Observation 2. Same argument also works when $Y_1 := (Y_{1,1}, Y_{1,2} \ldots, Y_{1,q}) \xleftarrow{\text{wor}} S$, $Y_2 := (Y_{2,1}, Y_{2,2}, \ldots, Y_{2,q}) \xleftarrow{\text{wor}} T$ are two q-samples and $Y_1 \perp Y_2$ where S and T are two subsets of $\{0,1\}^n$ of size $2^n - s$. 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 our Observation 1, the Equation (2) holds with $\epsilon_i = s_i'^2/(2^n - s'_i)^2$. After simplifying $\sum_i \epsilon_i$, we can conclude that $Z \succ_\epsilon U$ where $\epsilon = \frac{qs^2 + sq^2 + q^3/3}{(2^n - s - q)^2} \leq \frac{4qs^2 + 4sq^2 + 4q^3/3}{2^{2n}}$ provided $s + q < 2^{n-1}$.

Now we summarize our results in the view of all cases we initially aimed to answer. We denote $Z_i = X_i \oplus Y_i$ and $Z = (Z_1, \ldots, Z_q)$ and $U := (U_1, \ldots, U_q) \xleftarrow{\text{wr}} \{0,1\}^n$.

Corollary 1. *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*

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

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

Corollary 2. *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 (a) in (**Case-3**),*

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

over $\mathbb{F}_{2^n}^*$.
*If in addition if $q \leq s$ then $\Delta(Z \ ; \ U) \leq \frac{q}{2^n} + \frac{18s^3}{2^{2n}}$. (b) For $s = 0$ (i.e, in **Case-2**) we have $\Delta(Z \ ; \ U) \leq \frac{q}{2^n} + \frac{6q^3}{2^{2n}}$ over $\mathbb{F}_{2^n}^*$.*

4.2 Applications to PRF Security of Sum of 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 $\Pi^{(q)}(x) := (\Pi(x_1), \ldots, \Pi(x_q)) \stackrel{\text{wor}}{\leftarrow} \{0,1\}^n$. So when Π_1 and Π_2 are two independent uniform random permutations then, $\Pi_1^{(q)}(x) \stackrel{\text{wor}}{\leftarrow} \{0,1\}^n$, $\Pi_2^{(q)}(x) \stackrel{\text{wor}}{\leftarrow} \{0,1\}^n$ and $\Pi_1^{(q)}(x) \perp \Pi_2^{(q)}(x)$ where $x \in \mathsf{dist}$.

Case-a. The **Case-1** 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 Corollary 1, we have

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

Case-b. **Case-2** 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 (b) of Corollary 2 we have,

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

The above construction has been analyzed in [2].

Case-c. Now we come to the **Case-3** which deals with the pseudorandomness of $(\Pi^*(x_1) \oplus \Pi^*(x_2), \ldots, \Pi^*(x_{2q-2}) \oplus \Pi^*(x_{2q}))$ where $\Pi^* \stackrel{\$}{\leftarrow} \mathbb{P}_{a \to b}$ 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, for all $q \leq s$, we have

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

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 (a) of Corollary 2.

We define sum function over two blocks as follows: $\mathsf{sum}^{\pi}(x,y) = \pi(x) \oplus \pi(y)$ and $\mathsf{sum}^{\pi_1,\pi_2}(x,y) = \pi_1(x) \oplus \pi_2(y)$

Theorem 3. *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 $t_1, \ldots, t_q \in \{0,1\}^n$,*

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

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 $(Y_1, Y_2) \stackrel{\text{wor}}{\leftarrow} S := \{0,1\}^n \setminus y$. Hence we can apply Theorem 2 to conclude our theorem. □

A simpler version of the above theorem when $s = 0$ and we consider sum of two uniform random permutations, we have the following result. The proof is again straightforward from Observation 2.

Theorem 4. *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 $s + q \le 2^{n-1}$ then, for any non-zero $t_1, \ldots, t_q \in \{0,1\}^n$, $\frac{1}{(2^n - s)^q} \ge \mathsf{Pr}[(\sigma_i, \theta_i)_i \stackrel{\mathsf{sum}^{\Pi_1,\Pi_2}}{\longmapsto} t \mid x \stackrel{\Pi_1}{\longmapsto} y,\ x' \stackrel{\Pi_1}{\longmapsto} y'] \ge 2^{-nq}(1 - \frac{4qs^2 + 4sq^2 + 4q^3/3}{2^{2n}})$.*

5 A Generic Hash-then-Sum Construction

An **affine mode** is a deterministic oracle algorithm whose query computations (functions) are affine functions and its oracle is some random function.

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

$$\mathcal{C}^\pi(m_1) = (\Sigma_1, \Theta_1), \mathcal{C}^\pi(m_2) = (\Sigma_2, \Theta_2) \ \Rightarrow\ \Sigma_1 \ne \Theta_2.$$

For any double construction, 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 $\mathcal{C}' = (\Sigma', \Theta')$ is block-separated where $\Sigma' = \mathsf{fix0}(\Sigma)$ and $\Theta' = \mathsf{fix1}(\Theta)$.

A Composition Theorem: PRF(U) ≡ PRF. It is well known [24] 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 prove the theorem using Patarin's Coefficient-H Techhnique.

Theorem 5. *Let $F_{K_1,K_2} := g_{K_2} \circ \mathcal{H}_{K_1} : \{0,1\}^* \to \{0,1\}^n$. Then,*

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

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

Proof. For the sake of completeness, we quickly revise the proof of the statement by using coefficient H-technique. By using standard reduction argument, we can consider the composition function $\Gamma_n \circ \mathcal{H}_{K_1}$ 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

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

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 $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{univ}}(\ell) = O(2^{-2n})$ and g has beyond birthday prf-security then we can achieve beyond birthday prf-security for the composition function [4] . 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 [19] or Benes-Butterfly construction [21]. However, we do not know any such single key efficient construction.

5.1 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 [2, 14]. 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.

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 [6], 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.

[4] 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.

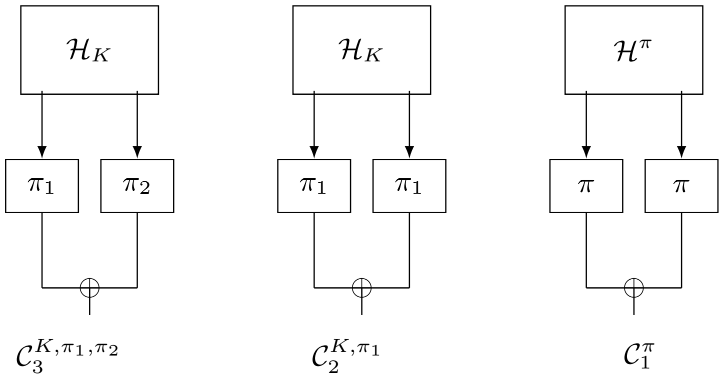

Fig. 5.1. Hash-then-Sum construction

5.1.1 Hash-then-sum based on PRF.

Lemma 4. *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,

$$E(\sigma, \theta) \;\equiv\; \big((\mathcal{H}_K(m_i))_{i \in [q]} = (\sigma_i, \theta_i)_{i \in [q]}\big).$$

Therefore,

$$\mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t \mid E] = \mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t] = \mathsf{Pr}[\varGamma_1(\sigma_i) \oplus \varGamma_2(\theta_i) = t_i, \forall i] = 2^{-nq}.$$

The first equation follows from the argument that the randomness for $\mathcal{H}$ is independent of $\varGamma_1$'s and $\varGamma_2$'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}. Therefore,

$$\begin{aligned}\mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t] &= \mathsf{Pr}[m \overset{\mathcal{C}_3}{\mapsto} t \mid E] \times \mathsf{Pr}[\ E] \\ &\leq \frac{(1-\epsilon)}{2^{nq}}\end{aligned}$$

where $\epsilon := \mathsf{Pr}[E^c]$. $\square$

Remark 1 *The above three-key construction is a potential candidate for having beyond birthday security. Note that from Definition2,* $\mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(q,\ell) \leq q^3\mathbf{Adv}^{\mathrm{cf}}_{\mathcal{H}}(3,\ell)$*. So, for any three messages* m_1, m_2, m_3 *with* $m_1 \neq m_2, m_3$*, if*

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

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 is feasible to have such a bound.*

5.1.2 Hash-then-Sum based on Pseudorandom Permutation.

Abstraction of PMAC+, 3kf9 PMAC_Plus [27] and 3kf9 [28] are block-cipher (assumed to be a pseudorandom permutation) based sum constructions. These are three-key construction like $\mathcal{C}_3$. After modeling a blockcipher to be a prf, one can apply the above Lemma 4. However, *block cipher can ensure prf with a maximum birthday bound security.* So we need to treat it differently to have beyond birthday analysis. The designers of PMAC_Plus and 3kf9 have proved the security for these individual constructions. Here, we abstract their analysis and provide a generic composition results. 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. As $\mathcal{H}_K$ is a 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.

Theorem 6. *Let* $\mathcal{H}_K$ *be a* (q, ϵ_{cf})*-cover-free function and for all* $i = 1, 2$*,* $\mathcal{H}_{K,i}$ *are* ϵ_{univ}*-universal hash functions. Then, the following holds.*

1. $\mathcal{C}_3 := \mathsf{sum}^{\Pi_1,\Pi_2} \circ \mathcal{H}_K$ *is* (q, ℓ, ϵ)*-prf where*

$$\epsilon = \epsilon_{cf} + (q + \frac{q^2}{2^n})\epsilon_{\mathrm{univ}} + \frac{6q^3\ell^3}{2^{2n}}.$$

2. $\mathcal{C}_2 := \mathsf{sum}^{\Pi} \circ \mathcal{H}_K$ *is* (q, ℓ, ϵ)*-prf where*

$$\epsilon = \epsilon_{\mathrm{cf}} + (2q + \frac{2q^2}{2^n})\epsilon_{\mathrm{univ}} + \frac{6q^3\ell^3}{2^{2n}}.$$

Proof. 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.

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 $\psi_i^{'}$, 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, this 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 to complete the interpolation probability for free indices.

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

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

For a random function Γ and for any adversary $\mathcal{A}$,

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

Now we fix any $t \notin \mathcal{V}_{bad}$ and a q-tuple m of distinct messages. We write $\mathcal{H}_K(m_i) = (\Sigma_i, \Theta_i)$, $1 \le i \le q$. Let $(\sigma_i, \theta_i)_{i \in [q]}$ be any tuple.

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
(iv) both σ_i and θ_i are not fresh.

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 $I = I_\Sigma \cup I_\Theta$.

We call a tuple $((\sigma_i, \theta_i)_{i \in [q]}, (\psi_j, w_j)_{j \in I})$ **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 $t_i = t_j$, $\sigma_i \ne \sigma_j$ and $\theta_i \ne \theta_j$,
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 that, w_j is the $\Pi(\psi_j)$.
Note, due to the choice of the q-tuple t, at most for $q/2$ pairs (i, j), $t_i = t_j$ can happen.

Interpolation probability for good tuple. 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 $m_I \xmapsto{\mathcal{C}_2} t_I$ is same as $\psi'_I \xmapsto{\Pi} w'_I$. Also, observe that, $\psi'_I \in \mathsf{dist}_s$ and $\psi \cap \psi' = \phi$ where $s = |I|$. 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, $(\psi'_I, \psi_I) \longleftrightarrow (w'_I, w_I)$.

Combining all these, 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

$$\begin{aligned}
\mathsf{Pr}[m \overset{\mathcal{C}_2}{\longmapsto} t \mid E] &= \mathsf{Pr}[m_{I^c} \overset{\mathcal{C}_2}{\longmapsto} t_{I^c} \mid E \wedge m_I \overset{\mathcal{C}_2}{\longmapsto} t_I] \times \mathsf{Pr}[m_I \overset{\mathcal{C}_2}{\longmapsto} t_I \mid E] \\
&\geq \mathsf{Pr}[(\sigma_i, \theta_i)_{i \in I^c} \overset{\mathsf{sum}^{\Pi}}{\longmapsto} t_{I^c} \mid (\psi_I, \psi'_I) \overset{\Pi}{\longmapsto} (w_I, w'_I)] \times \frac{1}{2^{ns}} \\
&\geq \frac{(1 - 6s^3/2^{2n})}{2^{nq}} \quad \text{[From (b) of Corollary 2]}
\end{aligned}$$

Now, we find our desired interpolation probability as we sum over all good tuples:

$$\begin{aligned}
\mathsf{Pr}[m \overset{\mathcal{C}_2}{\longmapsto} t] &\geq \sum_E \mathsf{Pr}[m \overset{\mathcal{C}_2}{\longmapsto} t \mid E] \times \mathsf{Pr}[E] \\
&\geq \frac{(1 - 6s^3/2^{2n})}{2^{nq}} \times (1 - \epsilon)
\end{aligned}$$

where $\epsilon = \mathsf{Pr}[(\Sigma_i, \Theta_i)_{i \in [q]}, (\Psi_i, \Pi(\Psi_i))_{i \in I}$ is not good $]$.

Bounding ϵ. By using the definition of good tuple and using the union bound, we have $\epsilon \leq \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4$ where $\epsilon_i = \mathsf{Pr}[E_i^c]$, $1 \leq i \leq 4$. Now we bound each ϵ_i as follows:

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

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

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

$$\begin{aligned}
\epsilon_3 &= \sum_{i \neq j : t_i \neq t_j} \mathsf{Pr}[i, j \in I, \Pi(\Psi_i) \oplus \Pi(\Psi_j) = t_i \oplus t_j] \\
&\leq \sum_{i,j,k,\psi_i,\psi_j : i \neq j, t_i \neq t_j} \mathsf{Pr}[\Pi(\Psi_i) \oplus \Pi(\Psi_j) = t_i \oplus t_j \mid \Psi_i = \Psi_k = \psi_i, \Psi_j = \psi_j] \\
&\qquad \times \mathsf{Pr}[\Psi_i = \Psi_k = \psi_i, \Psi_j = \psi_j] \\
&\leq \sum_{i,j,k,\psi_i,\psi_j : i \neq j, t_i \neq t_j} \mathsf{Pr}[\Pi(\psi_i) \oplus \Pi(\psi_j) = t_i \oplus t_j] \\
&\qquad \times \mathsf{Pr}[\Psi_i = \Psi_k = \psi_i, \Psi_j = \psi_j] \\
&\leq \sum_{i,k} \frac{1}{2^n - 1} \times \mathsf{Pr}[\Psi_i = \Psi_k]
\end{aligned}$$

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

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

Adding these four error terms, we obtain an upper bound of ϵ. By using coefficient H-technique, our result follows. □

5.2 PRF-security of Single Key Hash-then-Sum Construction

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 6. However, it requires to handle more bad cases. Now we first develop the basic notations and definitions similar to the two-key and three-key constructions.

Given any permutation π, let $\tau(\mathcal{H}(m) \rightarrow_q \pi) = (x, y)$ (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 $x = (x_{i,j} : i \in [q], j \in [L_i])$ and similarly y for the same index set. Note that $(\sigma_i, \theta_i)_i$ is uniquely determined by (x, y).

Definition 4. *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_k for any k. 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**. 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_j such that $\psi_i = x_j$, otherwise ψ_i is called **new**. We define $I_{old} = \{i : \psi_i \text{ is old}\}$ and similarly $I_{new} = \{i : \psi_i \text{ is new}\}$. Let $I = I_{old} \cup I_{new}$.

Definition 5. *We say that a tuple $((x, y), w_{I_{new}})$ 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. *$E_3 \equiv (x, \psi_I, \psi'_I) \longleftrightarrow (y, w_I, w'_I)$ where $w_i = y_{j,a}$ for all $i \in I_{old}$ with $\psi_i = x_{j,a}$ and $w'_i = w_i + t_i$, $\forall i \in I$.*

By definition of I and (ψ_I, ψ'_I) we have (i) $\psi'_I \in \mathsf{dist}$ and (ii) $\psi'_I \cap (x, \psi_I) = \phi$. Thus, the event E_3^c (in presence of E_1 and E_2) is equivalent to at least one of the following events happen:

1. $w_i \oplus w_j = t_i \oplus t_j$ for some $i, j \in I$ such that $t_i \neq t_j$.
2. $w_i \oplus t_i = y_{j,a}$ or $= w_k$ for some $k \in I$,

3. $w_i = y_{j,a}$ for some $i \in I_{new}$,
4. $(\psi_{I_{new}}, w_{I_{new}})$ is permutation compatible.

Note that the 4th bad equations can be easily avoided by choosing $w_{I_{new}}$ such that $(\psi_{I_{new}}, w_{I_{new}})$ is a permutation compatible. Now we identify and explicitly list down all the bad equations for which the tuple $((x, y), w_{I_{new}})$ is *not good*, in Table 5.2.

Fully 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)-Pseudo Cover-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)-Pseudo Cover-2	(L_{23}) $\Sigma_i = X_{k,a}, \Sigma_j = X_{l,b}, Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j$ (L_{24}) $\Theta_i = X_{k,a}, \Theta_j = X_{l,b}, Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j$ (L_{25}) $\Sigma_i = X_{k,a}, \Theta_j = X_{l,b}, Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j$
$(X, Y, w_{I_{new}})$ Pseudo Covered	(L_{31}) $\Sigma_i = X_{j,a}, Y_{j,a} \oplus t_i = w_{k,s}$ (L_{32}) $\Theta_i = X_{j,a}, Y_{j,a} \oplus t_i = w_{k,s}$ (L_{33}) $\Sigma_i = \Sigma_j, w_i + t_i = w_j + t_j$ (L_{34}) $\Sigma_i = \Sigma_j, w_i + t_i = w_j$ (L_{35}) $\Theta_j = X_{l,b}, Y_{k,a} \oplus Y_{l,b} = t_i \oplus t_j$

Table 1. Table representing bad equations for fully covered, pseudo-covered cases.

Definition 6. *1. A construction $\mathcal{H}^{\Pi}$ is called (q, ℓ, ϵ)-**extended-cover-free** if for all q-tuple m of distinct messages of size at most ℓ, $\mathsf{Pr}_{\Pi}[\exists$ fully covered $i] \leq \epsilon$.*

*2. It 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 $\mathsf{Pr}_{\Pi}[\exists i : i$ is(X, Y) pseudo-covered$] \leq \epsilon := \epsilon_1 + \epsilon_2$ where $\epsilon_1 := \mathsf{Pr}_{\Pi}[\exists i : i$ is(X, Y)-pseudo-cover-1$]$ and $\epsilon_2 := \mathsf{Pr}_{\Pi}[\exists i : i$ is(X, Y)-pseudo cover-2$]$.*

*3. It is called ϵ-**extended universal** if $\mathcal{H}_i^{\Pi}$'s are ϵ universal and 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 $j \in [L_i]$.*

Theorem 7. *If $\mathcal{H}$ is block-separated, $(q, \ell, \epsilon_{ecf})$-extended-cover-free, $(q, \ell, \epsilon_{pcf})$-pseudo-cover-free for a q-tuple t and ϵ_{euniv}-extended universal then $\mathcal{C}_1 := \mathsf{sum}^{\Pi} \circ \mathcal{H}^{\Pi}$ is (q, ϵ)-prf where*

$$\epsilon = \epsilon_{ecf} + \epsilon_{pcf} + 2q\epsilon_{euniv} + + \frac{18s^3}{2^{2n}}.$$

Note that we should expect $O(s^3/2^{2n})$ errors for ϵ_{ecf} and ϵ_{pcf} as it deals two (apparently) non-trivial equations. If so, then only we can claim *beyond birthday* security for the construction.

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

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

For a random function Γ and for any adversary $\mathcal{A}$,

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

Now we fix any $t \notin \mathcal{V}_{bad}$ and a q-tuple m of distinct messages.

Interpolation probability for good tuple. Let us fix a good tuple $((x, y), w_{I_{new}})$ as defined in Definition 5. We denote the event

$$E(x, y, w) \;\equiv\; \left(x \xmapsto{\Pi} y, \Pi(\Psi_i) = w_i \forall i \in I_{new}\right)$$

. 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 $s = |I|$. Due to the definition of good tuple $w_{I'} \in \mathsf{dist}$ and $w_{I'} \cap w_I = \phi$. Moreover (x, y) is permutation computable for Π. Therefore, $(x, \psi_I, \psi'_I) \longleftrightarrow (y, w_I, w'_I)$, where ψ'_I is element-wise distinct and distinct from other inputs.

Combining all these, 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

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

Now, we find our desired interpolation probability as we sum over all good tuples:

$$\begin{aligned}
\mathsf{Pr}[m \xmapsto{\mathcal{C}_1} t] &\geq \sum_E \mathsf{Pr}[m \xmapsto{\mathcal{C}_1} t \mid E] \times \mathsf{Pr}[E] \\
&\geq \frac{(1 - 18s^3/2^{2n})}{2^{nq}} \times (1 - \epsilon)
\end{aligned}$$

where $\epsilon = \mathsf{Pr}[(X, Y)_{i \in [q]}, (\Pi(\Psi_j))_{j \in I} \text{ is not good }]$.

Bounding ϵ. By using the definition of good tuple and using the union bound, we have $\epsilon \leq \epsilon_1 + \epsilon_2 + \epsilon_3$ where $\epsilon_i = \mathsf{Pr}[\ E_i^c], 1 \leq i \leq 3$. Now we bound each ϵ_i as

follows
(a) $\epsilon_1 = \mathsf{Pr}[(x, y)$ is not extended-cover-free$] \leq \epsilon_{\mathrm{ecf}}$.
(b) $\epsilon_2 = \sum_{i \neq j : t_i = t_j} (\mathsf{Pr}[\Sigma_i = \Sigma_j] + \mathsf{Pr}[\Theta_i = \Theta_j]) \leq 2q\epsilon_{\mathrm{univ}}$.
(c) $\epsilon_3 = \epsilon_{\mathrm{pcf}}$ as the event E_3^c in presence of E_1 and E_2 is same as violating pseudo-cover-free.
Summing these four error terms, we obtain an upper bound of ϵ. The rest follows by using coefficient H-technique. □

6 A Generic PRF Bound using Rank and Accident

6.1 Some Notes from Linear Algebra

A linear equation $L(X_1, \ldots, X_s) := L_1 \cdot X_1 + \cdots + L_s \cdot X_s$ over the finite field $\mathbb{F}_{2^n}$ [5] of size 2^n with s variables can be identified as an s-tuple $(L_1, \ldots, L_s)$. 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 $bX_1 + (a+c)X_2$. One can also eliminate X_1, X_3, X_5 and so the choice of free and determined variables are not unique. In this paper we keep the variables whose indices are minimum 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

$$\text{for all } x, \quad \sim_x = \sim \;\; \Rightarrow \;\; L^{\sim}(x_I) = L(x). \tag{5}$$

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 variablesof $\mathcal{R}$ after applying the linear restrictions

[5] 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.

$\mathcal{R}$. Let X_I be the free variables in $\mathcal{R}$ which determine the rest of the variables.[6] 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

$$\forall L' \in \mathcal{R}, L'(x) = 0 \Rightarrow L^{\mathcal{R}}(x_I) = L(x). \tag{6}$$

In the last section, we have seen that one-key sum-based construction can be bounded in term of the advantages of extended-cover-free, pseudo-cover-free and universal properties of the underlying construction $\mathcal{C}^{\Pi}$. In case of an affine mode, all these advantages are probability of some affine equations over Y, the intermediate output tuple. Even if the equations happens to be linearly independent, we cannot have an estimate of these events (i.e extended-cover-free, pseudo-cover-free and universal) as Y_i's are dependent. So we need to identify a sub-tuple Y_I which behaves "like uniform and independent random variables" and then express the linear equations in terms of Y_I. In the following subsection, we formally define what we mean by "behaves like uniform and independent".

6.2 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 7. *$(X_1, \ldots, X_q)$ is called* ϵ**-almost-independent** *if for all $t_1, \ldots, t_q$, and for all i, the conditional probability*

$$\mathit{Pr}[X_i = t_i \mid X_1 = t_1, \ldots, X_{i-1} = t_{i-1}] \leq \epsilon.$$

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.

Example 1. Suppose $\{\mathcal{E}_i(x) : 1 \leq i \leq s\}$ is a set of s affine equations[7] over $GF(2^n)$ in q variables $x_1, \ldots, x_q$. We write $\neg\mathcal{E}_i(x)$ to denote the affine inequation. We write the set

$$\mathcal{E}' = \{(x_1, \ldots, x_q) \in GF(2^n)^q : \forall i, \neg\mathcal{E}_i(x)\}.$$

Let $X := (X_1, \ldots, X_q)$ be a WR samples from S. Then, the conditional distribution of

$$X \mid (\neg\mathcal{E}_i(X))_i \text{ is } (2^n - s)^{-1}\text{-almost-independent.}$$

[6] Like collision relation, choice of I is not unique. However, we implicitly fix a choice.
[7] For example, when $\mathcal{E}(x) = \{x_i = x_j : i \neq j\}$.

As X is uniform, the conditional distribution is actually uniformly sampled from the set $\mathcal{E}'$ and hence the conditional distribution of X_i given $(X_j)_{j \neq i}$ is uniform over a set of size at least $2^n - s$.

Lemma 5. *Let $X_1, \ldots, X_q$ is ϵ-almost-independent over $GF(2^n)$, and let L_1, $\ldots$, 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*

$$\mathsf{Pr}[L_i(X_1, \ldots, X_q) = c_i, 1 \leq i \leq q] \leq \epsilon^r. \quad (7)$$

Proof. By using elementary operations on the vectors L_i's we can equivalently express the set of equations as $L'_i(X_1, \ldots, X_{a_i}) = c'_i$, $1 \leq i \leq r$. Now, note that X_i is almost independent conditioned on $X_1, \ldots, X_{i-1}$ with probability at most ϵ. As there are r many linearly independent equations we can find r many such $X'_i s$. Thus the result holds. □

Remark 2 *Almost-independent is important for bounding the set of linearly independent equations. In general, we can not bound it..*

6.2.1 Conditional WOR Sampling Now we consider a variant of WOR sampling, called **conditional WOR sampling**. This sampling scheme is motivated from the affine mode. More precisely, 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, $1 \leq i \leq \sigma'$. The samples $Y = (Y_1, \ldots, Y_L)$ is defined as follows.

1. For $i = 1$ to L, we define X_i and Y_i recursively as follows:
   - $X_i = A_i(Y_1, \ldots, Y_{i-1})$ and
   - $Y_i = \begin{cases} Y_j & \text{if for some } j < i, X_i = X_j; \\ \xleftarrow{\$} \{0,1\}^n \setminus \{Y_j : 1 \leq j < i\} & \text{otherwise.} \end{cases}$

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. The details are given below.

Definition 8. *Let $Y = (Y_1, \ldots, Y_L)$ be an A-conditional WOR L-sample. We define an (induced) equivalence relation $\sim_Y$ on $[L]$ 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

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

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

Definition 9 (accident [4, 18]). *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 $\sim$.

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 $(2^n - L^2)^{-1}$-almost-independence.*

Proof. We identify a set of inequations $\neg\mathcal{E}$ and then we show that $Y_I \mid \sim_Y = \sim$ and $U_I \mid \neg\mathcal{E}(U_I)$ have same distributions where U_I is the WR sample. Thus from Example 1 the result follows. □

6.3 Connection between conditional WOR sample and blockcipher based Affine Construction

Let $\mathcal{C}$ be an affine construction meaning that the intermediate inputs (the inputs of the blockcipher) is an affine function of previous intermediate outputs 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 (which is same as the **structure graph** in case of CBC construction) [4] on intermediate outputs Y with s many classes,
2. accident $a := \mathsf{acc}^m(\pi)$, representing the number of linearly independent restrictions and
3. and a set of indices I of size $s - a$ such that Y_I is $(2^n - (\sigma')^2)$-almost-indp where σ' is the total number of message blocks.

We say that a permutation is **not allowed** 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 6 ([18]). *For any realizable equivalence relation $\sim$ with accident a $\mathsf{Pr}[\sim_Y = \sim] \leq \frac{1}{(2^n-L)^a}$. 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 $\binom{s}{2}^a$.

Lemma 7. *Probability that a random permutation is not allowed for a tuple of q messages is at most*

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

A not allowed permutation will be treated as a bad permutation. 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).

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

Lemma 8. *If $\mathcal{C}$ is $(\epsilon, 3)$-extended-cover-free then $\mathcal{C}$ is $(\binom{q}{3}\epsilon, q)$-cover-free. Similarly, if $\mathcal{C}$ is $(\epsilon, 3)$-pseudo-cover-free-1 then $\mathcal{C}$ is $(\binom{q}{3}\epsilon, q)$-pseudo-cover-free-1. Moreover 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 7, 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 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 $\mathcal{L}'(Y_I)$ is the reduced form of the equation $\mathcal{L}(Y)$ after applying equivalence relation and the $'a'$ restrictions induced by the accidents. Let $\{\mathcal{L}_i : i \in B\}$ be a set of systems of linear equations. Note that for all $i \in B$, $\mathcal{L}_i$ 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 5.2. We have another set of single equations indexed by B' as shown in Table 6.4. Let $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4$ denote the set of system of bad equations defined as follows $\mathcal{B}_1 := \{L_{11}, L_{12}, L_{13}, L_{14}\}$, $\mathcal{B}_2 := \{L_{21}, L_{22}\}$, $\mathcal{B}_3 := \{L_{23}, L_{24}\}$(Refer to

(L_{31})	$\Sigma_i = \Sigma_j$
(L_{32})	$\Sigma_i = X_{j,a}$
(L_{33})	$\Theta_i = \Theta_j$
(L_{34})	$\Theta_i = X_{j,a}$

Table 2. Table representing single bad equations.

Table 5.2), and $\mathcal{B}_4 := \{L_{31}, L_{32}, L_{33}, L_{34}\}$(Refer to Table 6.4). Let $N_{r,j}$ denote the number of pairs of the form $(\sim, \mathcal{L}_i)$ for some $i \in \mathcal{B}_j$, for $j \in \{1, 2, 3, 4\}$ 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.

Lemma 9. *Let $m = (m_1, m_2, \ldots, m_q)$ be a q-tuple of distinct messages and $t = (t_1, t_2, \ldots, t_q) \notin \mathcal{V}_{bad}$. Let $L^3 \leq 2^n$. Then,*

$$Pr[\Pi \text{ is bad}] \leq O(q/2^{2n/3}) + q^3\epsilon_{ecf} + q^3\epsilon_{pcf1} + q^4\epsilon_{pcf2} + q\epsilon_{euniv}$$

Lemma 10. *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 $L^3 \leq 2^n$. Then,*

(1) $\epsilon_{ecf} \leq \sum_{r=0}^{4} N_{r,1}/2^{nr}$
(2) $\epsilon_{pcf1} \leq \sum_{r=0}^{4} N_{r,2}/2^{nr}$
(3) $\epsilon_{euniv} \leq \sum_{r=0}^{2} N_{r,4}/2^{n(r+1)}$

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 $\epsilon_{pcf2} \leq \sum_{r=0}^{5} N_{r,3}/2^{nr}$.

7 PRF Security Analysis of 1kf9

In this section we analyze the security of our propopsed construction 1kf9. Mainly we prove the following theorem.

Theorem 8.

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

where $t' = t + \mathcal{O}(qL)$ for any L-blocks message m.

7.1 Revisiting Structure Graph

In this section we revisit the structure graph introduced by Bellare et.al in [4]. 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 10. *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 [4].

Definition 11. *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.

7.2 Characterization of Valid Structure Graphs with 3 and 4 Messages

Definition 12. *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.

7.2.1 Important Properties of Valid Structure Graphs for 3 Messages

Lemma 11. *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. 7.1. Now we make the following two important observations :

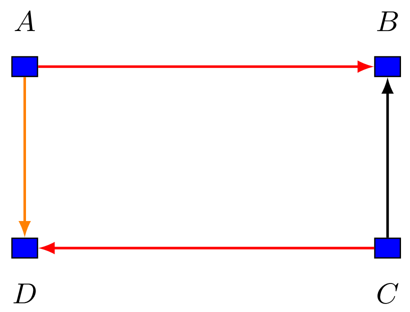

Fig. 7.1. Alternating cycle of length 4

(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 12. *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. □

7.2.2 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 11, a valid structure graph with 3 messages cannot contain a 4-length alternating cycle. □

Lemma 13. *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 14. *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 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 diagram. The other two edges must meet at a fifth node, say E. [Show the table].

Lemma 15. *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

7.2.3 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. 7.2:

(II) Acc = 1 for 3 **messages**: From Lemma 11, 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 7.3.

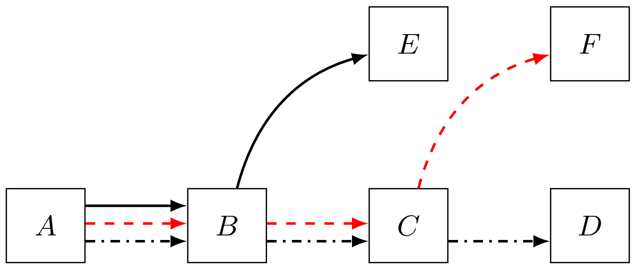

Fig. 7.2. Structure graph of 3 messages with $Acc = 0$

(III) Acc = 0 for 4 **messages** As no accident is present, the only possible structure graph has the following structure depicted in Fig. 7.4:

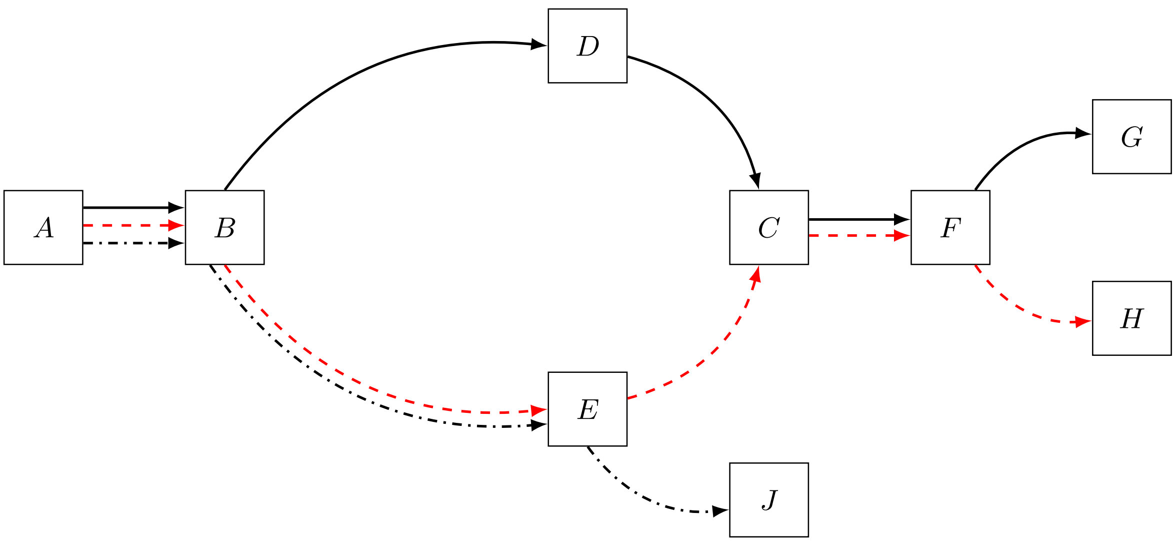

Fig. 7.3. Structure graph of 3 messages with $Acc = 1$ (at node C)

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

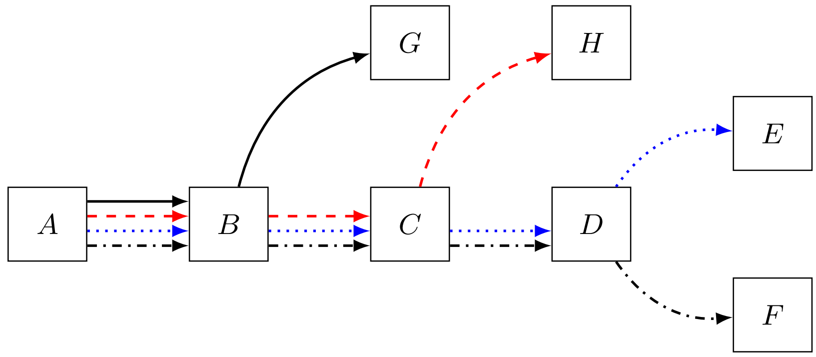

Fig. 7.4. Structure graph of 4 messages with $Acc = 0$

- 1 accident with 1 collision point: This graph is shown in Fig. 7.5 .
- Graph with 1-alternating cycle: This graph is shown in Fig. 7.6 .

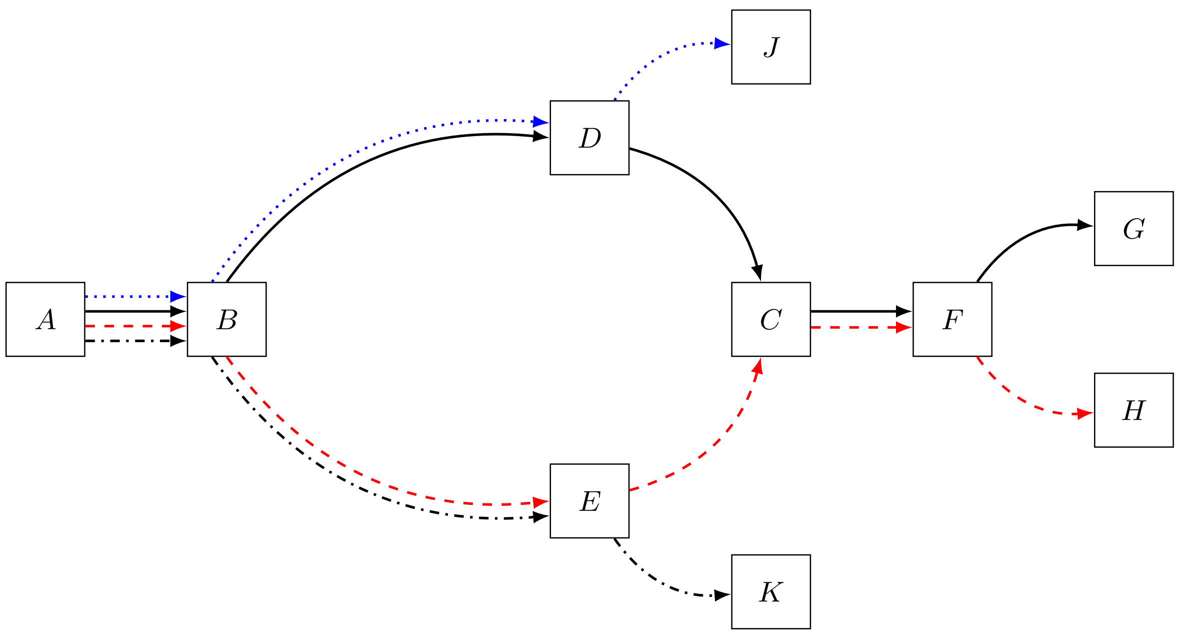

Fig. 7.5. Structure graph of 4 messages with $Acc = 1$ (at node C)

(V) Acc = 2 for 4 **messages**: From Lemma 13 and 15, we observe that, there can be no valid graphs with alternating 4-cycle or alternating 6 cycle. 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. 7.7.

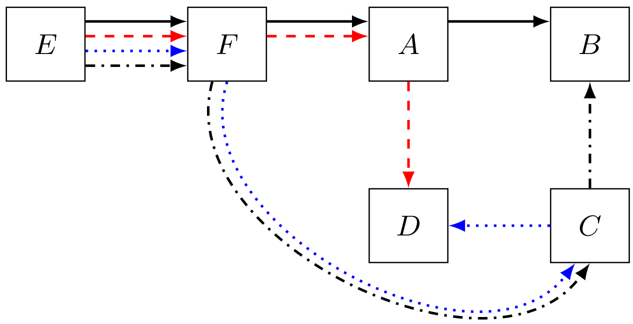

Fig. 7.6. Structure graph of 4 messages with $Acc = 1$ (at node B) and an induced collision (at node D)

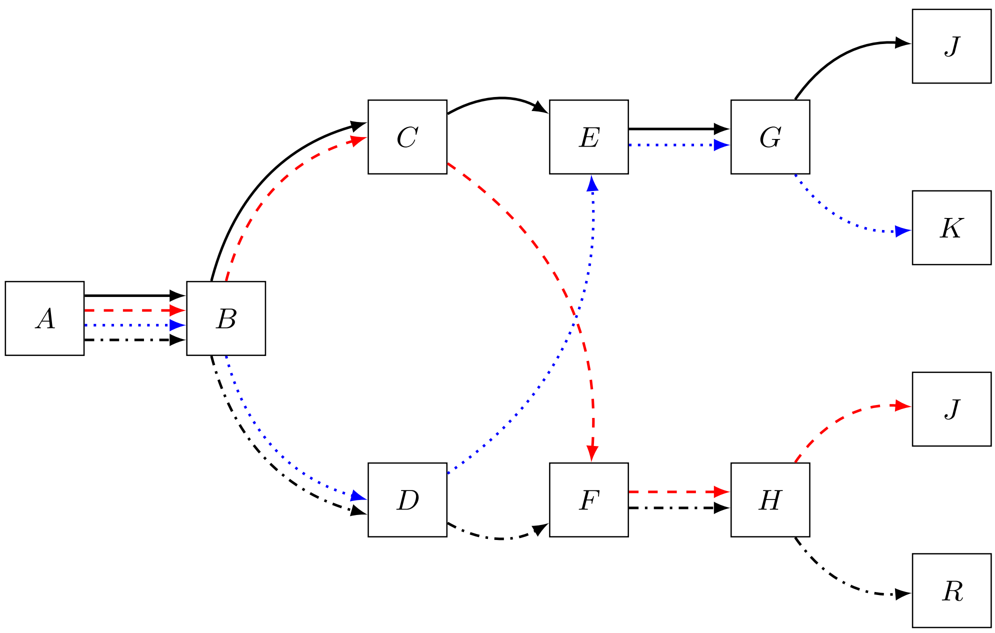

Fig. 7.7. Structure graph of 4 messages with $Acc = 2$ (at nodes E and F)

8 Rank Analysis of Systems of Equations for Bad Cases

8.1 Rank Analysis of Fully Covered Bad Equations

8.1.1 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:

$$\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = 0^{n-1}1 \tag{8}$$
$$Y_{i,p+1} + \dots Y_{i,l_i} + Y_{k,p+1} + \dots Y_{k,l_j} = 0 \tag{9}$$

Now it is to be noted that, if M_k is a prefix of M_i, then $Y_{i,p+1} + \dots Y_{i,l_i}$ 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 $Y_{i,p+1} + \dots Y_{i,l_i} + Y_{k,p+1} + \dots Y_{k,l_j}$ 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

$$Y_{i,\beta} + Y_{j,\gamma} = m \tag{10}$$

along with Equation (8) and (9). 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 $fix0(\alpha Y_{i,l_i}) = fix0(\alpha Y_{j,l_j})$. Note that, considering case (i), this is equivalent to considering the equation $Y_{i,\beta} + Y_{j,\gamma} = m$. According to our assumption p be the last index where M_i and M_k is identical. Therefore, as argued before, $Y_{i,p+1} + \dots Y_{i,l_i} + Y_{k,p+1} + \dots Y_{k,l_j}$ 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 (8). 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.

8.1.2 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:

$$\alpha Y_{i,l_i} + Y_{j,r-1} + M^{j,r} = 0 \tag{11}$$
$$Y_{i,p+1} + \dots Y_{i,l_i} + Y_{k,p+1} + \dots Y_{k,l_k} = 0 \tag{12}$$

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 (12). 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

$$Y_{i,\beta} + Y_{j,\gamma} = m \tag{13}$$

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 (12), such that the rank becoms 2 again.

8.1.3 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:

$$\alpha Y_{i,l_i} + \alpha Y_{j,l_j} = 0^{n-1}1 \tag{14}$$
$$\alpha(Y_{i,0} + Y_{i,1} + \ldots Y_{i,l_i}) = Y_{k,r-1} + m_r \tag{15}$$

From Equation (14) and (15), 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 (14) and (15), we have an additional equation

$$Y_{i,\beta} + Y_{j,\gamma} = m.$$

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 $fix0(\alpha Y_{i,l_i}) = fix0(\alpha Y_{j,l_j})$. Note that, considering case (i) is equivalent to considering the equation $Y_{i,\beta} + Y_{j,\gamma} = m$. 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 (14). Therefore, we identify Y_{i,l_i} and $Y_{i,0}$, such that the rank becomes 2 again.

8.1.4 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:

$$\alpha Y_{i,l_i} + Y_{j,s-1} = m^* \tag{16}$$
$$\alpha(Y_{i,0} + Y_{i,1} + \ldots Y_{i,l_i}) = Y_{k,r-1} + m^{**} \tag{17}$$

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

$$Y_{i,\beta} + Y_{j,\gamma} = m.$$

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

8.2 Rank Analysis of Single Equations

8.2.1 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 $fix0(\alpha Y_{i,l_i}) = fixo(\alpha Y_{j,l_j})$. Therefore, considering case (ii) boils down to considering the Equation (18) which is induced by the accident.

$$Y_{i,\beta} + Y_{j,\gamma} = m. \tag{18}$$

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

8.2.2 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 $Y_{i,\beta} + Y_{j,\gamma} = m$. 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.

8.2.3 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 $Y_{i,\beta} + Y_{k,\gamma} = m$. 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.

8.2.4 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

$$Y_{i,p+1} + \dots Y_{i,l_i} + Y_{j,p+1} + \dots Y_{j,l_j} = 0 \tag{19}$$

Note that there must be at least three distinct variables in Equation (19). 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 $Y_{i,\beta} + Y_{k,\gamma} = m$. 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.

8.3 Rank Analysis of Pseudo-Covered Bad Equations with 3 Messages

8.3.1 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:

$$\alpha Y_{i,l_i} + Y_{j,r-1} = m_{j,r} \tag{20}$$

$$Y_{j,r} + Y_* = t_i \tag{21}$$

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

$$Y_{i,s} + Y_{j,t} = m$$

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.

8.3.2 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.

8.4 Rank Analysis of Pseudo-Covered Bad Equations with 4 Messages

8.4.1 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:

$$\alpha Y_{i,l_i} + Y_{k,e-1} = m^* \tag{22}$$

$$\alpha Y_{j,l_j} + Y_{l,f-1} = m^{**} \tag{23}$$

$$Y_{k,e} + Y_{l,f} = t_i + t_j \tag{24}$$

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 (35) along with the previous three equations.

$$Y_{i,s} + Y_{j,t} = m. \tag{25}$$

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 (36) as below.

$$Y_{k,s'} + Y_{l,t'} = m'. \tag{26}$$

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.

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

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

$$\alpha Y_{i,l_i} + Y_{k,e-1} = m^* \tag{27}$$

$$\alpha(Y_{j,0} + Y_{j,1} + \ldots + Y_{j,l_j}) + Y_{l,f-1} = m^{**} \tag{28}$$

$$Y_{k,e} + Y_{l,f} = t_i + t_j \tag{29}$$

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 (35) along with the previous three equations.

$$Y_{i,s} + Y_{j,t} = m. \tag{30}$$

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 (36) as below.

$$Y_{k,s'} + Y_{l,t'} = m'. \tag{31}$$

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.

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

This case is similar to the previous case, where $\mathcal{L}(Y) = (\Sigma_i = X_{k,e}, \Theta_j = X_{l,f}, Y_{k,e} + Y_{l,f} = t_i + t_j$.

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

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

$$\alpha(Y_{i,0} + Y_{i,1} + \ldots + Y_{i,l_i}) + Y_{k,e-1} = m^* \tag{32}$$

$$\alpha(Y_{j,0} + Y_{j,1} + \ldots + Y_{j,l_j}) + Y_{l,f-1} = m^{**} \tag{33}$$

$$Y_{k,e} + Y_{l,f} = t_i + t_j \tag{34}$$

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 (35) along with the previous three equations.

$$Y_{i,s} + Y_{j,t} = m. \tag{35}$$

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 (36) as below.

$$Y_{k,s'} + Y_{l,t'} = m'. \tag{36}$$

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.

9 PRF Security Analysis of 1kPMAC_Plus

9.1 Preparation

Taking advantage of Theorem 7, to prove the PRF security of 1kPMAC_Plus, we need to upper bound its three items, extended-cover-free ϵ_{ecf}, pseudo-cover-free ϵ_{pcf}, and block-wise universal ϵ_{au}.

To show they are sufficiently small, we would define some bad events on inputs to block ciphers. Each bad event 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 events. Then notice that there are totally $2^n!$ permutations, we get the occurrence probability for each bad event.

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 $\mathit{\Delta}_1 = \pi(\mathrm{Cst}_1)$ and $\mathit{\Delta}_2 = \pi(\mathrm{Cst}_2)$, 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 $\mathit{\Delta}_1, \mathit{\Delta}_2$ 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,

$$\begin{bmatrix} 2^{l1-1} \oplus 2^{l2-1},\ 2^{2(l1-1)} \oplus 2^{2(l2-1)} \\ 2^{l1-1} \oplus 2^{l3-1},\ 2^{2(l1-1)} \oplus 2^{2(l3-1)} \end{bmatrix} \times \begin{bmatrix} \mathit{\Delta}_1 \\ \mathit{\Delta}_2 \end{bmatrix} = \begin{bmatrix} M_{i1,l1} \oplus M_{i2,l2} \\ M_{i1,l1} \oplus M_{i3,l3} \end{bmatrix}.$$

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 $\mathit{\Delta}_1$ and $\mathit{\Delta}_2$ 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.

9.2 Upper Bounding extended-cover-free ϵ_{ecf}

According to the definition of extended-cover-freeness, we have 9 bad events in this case, because in the previous inputs to block ciphers, we have both $\mathit{\Delta}_1 = \pi(\mathrm{Cst}_1)$, $\mathit{\Delta}_2 = \pi(\mathrm{Cst}_2)$, and $Y_{i,l} = \pi(X_{i,l})$, as listed in Table. 4.

1. $\exists \mathit{\Sigma}_i = \mathrm{Cst}_{j1}$ for some $j1 \in [2]$ and $\mathit{\Theta}_i = \mathrm{Cst}_{j2}$ 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 $(2^{l1-1} \oplus 2^{l2-1})\mathit{\Delta}_1 \oplus (2^{2(l1-1)} \oplus 2^{2(l2-1)})\mathit{\Delta}_2 = M_{l1}^i \oplus M_{l2}^i$, 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 $\mathit{\Delta}_1$, $\mathit{\Delta}_2$ 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

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 0, & 0, & \cdots, & 0 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 2^{\ell_u}, & 2^{\ell_u - 1}, & \cdots, & 2^1 \end{bmatrix} \times \overrightarrow{Y[i,u]} = \begin{bmatrix} \mathrm{Cst}_j \\ 0^n \end{bmatrix}, \tag{37}$$

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,ℓ_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,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 $[1, 0; 2^1 \oplus 2^2, 2^1]$ (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. (37) should be combined, if their corresponding variables belong to 2-collisions or trivial collisions. This makes the final coefficients matrix of Eq. (37) 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

$$\begin{bmatrix} 1, & 1, & \cdots, & 1, & 1, & 1, & \cdots, & 1 \\ 2^{\ell_i}, & 2^{\ell_i - 1}, & \cdots, & 2^1, & 2^{\ell_u}, & 2^{\ell_u - 1}, & \cdots, & 2^1 \end{bmatrix} \times \overrightarrow{Y[i,u]} = \begin{bmatrix} 0^n \\ 0^n \end{bmatrix}. \quad (38)$$

i. If $\ell_i = \ell_u$, let us denote $Y_{*,l} = Y_{i,l} \oplus Y_{u,l}$, then Eq. (38) 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. (38) 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. (38) 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

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

9.3 Upper Bounding pseudo-cover-free ϵ_{pcf}

According to the definition of ϵ_{pcf}, we need to upper bound the occurrence probability of 36 bad events, as listed in Table. 5 and 6.

1. For the cases from 1 to 6, $\Sigma_i = \mathrm{Cst}_{j1}$ for some $j1 \in [2]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} Y_{i,l} = \mathrm{Cst}_{j1}$, i.e. an equation over variables $Y_{i,l}$.
   On the other side, notice that by $\Sigma_i = \mathrm{Cst}_{j1}$ we have $\pi(\Sigma_i) = \pi(\mathrm{Cst}_{j1}) = \Delta_{j1}$. This means, $\pi(\Sigma_i) \oplus c_i = \Delta_{j1} \oplus c_i$. Then, though the cases from 1 to 6 imply different equations, they all depend on random variable Δ_{j1}. Notice that we have restrict $c_i \neq 0^n$ for all $i \in [q]$, so the equation from case 6 can't trivially hold.
   Then, we find two equations independent of each other, and by this we have at most $\sum_{i=1}^{6} \varsigma_i \leq 12q^2\ell((2^n-2)!)$ permutations.
2. For the cases from 7 to 12, $\Sigma_i = X_{u,v}$ for some $u \neq i$, $v \in [\ell_{j1}]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} Y_{i,l} = 2^{v-1}\Delta_1 \oplus 2^{2(v-2)}\Delta_2 \oplus M_v^u$, i.e. an equation over variables $Y_{i,l}$, Δ_1 and Δ_2.
   (a) For case 7, $\pi(\Sigma_i) \oplus c_i = \Delta_{j2}$, we get a non-singular submatrix $[1,1;1,0]$ or $[1,1;0,1]$ with variables Δ_1 and Δ_2.
   (b) For case 8, $\pi(\Sigma_i) \oplus c_i = Y_{j2,l2}$ depends only on $Y_{j2,l2}$, where $c_i \neq 0^n$ excludes trivial collisions $Y_{j2,l2} = Y'_{l2}$. Then we get two independent equations.
   (c) For cases from 9 to 12, we need only to consider $\pi(\Sigma_i) \oplus c_i = c_{i',j'}$ with $c_{i',j'} \notin \{c_{i,1}, c_{i,2}\}$ and $c_{i',j'} \notin \{\Delta_u, Y_{k,l}\}$. Such $c_{i',j'}$ are produced by $c_{i',j'} = \pi(\Sigma_{i',j'})$ with $\Sigma_{i',j'} \notin \{\mathrm{Cst}_u, X_{k,l}\}$ or $c_{i',j'} = \pi(\Theta_{i',j'})$ with $\Theta_{i',j'} \notin \{\mathrm{Cst}_u, X_{k,l}\}$ (otherwise such cases should have been analyzed in (a) and (b)), so they have independent randomness from $\{\Delta_u, Y_{k,l}\}$.

   Then, by two independent equations we have at most $\sum_{i=7}^{12} \varsigma_i \leq 6q^3\ell^2((2^n-2)!)$ permutations.
3. For cases from 13 to 18, $\Sigma_i = \Sigma_j$ is equivalent to $\bigoplus_{l=1}^{\ell_i} Y_{i,l} = \bigoplus_{l=1}^{\ell_j} Y_{j,l}$, depending only on $Y_{i,l}$ and $Y_{j,l}$. Also, we have $c_{i,1} = \pi(\Sigma_i) = \pi(\Sigma_j) = c_{j,1}$, which implies $\pi(\Sigma_i) \oplus c_i = c_{j,1} \oplus c_i$.
   (a) For case 13, $c_{j,1} \oplus c_i = \Delta_{j2}$ depending on Δ_1 or Δ_2, and this always holds regardless of whether $c_{j,1} \in \{\mathrm{Cst}_u, X_{k,l}\}$ or not.
   (b) For case 14, $c_{j,1} \oplus c_i = Y_{u,v}$ for some $u \in [q]$ and $v \in [L_u]$. When $c_{j,1} \in \{\Delta_1, \Delta_2\}$ or $c_{j,1} = P(\Sigma_j)$ with $\Sigma_j \notin \{\mathrm{Cst}_u, X_{k,l}\}$, the two equations are independent; when $c_{j,1} \in \{Y_{k,l}\}$, say $c_{j,1} = Y_{u',v'}$, then $c_i \neq 0^n$ excludes trivial collisions and so $Y_{u',v'}$ and $Y_{u,v}$ are independent, both with coefficients 1. Notice in the first equation that we have at least one $Y_{i,l1}$ on its left side, with coefficient 1. If $Y_{i,l1} \notin \{Y_{u',v'}, Y_{u,v}\}$, the two equations are independent. If $Y_{i,l1} \in \{Y_{u',v'}, Y_{u,v}\}$, we can get a non-singular submatrix $[1,0;1,1]$. It is possible that $\{Y_{i,l1}, Y_{j,l1}\} = \{Y_{u',v'}, Y_{u,v}\}$, which results in a singular submatrix $[1,1;1,1]$. In such a case, notice that there must be some other $Y_{i,l}$ or $Y_{u,l}$ in the first equation, otherwise we get a contradiction $Y_{i,l1} = Y_{j,l1}$. This helps the first equation to be independent of the second one. If there exist 2-collisions among

$\{Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, Y_{j,1}, Y_{j,2}, \cdots, Y_{j,\ell_j}\}$ in the first equation, then itself implies two independent equations.

(c) For cases from 15 to 18, $c_{j,1} \oplus c_i \notin \{\Delta_1, \Delta_1, Y_{k,l}\}$, then it has independent randomness from the first equation.

At last, by noticing that in each subcase we have two independent equations, here we can get at most $\sum_{i=13}^{18} \varsigma_i \leq 6q^3\ell((2^n - 2)!)$ permutations.

1. For the cases from 19 to 24, $\Theta_i = \mathrm{Cst}_{j1}$ for some $j1 \in [2]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} 2^{\ell_i - l + 1} Y_{i,l} = \mathrm{Cst}_{j1}$, i.e. an equation over variables $Y_{i,l}$.
   On the other side, notice that by $\Theta_i = \mathrm{Cst}_{j1}$ we have $\pi(\Theta_i) = \pi(\mathrm{Cst}_{j1}) = \Delta_{j1}$. This means, $\pi(\Theta_i) \oplus c_i = \Delta_{j1} \oplus c_i$. Then, though the cases from 1 to 6 imply different equations, they all depend on random variable Δ_{j1}. Notice that we have restrict $c_i \neq 0^n$ for all $i \in [q]$, so the equation from case 6 can't trivially hold.
   Then, we find two equations independent of each other, and by this we have at most $\sum_{i=19}^{24} \varsigma_i \leq 12q^2\ell((2^n - 2)!)$ permutations.
2. For the cases from 25 to 30, $\Theta_i = X_{u,v}$ for some $u \neq i$, $v \in [\ell_{j1}]$ is equivalent to $\bigoplus_{l=1}^{\ell_i} 2^{\ell_i - l + 1} Y_{i,l} = 2^{v-1}\Delta_1 \oplus 2^{2(v-2)}\Delta_2 \oplus M_v^u$, i.e. an equation over variables $Y_{i,l}$, Δ_1 and Δ_2.
   (a) For case 25, $\pi(\Theta_i) \oplus c_i = \Delta_{j2}$, we get a non-singular submatrix $[2^{v-1}, 2^{2(v-2)}; 1, 0]$ or $[2^{v-1}, 2^{2(v-2)}; 0, 1]$ with variables Δ_1 and Δ_2.
   (b) For case 26, $\pi(\Theta_i) \oplus c_i = Y_{j2,l2}$ depends only on $Y_{j2,l2}$, where $c_i \neq 0^n$ excludes trivial collisions $Y_{j2,l2} = Y'_{l2}$. Then we get two independent equations.
   (c) For cases from 27 to 30, we need only to consider $\pi(\Theta_i) \oplus c_i = c_{i',j'}$ with $c_{i',j'} \notin \{c_{i,1}, c_{i,2}\}$ and $c_{i',j'} \notin \{\Delta_u, Y_{k,l}\}$. Such $c_{i',j'}$ are produced by $c_{i',j'} = \pi(\Sigma_{i',j'})$ with $\Sigma_{i',j'} \notin \{\mathrm{Cst}_u, X_{k,l}\}$ or $c_{i',j'} = \pi(\Theta_{i',j'})$ with $\Theta_{i',j'} \notin \{\mathrm{Cst}_u, X_{k,l}\}$ (otherwise such cases should have been analyzed in (a) and (b)), so they have independent randomness from $\{\Delta_u, Y_{k,l}\}$.

   Then, by two independent equations we have at most $\sum_{i=25}^{30} \varsigma_i \leq 6q^2\ell^2((2^n - 2)!)$ permutations.
3. For cases from 31 to 36, $\Theta_i = \Theta_j$ is equivalent to $\bigoplus_{l=1}^{\ell_i} 2^{\ell_i - l + 1} Y_{i,l} = \bigoplus_{l=1}^{\ell_j} 2^{\ell_j - l + 1} Y_{j,l}$, depending only on $Y_{i,l}$ and $Y_{j,l}$. Also, we have $c_{i,2} = \pi(\Theta_i) = \pi(\Theta_j) = c_{j,2}$, which implies $\pi(\Theta_i) \oplus c_i = c_{j,2} \oplus c_i$.
   (a) For case 31, $c_{j,2} \oplus c_i = \Delta_{j2}$ depending on Δ_1 or Δ_2, and this always holds regardless of whether $c_{j,1} \in \{\mathrm{Cst}_u, X_{k,l}\}$ or not.
   (b) For case 32, $c_{j,2} \oplus c_i = Y_{u,v}$ for some $u \in [q]$ and $v \in [L_u]$. When $c_{j,2} \in \{\Delta_1, \Delta_2\}$ or $c_{j,2} = P(\Theta_j)$ with $\Theta_j \notin \{\mathrm{Cst}_u, X_{k,l}\}$, the two equations are independent; when $c_{j,2} \in \{Y_{k,l}\}$, say $c_{j,2} = Y_{u',v'}$, then $c_i \neq 0^n$ excludes trivial collisions and so $Y_{u',v'}$ and $Y_{u,v}$ are independent, both with coefficients 1. Notice in the first equation that $M_i \neq M_j$ implies $\exists l1 \in [\max\{\ell_i, \ell_j\}]$ s.t. $Y_{i,l1} \neq Y_{j,l1}$, where $Y_{i,l1} = 0^n$ if $l1 > \ell_i$ and $Y_{j,l1} = 0^n$ if $l1 > \ell_j$. The variable $Y_{i,l1} \oplus Y_{j,l1}$ has a coefficient $2^{\max\{\ell_i, \ell_j\} - l1 + 1} \neq 1$. If $Y_{i,l1} \oplus Y_{j,l1} \notin \{Y_{u',v'}, Y_{u,v}\}$, the two equations are

independent. If $Y_{i,l1} \oplus Y_{j,l1} \in \{Y_{u',v'}, Y_{u,v}\}$, we can get a non-singular submatrix $[2^{\max\{\ell_i,\ell_j\}-l1+1}, 0; 1, 1]$ or $[2^{\max\{\ell_i,\ell_j\}-l1+1}, 1; 1, 1]$. If there exist 2-collisions among $\{Y_{i,1}, Y_{i,2}, \cdots, Y_{i,\ell_i}, Y_{j,1}, Y_{j,2}, \cdots, Y_{j,\ell_j}\}$ in the first equation, then itself implies two independent equations.

(c) For cases from 33 to 36, $c_{j,2} \oplus c_i \notin \{\Delta_1, \Delta_1, Y_{k,l}\}$, then it has independent randomness from the first equation.
By noticing that in each subcase we have two independent equations, here we can get at most $\sum_{i=31}^{36} \varsigma_i \leq 6q^3\ell((2^n-2)!)$ permutations.

Finally, we can get

$$\epsilon_{pcf} \leq \frac{\sum_{i=1}^{36} \varsigma_i}{2^n!} \leq \frac{24q^3\ell^2((2^n-2)!)}{2^n!} \leq \frac{3q^3\ell^2}{2^{2n-4}}.$$

9.4 Upper Bounding block-wise universal ϵ_{au}

By its definition, we have two bad events in upper bounding ϵ_{au}.

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

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

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

10 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. 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.
3. Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, 2000.
4. Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC macs. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 527–545. Springer, 2005.
5. John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 384–397. Springer, 2002.
6. Yevgeniy Dodis and John P. Steinberger. Domain extension for macs beyond the birthday barrier. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 323–342. Springer, 2011.
7. David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu. On tweaking luby-rackoff blockciphers. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, volume 4833 of *Lecture Notes in Computer Science*, pages 342–356. Springer, 2007.
8. Tetsu Iwata and Kaoru Kurosawa. OMAC: one-key CBC MAC. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003,*

Lund, Sweden, February 24-26, 2003, Revised Papers, volume 2887 of *Lecture Notes in Computer Science*, pages 129–153. Springer, 2003.

9. Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2014.
10. Kaoru Kurosawa and Tetsu Iwata. TMAC: two-key CBC MAC. *IEICE Transactions*, 87-A(1):46–52, 2004.
11. Rodolphe Lampe and Yannick Seurin. Tweakable blockciphers with asymptotically optimal security. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 133–151. Springer, 2013.
12. Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012.
13. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.
14. Stefan Lucks. The sum of prps is a secure PRF. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 2000.
15. Bart Mennink. Optimally secure tweakable blockciphers. Cryptology ePrint Archive, Report 2015/363, 2015. http://eprint.iacr.org/.
16. Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In Orr Dunkelman, editor, *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*, pages 308–326. Springer, 2009.
17. Atsushi Mitsuda and Tetsu Iwata. Tweakable pseudorandom permutation from generalized feistel structure. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *Provable Security, Second International Conference, ProvSec 2008, Shanghai, China, October 30 - November 1, 2008. Proceedings*, volume 5324 of *Lecture Notes in Computer Science*, pages 22–37. Springer, 2008.
18. Mridul Nandi. A unified method for improving PRF bounds for a class of blockcipher based macs. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, volume 6147 of *Lecture Notes in Computer Science*, pages 212–229. Springer, 2010.
19. Jacques Patarin. About feistel schemes with six (or more) rounds. In Serge Vaudenay, editor, *Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings*, volume 1372 of *Lecture Notes in Computer Science*, pages 103–121. Springer, 1998.

20. Jacques Patarin. The "coefficients h" technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.
21. Jacques Patarin. A proof of security in $o(2^n)$ for the benes scheme. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 209–220. Springer, 2008.
22. Jacques Patarin. A proof of security in $o(2^n)$ for the xor of two random permutations. In Reihaneh Safavi-Naini, editor, *Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings*, volume 5155 of *Lecture Notes in Computer Science*, pages 232–248. Springer, 2008.
23. Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.
24. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.
25. Serge Vaudenay. Decorrelation: A theory for block cipher security. *J. Cryptology*, 16(4):249–286, 2003.
26. Kan Yasuda. The sum of CBC macs is a secure PRF. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, volume 5985 of *Lecture Notes in Computer Science*, pages 366–381. Springer, 2010.
27. Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 596–609. Springer, 2011.
28. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In Xiaoyun Wang and Kazue Sako, editors, *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 *Lecture Notes in Computer Science*, pages 296–312. Springer, 2012.

$\mathcal{L}(Y)$		$\#acc(\sim)$	#choices	Rank of $(\mathcal{L}(y),\sim)$	Total
3-message fully-covered	$\Sigma_i = \Sigma_j, \Theta_i = \Theta_k$	0 1	2 l^2	2 2	$\frac{l^2}{2^{2n}}$
	$\Sigma_i = \Sigma_j, \Theta_i = X_k$	0 1	l l^3	2 2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = \Theta_k$	0 1	l l^3	2 2	$\frac{l^3}{2^{2n}}$
	$\Sigma_i = X_j, \Theta_i = X_k$	0 1	l^2 l^4	2 2	$\frac{l^4}{2^{2n}}$
2-message single-covered	$\Sigma_i = \Sigma_j$	0 1	2 l^2	1 1	$\frac{l^2}{2^n}$
	$\Sigma_i = X_j$	0 1	l l^3	1 1	$\frac{l^3}{2^n}$
	$\Theta_i = X_k$	0 1	l l^3	1 1	$\frac{l^3}{2^n}$
	$\Theta_i = \Theta_k$	0 1	2 l^2	1 1	$\frac{l^2}{2^n}$
3-message pseudo-covered	$\Sigma_i = X_j, Y_j + t_i = Y_k$	0 1	$9l^2$ l^4	2 2	$\frac{l^4}{2^n}$
	$\Theta_i = X_j, Y_j + t_i = Y_k$	0 1	$9l^2$ l^4	2 2	$\frac{l^4}{2^n}$
4-message pseudo-covered	$\Sigma_i = X_e, \Sigma_j = X_f, Y_e + Y_f = t_i + t_j$	0 1 2	l^2 l^4 l^6	3 3 4	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$
	$\Sigma_i = X_e, \Theta_j = X_f, Y_e + Y_f = t_i + t_j$	0 1 2	l^2 l^4 l^6	3 3 4	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$
	$\Theta_i = X_e, \Sigma_j = X_f, Y_e + Y_f = t_i + t_j$	0 1 2	l^2 l^4 l^6	3 3 4	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$
	$\Theta_i = X_e, \Theta_j = X_f, Y_e + Y_f = t_i + t_j$	0 1 2	l^2 l^4 l^6	3 3 4	$\frac{l^4}{2^{3n}} + \frac{l^6}{2^{4n}}$

Table 3. Table for different cases of bad equations with no. of choice and ranks corresponding to accidents 0, 1 and 2.

Table 4. 9 Bad Events 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

Table 5. 18 out of 36 Bad Events in Upper Bounding ϵ_{pcf}: 1st Half.

$\Sigma_i =$ \ $\pi(\Sigma_i) \oplus c_i$	$\pi(\Sigma_{j2}) \oplus c_{j2}$	$\pi(\Theta_{j2}) \oplus c_{j2}$	$\pi(\Theta_{j2})$	$\pi(\Sigma_{j2})$	$Y_{j2,l}$	Δ_{j2}
Cst_{j1}	1	2	3	4	5	6
$X_{j1,l}$	9	10	11	12	8	7
Σ_{j1}	15	16	17	18	14	13

Table 6. 18 out of 36 Bad Events in Upper Bounding ϵ_{pcf}: 2nd half.

$\Theta_i =$ \ $\pi(\Theta_i) \oplus c_i$	$\pi(\Theta_{j2}) \oplus c_{j2}$	$\pi(\Sigma_{j2}) \oplus c_{j2}$	$\pi(\Sigma_{j2})$	$\pi(\Theta_{j2})$	$Y_{j2,l}$	Δ_{j2}
Cst_{j1}	19	20	21	22	23	24
$X_{j1,l}$	27	28	29	30	26	25
Θ_{j1}	36	35	34	33	32	31