One-Key Compression Function Based MAC with BBB Security

Avijit Dutta, Mridul Nandi, Goutam Paul

Indian Statistical Institute, Kolkata 700 108, India.
avirocks.dutta13@gmail.com, mridul.nandi@gmail.com, goutam.paul@isical.ac.in

Abstract. Gaži et al. [CRYPTO 2014] analyzed the NI-MAC construction proposed by An and Bellare [CRYPTO 1999] and gave a tight birthday-bound of $O(lq^2/2^n)$, as an improvement over the previous bound of $O(l^2q^2/2^n)$. In this paper, we design a simple extension of NI-MAC, called NI$^+$-MAC, and prove that it has $O(q2l^2/2^n)$ security bound. Our construction not only lifts the security of NI-MAC beyond birthday, it also reduces the number of keys from 2 (NI uses 2 independent keys) to 1. Before this work, Yasuda had proposed [FSE 2008] a single fixed-keyed compression function based BBB-secure MAC that uses an extra tweak. However, our proposed construction NI$^+$ does not require any extra tweak and thereby has reduced the state size compared to Yasuda’s proposal [FSE 2008]. Further, the security proof of Yasuda’s construction is straight-forward, as tweakable functions are replaced by uniform independent random functions. On the other hand, our proof technique is completely different and uses the structure graph based analysis introduced by Bellare et al. [CRYPTO 2005].

Keywords: Beyond Birthday, MAC, NI, Structure-Graph.

1 Introduction

In symmetric key paradigm, MAC (Message Authentication Code) is used for preserving message integrity and message origin authentication. The design of a MAC should not only consider achieving security, but also target attaining efficiency. In the literature, three different approaches of designing a MAC exists: (a) universal hash function based MAC, a popular example of which is UMAC [8], (b) a compression function based MAC, like NMAC [2], HMAC [2], NI [1] etc. (c) Block cipher based MAC, such as CBC MAC [4], PMAC [9], OMAC [17], etc.

Most of the popular MACs are block cipher based MACs, but each one of them suffers from the same problem - security is guaranteed up to the birthday bound. When the block length of the underlying block cipher is 128-bit, then birthday bound does not seem to be a problem, as we are guaranteed to have 64 bits of security which is well acceptable for many practical applications. But when we deal with 64-bit block cipher (e.g HIGHT [16], PRESENT [10]) as used in many light weight crypto devices (e.g RFID, smartcard) then birthday bound
problem becomes the main bottleneck.

**Related Work on NMAC and HMAC.** NMAC and its variant HMAC [2] is the first re-keying compression function based MAC where a key is appended to a message and then the appended message is hashed using Merkle-Damgård technique. It has been standardized in [23], and has become popular and widely used in many network protocols like SSH, IPSec, TLS etc. Bellare et al. in [2] proves that NMAC is a secure PRF based on the assumption (i) $f$ is a secure PRF and (ii) $\text{Casc}^f$ is a WCR (weakly collision resistant). HMAC when instantiated with MD4 or SHA-1, both of them play the role of $\text{Casc}^f$ then they have been found not to satisfy the WCR property [35, 36] and hence the security of HMAC [2] stands void. To restore the PRF security of NMAC, Bellare in [6] investigates the proof and drops assumption (ii). Koblitz and Menezes in [22] criticizes the way [6] discusses the practical implication of their result against uniform and non-uniform reductions used in the proof.

Dodis et.al in [12] investigates the indifferentiable property of HMAC from a keyed random oracle. In a recent line of researches, generic attack against iterated hash based MAC are being investigated [30, 31, 29, 24]. More recently, Gazi et al in [14] showed a tight bound on NMAC. There is also a recent result [15] on the generic security analysis of NMAC and HMAC with input whitening.

Yausda in [38] had proposed a novel way of iterating a compression function dedicated for the use of MAC which is more efficient than standard HMAC to process data much faster. In [40] Yasuda has showed that classical sandwiched construction with Merkle-Damgård iteration based hashing provides a secure MAC which is an alternative for HMAC, useful in situation where the message size is small and high performance is required. A new secret-prefix MAC based on hash functions is presented in [43] which is similar to HMAC but does not require the second key.

U.Maurer et. al in [26] has presented a MAC construction namely PDI, that transforms any FIL MAC to AIL MAC and investigated the tradeoff between the efficiency of MAC and the tightness of its security reduction. In [27] construction of AIL MAC from a FIL MAC with a single key was presented which is better than NI [1].

**Related Work on Beyond birthday Secure MAC.**

**Block Cipher Based BBB MAC.** In recent researches, many MAC constructions have been proposed with security beyond the birthday barrier without degrading the performance. The first attempt was made in ISO 9797-1 [3] without security proof. But Algorithm 4 of ISO 9797-1 was attacked by Joux et al. [20] that falsified the security bound. Algorithm 6 of ISO 9797-1 was proven to be secure against $O(2^{n/3})$ queries with restrictions on the message length [44]. In [44] Yasuda also presented SUM-ECBC, a 4-key rate-1/2 construction with beyond birthday bound security. In 2011, Yasuda improved the number of keys and rate over SUM-ECBC and proposed a 3-key rate-1 PMAC Plus construction [45] with beyond birthday security. In 2012, Zhang et al. [48] proposed a 3key version of f9 MAC (3kf9) that achieves BBB security.
There is also another deterministic MAC mode provides security beyond the birthday bound. Given an \( n \)-bit to \( n \)-bit fixed-key blockcipher with MAC security \( \epsilon \) against \( q \) queries, Dodis et al. [13] have designed a variable-length MAC achieving \( O(\epsilon \text{poly}(n)) \) MAC security. However, this design requires even longer keys and more block cipher invocations. By parity method, Bellare et al. present MACRX [3] with BBB security, conditioned on the input parameters are random and distinct. In [18], Jaulmes et al. proposed a randomized MAC that provides BBB security based on the ideal model (or possibly based on tweakable block cipher). Another BBB secure randomized construction called generic enhanced hash then MAC has been proposed in [28] by Minematsu. Recently Datta et al. in [11] unify PMAC Plus and 3kf9 in one key setting with beyond birthday security.

**Compression Function based BBB MAC.** Besides the block cipher based BBB MAC constructions, Yasuda in [39] proposed a compression function based MAC construction - Multi-lane HMAC, that achieves BBB security. In [42] Yasuda presented a double pipe mode operation (Lucks Construction [25]) for constructing AIL MAC from a FIL MAC that achieves BBB security. This work is further extended to provide full security in [46]. In [41] Yasuda has proposed a fixed single keyed compression function based cascaded MAC in a tweakable setting where the tweaks are some distinct masking keys of \( b \) bits. Thus for a \( l \) blocks message, one needs to compute \( l \) many different masks where the masks are generated from a single mask \( \Delta_0 \) using the field multiplication. The security of the scheme has been proved to be \( O(lq^2/2^{2n}) \). Further improvement on [41] is followed in [47].

**Related Work on fixed-key MAC.** An et al. in [1] proposed a fixed-keyed compression function based MAC called NI-MAC. The construction of NI-MAC is similar to that of NMAC [2], the only difference is that NI-MAC uses two independent keyed compression functions \( f_1, f_2 \). The motivation of designing NI was to avoid constant re-keying on multi-block messages in NMAC and to allow for a security proof starting by the standard switch from a PRF to a random function, followed by information-theoretic analysis.

We mention here that the security proof technique for re-keying compression function based MAC is completely different from that of fixed-keyed compression function based MAC. The security of the former scheme is proved using reduction argument, whereas that of the latter is proved by replacing the fixed-keyed compression function with a random function.

Gazi et al. in [14] revisited the proof of NI-MAC and gave a tight birthday bound of \( O(q^2/2^n) \), a better bound than earlier \( O(q^2/2^{2n}) \).

**Our Contributions.** The main disadvantage of the scheme of [41] is that one needs to store the masking key \( \Delta_0 \). Thus, from the hardware point of view, it is infeasible to use the scheme in low-buffer and light-weight crypto devices, which are the basic target for achieving BBB security of a cryptographic scheme. Moreover, the proof technique of [41] is straight forward, as tweakable keyed functions are replaced by independent uniform random functions. In this paper, we propose \( \text{NI}^+ \), a non-tweakable single-keyed, rate-\( b/(b + n) \), compression function
based MAC that achieves beyond-birthday security, where $b$ is the block length and $n$ is the number of output bits. Moreover, our scheme is better than [41] in terms of required state size. Since our scheme does not use any extra tweak, our security proof technique is completely different than [41]. For our proof, we use the structure graph analysis of [5] and consider more bad events.

We mention here that NI$^+$ is an extension of NI-MAC, and it not only lifts the security of NI beyond birthday (Sect. 4), but also reduces the number of required keys from two (NI uses two independent keys) to one. In this context, we have shown that keeping the original structure of NI-MAC, with $\Theta$ being the sum of all intermediate chaining variables and $\Sigma$ being the last block output $(\Sigma, \Theta$ defined in Sect. 3), cannot achieve BBB security.

In the following table we compare the different parameters along with their security bound of known BBB secure MACs. We write BC to denote block cipher based MAC, CF$_{rk}$ denotes re-keying compression function based MAC (e.g HMAC), CF$_{fk}$ denotes fixed-keyed compression function based MAC (e.g NI), Rate $\triangleq b/\sqrt{2^n}$, where $b$-size of message block, $s$-total input size of the function without the key part and $r$ is the total number of function calls to process a single message block.

<table>
<thead>
<tr>
<th>Construction</th>
<th>Type</th>
<th># Keys</th>
<th>Rate</th>
<th>Security Bound</th>
<th>State size (#bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUM-ECBC [44]</td>
<td>BC</td>
<td>4</td>
<td>1/2</td>
<td>$O(lq^2/2^2n)$</td>
<td>$2n$</td>
</tr>
<tr>
<td>PMAC_PLUS [45]</td>
<td>BC</td>
<td>3</td>
<td>1</td>
<td>$O(lq^2/2^2n)$</td>
<td>$4n$</td>
</tr>
<tr>
<td>3kf9 [48]</td>
<td>BC</td>
<td>3</td>
<td>1</td>
<td>$O(lq^2/2^2n)$</td>
<td>$2n$</td>
</tr>
<tr>
<td>1kf9 [11]</td>
<td>BC</td>
<td>1</td>
<td>1</td>
<td>$O(q^2/2^2n)$</td>
<td>$2n$</td>
</tr>
<tr>
<td>1k_PMAC+ [11]</td>
<td>BC</td>
<td>1</td>
<td>1</td>
<td>$O(q^2/2^2n)$</td>
<td>$4n$</td>
</tr>
<tr>
<td>L-Lane (L = 2) HMAC [39]</td>
<td>CF$_{rk}$</td>
<td>3</td>
<td>1/2</td>
<td>$O(q^2/2^2n)$</td>
<td>$2n$</td>
</tr>
<tr>
<td>1-pass mode [41]</td>
<td>CF$_{fk}$</td>
<td>1</td>
<td>1</td>
<td>$O(q^2/2^2n)$</td>
<td>$(2b + 2n)$</td>
</tr>
<tr>
<td>NI$^+$ [This paper]</td>
<td>CF$_{fk}$</td>
<td>1</td>
<td>$\frac{b}{b+n}$</td>
<td>$O(q^2/2^2n)$</td>
<td>$(b + 2n)$</td>
</tr>
</tbody>
</table>

2 Preliminaries

In this section, we briefly discuss the notations and definitions used in this paper. We also state some existing basic results.

2.1 Notation and Definitions

We denote $|S|$ as the cardinality of set $S$. Let $x \leftarrow S$ denote that $x$ is chosen uniformly at random from $S$. $[n]$ denotes the set of integers $\{1, 2, \ldots, n\}$. $(s)_n$ denotes the last $n$ bit substring of $b$ bit string $s$.

Let $M$ be a binary string over $\{0, 1\}$. Length of $M$ in bits is denoted by $|M|$. When $|M| \mod b \neq 0$, we pad $10^d$ to $M$ to make $|M| \mod b = 0$ where $d = n - 1 - |M| \mod b$ and $b$ denotes the block length of $M$. $M_1 || M_2 || \ldots || M_l$ denotes the partition of message $M$ after $M$ is being padded, where each $M_i \in \{0, 1\}^b$ and $l$ denotes the number of blocks of $M$. $\ell$ denotes the maximum number of blocks in a message. By a $q$-set or a $q$-tuple $x := (x_i : i \in I)$ for an index set $I$, we mean a set or a tuple of size $q$. When all elements $x_i$'s are distinct we write $x \in \text{dist}_q$. 

**RANDOM FUNCTIONS.** Let \( Func(A, B) \) denote the set of all functions from \( A \) to \( B \). A **random function** \( F \) is a function which is chosen from \( Func(A, B) \) following some distribution, not necessarily uniform. In particular, a function \( \rho_n \) is said to be a uniform random function, if \( \rho_n \) is chosen uniformly at random from the set of all functions from a specified finite domain \( D \) to \( \{0, 1\}^n \). Throughout the paper we fix a positive integer \( n \).

We will specify a uniform random function by performing *lazy sampling*. In lazy sampling, initially the function \( \rho \) is undefined at every point of its domain. We maintain a set \( Dom(\rho) \) that grows dynamically to keep the record of already defined domain points of \( \rho \). \( Dom(\rho) \) is initialized to be empty. If \( x \notin Dom(\rho) \) then we will choose \( y \overset{\$}{\leftarrow} \{0, 1\}^n \) and add \( x \) in \( Dom(\rho) \). In this regard, \( x \) is said to be *fresh*. On the other hand, if \( x \in Dom(\rho) \) (i.e \( x = x' \)) then \( y \leftarrow f(x') \). In this regard \( x \) is said to be **covered**.

### 2.2 Security Definitions

We consider that an adversary \( A \) is an oracle algorithm with access to its oracle \( O(\cdot) \) and outputs either 1 or 0. Accordingly, we write \( A^{O(\cdot)} = 1 \) or 0. The resource of \( A \) is measured in terms of the time complexity \( t \) which takes into account the time it takes to interacts with its oracle \( O(\cdot) \) and the time for its internal computations, query complexity \( q \) takes into account the number of queries asked to the oracle by the adversary, data complexity \( \ell \) takes into account the maximum number of blocks in each query.

**Pseudo-random function.** We define **distinguishing advantage** of an oracle algorithm \( A \) for distinguishing two random functions \( F \) from \( G \) as

\[
Adv_A(F; G) := Pr[A^F = 1] - Pr[A^G = 1].
\]

We define prf-advantage of \( A \) for an \( n \)-bit construction \( F \) by

\[
Adv^{prf}_F(A) := Adv_A(F; \rho_n).
\]

We call \( A \) a \((q, \ell, t)\)-distinguisher if it makes at most \( q \) queries with at most \( \ell \)-blocks in each query and runs in time at most \( t \). We write \( Adv^{prf}_F(q, \ell, t) = \max_A Adv^{prf}_F(A) \) where maximum is taken over all \((q, \ell, t)\)-distinguisher \( A \). In an information theoretic situation we also ignore the time parameter \( t \). We call a keyed construction \( F \) is \((q, \ell, \epsilon)\)-prf if \( Adv^{prf}_F(q, \ell) \leq \epsilon \). Informally, if \( \epsilon \) is negligible then \( F \) is said to be a secure PRF.

**Collision-free and Cover-free.** Now we define some other information-theoretic security advantages (in which there is no presence of an adversary).

Let \( H \) be a random function which outputs two \( n \) bit blocks, denoted by \((\Sigma, \Theta) \in (\{0, 1\}^n)^2 \). For a \( q \)-tuple of distinct messages \( M = (M_1, \ldots, M_q) \), we write \( H(M_i) = (\Sigma^i, \Theta^i) \). For a \( q \)-tuple of pairs \((\Sigma^i, \Theta^i)_i \), we say that

1. A tuple \((\Sigma^i, \Theta^i)_i \) is **collided** if \( \exists i, j \in [q] \) such that \( \Sigma^i = \Sigma^j \) and \( \Theta^i = \Theta^j \) for some \( j \neq i \). Otherwise the tuple is said to be **collision-free**.
2. A tuple \((\Sigma^i, \Theta^i)_i \) is **covered** if \( \exists i, j \in [q] \) such that \( \Sigma^i = (M^i_a)_{a, j} \) and \( \Theta^i = Y^i_{\alpha-1} \) where \( \alpha \in [I_i] \) or \( \alpha \in [I_j] \) and \( j \) could be equal to \( i \), \( M^i_a \) denotes the
$\alpha$th block of $j$th message $M_j$ and $Y_{\alpha-1}^j \in \{0, 1\}^n$. Otherwise the tuple is said to be cover-free.

**Definition 1.** We define $(q, \ell)$-collision advantage and $(q, \ell)$-cover-free advantage as

\[
\text{Adv}^{\text{coll}}_F (q, \ell) = \max_{M \in \text{dist}_q} \Pr[(\Sigma, \Theta) \text{ is not collision-free}],
\]

\[
\text{Adv}^{\text{cf}}_F (q, \ell) = \max_{M \in \text{dist}_q} \Pr[(\Sigma, \Theta) \text{ is not cover-free}].
\]

Clearly, $\text{Adv}^{\text{coll}}_F (q, \ell) \leq \frac{q^2}{2} \text{Adv}^{\text{coll}}_F (2, \ell)$. Similarly, $\text{Adv}^{\text{cf}}_F (q, \ell) \leq \frac{q^2}{2} \text{Adv}^{\text{cf}}_F (2, \ell)$.

So it would be sufficient to concentrate on a pair of messages while bounding collision free or cover-free advantages. We say that a construction $F$ is ($q, \ell, \varepsilon$)-xxx if $\text{Adv}^{\text{xxx}}_F (q, \ell) \leq \varepsilon$ where xxx denotes either collision-free or cover-free.

### 2.3 Structure Graphs

In this section, we briefly revisit the structure graph analysis [5, 14].

Consider a cascaded construction with a function $f$, where $f$ is a uniform random function, that works on a message $M = M_1 \| M_2 \| \ldots \| M_l$ of length $l$ blocks as follows:

\[
Y_0 = 0, \text{ and } Y_i = f(Y_{i-1}, M_i) \text{ for } i = 1, \ldots, l.
\]

Informally, for a set of any two fixed distinct messages $M = \{M_1, M_2\}$ and a uniformly chosen random function $f$, we construct the structure graph $G^f(M)$ with $\{0, 1\}^n$ as the set of nodes as follows. We follow the computations for $M_1$ followed by those of $M_2$ by creating nodes labelled by the values $y_i$ of the intermediate chaining variables $Y_i$ with the edge $(y_i, y_{i+1})$ labelled by the block $M_{i+1}$. In this process, if we arrive at a vertex already labelled, while not following an existing edge, we call this event an $f$-collision. The sequence of alternating vertices and edges corresponding to the computations for a message $M_j$ is called an $M_j$-walk, denoted by $W_j$. A more formal discussion on structure graph appears in Appendix A.

Let $G(M)$ denote the set of all structure graphs corresponding to the set of messages $M$ (by varying $f$ over a function family). For a fixed graph $G \in G(M)$, let $f\text{Coll}(G)$ denote the set of all $f$-collisions in $G$. We state the following known results.

**Proposition 1.** [14, Lemma 2] For a fixed graph $G$, $\Pr[G \in f\text{Coll}(M) = G] \leq 2^{-n|f\text{Coll}(G)|}$

**Proposition 2.** [14, Lemma 3] $\Pr[G \in G(M) : |f\text{Coll}(G)| \geq 2] \leq \frac{4\tau}{n^2}$, where $\tau$ is the total number of blocks of the messages in $M$.

It is to be noted that for CBC-MAC analysis [5], $f(\alpha, \beta)$ is taken as $\pi(\alpha \oplus \beta)$ and for the NI-MAC analysis [14], $f(\alpha, \beta)$ is taken as $\rho(\alpha||\beta)$, where $\pi$ is a random permutation over $n$ bits and $\rho$ is a random function from $b + n$ bits to $n$ bits, where $b$ is the message block-length and $n$ is the length of the chaining variable as well as the tag.
3 Proposed Construction of NI⁺ for Beyond-Birthday Secure MAC

We present the schematic diagram of NI⁺ in Fig. 3.1 followed by the description in Algorithm 1. Let \( f_{K_1} : \{0,1\}^{b+n} \rightarrow \{0,1\}^n \) be a keyed function from \( b+n \) bits to \( n \) bits where \( b > n \). Recall that \( b \) refers to the block length of a message block and \( n \) refers to the output length in bits. Let \( M \in \{0,1\}^b \). So we can write \( M = (M_1, M_2, \ldots, M_l) \) where each \( M_i \in \{0,1\}^b \). We define a checksum block \( CS = \bigoplus_{i=1}^l M_i \). We denote \( \text{Casc}^{f_{K_1}}(M) := f_{K_1}(\ldots(f_{K_1}(f_{K_1}(0, M_1), M_2), \ldots, M_l)) \). Output of \( \text{Casc}^{f_{K_1}}(M) \) and the checksum block \( CS \) is passed through the same function \( f_{K_1} \) and the output is denoted as \( \Sigma \). We obtain \( \Theta \) by xoring all the intermediate chaining values (i.e \( \bigoplus_{i=1}^l Y_i \oplus \Sigma \)). We concatenate a fixed \( b-n \) bit string \( c = 10^{b-n-1} \) with the \( 2n \) bit string \( \Sigma||\Theta \) to match the input size of \( f_{K_1} \) and then the entire concatenated \( b \) bit string (i.e \( c||\Sigma||\Theta \)) is passed through \( f_{K_1} \) and finally outputs the tag \( T \). We sometimes denote \( CS \) by \( M_{l+1} \).

Note that, NI⁺ is similar to that of NI upto \( \text{Casc}^{f_{K_1}}(M) \) except the following differences.

**Algorithm 1**: Algorithm for NI⁺ MAC

\[ \begin{align*}
\text{Input: } & f_{K_1} : K_1 \triangleleft \mathcal{K}, \ M \leftarrow \{0,1\}^*, \ c \leftarrow 10^{b-n-1} \\
\text{Output: } & T \in \{0,1\}^n \\
1 & M_1||M_2||\ldots||M_l \leftarrow M||10^*; \ //l \text{ is the number of message blocks in } M \\
2 & Z \leftarrow 0^n; \ Y \leftarrow 0^n; \\
3 & \text{for } i = 1 \text{ to } l \text{ do} \\
4 & \quad Y \leftarrow f_{K_1}(M_i,Y); \ Z \leftarrow Z \oplus Y; \\
5 & \text{end} \\
6 & CS \leftarrow \bigoplus_{i=1}^l M_i; \\
7 & Y \leftarrow f_{K_1}(CS,Y); \ Z \leftarrow Z \oplus Y; \\
8 & \Sigma \leftarrow Y; \ \Theta \leftarrow Z; \\
9 & T \leftarrow f_{K_1}(c||\Sigma,\Theta); \\
10 & \text{Return } T;
\end{align*} \]
(a) In NI construction, b-bit encoding of $|M|$ and the last message block output $Y_l$ is passed through a different keyed compression function $f_{K_2}$. In NI$, we substitute the b-bit length encoding by the checksum block $CS$. Moreover, $CS$ and $Y_l$ is passed through the same keyed compression function.

(b) NI is a two fixed-keyed compression function based MAC. NI$^+$ is a single fixed-keyed compression function based MAC.

(c) NI provides only birthday bound ($lq^2/2^n$) security. NI$^+$ provides beyond birthday bound security ($q^2l^4/2^{2n}$).

3.1 Design Rationale

We mention here that beyond birthday security is not possible to achieve if we just keep the original structure of NI-MAC and output $\Sigma$ as the last block output (i.e $\Sigma = f_{K_2}(|M|, Y_l)$) and $\Theta$ as the sum of all intermediate chaining variables (i.e $\Theta = \oplus_{i=1}^{l} Y_i \oplus \Sigma$). This is justified by the following attack.

Let us assume that the adversary $A$ makes $q$ many queries of fixed number of blocks $l$ where the second message block is different in each query. The probability of $Y_{2i} = Y_{2j}$ for $1 \leq i \neq j \leq q$ is $\frac{1}{2^n}$. Given that the event $Y_{2i} = Y_{2j}$ occurs, $\Sigma^i = \Sigma^j$ and $\Theta^i = \Theta^j$ would be a trivial event which implies the collision in output. Therefore, for any adversary the collision probability would become $\frac{q^2}{2^n}$. Note that we keep all the queried message length same. To resist this attack, we introduce a checksum block which is processed through the same function after all the message blocks are processed. We mention two important properties of checksum:

(i) Difference in a single block of two distinct messages makes the different checksum value.

(ii) Difference in at least two blocks of two distinct messages may equalize the checksum value.

Now due to property (i) the above attack cannot make a trivial match in $\Sigma$. Moreover, due to property (ii) if differences in two message blocks of two distinct messages (a$^th$ block and b$^th$ block), ($M_{ia} \neq M_{ib}$) and ($M_{ja} \neq M_{jb}$) makes the checksum value equal, we are still guaranteed to obtain two output blocks for which $\Theta^i$ and $\Theta^j$ will not have a trivial match.

4 Security Analysis of NI$^+$-MAC

Gaži et. al in [14] have shown that the advantage of NI-MAC is bounded above by $\frac{q^2}{2^n} \left(l + \frac{64l^4}{2^n}\right)$. In this section we analyse the advantage of our construction NI$^+$-MAC and show that the advantage of NI$^+$-MAC achieves beyond birthday bound security; better than that of NI-MAC. Thus we have the following theorem.

$^1$ All the two properties are followed from Hamming distance of checksum is 2.
Theorem 1. Let \( f : \{0,1\}^k \times \{0,1\}^b \times \{0,1\}^n \rightarrow \{0,1\}^n \) be a \((\epsilon,t,q)\) secure PRF. Then NI\(^+\) be a \((\epsilon',t',q,l)\) secure PRF, where
\[
\epsilon' \leq \epsilon + \frac{q \cdot 2^2 t^2}{2^n} + \frac{4q^2 l^4}{2^n},
\]
such that \( t = t' + O(lq) \).

Proof. Let \( A \) be a adaptive PRF-adversary against NI\(^+\) running in time \( t \) and asking at most \( q \) queries, each of length at most \( \ell \) blocks. NI\(^+\) uses a single keyed function \( f \). Now if we replace \( f \) by a uniformly distributed random function \( r \) such that \( r \overset{\$}{\longleftarrow} \mathcal{R}(\{0,1\}^b \times \{0,1\}^n,\{0,1\}^n) \) and call the resulting construction \( \text{NI}^+ \), then using the standard reduction from information theoretic setting to complexity theoretic setting we have,
\[
\text{Adv}_{\text{NI}^+}^{\text{prf}} \leq \epsilon + \text{Adv}_{\text{NI}^+}^{\text{prf}}.
\]

Therefore to prove Theorem 1, we only need to prove
\[
\text{Adv}_{\text{NI}^+}^{\text{prf}} \leq \frac{q \cdot 2^2 t^2}{2^n} + \frac{4q^2 l^4}{2^n}.
\]

Consider the following Game as shown in Algorithm 2 where the adversary \( A \) queries to oracle \( O \) with distinct messages \( M \) and obtains the response \( T \).

Note that Game \( G_0 \) truly simulates a uniform random function and \( G_1 \) simulates the actual construction \( \text{NI}^+ \). Therefore using the fundamental lemma of game-playing technique [7], we have the following:
\[
\text{Adv}_{\text{NI}^+}^{\text{prf}} = \left| \Pr[A^{G_1} = 1] - \Pr[A^{G_0} = 1] \right|
\leq \Pr[A^{G_1} \text{ sets } \text{badsigma} \lor A^{G_1} \text{ sets } \text{bad}] 
\leq \Pr[A^{G_1} \text{ sets } \text{badsigma}] + \Pr[A^{G_1} \text{ sets } \text{bad}]. \quad (1)
\]

Therefore, we evaluate now the probability \( \Pr[A^{G_1} \text{ sets } \text{bad}] \). To evaluate this, let us define a double block function \( \mathcal{H}_f(M) := (\Sigma,\Theta) \) with respect to a uniform random function \( f \). Recall that the tuple \( \mathcal{H}_f(M^i) := (\Sigma^i,\Theta^i) \), \( \forall i \in [q] \) is said to be collision-free if \( \forall i \), either \( \Sigma^i \neq \Sigma^j \) or \( \Theta^i \neq \Theta^j \) or both \( \forall j \in [i-1] \). Similarly, the tuple \( (\Sigma^i,\Theta^j) \), is said to be cover-free if \( \forall i \), either \( \Sigma^i \neq (M^j_n) \) or \( \Theta^i \neq \gamma_{\alpha-1}^j \) or both \( \forall j \in [i] \). Therefore, it is then easy to see that
\[
\Pr[A^{G_1} \text{ sets } \text{bad}] \leq \text{Adv}_{\text{NI}^+}^{\text{coll}}(q,\ell) + \text{Adv}_{\text{NI}^+}^{\text{cf}}(q,\ell) 
\leq \frac{q^2}{2} \left( \text{Adv}_{\text{NI}^+}^{\text{coll}}(2,\ell) + \text{Adv}_{\text{NI}^+}^{\text{cf}}(2,\ell) \right). \quad (2)
\]

Now we state the following four lemmas, proof of which is deferred until next section. The first two lemmas (i.e Lemma 1 and 2) bounds the collision-free advantage and the last two lemmas (Lemma 3 and 4) bounds the cover-free advantage of function \( H_f(\cdot) \).

Lemma 1. For any two distinct messages \( M^i \) and \( M^j \), each of length at most \( \ell \) blocks,
\[
\Pr[\Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \land |fCol(G)| = 0] \leq \frac{1}{2^{\sqrt{n}}}.
\]
Initialize: badsigma, bad ← false;  
On the $j^{th}$ query $M_j$;  
$M_1||M_2||\ldots||M_l$ ← $M_1||10^* \leftarrow \text{Partition}(M_1)$, $Y_0 = 0$;  
for $i = 1$ to $l$;  
if ($M_i, Y_{i-1}) \in \text{Dom}(f)$) $Y_i \leftarrow f(M_i, Y_{i-1})$;  
else $Y_i \leftarrow \{0, 1\}^n$;  
$f(M_i, Y_{i-1}) \leftarrow Y_i$;  
$\text{Dom}(f) \leftarrow \text{Dom}(f) \cup \{M_i, Y_{i-1}\}$;  
if ($\oplus_{i=1}^l M_i, Y_i) \in \text{Dom}(f)$) $Y_{i+1} \leftarrow f(\oplus_{i=1}^l M_i, Y_i)$;  
else $Y_{i+1} \leftarrow \{0, 1\}^n$;  
$f(\oplus_{i=1}^l M_i, Y_i) \leftarrow Y_{i+1}$;  
$\text{Dom}(f) \leftarrow \text{Dom}(f) \cup \{\oplus_{i=1}^l M_i, Y_i\}$;  
$\Sigma^j \leftarrow Y_{i+1}$;  
$\Theta^j \leftarrow \oplus_{i=1}^l Y_i$;  
if ($\Sigma^j = 0$) badsigma ← true;  
$T^j \notin \{0, 1\}^n$;  
if ($\Sigma^j, \Theta^j = \Sigma^i, \Theta^i$ for some $i \in \{1, 2, \ldots, j-1\}$, or ($c||\Sigma^j, \Theta^j) = (M^*_s, Y^*_s)$ such that $s \in [i+1]$) or $s \in [j+1]$,$* \in \{i, j\}$;  
if ($\neg \text{bad}$)  
Coll(i, j) ← true, bad ← true;  
if ($\Sigma^j, \Theta^j = \Sigma^i, \Theta^i)$  
$T^j \leftarrow f(\Sigma^j, \Theta^j)$  
Else  
$T^j \leftarrow f(\Sigma^j, \Theta^j)$  
Return $T^j$;

Algorithm 2: Game $G_0$ is without boxed statement and $G_1$ is with boxed statement.

**Lemma 2.** For any two distinct messages $M^i$ and $M^j$, each of length at most $\ell$ blocks,
\[
\Pr[\Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \land |f\text{Coll}(G)| = 1] \leq \frac{\rho}{2^{\pi n}}.
\]

**Lemma 3.** For any two distinct messages $M^i$ and $M^j$, each of length at most $\ell$ blocks, and a particular $n$ bit constant $x$,
\[
\Pr[\Sigma^i = x \land \Theta^i = Y^i \land |f\text{Coll}(G)| = 0] \leq \frac{1}{2^{\pi n}}.
\]

**Lemma 4.** For any two distinct messages $M^i$ and $M^j$, each of length at most $\ell$ blocks, and a particular $n$ bit constant $x$,
\[
\Pr[\Sigma^i = x \land \Theta^i = Y^i \land |f\text{Coll}(G)| = 1] \leq \frac{\rho}{2^{\pi n}}.
\]

**Resume the proof of Theorem 1:** Now we have all the materials to prove Theorem 1 which is given in the following.
Thus, \( \Pr \) It is obvious that \( \Pr \) have been distinct as \( M \) and \( M \)

Substituting these two probability expressions back to Equation (1) will give

\[ \Pr[A^G \text{ sets bad}] \leq \frac{2q^2l^2}{2n} + \frac{4q^2l^4}{2^n}. \] (3)

Moreover it is easy to see that \( \Pr[A^G \text{ sets badsigma}] \leq \frac{q}{2^n} \). Therefore, substituting these two probability expressions back to Equation (1) will give

\[ \text{Adv}_{\text{NI}} \leq \frac{q}{2^n} + \frac{2q^2l^2}{2n} + \frac{4q^2l^4}{2^n}. \] □

### 4.1 Proof of \( \Pr[\Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \land |fColl(G)| = 0] \leq \frac{1}{2^{2n}} \)

In this section we will prove the following lemma.

**Lemma 1.** For any two distinct messages \( M^i \) and \( M^j \), each of length at most \( \ell \) blocks,

\[ \Pr[\Sigma^i \land \Theta^i = \Theta^j \land |fColl(G)| = 0] \leq \frac{1}{2^{2n}}. \]

**Proof.** We prove the lemma using the structure graph. After fixing two distinct messages \( M^i \) and \( M^j \) and choosing a function \( f \) uniformly at random from the set of all functions over \( \{0, 1\}^b \times \{0, 1\}^n \rightarrow \{0, 1\}^n \), we analyse the structure graph \( G := G_f(M^i, M^j) \). In particular, we analyse the probability of the event \( \Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \) in view of the number of collisions \( |fColl(G)| = 0 \) occurred in the corresponding structure graph \( G \). Let \( W \) denotes the event \( \Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \).

**Case a.** Let us consider \( M^i \) is not a prefix of \( M^j \) and \( M^j \) is not a prefix of \( M^i \). Let \( p \) be the longest common prefix (lcp) of \( M^i \) and \( M^j \). That means \( M^i_{p+1} \neq M^j_{p+1} \) and \( M^i_p = M^j_p \) where \( 1 \leq p \leq \alpha \). Therefore, \( Y^i_\alpha = Y^j_\alpha \) and \( Y^i_\beta \neq Y^j_\beta \) where \( p + 1 \leq \beta \leq \min\{l_i, l_j\} \) as \( |fColl(G)| = 0 \). Moreover, if \( l_i > l_j \) then all \( Y^i_\beta \) would have been distinct as \( |fColl(G)| = 0 \) where \( l_j + 1 \leq \beta \leq l_i \). Note that, it is also true that \( Y^i_\alpha \neq Y^j_\alpha \). Therefore, we have,

\[ \Pr[W \land |fColl(G)| = 0] = \Pr[\Theta^i = \Theta^j \land |fColl(G)| = 0 | \Sigma^i = \Sigma^j] \cdot \Pr[\Sigma^i = \Sigma^j] \]

It is obvious that \( \Pr[\Sigma^i = \Sigma^j] \leq \frac{1}{2^{2n}} \) and the event \( \Theta^i = \Theta^j \land |fColl(G)| = 0 \) conditioned on the event \( \Sigma^i = \Sigma^j \) implies a non trivial equation on \( Y \) as we will obtain some \( Y^i_{p+1} \) and \( Y^j_{p+1} \) for which \( \Theta^i \land \Theta^j = 0 \) would become non-trivial. Thus, \( \Pr[\Theta^i = \Theta^j \land |fColl(G)| = 0 | \Sigma^i = \Sigma^j] \leq \frac{1}{2^n} \). Therefore,

\[ \Pr[\Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \land |fColl(G)| = 0 \leq \frac{1}{2^{2n}}. \]
Case b. Let us consider that either of the two messages is a prefix of other (w.l.o.g $M_j$ is a prefix of $M_i$). Since $l_i > l_j$, therefore, $p = l_j$. Since $|\text{Coll}(G)| = 0$, $Y_i^{l_i}, \ldots, Y_i^p$ are all distinct with each other and with $Y_j^{l_j}, \ldots, Y_j^p$. This implies that $Y_i^p \neq Y_j^p$ as depicted in Fig. 4.1. Therefore, the probability of $\Theta^i = \Theta^j \wedge |\text{Coll}(G)| = 0$ conditioned on the event $\Sigma^i = \Sigma^j$ will be $O(1/2^n)$ as we will obtain two random variables $Y_i^p$ and $Y_j^p$ for which $\Theta^i \oplus \Theta^j = 0$ would become non-trivial. Moreover, $\Pr[\Sigma^i = \Sigma^j] \leq \frac{1}{2^n}$. Therefore again,

$$\Pr[\Sigma^i = \Sigma^j \wedge \Theta^i = \Theta^j \wedge |\text{Coll}(G)| = 0] \leq \frac{1}{2^{2n}}. \square$$

![Fig. 4.1: Structure Graph of accident 0](image)

4.2 Proof of $\Pr[\Sigma^i = \Sigma^j \wedge \Theta^i = \Theta^j \wedge |\text{Coll}(G)| = 1] \leq \frac{1}{2^{2n}}$. In this section we will prove the following lemma.

**Lemma 2.** For any two distinct messages $M^i$ and $M^j$, each of length at most $\ell$ blocks,

$$\Pr[\Sigma^i = \Sigma^j \wedge \Theta^i = \Theta^j \wedge |\text{Coll}(G)| = 1] \leq \frac{\ell^2}{2^{2n}}.$$  

Proof. Again we prove the lemma using the structure graph analysis. We fix two distinct messages $M^i$ and $M^j$ and a uniformly chosen function $f$ from the set of all functions over $\{0, 1\}^b \times \{0, 1\}^n \to \{0, 1\}^n$. Then we analyze the structure graph $G := G(f(M^i, M^j))$. In particular, here we will analyze the probability of the event $\Sigma^i = \Sigma^j \wedge \Theta^i = \Theta^j$ in view of number of collisions $|\text{Coll}(G)| = 1$ occurred in the corresponding structure graph $G$. Let $W$ denote the event $\Sigma^i = \Sigma^j \wedge \Theta^i = \Theta^j$.

We analyze the probability of the above event in two subcases. a) We consider all those structure graphs $G$ having $|\text{Coll}(G)| = 1$ with respect to $M := \{M^i, M^j\}$ where none of $W_i$ and $W_j$, where $W_i$ and $W_j$ is the walk of message $M^i$ and $M^j$ in structure graph $G$, contains a loop. It essentially implies that $W_i$ and $W_j$ are path which are denoted as $P_i$ and $P_j$ respectively. b) We consider all those structure graphs where either of $W_i$ or $W_j$ contains a loop.

Let $G$ denote the set of all structure graphs $G$ with $|\text{Coll}(G)| = 1$. Without loss of generality, let $l_i$ and $l_j$ be the lengths of the messages $M^i$ and $M^j$ respectively, with $l_i \geq l_j$. Let $G_1 \subset G$ be the set of all structure graphs such that the $M^i, M^j$-path does not contain any loop. The $G_2 = G \setminus G_1$ is the set of the remaining structure graphs.
a) Analysis of $G_1$. It is to be noted that if $M^j$ is a proper prefix of $M^i$ then $|G_1| = 0$, as in that case $|fColl(G)| = 0$. So without loss of generality, let’s assume that $M^j$ is not a prefix of $M^i$. Suppose the first $p$ blocks constitute the longest common prefix of $M^i$ and $M^j$. Therefore, $Y^i_\alpha = Y^j_\beta$, $1 \leq \alpha \leq p$. As number of collision is 1 therefore, the colliding pair is $(Y^i_{\beta_1}, Y^j_{\beta_2})$, where $p + 1 \leq \beta_1 \leq l_i, p + 1 \leq \beta_2 \leq l_j$.

**Case 1.** Let $\beta_i = \beta_j = p + 1$ and $l_i = l_j$ and after the collision $Y^i_\beta = Y^j_\beta$, for $p + 2 \leq \beta \leq l_i$. In this case, it is clear that checksum block of $i^{th}$ message $CS^i$ and checksum block of $j^{th}$ message $CS^j$ would not be equal due to property (i) stated in Section 3.1 and hence, even if $Y^i_\beta = Y^j_\beta$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial. Therefore, even though $\Pr[\Theta^i = \Theta^j]$, the event $\Sigma^i = \Sigma^j$ would not be trivial.

Therefore, in general, we assume that the colliding pair is $(Y^i_{\beta_1}, Y^j_{\beta_2})$, where $p + 1 \leq \beta_1 \leq l_i, p + 1 \leq \beta_2 \leq l_j$. Since the number of collision allowed in $G$ is 1, after the collision point either $P_i$ and $P_j$ follow the same path or they will get bifurcated right from the collision point and will never meet again. If $P_i$ and $P_j$ follow the same path, then for Case 1 we have shown that we can ensure to get the probability $O(1/2^n)$. If not, then except Case 3 where $\beta_i = \beta_j = p + 2$, we will obtain two random variables $Y^j_k$ and $Y^j_{k'}$ such that equation $\Theta^i \oplus \Theta^j = 0$ becomes non-trivial. If $P_i$ and $P_j$ gets bifurcated right after the collision point, then the equality of $\Theta$ becomes non-trivial for two random variables $Y^j_{p+1}$ and $Y^j_{l_j}$ as depicted in Fig. 4.2 and Fig. 4.3. Note that it is easy to follow that we will always obtain two such random variables.

![Fig. 4.2: Structure Graph of type $G_1$](image-url)
Since the structure graph involving only one collision is determined by the collision point, \(|G_1| \leq l^2\) and for each of this graph we have seen that the probability of desired event is \(O(1/2^{2n})\). Therefore,
\[
\Pr[W \land |fColl(G)| = 1] = \sum_{G \in \mathcal{G}} \Pr[W \land |fColl(G)| = 1] \leq \frac{l^2}{2^n}.
\]

b) Analysis of \(\mathcal{G}_2\). Recall that \(\mathcal{G}_2\) is the set of all structure graphs with respect to \(\mathcal{M}\) such that the number of collision is 1 and containing a loop. Without loss of generality we assume that \(W_i\) contains a loop. That means \(Y_a = Y_{a+c}\) for \(c \geq 1\). Here \(c\) denotes the loop size. Note that, the loop actually creates a collision and therefore, neither (i) \(W_j\) or \(W_i\) makes another different loop, nor (ii) \(W_j\) collides with \(W_i\) as in both of the cases number of collisions will increase to 2. Thus, the only possibilities are either (1) \(W_j\) completely lies on \(W_i\), or (2) \(W_j\) could follow \(W_i\) but after a point \(W_j\) and \(W_i\) gets bifurcated and never meets. We will analyze the probability of the event \(\Sigma^i = \Sigma^j \land \Theta^i = \Theta^j \land |fColl(G)| = 1\) separately for each of the above cases.

**Case 1.** Let us assume \(W_i = Y_1^i \mid \ldots \mid Y_{a-1}^i \mid (Y_a^i \mid \ldots \mid Y_{a+c-1}^i)^k \mid \ldots \mid Y_l^i\) and \(W_j = Y_1^j \mid \ldots \mid Y_{a-1}^j \mid (Y_a^j \mid \ldots \mid Y_{a+c-1}^j)^k \mid \ldots \mid Y_l^j\) where \(k' \geq 0\).

Now we have the following cases:

**Case 1.1.** As \(W_j\) lies on \(W_i\), it is easy to see that if \(k' = 0\) then \(W_j\) be a subsequence of \(Y_1^i \mid \ldots \mid Y_{a-1}^i\) and therefore one can ensures the non-triviality of equation \(\Theta^i = \Theta^j\) which holds with probability \(\frac{1}{\pi}\). Moreover, \(Y_1^i \neq Y_1^j\) and thus \(\Sigma^i = \Sigma^j\) also holds with probability \(\frac{1}{\pi}\) and therefore \(\Pr[W \land |fColl(G)| = 1] \leq \frac{1}{\pi}\).

**Case 1.2.** If \(k' \geq 1\), then it is obvious that \(Y_1^j \mid \ldots \mid Y_{a-1}^j = Y_1^i \mid \ldots \mid Y_{a-1}^i\). Now if we assume that the length of the tail of \(W_i\) (i.e. \(Y_{a+c-1}^i \mid \ldots \mid Y_l^i\)) is same as that of \(W_j\) then it must have been the case that \(k \neq k'\) and without loss of generality we can assume that \(k > k'\). Since \(Y_i^l = Y_j^l\), depending on the equality of \(CS^i\) and \(CS^j\) we have \(\Pr[\Sigma^i = \Sigma^j \mid |fColl(G)| = 1] = 1\). Therefore,
\[
\Pr[W \land |fColl(G)| = 1] = \Pr[\Theta^i = \Theta^j \land \Sigma^i = \Sigma^j \land |fColl(G)| = 1] \\
\cdot \Pr[\Sigma^i = \Sigma^j \mid |fColl(G)| = 1] \cdot \Pr[|fColl(G)| = 1]
\]
As \(k > k'\), therefore, it is obvious to see that there must be at least two random variables \(f^1\) and \(f^2\) for which \(\Theta^i = \Theta^j\) would become non-trivial as depicted in Fig. 4.4. Thus in the above equation, \(\Pr[\Theta^i = \Theta^j \land \Sigma^i = \Sigma^j \land |fColl(G)| = 1] \leq \frac{1}{\pi^2}\).
Moreover, if we assume that the tail length of \( W_i \) and \( W_j \) are not same (w.l.o.g \( \text{tail}(W_i) > \text{tail}(W_j) \)) then we have either \( k = k' \) or \( k \neq k' \). The case of \( k = k' \) has already been taken care of. If \( k \neq k' \) then \( Y_{i}^{k} \neq Y_{j}^{k} \) and therefore, \( \Theta^i \oplus \Theta^j = 0 \) would become non-trivial for the random variable \( Y_{i}^{k} \) and \( Y_{j}^{k} \).

Moreover, \( \Pr[\Sigma^i = \Sigma^j] \leq \frac{1}{2^n} \). Thus,

\[
\Pr[W \land |fColl(G)| = 1] \leq \frac{1}{2^n}.
\]

**Case 2.** In this case \( W_j \) bifurcates from \( W_i \) right after some point \( X \). This condition necessarily implies that \( Y_{i}^{k} \neq Y_{j}^{k} \). Now it is to be noted that if \( W_j \) completely lies on \( W_i \) (as in \( \text{head}(W_i) = \text{head}(W_j) \) and \( k = k' \)) and bifurcates right from the point \( X = Y_{i}^{k-1} \), then \( \Theta^i = \Theta^j \) would imply \( Y_{i}^{k} = Y_{i}^{k}^{j} \), introduces one more collision and hence the number of collision would increase. Therefore, even if \( \text{head}(W_i) = \text{head}(W_j) \) either \( k \neq k' \) or \( W_j \) must get bifurcated from \( W_i \) from some earlier point of \( Y_{i}^{k-1} \). In both of these cases one should obtain at least two random variables (either from portion of loop or from portion of tail) \( Y_{i}^{s} \) and \( Y_{j}^{s'} \) for some \( s \) and \( s' \) that ensures the non-triviality of equation on \( \Theta \) as depicted in Fig. 4.5.

Moreover as \( Y_{i}^{k} \neq Y_{j}^{k} \) this ensures that \( \Pr[\Sigma^i = \Sigma^j] \leq \frac{1}{2^n} \). Hence, \( \Pr[W \land |fColl(G)| = 1] \leq \frac{1}{2^n} \).

Note that in all of these cases we have seen that the probability of the desired event becomes \( \frac{1}{2^n} \) and \( |G_2| \leq l^2 \) as the structure graph \( G \) is completely determined by the size of the loop which is formed by choosing any two \( Y \) values in \( \binom{l}{2} \) ways. Therefore,
\[
\Pr[W \wedge |f\text{Coll}(G)| = 1] = \sum_{G \in G_2} \Pr[W \wedge |f\text{Coll}(G)| = 1] \leq \frac{e}{2n^2}.
\]

### 4.3 Proof of \( \Pr[\Sigma^i = x \wedge \Theta^i = Y^i_s \wedge |f\text{Coll}(G)| = 0] \leq \frac{1}{22n} \).

In this section we will prove the following lemma.

**Lemma 3.** For any two distinct messages \( M^i \) and \( M^j \), each of length at most \( \ell \) blocks, and a particular \( n \) bit constant \( x \),

\[
\Pr[\Sigma^i = x \wedge \Theta^i = Y^i_s \wedge |f\text{Coll}(G)| = 0] \leq \frac{1}{22n}.
\]

**Proof.** We again prove the lemma using structure graph where we fix two distinct messages \( M^i \) and \( M^j \) and a function \( f \) uniformly at random from the set of all functions over \( \{0, 1\}^b \times \{0, 1\}^n \to \{0, 1\}^n \), we construct the structure graph \( G := G^i(M^i, M^j) \) such that there is no accidental collision (i.e. \( f \)-collision) in \( G \). Then we analyze the probability of the event denoted by \( W := \Sigma^i = x \wedge \Theta^i = Y^i_s \) in view of the number of \( f \)-collisions \( |f\text{Coll}(G)| = 0 \) occurred in the corresponding structure graph \( G \) where \( x \) is any non-zero \( n \) bit constant.

We analyse the probability of the event \( W \wedge |f\text{Coll}(G)| = 0 \) in two separate subcases when (a) None of \( M^i, M^j \) is a prefix of each other and (b) either of \( M^i, M^j \) is a prefix of the other.

**Case a.** Let us consider \( M^i \) is not a prefix of \( M^j \) and \( M^j \) is not a prefix of \( M^i \). Let \( p \) be the longest common prefix (lcp) of \( M^i \) and \( M^j \). Therefore, \( Y^i_\alpha = Y^j_\alpha \) where \( 1 \leq \alpha \leq p \) and \( Y^i_\beta \neq Y^j_\beta \) where \( p + 1 \leq \beta \leq \min\{l_i, l_j\} \) as \( |f\text{Coll}(G)| = 0 \). Moreover, if \( l_i > l_j \) then all \( Y^j_\beta \) would have been distinct as \( |f\text{Coll}(G)| = 0 \) where \( l_j + 1 \leq \beta \leq l_i \). Note that, it is also true that \( Y^i_{l_i} \neq Y^j_{l_j} \). Therefore, we have the following set of equations:

\[
\begin{align*}
Y^i_{l_i+1} &= x, \\
Y^i_1 + Y^j_2 + \ldots + Y^i_{l_i+1} + Y^s_t &= 0,
\end{align*}
\]

where \( s \) could be either \( i \) or \( j \) and \( t \in [l_i + 1] \) or \( t \in [l_j + 1] \). For each of these cases one can easily check that the above system of equation has rank 2. Therefore, \( \Pr[W \wedge |f\text{Coll}(G)| = 0] \leq \frac{1}{22n} \).

**Case b.** W.l.o.g let us consider that \( M^j \) is a prefix of \( M^i \). Since \( l_i > l_j \) therefore, \( p = l_j \). Since \( |f\text{Coll}(G)| = 0 \), \( Y^i_{p+1}, \ldots Y^i_{l_i} \) are all distinct with each other and with \( Y^j_1, \ldots, Y^j_{l_j} \). This implies that \( Y^i_p \neq Y^j_{l_j} \) as depicted in Fig. 4.1. Therefore, the set of equations (Equation (5) and (6)) has the full rank. Therefore, again we have, \( \Pr[W \wedge |f\text{Coll}(G)| = 0] \leq \frac{1}{22n} \).

Therefore, combining Case a and b we have,

\[
\Pr[\Sigma^i = x \wedge \Theta^i = Y^i_s \wedge |f\text{Coll}(G)| = 0] \leq \frac{1}{22n}
\]

for any non-zero \( n \) bit constant \( x \). \( \square \)
4.4 Proof of \( \Pr[\Sigma^i = x \land \Theta^i = Y_s^i \land |f\text{Coll}(G)| = 1] \leq \frac{i^2}{2^{2n}}. \)

In this section we will prove the following lemma.

**Lemma 4.** For any two distinct messages \( M^i \) and \( M^j \), each of length at most \( \ell \) blocks, and a particular \( n \) bit constant \( x \),

\[
\Pr[\Sigma^i = x \land \Theta^i = Y_s^i \land |f\text{Coll}(G)| = 1] \leq \frac{i^2}{2^{2n}}.
\]

*Proof.* We prove this lemma using the structure graph analysis. The primary concern of this proof will be to analyze the probability of the event \( W := \Sigma^i = x \land \Theta^i = Y_s^i \) in view of number of collisions \( |f\text{Coll}(G)| = 1 \) occurred in the corresponding structure graph \( G \) where \( G := G^i(M^i, M^j) \).

We analyze the probability of the event \( W \land |f\text{Coll}(G)| = 1 \) in two separate subcases. a) When we consider all structure graphs \( G \) with respect to \( M := \{M^i, M^j\} \) such that \( |f\text{Coll}(G)| = 1 \) and none of \( W_i \) and \( W_j \), where \( W_i \) and \( W_j \) is the walk of message \( M^i \) and \( M^j \) in structure graph \( G \), contains a loop. It implies that \( W_i \) and \( W_j \) are path which are denoted as \( P_i \) and \( P_j \) respectively.

b) When we consider all those structure graphs where either \( W_i \) or \( W_j \) contains a loop.

As before, let \( \mathcal{G} \) denote the set of all structure graphs \( G \) with \( |f\text{Coll}(G)| = 1 \). Without loss of generality, let \( l_i \) and \( l_j \) be the lengths of the messages \( M^i \) and \( M^j \) respectively, with \( l_i \geq l_j \). Let \( \mathcal{G}_1 \subset \mathcal{G} \) be the set of all structure graphs such that the \( W_i, W_j \) does not contain any loop. The \( \mathcal{G}_2 = \mathcal{G} \setminus \mathcal{G}_1 \) is the set of the remaining structure graphs.

**a) Analysis of \( \mathcal{G}_1 \).** As before \( M^i \) or \( M^j \) could not be a prefix of each other. Let \( p \) be the lcp of \( M^i \) and \( M^j \) and let the colliding pair is \((Y_{\beta_i}^i, Y_{\beta_j}^j)\), where \( p + 1 \leq \beta_i \leq l_i, p + 1 \leq \beta_j \leq l_j \). In this case, it is easy to check that the following system of equations will have rank 2.

\[
\begin{align*}
Y_{i+1}^i &= x, \\
Y_1^i + Y_2^j + \ldots + Y_{i+1}^i + Y_s^i &= 0.
\end{align*}
\]

Therefore, we have \( \Pr[W \land |f\text{Coll}(G)| = 1] \leq \frac{1}{2^{2n}} \).

Note that \( |\mathcal{G}_1| \) is \( i^2 \) as the graph is uniquely determined by the accident point and the set of messages \( \mathcal{M} \). Therefore, \( \Pr[W \land |f\text{Coll}(G)| = 1] \leq \frac{i^2}{2^{2n}} \).

**b) Analysis of \( \mathcal{G}_2 \).** As before let us assume that \( W_i \) contains a loop of size \( c \) such that \( Y_{\alpha}^i = Y_{\alpha+c}^i \) for \( c \geq 1 \). Since the loop creates a \( f \)-collision, neither (i) \( W_j \) or \( W_i \) makes another different loop, nor (ii) \( W_j \) collides with \( W_i \) as in both of the cases the number of collisions will increase to 2. Thus we have the following two possibilities.

1. \( W_j \) coincides with \( W_i \)
2. \( W_j \) could follow \( W_i \) but after a point \( W_i \) and \( W_j \) departs and never meets again.
We analyze the probability of the event $W \land |f\text{Coll}(G)| = 1$ separately for each of the two above cases. In particular, in each of the following analysis our main concern will be to show the rank of the set of equations as defined earlier (i.e Equation (5) and (6)) to be 2, that is it achieves full rank in each of the following subcases.

**Case 1.** Let $k$ denotes the number of iterations in the loop of $W_i$ and $k'$ be the number of iterations in the loop of $W_j$. Now irrespective of the value of $k$ and $k'$, the system of equations (Equation (5) and (6)) will have rank 2 and therefore, we can upper bound the probability of our desired event to $\frac{1}{2^n}$. Note that $G \in G_2$ is uniquely determined by the size of the loop $c$ and hence, $|G_2| \leq l^2$, Thus,

$$\Pr[W \land |f\text{Coll}(G)| = 1] \leq \frac{l^2}{2^{2n}}.$$  \(7\)

**Case 2.** The analysis for this case would be similar to Case 1. Here $W_i$ and $W_j$ bifurcates from a certain point say $X$ and $l_i - X, l_j - X \neq 0$. Therefore, it is trivial to see that the set of equations (i.e Equation (5) and (6)) will have full rank. Again, as we have shown in the previous case that $|G_2| \leq l^2$ and therefore Equation (7) will also hold in this case.

Combining the probability bound of the event $W \land |f\text{Coll}(G)| = 1$ from each of the two above subcases, we have derived $\Pr[W \land |f\text{Coll}(G)| = 1] \leq \frac{l^2}{2^{2n}}$.  

5 Conclusion

In this paper, we have proposed a variant of NI-MAC, which we call as NI$^+$-MAC and have shown that NI$^+$-MAC achieves BBB security. We have also shown that keeping the original structure of NI as discussed in Section 3.1 cannot achieve BBB security. Moreover, our non-tweaked proposed construction is better than Yasuda’s proposed single-fixed key compression function based MAC construction that uses an extra tweak. NI$^+$ is also efficient than NI-MAC in terms of number of keys and providing better security.

References

35. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Shoup [32], pages 17–36.
A Formal Discussion on Structure Graph

Let for two distinct messages $M^1$ and $M^2$ of $l_1$ and $l_2$ blocks respectively, where $M^1 = M^1_1 || M^1_2 || ... || M^1_l$ and $M^2 = M^2_1 || M^2_2 || ... || M^2_l$, and the corresponding $Y$-values be given by $y^1_0, y^1_1, y^1_2, ..., y^1_l$ and $y^2_0, y^2_1, y^2_2, ..., y^2_l$ respectively. Let $\tau = l_1 + l_2$. We use the notation $M_i$ where $1 \leq i \leq \tau$ to refer to the block $M^1_i$, when $i \leq l_1$, otherwise refer to the block $M^2_{i-l_1}$. Similarly, let $Y_i$ to refer to 0 when $i = 0$; $Y^1_i$, when $1 \leq i \leq l_1$; and $Y^2_{i-l_1}$, when $l_1 + 1 \leq i \leq \tau$.

Now, we give a few definitions.

Definition 2. We define two mappings $[\cdot]$ and $[\cdot]'$ on $\{0, \ldots, \tau\}$ as follows:
1. $[\cdot] \triangleq \min \{ j : Y_j = Y_j \}$, and
2. $[\cdot]' \triangleq [\cdot]$ for $i \neq 1$ except that $[1]' = 0$.

Definition 3. For any fixed $f$ and any two distinct messages $M = \{M^1, M^2\}$, we define the structure graph $G^f(M)$ as follows:
$G^f(M) \triangleq (V, E, L)$, where $V = \{[[i]] : 0 \leq i \leq \tau\}$, $E = \{([[i-1]]', [[i]]) : 1 \leq i \leq \tau\}$, and $L((u, v)) = \{M_i : [[i-1]]' = u$ and $[[i]] = v\}$ is an edge-labeling.

Definition 4. For the computation of $M^1$, the sequence $0, ([[0]]', [[1]]), ([1]), ([[1]]', [[2]]), ..., ([[1]]', ...), ([[1]]')$ of alternating vertices and edges is called an $M^1$-walk. (An $M^2$-walk is defined analogously).

Let $(V_i, E_i, L_i)$ be the graph obtained after processing only the first $i$ out of $\tau$ blocks of $M$. We define a collision event as follows.

Definition 5. $(i, [[i]])$ is an f-collision if $[[i]] < i$ and $M_i \notin L_{i-1}([[i-1]]', [[i]])$.

Note that the last condition on $M_i$ implies that collision occurred due to parallel edges with the same message label is not considered.