Improved Security Analysis of PMAC

Mridul Nandi and Avradip Mandal

University of Waterloo, Canada

Abstract. In this paper we provide a simple, concrete and improved security analysis of **PMAC**, a Parallelizable Message Authentication Code. We show that the advantage of any distinguisher for **PMAC** based on a random permutation is at most $\mathbf{\frac{5q\sigma - 3.5q^2}{2^n}}$, where σ is the total number of message blocks in all q queries made by the distinguisher. In the original paper by Black and Rogaway in Eurocrypt-2002, the bound was $\frac{(\sigma+1)^2}{2^{n-1}}$. Very recently, Minematsu and Matsushima in FSE-2007, have provided a bound $\frac{10\ell q^2}{2^n}$ where ℓ is the maximum block length of all messages queried by the distinguisher. Our new bound is better than both original and recently proposed bound and guarantees much more security of PMAC. We also have provided a complete, independent and simple combinatorial proof. This proof idea may help us to find a similar result for other MAC algorithms.

Keywords : MAC, PMAC, Distinguishing attack, pseudo random function, random permutation.

1 Introduction

Modes of operation is an important tool in defining arbitrary length pseudo random functions (PRF), pseudo random permutation (PRP) and MAC algorithms. Intuitively, it is a method which extends a PRF (or PRP) of small and fixed size domain into a PRF (or PRP) of arbitrary domain. Thus, it is also called as a *domain extension*. The first modes of operation is Cipher Block Chaining or CBC [3] which is a sequential construction. There are many literatures on improving runtime and key size over CBC. Some of them can be found in XCBC [6], TMAC [12], OMAC [10]. All these constructions are CBC type, sequential and reducing key size mainly.

Black and Rogaway [7] in Eurocrypt-2002 proposed a parallelizable modes of operation called as parallelizable Message Authentication Code or PMAC. It would be more suitable and efficient where a parallel environment is possible. At the same time it can be implemented in sequential with almost same performance as CBC types modes of operations. Thus, it would be worthwhile to have an improved security analysis of PMAC. Besides PMAC and all CBC-type modes of operations, we have a wide class of DAG based modes of operations provided by Jutla [11] and Nandi [16]. There are other modes of operations based on different universal hash families [9, 17, 18]. Any secure modes of operation can provide a MAC algorithm since any PRF is proven to be a secure MAC. Thus, in this paper we mainly consider PRF security analysis of PMAC based on a small domain PRP.

Intuitively, if a keyed family of functions is known as pseudo random function if it is hard to distinguish from an ideal keyed family of functions or random function[1]. Here, we consider a distinguisher which can make at most q queries altogether having at most σ many blocks with ℓ as the maximum block length among all queries. Advantage of a distinguisher is roughly measures the success probability to distinguish a keyed family of functions and arbitrary domain uniform random function. In all original papers of all known modes of operations, the advantages are $\mathrm{O}(\frac{\sigma^2}{2^n})$ (sometimes a weaker bound $\mathrm{O}(\frac{\ell^2 q^2}{2^n})$). Bellare, Pietrzak and Rogaway [2] in Crypto-2005 provided an improved bound $\frac{12\ell q^2}{2^n} + \mathrm{o}(\frac{\ell q^2}{2^n})$ for CBC. Recently, Minematsu and Matsushima [15] in FSE-2007 have provided a bound $\frac{10\ell q^2}{2^n}$ for PMAC. Even if they have claimed that these are improved bound, we would like to mention that these bound can be weaker for some attackers. In particular, if an attacker makes only one query of large block length $\ell = q$ and all other queries have block length one then the original bound [7] for PMAC is $\frac{8q^2}{2^n}$ whereas the recent bound is $\frac{10q^3}{2^n}$ [15].

Our work : In this paper we provide an improved bound for PMAC based on a random permutation for all possible distinguishers. We show that the advantage for any distinguisher of PMAC is at most $\frac{5q\sigma - 3.5q^2}{2^n}$ which is always less than the original bound [7] as well as the recent bound [15]. We have used a purely combinatorial approach to prove this bound. In this paper we have provided a concrete proof. In the original paper [7] one step in the proof of the main theorem has been intuitively justified which needs rigorous analysis. In particular, the authors of [7] stated that the advantage is bounded by probability of some "bad" event defined in [7]. A similar type of argument was popularly used in distinguishing pseudo random function and pseudo random permutation which was later found to be wrong [4]. Thus, a detail argument on this statement is required to understand the proof. On the other hand the proof of the recent bound of PMAC [15] does not use the same argument, instead it is based on Maurer's methodology [14]. Here, we provide a counting based, completely independent and concrete proof for our proposed improved bound.

Organization of the paper : In section 2 we briefly state MAC and its related security notions. Then we provide some basic results and terminologies in section 3 which would be used in this paper. In section 4, we provide a complete definition of PMAC. An improved security bound is proved in section 5 and finally we conclude with possible future works in section 6.

[1] we also call it an uniform random function

2 Message Authentication Codes (MAC) and its Security Notions

MAC or Message Authentication Code. A MAC is a family of functions $\{F_k\}_{k \in \mathcal{K}}$ where $F_k : \mathcal{M} \to T$, $\mathcal{M}$ is a message space, T is a set of all tag space and $k \in \mathcal{K}$ is a secret key chosen uniformly from a key space. If $t = F_k(M)$ then t is called the *tag* of the message M. In this paper, we assume the following :

1. $T = \mathbb{F}_{2^n}$, the finite field of size 2^n. We can represent $\mathbb{F}_{2^n}$ by $\{0,1\}^n$ with field addition $+$ (or $\oplus$, XOR) and field multiplication $*$ (for a suitably chosen primitive polynomial of degree n). In this paper the choice of the polynomial is not important and hence we fix a primitive polynomial and the multiplication $*$ on $\{0,1\}^n$ is defined based on the polynomial. We denote $\mathbf{0} = 0^n$ for the additive identity.
2. $\mathcal{M} = \{0,1\}^{\leq L} = \cup_{i \leq L} \{0,1\}^i$ (for a sufficiently large integer L). For example, $L = 2^{64}$.
3. $\mathcal{K} = \{0,1\}^{\text{KeyLen}}$. The value of KeyLen or key size depends on the construction. For example, PMAC based on AES has key size 128 with $n = 128$.

A distinguisher and its advantage. $\text{Func}(\mathcal{M}, T)$ is the set of all functions from $\mathcal{M}$ to T. Let $\{F_k\}_{k \in \mathcal{K}}$ be a keyed function family whose security is to be considered. Let K be the uniform random variable on $\mathcal{K}$ and $f = f_K$ is the induced random variable taking values on $\text{Func}(\mathcal{M}, T)$. Any random variable taking values on $\text{Func}(\mathcal{M}, T)$ is called as a **random function**. Let u denote the uniform random variable on $\text{Func}(\mathcal{M}, T)$ known as **uniform random function**.

A **distinguisher** $\mathcal{A}^{\mathcal{O}}$ is an oracle algorithm where $\mathcal{O}$ is an oracle from $\text{Func}(\mathcal{M}, T)$. A distinguisher can make at most q queries adaptively consisting of at most σ many "blocks" (the definition of block will be given later). Finally, it returns either 1 or 0. **Advantage** for a distinguisher $\mathcal{A}^{\mathcal{O}}$ is computed as follows :

$$\mathbf{Adv}_{f,u}(\mathcal{A}) \triangleq \mathbf{Adv}_f(\mathcal{A}) \triangleq \big|\ \mathbf{Pr}[\mathcal{A}^f = 1] - \mathbf{Pr}[\mathcal{A}^u = 1]\ \big|.$$

$$\mathbf{Adv}_{f,u}(q, \sigma) \triangleq \mathbf{Adv}_f(q, \sigma) \triangleq \mathbf{max}_{\mathcal{A}}\ \mathbf{Adv}_f(\mathcal{A})$$

where the maximum is taken over all distinguishers $\mathcal{A}$ making at most q queries consisting of at most σ many blocks. Since we consider the distinguisher with out any time restriction it is enough to consider a deterministic algorithm. A random function f is said to be (q, σ, ϵ)**-PRF** if $\mathbf{Adv}_f(q, \sigma) \leq \epsilon$. MAC forgery security is also a popular security notion for MAC algorithms. In this paper we only consider PRF security as it is a stronger security notion than the MAC forgery security.

3 Some useful Results and Terminologies

In this section we state two interpolation theorems. The strong version of the theorem would be used to provide our improved security analysis. We also present some related terminologies on tuples and permutations.

3.1 Interpolation Theorem

We say that $\mathbf{M} = (M^1, \cdots, M^q)$ is **q-distinct** if M^i's are distinct where $M^i \in \mathcal{M}$. Suppose $f' \in \mathrm{Func}(\mathcal{M}, \{0,1\}^n)$ and $\mathbf{M}$ is q-distinct. We write $f'^{(q)}(\mathbf{M}) \stackrel{\Delta}{=} (f'(M^1), \cdots, f'(M^q))$ and call as an q-interpolation of f'. Now we describe our main tool which says that if the q-interpolation probability for f is close to that of u then the advantage for any distinguisher is also small. We denote $||M||_n = \lceil \frac{|M|}{n} \rceil$ and called it as the number of **blocks** of M.

Theorem 1. (interpolation theorem)
Suppose for each q-distinct $\mathbf{M} = (M^1, \cdots, M^q)$ with $\sum_{i=1}^{q} ||M^i||_n \leq \sigma$ and any $\mathbf{y} = (y^1, \cdots, y^q) \in (\{0,1\}^n)^q$ we have

$$\Pr[f^{(q)}(\mathbf{M}) = \mathbf{y}] \geq (1-\epsilon) \times \Pr[u^{(q)}(\mathbf{M}) = \mathbf{y}]$$

then $\mathbf{Adv}_f(q,\sigma) \leq \epsilon$ where f is a random function and u is an uniform random function on $\mathrm{Func}(\mathcal{M}, \{0,1\}^n)$.

For any $\mathbf{y} \in \{0,1\}^{nq}$, and any distinct $\mathbf{M}$, $\Pr[u^{(q)}(\mathbf{M}) = \mathbf{y}] = \frac{1}{N^q}$ where $N = 2^n$. Thus above theorem says that if

$$\forall \mathbf{y} \in (\{0,1\}^n)^q, \text{ and } \forall\ q\text{-distinct } \mathbf{M},\ \Pr[f^{(q)}(\mathbf{M}) = \mathbf{y}] \geq \frac{1-\epsilon}{N^q}$$
$$\Rightarrow \quad \mathbf{Adv}_f(q,\sigma) \leq \epsilon.$$

This theorem has been proved in [16] and a variant of the theorem has been proved in [5]. In [16], a strong version of the theorem has been proved. In this paper we need the strong version of the theorem to prove our improved bound.

Theorem 2. (strong interpolation theorem)

$$\forall \mathbf{y} \in (\{0,1\}^n)^q \setminus \mathtt{Bad},\ \textit{and}\ \forall\ q\textit{-distinct}\ \mathbf{M},\ \Pr[f^{(q)}(\mathbf{M}) = \mathbf{y}] \geq \frac{1-\epsilon_1}{N^q}$$
$$\Rightarrow \quad \mathbf{Adv}_f(q,\sigma) \leq \epsilon_1 + \epsilon_2 \ \textit{where}\ \frac{|\mathtt{Bad}|}{N^q} \leq \epsilon_2.$$

3.2 Some more results and terminologies

We denote $\mathbf{P}(m,r) = m(m-1)\cdots(m-r+1)$ where $r \leq m$ are nonnegative integers. The number of ways we can choose distinct $a_1, \cdots, a_r$ from a set of size m is $\mathbf{P}(m,r)$. We denote $\mathbf{P}(N,q) = N^q(1-\delta_{N,q})$. Thus, $\delta_{N,q} = 1 - \frac{\mathbf{P}(N,q)}{N^q}$.

Consider a s-tuple $\mathbf{a} = (a_1, \cdots, a_s)$. We call the size of the tuple, denoted as $|\mathbf{a}|$ by the number of distinct elements. For example, $|(1,2,2,3,5,1,3)| = 4$. Two s-tuples $\mathbf{a}$ and $\mathbf{b}$ are said to be **matching** (or $\mathbf{a}$ is matching tuple with respect to **b**) if $a_i = a_j$ if and only if $b_i = b_j$. For example, (x, y, y, z, w, x, z) is matching tuple w.r.t. $(1, 2, 2, 3, 5, 1, 3)$. Trivially, for any two matching tuples **a** and **b**, $|\mathbf{a}| = |\mathbf{b}|$. Now we have following simple and useful lemma. We leave readers to verify the lemma by themselves.

Lemma 1. *Given a tuple* **a** *of size* r*, the total number of matching tuples w.r.t.* **a** *whose elements are from a set of size* m *is* $\mathbf{P}(m, r)$*.*

Suppose **a** and **b** are matching tuples with elements from S. Then the total number of permutations π on S such that $\pi(a_1) = b_1, \cdots, \pi(a_s) = b_s$ is $(|S| - |\mathbf{a}|)!$. The conditions $\pi(a_1) = b_1, \cdots, \pi(a_s) = b_s$ actually restrict on outputs of $|\mathbf{a}|$ inputs. Outputs of remaining $(|S| - |\mathbf{a}|)$ many inputs can be defined in $(|S| - |\mathbf{a}|)!$ ways.

Now we state some elementary results which would be used in this paper frequently.

Lemma 2. *1. Suppose* $a \leq b$*,* c *are positive integers then* $\frac{a}{b} \leq \frac{a+c}{b+c}$*.*
2. For $0 < a_1, a_2, \cdots a_s < 1$*,* $(1 - a_1)(1 - a_2) \cdots (1 - a_s) \geq (1 - a_1 - a_2 \cdots - a_s)$*.*

4 Definition of PMAC

In this section we will describe PMAC. Later we will analyze the security of it. Let $\pi : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a permutation. Now we define an extended function, known as **PMAC** function, $\mathrm{P}_\pi : \mathcal{M} \rightarrow \{0, 1\}^n$. We first define a *padding rule* which makes message size a multiple of n if it is not so.

$$\left.\begin{array}{ll} \mathbf{pad}(M) = M \parallel 10^s & \text{if } n \not| \, |M| \\ \phantom{\mathbf{pad}(M)} = M & \text{otherwise} \end{array}\right\} \qquad (1)$$

where s is the smallest nonnegative integer such that $s + 1 + |M|$ is a multiple of n.

<u>**Algorithm PMAC :**</u> $Y = \mathrm{P}_\pi(M)$

step-1 Write $\mathbf{pad}(M) = x_1 \parallel \cdots \parallel x_\ell \parallel z$, where $\ell \geq 0$ and $|x_1| = \cdots |x_\ell| = |z| = n$. \\ We say these x_i's and z as *blocks*. If $\ell = 0$, then $\mathbf{pad}(M)$ is nothing but z. Thus, $\ell + 1$ is the total number of message blocks for $\mathbf{pad}(M)$.

step-2 Compute $w = \pi(0)$. \\ Since π is a random permutation and kept secret the value of $\pi(0)$ has some distribution and can be used as a part of the key of the algorithm.

step-3 Compute $v_i = x_i + c_i * w, 1 \leq i \leq \ell$. \\ c_i's are some fixed distinct nonzero constants as given in [7]. For our security analysis, we only need that $c_i \neq 0$ and they are distinct. $(\{0, 1\}^n, +, *)$ is any Galois field $GF(2^n)$. One can think $+$ as $\oplus$ as it is the simplest operation in both hardware and software.

step-4 Compute $w_i = \pi(v_i), 1 \leq i \leq \ell$.

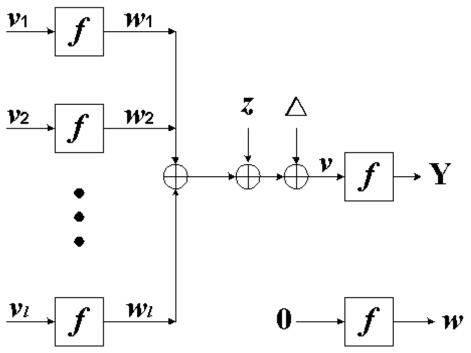

Fig. 1. PMAC Algorithm : $\mathbf{pad}(M) = x_1 \parallel \cdots \parallel x_\ell \parallel z$, $v_i = x_i + c_i * w$ and $\Delta = c * w$ if $n \mid |M|$ otherwise $\Delta = 0$. $\mathrm{P}_f(M) = Y$.

step-5 Compute $v = z + \Delta + \sum_{1\leq i\leq \ell} w_i$, where $\Delta = c * w$ if $|M|$ is multiple of n, otherwise we set $\Delta = 0$. \\ Again, c is a nonzero fixed constant which is different from $c_1, c_2, \cdots$, and it is given in [7].

step-6 Finally, $Y \overset{\Delta}{=} \mathrm{P}_\pi(M) = \pi(v)$.

0 and v_i's are **intermediate inputs**, w and w_i's are **intermediate outputs** and v is the **final input**. The final input v is said to be **new** if $v \neq 0$ and $v \neq v_i$, $1 \leq i \leq \ell$. Given a message M, all these intermediate inputs, intermediate outputs, final inputs depend only on the underlying permutation π. If v is new then we also say that π is new for M. We can define similarly for q distinct messages $M^1, \cdots, M^q$.

1. We say final inputs are **new** if all q final inputs are distinct and different from all intermediate inputs.
2. The underlying permutation π is said to be **new** for $\mathbf{M} = (M^1, \cdots, M^q)$ if the final inputs are new.
3. A new permutation π is said to be a **good** permutation for $\mathbf{M}$ with respect to a q-distinct $\mathbf{y} = (y^1, \cdots, y^q)$ if the set of all intermediate outputs are disjoint from the set $\{y_1, \cdots, y^q\}$.

5 Improved Security Analysis of PMAC

Now we give a lower bound of size of the set $I_\mathbf{y} = \{\pi : \mathrm{P}_\pi(M^1) = y^1, \cdots, \mathrm{P}_\pi(M^q) = y^q\}$ for q-distinct $\mathbf{M} = (M^1, \cdots, M^q)$ and q-distinct $\mathbf{y} = (y^1, \cdots, y^q)$. This estimation provide a lower bound of interpolation probability and hence we can use strong interpolation theorem.

Let $||M^i||_n = \ell_i$ and write $M^i = M^i_1 \parallel \cdots M^i_{\ell_i} \parallel z^i$, where $|M^i_j| = |z^i| = n$, $1 \leq i \leq q$ and $1 \leq j \leq \ell_i$. We write $\sigma' = \sum_{i=1}^q \ell_i$ and $\sigma = \sigma' + q$ and $N = 2^n$. Let $\Delta = c * w$ if $n \mid |M|$ otherwise $\Delta = 0$. Given a permutation π,

1. $w[\pi] = \pi(0)$, $v^i_j[\pi] = c_i * w[\pi] + M^i_j$,
2. $w^i_j[\pi] = \pi(v^i_j[\pi])$.
3. $v^i[\pi] = z^i + \varDelta^i + \sum_{1 \le j \le \ell_i} w^i_j[\pi]$.

Definition 1. *Given $w \in \mathbb{F}_{2^n}$, we define $v^i_j = c_i * w + M^i_j$ and denote $\mathbf{V}_w = (0, v^1_1, \cdots, v^1_{\ell_1}, \cdots, v^q_1, \cdots v^q_{\ell_q})$. Given a tuple $\mathbf{W} = (w, w^1_1, \cdots, w^1_{\ell_1}, \cdots, w^q_1, \cdots, w^q_{\ell_q})$ we define a* corresponding input tuple $\mathbf{V}_{\mathbf{W}} = (\mathbf{V}_w, v^1, \cdots, v^q)$ *where $v^i = z^i + \varDelta^i + \sum_{1 \le j \le \ell_i} w^i_j$.*

Given π, we define $\mathbf{W}[\pi] = (w[\pi], w^1_1[\pi], \cdots, w^1_{\ell_1}[\pi], \cdots, w^q_1[\pi], \cdots, w^q_{\ell_q}[\pi])$. We denote $\mathbf{V}[\pi] = (0, v^1_1[\pi], \cdots, v^1_{\ell_1}[\pi], \cdots, v^q_1[\pi], \cdots v^q_{\ell_q}[\pi], v^1[\pi], \cdots, v^q[\pi])$ Note that $\mathbf{V}[\pi]$ is the corresponding input tuple of $\mathbf{W}[\pi]$ and hence $\mathbf{V}[\pi] = \mathbf{V}_{\mathbf{W}[\pi]}$.

Let $\mathcal{T}_s$ denote the set of s-tuples whose elements are from $\mathbb{F}_{2^n}$. We define a mapping

$$\mathcal{W} : \mathrm{Perm}(\mathbb{F}_{2^n}) \to \mathcal{T}_{\sigma'+1} : \mathcal{W}(\pi) = \mathbf{W}[\pi].$$

A tuple $\mathbf{W} = (w, w^1_1, \cdots, w^1_{\ell_1}, \cdots, w^q_1, \cdots w^q_{\ell_q})$ is said to be *permutation compatible* if $\mathbf{W}$ and $\mathbf{V'}_w$ are matching tuples and we denote the set of all permutation compatible tuples by $\mathcal{T}^{\mathrm{perm}}_{\sigma'+1} \subset \mathcal{T}_{\sigma'+1}$.

Lemma 3. *$\mathcal{W}(\mathrm{Perm}(\mathbb{F}_{2^n})) = \mathcal{T}^{\mathrm{perm}}_{\sigma'+1}$ and for any tuple $\mathbf{W} \in \mathcal{T}^{\mathrm{perm}}_{\sigma'+1}$ of size s there are $(N-s)!$ permutations π such that $\mathcal{W}(\pi) = \mathbf{W}$.*

Proof. Given any permutation $\mathbf{W}[\pi]$ and $\mathbf{V}_{\pi(0)}$ are matching tuples. Thus, $\mathcal{W}(\mathrm{Perm}(\mathbb{F}_{2^n})) \subseteq \mathcal{T}^{\mathrm{perm}}_{\sigma'+1}$. Conversely, if $\mathbf{W} = (w, w^1_1, \cdots, w^q_{\ell_q})$ and $\mathbf{V'}_w = (0, v^1_1, \cdots, v^q_{\ell_q})$ are matching tuples then for any permutation π such that $\pi(0) = w, \pi(v^i_j) = w^i_j$, $\mathcal{W}(\pi) = \mathbf{W}$. Thus, $\mathcal{W}(\mathrm{Perm}(\mathbb{F}_{2^n})) \supseteq \mathcal{T}^{\mathrm{perm}}_{\sigma'+1}$. Since $|\mathbf{W}| = s$, we can choose the above permutations in $(N-s)!$ ways. ■

Two tuples are said to be *disjoint* if they do not have any common elements. A tuple $\mathbf{W} = (w, w^1_1, \cdots, w^1_{\ell_1}, \cdots, w^q_1, \cdots, w^q_{\ell_q})$ is said to be $\mathbf{y}$-*disjoint* if $\mathbf{W}$ and $\mathbf{y}$ are disjoint. Thus, a permutation π is said to be new if $(v^1[\pi], \cdots, v^q[\pi])$ is disjoint from $\mathbf{V}_{\pi(0)} = (0, v^1_1, \cdots, v^q_{\ell_q})$. For a q-distinct $\mathbf{y}$, a good permutation π satisfies two conditions :

1. $(v^1[\pi], \cdots, v^q[\pi])$ is disjoint from $\mathbf{V}_{\pi(0)}$ and
2. $\mathbf{W}$ and $\mathbf{y}$ are disjoint.

Proposition 1. *The number of permutations π such that $\mathbf{W}[\pi]$ is $\mathbf{y}$-disjoint is at least $N!(1 - \frac{q\sigma - q^2 - \sigma + 2q}{N})$.*

Proof. let $S = \{0,1\}^n \setminus \{y^1, \cdots, y^q\}$. Write $S = \sqcup_{i \ge 1} S_i$ (disjoint union) where $S_i = \{a \in S : |\mathbf{V'}_a| = i\}$. For a fixed choice of $a \in S_i$, the number of matching tuples $\mathbf{W} = (a, w^1_i, \cdots, w^q_{\ell_q})$ with respect to $\mathbf{V}_a$ where the elements are chosen from S is $\mathbf{P}(N-q, i-1)$ since we can choose $(i-1)$ distinct elements from the set of size $N-q$. For any such $\mathbf{W}$, there are $(N-i)!$ many permutations π

such that $\mathbf{W}[\pi] = \mathbf{W}$. Hence we have $\sum_{i=1}^{\sigma'+1} |S_i| \times (N-i)! \times \mathbf{P}(N-q, i-1)$ permutations π such that $\mathbf{W}[\pi]$ is $\mathbf{y}$-disjoint. Now for each $1 \leq i \leq \sigma' + 1$,

$$\mathbf{P}(N-q, i-1) \geq \mathbf{P}(N-1, i-1) \times (1 - \frac{q-1}{N})^{i-1} \geq \mathbf{P}(N-1, i-1) \times (1 - \frac{\sigma'(q-1)}{N}).$$

and hence,

$$\sum_{i=1}^{\sigma'+1} |S_i| \times (N-i)! \times \mathbf{P}(N-q, i-1) \geq N!(1 - \frac{q}{N})(1 - \frac{\sigma'(q-1)}{N})$$

$$\geq N!(1 - \frac{q\sigma - q^2 - \sigma + 2q}{N}). \qquad \blacksquare$$

Proposition 2. *The number of new permutations for* 2*-distinct* (M^1, M^2) *is at least* $N!(1 - \frac{4\ell_1 + 4\ell_2 + 3}{N})$*. Thus, the number of new permutations for* q*-distinct* $\mathbf{M} = (M^1, \cdots, M^q)$ *is at least* $N!(1 - \frac{4(q-1)\sigma' + 1.5q(q-1)}{N})$*.*

Proof of the proposition is given at the end of the section. It needs several cases. The second part of the proposition directly follows from the first part. Since a permutation is new for $\mathbf{M}$ implies the permutation is new for M^{i_1}, M^{i_2} for all choices of i_1 and i_2. Note that $\sum_i \ell_i = \sigma'$. From Proposition 1 and Proposition 2, we can say that the total number of good permutations is at least $N!(1 - \frac{5q\sigma - 3.5q^2}{N})$. Let I_{G} be the set of all good permutations.

Lemma 4. *For* q*-distinct* $\mathbf{y}$*,* $|I_{\mathbf{y}} \cap I_{\mathrm{G}}| \geq \frac{|I_{\mathrm{G}}|}{\mathbf{P}(N,q)}$*.*

Proof. Consider the restricted function $\mathcal{W} : I_{\mathrm{G}} :\longrightarrow \mathcal{T}_{\sigma'+1}$. Now for any $\mathbf{W} \in \mathcal{W}(I_{\mathrm{G}})$ with $|\mathbf{W}| = i$ we have $(N-i)!$ permutations π such that $\mathcal{W}(\pi) = \mathbf{W}$. Since all these permutations are good (that is, final inputs are new and intermediate outputs are disjoint from $\{y^1, \cdots, y^q\}$) there are $(N-i-q)!$ many permutations π such that $\mathcal{W}(\pi) = \mathbf{W}$ and $\pi(v^i) = y^i$, $1 \leq i \leq q$. Let m_i be the number of tuples from $\mathcal{W}(I_{\mathrm{G}})$ with size i. Thus, $|I_{\mathrm{G}}| = \sum_i m_i (N-i)!$ and $|I_{\mathrm{G}} \cap I_{\mathbf{y}}| = \sum_i m_i (N-i-q)! \geq \frac{1}{\mathbf{P}(N,q)} \sum_i m_i (N-i)! \geq \frac{|I_{\mathrm{G}}|}{\mathbf{P}(N,q)}$. $\blacksquare$

$$\frac{|I_{\mathbf{y}}|}{N!} \geq \frac{|I_{\mathrm{G}}|}{\mathbf{P}(N,q) \times N!} \geq \frac{1}{N^q} \times \frac{(1 - \frac{5q\sigma - 3.5q^2}{N})}{1 - \delta_{N,q}} \geq \frac{(1 - \epsilon_1)}{N^q}$$

where $\epsilon_1 = \frac{5q\sigma - 3.5q^2}{N} - \delta_{N,q}$. Let $\mathtt{Bad} = \{\mathbf{y} : \mathbf{y} \text{ is not } q\text{-distinct }\}$. So, $\frac{|\mathtt{Bad}|}{N^q} = 1 - \frac{\mathbf{P}(N,q)}{N^q} = \delta_{N,q}$. By using strong interpolation theorem, we have $\mathbf{Adv}_{P_{\Pi}}(q, \sigma) \leq \frac{5q\sigma - 3.5q^2}{N}$.

Theorem 3. (Improved security bound for PMAC)
Let Π be a random function taking uniform distribution on $\mathrm{Perm}(\{0,1\}^n)$. *Let P_Π be the PMAC random function based on the uniform random permutation Π. Then for any distinguisher $\mathcal{A}$ making at most q many queries having at most σ many blocks in total, has distinguishing advantage less than $\frac{5q\sigma-3.5q^2}{2^n}$. Thus,*

$$\mathbf{Adv}_{\mathrm{P}_\pi}(q,\sigma) \leq \frac{5q\sigma - 3.5q^2}{2^n}.$$

This is indeed an improved bound.

Bellare, Pietrzak and Rogaway [2] have shown that $\mathbf{Adv}_{\mathbf{CBC}}(q,\ell) \leq \frac{12\ell q^2}{2^n} + \frac{64\ell^4 q^2}{2^{2n}}$ where CBC is the cipher-block-chaining MAC algorithms and ℓ is the maximum block length among all q queries. The original bound of CBC [3] is $\frac{\ell^2 q^2}{2^n}$. Bellare, Pietrzak and Rogaway [2] have claimed their new bound as an improved bound. But it is easy to see that if we choose $\ell \leq 3$ then the original bound [3] is better than the new bound [2].

In this paper we consider PMAC. Let us write down all the bounds till now we have for PMAC. In the original paper by Black and Rogaway [7], the bound is $\frac{(\sigma+1)^2}{2^{n-1}}$. Very recently, Minematsu and Matsushima [15] in FSE-2007, have provided a bound $\frac{10\ell q^2}{2^n}$. Again, the authors have claimed this recent bound as an improvement bound over the original bound. For example, an adversary is making $(q-1)$ queries of block length one and one query of block length q. Then, $\sigma = 2q-1$, $\ell = q$ and hence original bound becomes $\frac{8q^2}{2^n}$, whereas the recent bound is $\frac{10\ell^3}{2^n}$ which is not at all an improved bound. So, we should be careful when we are looking for improved (in real sense) bounds.

In this paper, we have provided a bound $\frac{5\sigma q-3.5q^2}{2^n}$. It is easy to see that for $1 \leq q \leq \sigma = \sum_{i=1}^{q} \ell_i$, and $\ell = \mathbf{max}_i \ell_i$,

$$(1)\ \ \frac{5q\sigma - 3.5q^2}{N} < \frac{2(\sigma+1)^2}{N}.$$

$$(2)\ \ \frac{5q\sigma - 3.5q^2}{N} < \frac{10\ell q^2}{N}.$$

Thus our bound is better than all previously known bounds for PMAC. The analysis we have used can also be used for other constructions like OMAC which does not have any improved security analysis yet.

Proof of the Proposition 2

We first assume that $\ell_1, \ell_2 > 0$. We have four possible cases.

Case-1 : $\boldsymbol{\ell_1 = \ell_2 = \ell}$ (say), $\boldsymbol{x^1_1 = x^2_1, \cdots, x^1_\ell = x^2_\ell, z^1 = z^2}$.

This case can happen only if $\mathbf{pad}(M^1) = M^1 = M^2 \parallel 10^s = \mathbf{pad}(M^2)$ (or in other way). Let $S = \{w \in \mathbb{F}_{2^n} : (v^1_1, v^2_1)$ is disjoint from $(0, v^1_2, \cdots, v^1_\ell, v^2_2, \cdots, v^2_\ell)$ and $\Delta^1 + z^1 \neq \Delta^2 + z^2\}$. Clearly, $|S| \geq N - \ell - 1$ since

$$S = \{0,1\}^n \setminus (\{\frac{x^2_j - x^2_1}{c_1 - c_j} : 2 \leq j \leq \ell\} \cup \{\frac{-x^2_1}{c_1}\} \cup \{\frac{z^2 - z^1}{c}\}).$$

We write $S = \sqcup_i S_i$ (disjoint union) where $S_i = \{a \in S : |\mathbf{V}_a| = i\}$. Now for each $a \in S_i$, there are $\mathbf{P}(N-1, i-2)$ tuples $\mathbf{W}_1 = (a, w^1_2, \cdots, w^1_{\ell_1}, w^2_2, \cdots, w^2_{\ell_2})$ such that W_1 is matching with $\mathbf{V}_1 = (0, v^1_2, \cdots, v^1_{\ell_1}, v^2_2, \cdots, v^2_{\ell_2})$.

1. For each such tuple we have at least $(N - 2\ell - 2 - i)$ choices of $w^1_1 = w^2_1$ such that $\mathbf{W} = (a, w^1_1, \cdots, w^1_{\ell_1}, w^2_1, \cdots, w^2_{\ell_2})$ is matching with $\mathbf{V}_a$ and (v^1, v^2) is disjoint from $\mathbf{V}_a$. This is true since we can choose

   $w^1_1 \in \{0,1\}^n \setminus (\{w^1_j : 2 \leq j \leq \ell\} \cup \{a\} \cup \{w : v^1 = 0, v^1_j\} \cup \{w : v^2 = 0, v^1_j, v^1\})$

   The size of the above set is at least $N - (i-1) - (\ell+1) - (\ell+2) = N - 2\ell - 2 - i$.
2. For each such tuple $\mathbf{W}$, there are $(N-i)!$ many permutations such that $\mathcal{W}(\pi) = \mathbf{W}$. Hence, the number of new permutations is at least

$$\sum_i |S_i| \mathbf{P}(N-1, i-2)(N - 2\ell - i - 2)(N-i)!$$
$$\geq N! \times \frac{N - \ell - 1}{N} \times \frac{N - 2\ell - i - 2}{N - i + 1} \geq N!(1 - \frac{3\ell + 4}{N})$$

Case-2 : $\boldsymbol{\ell_1 = \ell_2 = \ell}$ (say) and $\boldsymbol{x^1_1 = x^2_1, \cdots, x^1_\ell = x^2_\ell, z^1 \neq z^2}$.

A similar analysis like Case-1 shows that there are at least $N!(1 - \frac{3\ell+5}{N})$ many permutations generating new final inputs. Thus, we ignore the detail proof of this case. Now we assume that $x^1_1 \cdots x^1_{\ell_1} \neq x^2_1 \cdots x^2_{\ell_2}$. Thus, we have either $x^1_1 = x^2_1, \cdots, x^1_{\ell_1} = x^2_{\ell_2}$ or $x^1_1 \neq x^2_1$ (without loss of generality).

Case-3 : $\boldsymbol{\ell_2 > \ell_1 : x^1_1 = x^2_1, \cdots, x^1_{\ell_1} = x^2_{\ell_2}}$.

We want to choose $\mathbf{W} = (w, w^1_1, \cdots, w^1_{\ell_1}, w^2_1, \cdots, w^2_{\ell_2})$-tuple, such that $(v^1_1, v^2_{\ell_2}, v^1, v^2)$ is 4-distinct tuple and disjoint from $(0, v^1_2, \cdots, v^1_{\ell_1}, v^2_2 \cdots, v^2_{\ell_2 - 1})$. Note that, here we choose $\mathbf{W}$ such that $w^1_1 = w^2_1, \cdots, w^1_{\ell_1} = w^2_{\ell_1}$.

1. Let S denote the the set of all w such that $(v^1_1, v^2_{\ell_2})$ is 2-distinct and disjoint from $(0, v^1_2, \cdots, v^1_{\ell_1}, v^2_2 \cdots, v^2_{\ell_2 - 1})$.
   Hence, $w \neq \frac{x^1_1 - x^2_j}{c_j - c_1}, \frac{x^2_{\ell_2} - x^2_j}{c_j - c_{\ell_2}}, -\frac{x^1_1}{c_1}, -\frac{x^2_{\ell_2}}{c_{\ell_2}}$ for $2 \leq j \leq \ell_2 - 1$. Thus, $|S| \geq (N - 2\ell_2 + 2)$.
   We write $S = \sqcup_i S_i$, where $S_i = \{a \in S : |\mathbf{V}_a| = i\}$. Now for each $a \in S_i$, there are $\mathbf{P}(N-1, i-3)$ tuples $\mathbf{W}_1 = (a, w^1_2, \cdots, w^1_{\ell_1}, w^2_2, \cdots, w^2_{\ell_2 - 1})$ such that W_1 is matching with $\mathbf{V}_1 = (0, v^1_2, \cdots, v^1_{\ell_1}, v^2_2, \cdots, v^2_{\ell_2 - 1})$.

2. We choose $w_1^1 \notin (a, w_2^1, \cdots, w_{\ell_1}^1, w_2^2, \cdots, w_{\ell_2-1}^2)$ such that $v^1 \neq 0, v_j^2 : 1 \leq j \leq \ell_2$. Thus, total number of choices of w_1^1 is at least $(N - i + 2 - \ell_2 - 1) = (N - i - \ell_2 + 1)$. Similarly, we can choose w_1^2 in $(N - i - \ell_2 - 1)$ ways (here we have two more restrictions that $w_1^2 \neq w_1^1$ and $v^2 \neq v^1$).
3. For each such tuple $\mathbf{W}$, there are $(N - i)!$ many permutations such that $\mathcal{W}(\pi) = \mathbf{W}$. Hence, the number of new permutations is at least

$$\sum_i |S_i|\mathbf{P}(N-1, i-3)(N-i)!(N-i-\ell_2-1)(N-i-\ell_2+1)$$
$$\geq N! \times \frac{N-2\ell_2+2}{N} \times \frac{N-i-\ell_2-1}{N-i+1} \times \frac{N-i-\ell_2+1}{N-i+2}$$
$$\geq N!(1 - \frac{4\ell_2+1}{N})$$

Case-4 : $\boldsymbol{x_1^1 \neq x_1^2}$.

We want to choose $(w, w_1^1, \cdots, w_{\ell_1}^1, w_1^2, \cdots, w_{\ell_2}^2)$-tuple (some of them may be equal), such that (v_1^1, v_1^2, v^1, v^2) is 4-distinct tuple and disjoint from $(0, v_2^1, \cdots, v_{\ell_1}^1, v_2^2 \cdots, v_{\ell_2}^2)$.

1. Let S denote the the set of all w such that (v_1^1, v_1^2) is 2-distinct and disjoint from $(0, v_2^1, \cdots, v_{\ell_1}^1, v_2^2 \cdots, v_{\ell_2}^2)$.
   Hence, $w \neq \frac{x_1^1-x_i^1}{c_i-c_1}, \frac{x_1^2-x_i^2}{c_i-c_1}, \frac{x_1^1-x_j^2}{c_j-c_1}, \frac{x_1^2-x_j^1}{c_j-c_1}, -\frac{x_1^1}{c_1}, -\frac{x_1^2}{c_1}$ for $2 \leq i \leq \ell_1, 2 \leq j \leq \ell_2$.
   Thus, $|S| \geq (N - 2\ell_1 - 2\ell_2 + 2)$.
   We write $S = \sqcup_i S_i$, where $S_i = \{a \in S : |\mathbf{V}_a| = i\}$. Now for each $a \in S_i$, there are $\mathbf{P}(N-1, i-3)$ tuples $\mathbf{W}_1 = (a, w_2^1, \cdots, w_{\ell_1}^1, w_2^2, \cdots, w_{\ell_2}^2)$ such that W_1 is matching with $\mathbf{V}_1 = (0, v_2^1, \cdots, v_{\ell_1}^1, v_2^2, \cdots, v_{\ell_2}^2)$.
2. We choose $w_1^1 \notin (a, w_2^1, \cdots, w_{\ell_1}^1, w_2^2, \cdots, w_{\ell_2}^2)$ such that $v^1 \neq 0, v_i^1, v_j^2 : 1 \leq i \leq \ell_1, 1 \leq j \leq \ell_2$. Thus, total number of choices of w_1^1 is at least $(N - i + 2 - \ell_1 - \ell_2 - 1) = (N - i - \ell_1 - \ell_2 + 1)$. Similarly, we can choose w_1^2 in $(N - i - \ell_1 - \ell_2 - 1)$ ways (here we have two more restrictions that $w_1^2 \neq w_1^1$ and $v^2 \neq v^1$).
3. For each such tuple $\mathbf{W}$, there are $(N - i)!$ many permutations such that $\mathcal{W}(\pi) = \mathbf{W}$. Hence, the number of new permutations is at least

$$\sum_i |S_i|\mathbf{P}(N-1, i-3)(N-i)!(N-i-\ell_1-\ell_2-1)(N-i-\ell_1-\ell_2+1)$$
$$\geq N! \times \frac{N-2\ell_1-2\ell_2+2}{N} \times \frac{N-i-\ell_1-\ell_2-1}{N-i+1} \times \frac{N-i-\ell_1-\ell_2+1}{N-i+2}$$
$$\geq N!(1 - \frac{4\ell_1+4\ell_2+1}{N})$$

We note that in all these cases we have assumed that $\ell_1, \ell_2 \geq 1$. Now we prove the statement for other two possible cases where ℓ_1 or ℓ_2 can be zero.

1. Let $\ell_1 = 0 = \ell_2$. Thus, $v^1 = c{*}w + z^1$ or $v^1 = z^1$ (depending on the padding). Similarly for v^2. It is easy to see that there are at least $(N-3)(N-1)! = N!(1-\frac{3}{N})$ new permutations.
2. The last remaining case is $\ell_1 = 0$, but $\ell_2 > 0$. We choose w such that (v^1, v_1^2) is disjoint from $(0, v_2^2, \cdots, v_{\ell_2}^2)$. There are at least $(N - 2\ell_2)$ such choices of w. Now for each such choice $w \in S_i$ (as defined in case-3 or case-4), we have $(N - \ell_2 - 1 - i)$ choices of $w_{\ell_2}^2$ such that $v^2 \notin (0, v_1^2, \cdots, v_{\ell_2}^2, v^1)$ and $w_1^2 \notin (w, w_2^2, \cdots, w_{\ell_2}^2)$. Thus, the number of new permutations is at least

$$\begin{aligned}\sum_i |S_i|\mathbf{P}(N-1, i-2)(N-i)!(N-i-\ell_2-1) \\ \geq N! \times \frac{N-2\ell_2}{N} \times \frac{N-i-\ell_2-1}{N-i+1} \\ \geq N!(1-\frac{3\ell_2+2}{N})\end{aligned}$$

Thus, the number of new permutations is at least $N!(1-\frac{4\ell_1+4\ell_2+3}{N})$.

6 Conclusion

This paper provides a simpler and improved upper bound $\frac{5q\sigma-3.5q^2}{2^n}$ for the distinguishing advantage of PMAC. This bound is always better than the recent as well as the original bound in a true sense. We have provided a purely combinatorial approach which seems to be a strong tool in this areas of cryptography. As a future research work, we hope our improved security analysis can be extended to have an improved bound on a general class given in [11, 16] and other constructions such as XCBC, TMAC and possibly OMAC.

References

1. M. Bellare, A. Boldyreva, L. Knudsen and C. Namprempre. On-Line Ciphers and the Hash-CBC constructions. Advances in Cryptology - CRYPTO 2001. Lecture Notes in Computer Science, Volume **2139**, pp 292-309.
2. M. Bellare, K. Pietrzak and P. Rogaway. Improved Security Analysis for CBC MACs. Advances in Cryptology - CRYPTO 2005. Lecture Notes in Computer Science, Volume **3621**, pp 527-545.
3. M. Bellare, J. Killan and P. Rogaway. The security of the cipher block chanining Message Authentication Code. Advances in Cryptology - CRYPTO 1994. Lecture Notes in Computer Science, Volume **839**, pp 341-358.
4. M. Bellare and P. Rogaway. Code-Based Game-Playing Proofs and the Security of Triple Encryption. Available in http://eprint.iacr.org/2004/331.pdf
5. Daniel J. Bernstein. A short proof of the unpredictability of cipher block chaining (2005). URL: http://cr.yp.to/papers.html#easycbc.

6. J. Black and P. Rogaway. CBC MACs for arbitrary length messages. Advances in Cryptology - CRYPTO 2000. Lecture Notes in Computer Science, Volume **1880**, pp 197-215.

7. J. Black and P. Rogaway. A Block-Cipher Mode of Operations for Parallelizable Message Authentication. Advances in Cryptology - Eurocrypt 2002. Lecture Notes in Computer Science, Volume **2332**, pp 384-397.

8. J. Daemen and V. Rijmen. Resistance Against Implementation Attacks. A Comparative Study of the AES Proposals. In Proceedings of the Second AES Candidate Conference (AES2), Rome, Italy, March 1999. Available at http://csrc.nist.gov/encryption/aes/aes_ home.htm.

9. H. Krawczyk. LFSR-based hashing and authenticating. Advances in Cryptology, CRYPTO 1994, Lecture Notes in Computer Science, Volume **839**, pp 129-139, Springer-Verlag 1994.

10. T. Iwata and K. Kurosawa. OMAC : One-Key CBC MAC. Fast Software Encryption, 10th International Workshop, FSE 2003. Lecture Notes in Computer Science, Volume **2887**, pp 129-153.

11. C. S. Jutla. PRF Domain Extension using DAG. Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006. Lecture Notes in Computer Science, Volume **3876** pp 561-580.

12. K. Kurosawa and T. Iwata. TMAC : Two-Key CBC MAC. Topics in Cryptology - CT-RSA 2003: The Cryptographers' Track at the RSA Conference 2003. Lecture Notes in Computer Science, Volume **2612**, pp 33-49.

13. M. Luby and C. Rackoff. How to construct pseudo-random permutations from pseudo-random functions. Advances in Cryptology, CRYPTO' 85, Lecture Notes in Computer Science, Volume **218**, pp 447, Springer-Verlag 1985.

14. U. Maurer. Indistinguishability of Random Systems. Advances in Cryptology-EUROCRYPT02, LNCS **2332**, pp. 110-132, 2002.

15. K. Minematsu and T. Matsushima. New Bounds for PMAC, TMAC, and XCBC. to be published in FSE 2007.

16. M. Nandi. A Simple and Unified Method of Proving Indistinguishability. Indocrypt 2006, Lecture Notes in Computer Science, Volume **4329**, pp 317-334.

17. P. Rogaway. Bucket Hashing and Its Application to Fast Message Authentication. Advances in Cryptology, CRYPTO 1995, Lecture Notes in Computer Science, Volume **963**, pp 29-42, Spronger-Verlag, 1995.

18. D. R. Stinson. On the connections between universal hashing, combinatorial designs and error-correcting codes. Congressus Numerantium **114**, 1996, pp 7-27.