J. Math. Crypt. **2** (2008), 149–162
DOI 10.1515 / JMC.2008.007

Improved security analysis of PMAC

Mridul Nandi and Avradip Mandal

Communicated by Kaoru Kurosawa

Abstract. In this paper we provide a simple, concrete and improved security analysis of Parallelizable Message Authentication Code or PMAC. In particular, we show that the advantage of any distinguisher $\mathcal{A}$ at distinguishing PMAC from a random function is at most $(5q\sigma - 3.5q^2)/2^n$. Here, σ is the total number of message blocks in all q queries made by $\mathcal{A}$ and PMAC is based on a random permutation over $\{0,1\}^n$. In the original paper of PMAC by Black and Rogaway in Eurocrypt-2002, the bound was shown to be $(\sigma+1)^2/2^{n-1}$. In FSE-2007, Minematsu and Matsushima provided a bound $5\ell q^2/(2^n - 2\ell)$, where ℓ is the number of blocks of the longest queried made by the distinguisher. Our proposed bound is sharper than these two previous bounds.

Keywords. MAC, PMAC, distinguishing attack, pseudorandom function, random permutation.

AMS classification. 94A60, 68P25.

1 Introduction

A keyed family of functions is known as a pseudorandom function or PRF if it is hard to distinguish from a (uniform) random function. (whose output is uniformly and independently distributed on the output space). Similarly, if a family is indistinguishable from (uniform) random permutation then we say it as a pseudorandom permutation or PRP. Modes of operation is a method which extends a PRF (or PRP) of smaller domain into a PRF (or PRP) of arbitrary domain. To our knowledge, the first known modes of operation is *Cipher Block Chaining* or CBC [1] which extends small domain PRP into a large domain PRF. It is a sequential modes of operation. There are many literatures in extending the definition to arbitrary domain. We list some of these as XCBC, TMAC [9], OMAC [6]. All these constructions are CBC type, sequential and reducing key size mainly. On the other hand, Black and Rogaway [5] in Eurocrypt-2002 proposed a parallelizable modes of operation called as a 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 PRF-security analysis of PMAC. Besides PMAC and all CBC-type modes of operations, we have a wide class of directed acyclic graph or DAG based modes of operations found in [7, 12]. There are other modes of operations based on different universal hash families [8, 4, 13].

Message authentication code or MAC is an important object in cryptography, There are two popular security notions for MAC, namely unforgability and PRF-security. Since PRF is a strong security notion we mainly consider PRF security analysis. In particular we consider PRF-security of PMAC based on a small domain PRP. 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 roughly measures the success probability to distinguish a keyed family of functions and arbitrary domain uniform random functions.

In all original papers of all known modes of operations, the advantages are $O(\frac{\sigma^2}{2^n})$ (sometimes a weaker form $O(\frac{\ell^2 q^2}{2^n})$). For example, Black and Rogaway in Eurocrypt-2002 provided a security bound for PMAC which was $\frac{(\sigma+1)^2}{2^{n-1}}$. Later Bellare, Pietrzak and Rogaway [2] in Crypto-2005 provided a different (and improved in some cases) bound of the form $\frac{12\ell q^2}{2^n} + o(\frac{\ell q^2}{2^n})$ for CBC with prefix-free messages. Recently, Minematsu and Matsushima [11] in FSE-2007 have provided a new bound $\frac{5\ell q^2}{2^n - 2\ell}$ (or a simpler form $\frac{10\ell q^2}{2^n}$) for PMAC. Unfortunately, these bounds can be much weaker for some kind of attackers. For example, for PMAC, 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 [5] for PMAC is $\frac{8q^2}{2^n}$ whereas the recent bound is at least $\frac{5q^3}{2^n}$ [11] which is cubic in q. Similarly, the improved bound of CBC for prefix-free message [2] would be an improved bound only if $\ell \geq 4$.

Our work. In this paper we provide an improved bound (in a true sense) for PMAC based on a random permutation for all possible distinguishers (in other words for all choices of parameters ℓ, q and σ). As we have discussed in the previous paragraph that the two known new bounds for PMAC are not always improved bounds. 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 [5] as well as the recent bound [11].

Now we briefly describe why we are getting improved bound of the form $\frac{q\sigma}{N}$ instead of $\frac{\sigma^2}{N}$. When adversary is making q queries with total σ many blocks then we have roughly σ many intermediate inputs to the underlying block cipher. Among which q many inputs are final inputs (output of which is the final output). Probability of collision between any final input and intermediate input is roughly $\frac{1}{2^n}$ on the average and there are $q\sigma$ such pairs. Given that final inputs are completely new among all intermediate inputs the distribution of final output is very close to the uniform distribution and hence it is difficult to distinguish from an uniform random function. This is why, we get an improved bound of the form $\frac{q\sigma}{2^n}$. If we consider the event that all intermediate inputs are distinct then we would likely to get the bound of the form $\frac{\sigma^2}{N}$. Thus, in case of improved bound, collision among all intermediate non-final inputs are allowed. Here, we provide a counting based, completely independent and concrete proof for the computation of collision probability. A similar and probabilistic approach can be found in [10].

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.

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

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 Func$(\mathcal{M}, T)$. Any random variable taking values on Func$(\mathcal{M}, T)$ is called as a **random function**. Let u denote the uniform random variable on 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 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) with ℓ as the number of blocks of longest query. Finally, it returns either 1 or 0. **Advantage** for a distinguisher $\mathcal{A}^{\mathcal{O}}$ is computed as follows :

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

$$\mathbf{Adv}_{f,u}(q,\sigma,\ell) \stackrel{\Delta}{=} \mathbf{Adv}_f(q,\sigma,\ell) \stackrel{\Delta}{=} \mathbf{max}_{\mathcal{A}}\, \mathbf{Adv}_f(\mathcal{A})$$

where the maximum is taken over all distinguishers $\mathcal{A}$ making at most q queries consisting of at most σ many blocks with ℓ as the maximum number of blocks of a query. Since we consider the distinguisher without any time restriction it is enough to consider a deterministic algorithm. A random function f is said to be (q,σ,ℓ,ϵ)-**PRF** if $\mathbf{Adv}_f(q,\sigma,\ell) \leq \epsilon$. If we have a bound of advantage independent of ℓ (or σ) then we simply drop ℓ (or σ respectively). 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 $\mathbf{M} = (M^1, \ldots, M^q)$ is q-**distinct** if M^i's are distinct where $M^i \in \mathcal{M}$. Suppose $f' \in \text{Func}(\mathcal{M}, \{0,1\}^n)$ and $\mathbf{M}$ is q-distinct. We write

$$f'^{(q)}(\mathbf{M}) \stackrel{\Delta}{=} (f'(M^1), \ldots, f'(M^q))$$

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. A similar version of the result can be found in [3, 14].

Theorem 3.1. (interpolation theorem)
Suppose for each q-distinct $\mathbf{M} = (M^1, \ldots, M^q)$ with $\sum_{i=1}^q ||M^i||_n \le \sigma$ and any $\mathbf{y} = (y^1, \ldots, y^q) \in (\{0,1\}^n)^q$ we have

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

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

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

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

In this paper we need the strong version of the theorem to prove our improved bound.

Theorem 3.2. (strong interpolation theorem)
Suppose, for all $\mathbf{y} \in (\{0,1\}^n)^q \setminus \mathtt{Bad}$ and for all q-distinct $\mathbf{M}$, we have $\Pr[f^{(q)}(\mathbf{M}) = \mathbf{y}] \ge \frac{1-\epsilon_1}{N^q}$ *where* $\mathtt{Bad} \subseteq (\{0,1\}^n)^q$. *Then,* $\mathbf{Adv}_f(q,\sigma) \le \epsilon_1 + \epsilon_2$ *provided* $\frac{|\mathtt{Bad}|}{N^q} \le \epsilon_2$.

3.2 Some more results and terminologies

We denote $\mathbf{P}(m,r) = m(m-1)\cdots(m-r+1)$ where $r \le m$ are nonnegative integers. The number of ways we can choose distinct $a_1, \ldots, a_r$ 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 an s-tuple $\mathbf{a} = (a_1, \ldots, a_s)$. 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 tuple** (or $\mathbf{a}$ is matching tuple with respect to $\mathbf{b}$) 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 $\mathbf{a}$ and $\mathbf{b}$, $|\mathbf{a}| = |\mathbf{b}|$. Now we have a following simple and useful lemma. We leave readers to verify the lemma by themselves.

Lemma 3.3. *Given a tuple* $\mathbf{a}$ *of size* r*, the total number of matching tuples w.r.t.* $\mathbf{a}$ *whose elements are from a set of size* m *is* $\mathbf{P}(m, r)$.

Suppose $\mathbf{a}$ and $\mathbf{b}$ are matching tuples with elements from S. Then the total number of permutations π on S such that $\pi(a_1) = b_1, \ldots, \pi(a_s) = b_s$ is $(|S| - |\mathbf{a}|)!$. The conditions $\pi(a_1) = b_1, \ldots, \pi(a_s) = b_s$ 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 3.4. *(1) Suppose* $a \leq b$*,* c *are positive integers then* $\frac{a}{b} \leq \frac{a+c}{b+c}$.

(2) For $0 < a_1, a_2, \ldots, a_s < 1$, $\prod_{i=1}^{s}(1 - a_i) \geq 1 - \sum_{i=1}^{s} a_i$.

4 Definition of PMAC

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

$$\left.\begin{array}{rcll} \mathbf{pad}(M) & = & M \parallel 10^s & \text{if } n \nmid |M| \\ & = & M & \text{otherwise} \end{array}\right\} \tag{4.1}$$

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

Algorithm PMAC : $Y = \mathrm{P}_\pi(M)$

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 [5]. 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 $w_i = \pi(v_i), 1 \leq i \leq \ell$.

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 $c_1, c_2, \ldots$, and it is given in [5].

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

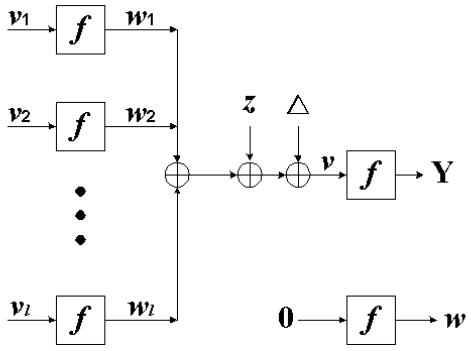

Figure 1. PMAC Algorithm : $\mathbf{pad}(M) = x_1 \parallel \cdots \parallel x_\ell \parallel z$, $v_i = x_i + c_i * w$ and $\Delta = c * w$ if $n \mid |M|$ otherwise $\Delta = 0$. $\mathrm{P}_f(M) = Y$. Here the underlying permutation is f.

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 $M^1, \ldots, M^q$.

(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 $\mathbf{M} = (M^1, \ldots, M^q)$ 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 $\mathbf{y} = (y^1, \ldots, y^q)$ if the set of all intermediate outputs are disjoint from the set $\{y_1, \ldots, y^q\}$.

5 Improved security analysis of PMAC

Now we give a lower bound of size of the set

$$I_{\mathbf{y}} = \{\pi : \mathrm{P}_\pi(M^1) = y^1, \ldots, \mathrm{P}_\pi(M^q) = y^q\}$$

where $\mathbf{M} = (M^1, \ldots, M^q)$ and $\mathbf{y} = (y^1, \ldots, y^q)$ are any q-distinct tuples. 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 $M^i = M^i_1 \parallel \cdots \parallel M^i_{\ell_i} \parallel z^i$, 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 $\Delta = \mathbf{0}$. Given a permutation π,

(1) $w[\pi] = \pi(\mathbf{0})$, $v^i_j[\pi] = c_i * w[\pi] + M^i_j$.

(2) $w^i_j[\pi] = \pi(v^i_j[\pi])$.

(3) $v^i[\pi] = z^i + \Delta^i + \sum_{1 \leq j \leq \ell_i} w^i_j[\pi]$.

Thus, while we compute $\mathbf{P}_\pi(M^1), \ldots, \mathbf{P}_\pi(M^q)$, the elements $\mathbf{0}$, $v^i_j[\pi]$ are the set of all intermediate inputs and $v^i[\pi]$ is final input for the message M^i. Similarly, $w[\pi]$, $w^i_j[\pi]$ are the set of all intermediate outputs. We fix the message tuple $\mathbf{M} = (M^1, \ldots, M^q)$. Note that, the set of all intermediate inputs and final inputs are completely determined by the set of all intermediate outputs (not even on the permutation!).

(1) $w[\pi]$ determines all intermediate inputs $v^i_j[\pi] = c_i * w[\pi] + M^i_j$, $1 \leq j \leq \ell_i$, $1 \leq i \leq q$.

(2) $\{w^i_j[\pi] : 1 \leq j \leq \ell_i, 1 \leq i \leq q\}$ determines all final inputs as $v^i[\pi] = z^i + \Delta^i + \sum_{1 \leq j \leq \ell_i} w^i_j[\pi]$.

Thus, we have the following definitions.

Definition 5.1.
(1) Given $w \in \mathbb{F}_{2^n}$, we define *corresponding intermediate input tuple* as

$$\mathbf{V}'_w = (0, v^1_1, \ldots, v^1_{\ell_1}, \ldots, v^q_1, \ldots, v^q_{\ell_q}) \text{ where } v^i_j = c_i * w + M^i_j.$$

(2) $\mathbf{W}[\pi] = (w[\pi], w^1_1[\pi], \ldots, w^1_{\ell_1}[\pi], \ldots, w^q_1[\pi], \ldots, w^q_{\ell_q}[\pi])$.

(3) $\mathbf{V_0}[\pi] = (0, v^1_1[\pi], \ldots, v^1_{\ell_1}[\pi], \ldots, v^q_1[\pi], \ldots, v^q_{\ell_q}[\pi]) = V'_{\pi(\mathbf{0})}$ (corresponding intermediate input tuple).
(4) $\mathbf{V}[\pi] = (0, v^1_1[\pi], \ldots, v^1_{\ell_1}[\pi], \ldots, v^q_1[\pi], \ldots, v^q_{\ell_q}[\pi], v^1[\pi], \ldots, v^q[\pi]) = V_{W[\pi]}$ (corresponding input tuple).

Let $\mathcal{T}_s$ denote the set of s-tuples whose elements are from $\mathbb{F}_{2^n}$. A tuple $\mathbf{W} = (w, w^1_1, \ldots, w^1_{\ell_1}, \ldots, w^q_1, \ldots, w^q_{\ell_q})$ 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 $\mathcal{T}^{\text{perm}}_{\sigma'+1} \subset \mathcal{T}_{\sigma'+1}$. Trivially, $\mathbf{V_0}[\pi]$ and $\mathbf{W}[\pi]$ are matching tuple as $\mathbf{W}[\pi]$ is the intermediate output tuple for the intermediate input tuple $\mathbf{V_0}[\pi]$ with respect to the permutation π.

Conversely, if $\mathbf{W}$ and $\mathbf{V'}_w$ are matching tuples then we have a permutation π with $\pi(\mathbf{0}) = w, \pi(v^i_j) = w^i_j$. For any permutation π satisfying above, we have $\mathbf{V_0}[\pi] = \mathbf{V'}_w$ and $\mathbf{W}[\pi] = \mathbf{W}$. We define a mapping

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

where $\text{Perm}(\mathbb{F}_{2^n})$ denotes the set of all permutations of $\mathbb{F}_{2^n}$. We denote $N = 2^n = |\mathbb{F}_{2^n}|$.

Lemma 5.2. *$\mathcal{W}(\text{Perm}(\mathbb{F}_{2^n})) = \mathcal{T}^{\text{perm}}_{\sigma'+1}$ and for any tuple $\mathbf{W} \in \mathcal{T}^{\text{perm}}_{\sigma'+1}$ of size s there are $(N-s)!$ permutations π such that $\mathcal{W}(\pi) = \mathbf{W}$.*

Proof. The proof follows from the above discussion. Since $|\mathbf{W}| = s$, we can choose the above permutations in $(N-s)!$ ways. □

We partition the set of all permutation compatible $(\sigma'+1)$-tuples $\mathcal{T}^{\text{perm}}_{\sigma'+1}$ (or we simply denote $\mathcal{T}$ since σ' is fixed) by $\sqcup_{i=1}^{\sigma'+1}\mathcal{T}^{\text{perm}}_{\sigma'+1}[i]$ where $\mathcal{T}^{\text{perm}}_{\sigma'+1}[i]$ or $\mathcal{T}[i]$ is the tuples of size i. Let $n_i = |\mathcal{T}[i]|$ then from the above Lemma 5.2 we have $N! = \sum_{i=1}^{\sigma'+1} n_i \times (N-i)!$.

Two tuples are said to be *disjoint* if they do not have any common elements. Thus, if X_1 and X_2 are two disjoint tuples then we have, $|(X_1, X_2)| = |X_1| + |X_2|$. A tuple $\mathbf{W} = (w, w^1_1, \ldots, w^1_{\ell_1}, \ldots, w^q_1, \ldots, w^q_{\ell_q})$ is said to be $\mathbf{y}$-*disjoint* if $\mathbf{W}$ and $\mathbf{y}$ are disjoint. We have already defined new permutation. We can describe these in terms of the new terminologies as in below.

(1) A permutation π is said to be new if $(v^1[\pi], \ldots, v^q[\pi])$ is q-distinct tuple and disjoint from $\mathbf{V_0}[\pi]$.

(2) For a q-distinct $\mathbf{y}$, a good permutation π satisfies two conditions :

   a) π is new : $(v^1[\pi], \ldots, v^q[\pi])$ is q-distinct and disjoint from $\mathbf{V_0}[\pi]$,

   b) $\mathbf{W}[\pi]$ and $\mathbf{y}$ are disjoint.

Proposition 5.3. *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 $S = \{0,1\}^n \setminus \{y^1, \ldots, y^q\}$. Write $S = \sqcup_{i \geq 1} S_i$ (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 $\mathbf{W} = (a, w^1_i, \ldots, w^q_{\ell_q})$ 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,

$$\sum_{i=1}^{\sigma'+1} |S_i| \times (N-i)! \times \mathbf{P}(N-q, i-1) \geq N!(1-\frac{q}{N})(1-\frac{\sigma'(q-1)}{N})$$
$$\geq N!(1-\frac{q\sigma - q^2 - \sigma + 2q}{N}).$$

□

Proposition 5.4. *The number of new permutations for* 2*-distinct* (M^1, M^2) *is at least* $N!(1-\frac{4\ell_1+4\ell_2+3}{N})$. *In general, the number of new permutations for* q*-distinct* $\mathbf{M} = (M^1, \ldots, M^q)$ *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 5.3 and Proposition 5.4, 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 5.5. *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 $\mathcal{W} : I_{\mathrm{G}} :\rightarrow \mathcal{T}_{\sigma'+1}$. 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 $\{y^1, \ldots, y^q\}$) 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 $|I_{\mathrm{G}} \cap I_{\mathbf{y}}| = \sum_i m_i(N-i-q)! \geq \frac{1}{\mathbf{P}(N,q)} \sum_i m_i(N-i)! \geq \frac{|I_{\mathrm{G}}|}{\mathbf{P}(N,q)}$. □

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

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 5.6. (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 for prefix-free messages and ℓ is the maximum block length among all q queries. The original bound of CBC [1] 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 [1] 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 [5], the bound is $\frac{(\sigma+1)^2}{2^{n-1}}$. Very recently, Minematsu and Matsushima [11] in FSE-2007, have provided a bound $\frac{5\ell q^2}{2^n - 2\ell}$. If 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 at least $\frac{5\ell^3}{2^n}$ which is in higher order of q. So, we should be careful when we are looking for improved (in real sense) bounds.

In this paper, we have provided a bound $\frac{5\sigma q - 3.5q^2}{2^n}$. The bound of the form $\sigma q/N$ is better than $\ell q^2/N$ if the values of ℓ_i are more dispersed. If ℓ_i's are close to ℓ then both forms are similar. It is easy to see that for $1 \leq q \leq \sigma = \sum_{i=1}^{q} \ell_i$, and $\ell = \mathbf{max}_i \ell_i$,

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

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

The second inequality is trivial as $\sigma \leq \ell q$. For the first inequality it is sufficient to show that $4\sigma^2 + 7q^2 > 10q\sigma$. This is trivially true since arithmetic mean of two positive integers is always more than that of geometric mean. Thus, our bound is better than all previously known bounds for PMAC.

From the above discussion we see that there are four forms of bounds are known, namely, $\mathrm{O}(\ell^2 q^2)$, $\mathrm{O}(\sigma^2)$, $\mathrm{O}(\ell q^2)$ and $\mathrm{O}(\sigma q)$. Obviously $\mathrm{O}(\ell q^2)$ is sharper than $\mathrm{O}(\ell^2 q^2)$. Above we have already made comparison between $\mathrm{O}(\ell q^2)$ and $\mathrm{O}(\sigma^2)$. Now we give a comparison study between $\mathrm{O}(\ell q^2)$ and $\mathrm{O}(\sigma q)$. We know that $\sigma \leq \ell q$ and hence $\sigma q = \mathrm{O}(\ell q^2)$. Note that $\sigma = \sum_{i=1}^{q} \ell_i$ and $\ell = \max_i \ell_i$ where ℓ_i denotes the number of message blocks of i^{th} query. If ℓ_i are scattered (in other words, $\sigma \ll \ell q$) then σq is much sharper than ℓq^2. On the other hand if ℓ_i's are close to each other then $\sigma \approx \ell q$ and hence both bounds are similar.

Proof of the Proposition 5.4

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

Case-1 : $\ell_1 = \ell_2 = \ell$ (say), $x_1^1 = x_1^2, \ldots, x_\ell^1 = x_\ell^2, z^1 = z^2$

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 $S = \{w \in \mathbb{F}_{2^n} : (v_1^1, v_1^2)$ is disjoint from $(0, v_2^1, \ldots, v_\ell^1, v_2^2, \ldots, v_\ell^2)$ and $\Delta^1 + z^1 \neq \Delta^2 + z^2\}$. Clearly, $|S| \geq N - \ell - 1$ since

$$S = \{0,1\}^n \setminus (\{\frac{x_j^2 - x_1^2}{c_1 - c_j} : 2 \leq j \leq \ell\} \cup \{\frac{-x_1^2}{c_1}\} \cup \{\frac{z^2 - z^1}{c}\}).$$

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 $\mathbf{W}_1 = (a, w_2^1, \ldots, w_{\ell_1}^1, w_2^2, \ldots, w_{\ell_2}^2)$ such that W_1 is matching with $\mathbf{V}_1 = (0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2}^2)$.

(1) For each such tuple we have at least $(N - 2\ell - 2 - i)$ choices of $w_1^1 = w_1^2$ such that $\mathbf{W} = (a, w_1^1, \ldots, w_{\ell_1}^1, w_1^2, \ldots, w_{\ell_2}^2)$ is matching with $\mathbf{V}_a$ and (v^1, v^2) is disjoint from $\mathbf{V}_a$. This is true since we can choose

$$w_1^1 \in \{0,1\}^n \setminus (\{w_j^1 : 2 \leq j \leq \ell\} \cup \{a\} \cup \{w : v^1 = 0, v_j^1\} \cup \{w : v^2 = 0, v_j^1, v^1\}).$$

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 : $\ell_1 = \ell_2 = \ell$ (say) and $x_1^1 = x_1^2, \ldots, x_\ell^1 = x_\ell^2, z^1 \neq z^2$

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 $x_1^1 \cdots x_{\ell_1}^1 \neq x_1^2 \cdots x_{\ell_2}^2$. Thus, we have either $x_1^1 = x_1^2, \ldots, x_{\ell_1}^1 = x_{\ell_2}^2$ or $x_1^1 \neq x_1^2$ (without loss of generality).

Case-3 : $\ell_2 > \ell_1$: $x_1^1 = x_1^2, \ldots, x_{\ell_1}^1 = x_{\ell_1}^2$

We want to choose $\mathbf{W} = (w, w_1^1, \ldots, w_{\ell_1}^1, w_1^2, \ldots, w_{\ell_2}^2)$-tuple, such that $(v_1^1 Z$, $v_{\ell_2}^2$, v^1, $v^2)$ is 4-distinct tuple and disjoint from $(0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2-1}^2)$. Note that, here we choose $\mathbf{W}$ such that $w_1^1 = w_1^2, \ldots, w_{\ell_1}^1 = w_{\ell_1}^2$.

(1) Let S denote the set of all w such that $(v_1^1, v_{\ell_2}^2)$ is 2-distinct and disjoint from $(0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2-1}^2)$.

Hence, $w \neq \frac{x_1^1 - x_j^2}{c_j - c_1}, \frac{x_{\ell_2}^2 - x_j^2}{c_j - c_{\ell_2}}, -\frac{x_1^1}{c_1}, -\frac{x_{\ell_2}^2}{c_{\ell_2}}$ 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 $\mathbf{W}_1 = (a, w_2^1, \ldots, w_{\ell_1}^1, w_2^2, \ldots, w_{\ell_2-1}^2)$ such that W_1 is matching with $\mathbf{V}_1 = (0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2-1}^2)$.

(2) We choose $w_1^1 \notin (a, w_2^1, \ldots, w_{\ell_1}^1, w_2^2, \ldots, w_{\ell_2-1}^2)$ 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

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

Case-4 : $x_1^1 \neq x_1^2$

We want to choose $(w, w_1^1, \ldots, w_{\ell_1}^1, w_1^2, \ldots, w_{\ell_2}^2)$-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 $(0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2}^2)$.

(1) Let S denote the set of all w such that (v_1^1, v_1^2) is 2-distinct and disjoint from $(0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2}^2)$.

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 $\mathbf{W}_1 = (a, w_2^1, \ldots, w_{\ell_1}^1, w_2^2, \ldots, w_{\ell_2}^2)$ such that W_1 is matching with $\mathbf{V}_1 = (0, v_2^1, \ldots, v_{\ell_1}^1, v_2^2, \ldots, v_{\ell_2}^2)$.

(2) We choose $w_1^1 \notin (a, w_2^1, \ldots, w_{\ell_1}^1, w_2^2, \ldots, w_{\ell_2}^2)$ 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

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

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 $(0, v_2^2, \ldots, v_{\ell_2}^2)$. 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 $v^2 \notin (0, v_1^2, \ldots, v_{\ell_2}^2, v^1)$ and $w_1^2 \notin (w, w_2^2, \ldots, w_{\ell_2}^2)$. 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 [7, 12] and other constructions such as XCBC, TMAC and possibly OMAC.

Acknowledgments. We would like to thank the anonymous reviewers for their valuable comments on earlier drafts of this paper.

References

[1] 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 839, pp. 341–358. Springer, Berlin, 1994.

[2] M. Bellare, K. Pietrzak, and P. Rogaway, *Improved Security Analysis for CBC MACs*. Advances in Cryptology – Crypto 2005, Lecture Notes in Computer Science 3621, pp. 527–545. Springer, Berlin, 2005.

[3] D. J. Bernstein, *A short proof of the unpredictability of cipher block chaining*, available at http://cr.yp.to/papers.html#easycbc, 2005.

[4] J. Black and P. Rogaway, *CBC MACs for arbitrary length messages*. Advances in Cryptology – Crypto 2000, Lecture Notes in Computer Science 1880, pp. 197–215. Springer, Berlin, 2000.

[5] 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 2332, pp. 384–397. Springer, Berlin, 2002.

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

[7] C. S. Jutla, *PRF Domain Extension using DAG*. Theory of Cryptography: Third Theory of Cryptography Conference – TCC 2006, Lecture Notes in Computer Science 3876, pp. 561–580. Springer, Berlin, 2006.

[8] H. Krawczyk, *LFSR-based hashing and authenticating*. Advances in Cryptology – Crypto 1994, Lecture Notes in Computer Science 839, pp. 129–139. Springer-Verlag, New York, 1994.

[9] 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 2612, pp. 33–49. Springer, Berlin, 2003.

[10] U. Maurer, *Indistinguishability of Random Systems*. Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Computer Science 2332, pp. 110–132. Springer, Berlin, 2002.

[11] K. Minematsu and T. Matsushima, *New Bounds for PMAC, TMAC, and XCBC*. Fast Software Encryption – FSE 2007, Lecture Notes in Computer Science 4593, pp. 434–451. Springer, Berlin, 2007.

[12] M. Nandi, *A Simple and Unified Method of Proving Indistinguishability*. Progress in Cryptology – Indocrypt 2006, Lecture Notes in Computer Science 4329, pp. 317–334. Springer, Berlin, 2006.

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

[14] S. Vaudenay, *Decorrelation: A Theory for Block Cipher Security*. Journal of Cryptology 16(4), Lecture Notes in Computer Science, pp. 249–286. Springer-Verlag, New York, 2003.

Received 16 May, 2007; revised 26 January, 2008

Author information

Mridul Nandi, CINVESTAV-IPN, Mexico City, Mexico.
Email: mridul.nandi@gmail.com

Avradip Mandal, Waterloo, Canada.
Email: avradip@gmail.com