Cryptanalysis of the MEM Mode of Operation

Peng Wang[1] and Dengguo Feng[1,2] and Wenling Wu[2]

[1] State Key Laboratory of Information Security
Graduate School of Chinese Academy of Sciences, Beijing 100049, China
wp@is.ac.cn
[2] State Key Laboratory of Information Security
Institution of Software of Chinese Academy of Sciences, Beijing 100080, China
{feng,wwl}@is.iscas.ac.cn

Abstract. The MEM mode is a nonce-based enciphering mode of operation proposed by Chakraborty and Sarkar, which was claimed to be secure against symmetric nonce respecting adversaries. We show that this is not correct by using two very simple attcks. One attack need one decryption and one decryption queries, and the other only need one encryption query.

Keywords. Blockcipher, tweakable blockcipher, modes of operation, nonce-based encryption.

1 Introduction

A *mode of operation*, or mode, for short, is a scheme that specifies how to use a *blockcipher* to provide some cryptographic services, such as privacy or authenticity. Recently, Chakraborty and Sarkar proposed the MEM (Mask Encrypt Mask) mode, a *nonce-based* enciphering, or length preserving encryption, mode of operation which was claimed to be secure against *symmetric nonce respecting* adversaries.

Suppose the underlying blockcipher is

$$E : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$$

where $\mathcal{K}$ is a key space, then the MEM mode is

$$\mathrm{MEM}[E] : \mathcal{K} \times \mathcal{N} \times (\{0,1\}^n)^+ \rightarrow (\{0,1\}^n)^+$$

where $\mathcal{N} = \{0,1\}^n$ is a nonce space and the key space $\mathcal{K}$ is same as that of the underlying blockcipher E. Let $\mathbf{E}_K(\cdot,\cdot)$ and $\mathbf{D}_K(\cdot,\cdot)$ be the encryption and the decryption algorithms of MEM respectively, and let D_K be the inverse of E_K.

Symmetric Nonce Respecting Adversaries. The nonce-based encryption is a syntax for an encryption scheme where the encryption process is a deterministic algorithm which surfaces an initial vector. This syntax was advocated by Rogaway, Bellare, *et al.* [RBBK01,Rog04b], and first used in the OCB mode [RBBK01,Rog04a], then adopted by the GCM mode [MV02], the CWC mode [KVW04], the EAX mode [BRW04], etc.

The security model of MEM assumes that the adversary be symmetric nonce respecting, i.e., the adversary can not repeat nonce in either encryption or decryption query. Note that an adversary is allowed to choose the same nonce for both the encryption and the decryption queries. Without loss generality, we also assume that the adversary does not make *pointless* query, such as as a decryption query of (N, C) after get it as an answer to an encryption query, etc. To sum up, the disallowed queries for the symmetric nonce respecting adversaries are listed bellow:

When query	and get	then these queries are disallowed:
$\mathbf{E}_K(N, P)$	C	$\mathbf{E}_K(N, \cdot)$, $\mathbf{D}_K(N, C)$
$\mathbf{D}_K(N, C)$	P	$\mathbf{D}_K(N, \cdot)$, $\mathbf{E}_K(N, P)$

Symmetric nonce respecting model is a reasonable in certain scenarios [CS06]. Get rid of the nonce respecting restriction, the security mode is exactly that of strong secure *tweakable blockcipher* [LRW02]. Dedicated strong secure tweakable blockcipher constructions, such as CMC [HR03], EME [HR04], HCTR [WFW05], etc. are of course secure against symmetric nonce respecting adversaries.

Security Claimed by [CS06]. Chakraborty, *et al.* claimed that the symmetric nonce respecting adversary cannot distinguish the output of $\mathbf{E}_K(\cdot, \cdot)$ and $\mathbf{D}_K(\cdot, \cdot)$ from that of a *random tweakable permutation* and its inverse; Or equivalently saying [CS06,HR03,HR04], this kind of adversary cannot distinguish the output of $\mathbf{E}_K(\cdot, \cdot)$ and $\mathbf{D}_K(\cdot, \cdot)$ from that of $\$(\cdot, \cdot)$ and $\$(\cdot, \cdot)$, where $\$(N, P)$ returns a random string of length $|P|$. Let $\approx$ denote the indistinguishability. They "proved" that:

$$\mathbf{E}_K(\cdot, \cdot), \mathbf{D}_K(\cdot, \cdot) \;\approx\; \$(\cdot, \cdot), \$(\cdot, \cdot).$$

The security proof is always a subtle thing, especial a long one. For example, the EMD mode [Rog02] proposed by Rogaway also had a proof, but was soon broken by Joux [Jou03].

Our Contributions. We show that EME is not secure against symmetric nonce respecting adversaries at all. The first attack makes one decryption and one encryption queries. The second attack makes only one encryption query.

2 Specifications of MEM

An n-bit string is viewed as an element in the finite field $GF(2)[x]/\tau(x)$, where $\tau(x)$ is a fixed irreducible polynomial of degree n.

MEM makes use of the polynomials $p_i(x)$ which are defined as following. For $0 < i < m$ and $(n + 1) \nmid i$, define $p_i(x) = x^{j-1} + x^j$, where $j = (i - 1)$

mod $(n+1)+1$; for $0 < i < m$ and $(n+1) \mid i$, define $p_i(x) = x^n + 1$; for $i = m$, define $p_i = x^{j-1} + 1$, where $j = (i-1) \mod (n+1) + 1$.

The encryption and decryption algorithms of EME are listed in the figure 1, which consists of three cases: $m = 1$, $m = 2$ and $m > 2$. In our attacks we only make use of the case $m > 2$. Figure 2 shows the enciphering of a four-block message.

Algorithm $\mathbf{E}_K^N(P_1, P_2, \cdots, P_m)$	**Algorithm** $\mathbf{D}_K^N(C_1, C_2, \cdots, C_m)$
$EN \leftarrow E_K(N)$; $EEN \leftarrow E_K(xEN)$;	$EN \leftarrow E_K(N)$; $EEN \leftarrow E_K(xEN)$;
$MP \leftarrow P_1 \oplus P_2 \cdots \oplus P_m$;	$MC \leftarrow C_1 \oplus C_2 \cdots \oplus C_m$;
if $m = 1$ **then**	**if** $m = 1$ **then**
$M_1 \leftarrow E_K(MP \oplus EN)$;	$M_2 \leftarrow D_K(MC \oplus xEEN)$;
$C_1 \leftarrow M_1 \oplus xEEN$;	$P_1 \leftarrow M_2 \oplus EEN$;
return C_1	**return** P_1
if $m = 2$ **then**	**if** $m = 2$ **then**
$M_1 \leftarrow E_K(MP \oplus EN)$;	$M_2 \leftarrow E_K(MC \oplus EN \oplus EEN)$;
$PP_1 \leftarrow M_1 \oplus P_1$; $PP_2 \leftarrow M_1 \oplus EEN \oplus P_2$;	$CC_1 \leftarrow M_2 \oplus C_1$; $CC_2 \leftarrow M_2 \oplus EN \oplus C_2$;
$CC_1 \leftarrow E_K(PP_1)$; $CC_2 \leftarrow E_K(PP_2)$;	$PP_1 \leftarrow D_K(CC_1)$; $PP_2 \leftarrow D_K(CC_2)$;
$M_2 \leftarrow E_K(CC_1 \oplus CC_2 \oplus EEN)$;	$M_1 \leftarrow E_K(PP_1 \oplus PP_2 \oplus EEN \oplus EN)$;
$C_1 \leftarrow M_2 \oplus CC_1$; $C_2 \leftarrow EN \oplus CC_2$;	$P_1 \leftarrow M_1 \oplus PP_1$; $P_2 \leftarrow M_1 \oplus EEN \oplus PP_2$;
return C_1, C_2	**return** P_1, P_2
if $m > 2$ **then**	**if** $m > 2$ **then**
$M_1 \leftarrow E_K(MP \oplus EN)$; $MC \leftarrow 0^n$;	$M_2 \leftarrow E_K(MC \oplus EEN)$; $MP \leftarrow 0^n$;
for $i = 1$ **to** m	**for** $i = 1$ **to** m
if $(i-1 > 0 \wedge i-1 \mod (n+1) = 0)$	**if** $(i-1 > 0 \wedge i-1 \mod (n+1) = 0)$
$M_1 \leftarrow E_K(M_1)$;	$M_2 \leftarrow E_K(M_2)$;
$PP_i \leftarrow P_i \oplus p_i(x) M_1$;	$CC_i \leftarrow C_i \oplus p_i(x) M_2$;
$CC_i \leftarrow E_K(PP_i)$; $MC \leftarrow MC \oplus CC_i$;	$PP_i \leftarrow D_K(CC_i)$; $MP \leftarrow MP \oplus PP_i$;
for $i = 1$ **to** m	**for** $i = 1$ **to** m
if $(i-1 > 0 \wedge i-1 \mod (n+1) = 0)$	**if** $(i-1 > 0 \wedge i-1 \mod (n+1) = 0)$
$M_2 \leftarrow E_K(M_2)$;	$M_1 \leftarrow E_K(M_1)$;
$C_i \leftarrow CC_i \oplus p_i(x) M_2$;	$P_i \leftarrow PP_i \oplus p_i(x) M_1$;
return $C_1, C_2, \cdots, C_m$	**return** $P_1, P_2, \cdots, P_m$

Fig. 1. The MEM Mode

3 Distinguishers against MEM

We can distinguish $\mathbf{E}_K(\cdot,\cdot), \mathbf{D}_K(\cdot,\cdot)$ from $\$(\cdot,\cdot), \$(\cdot,\cdot)$ with overwhelming advantage of $1 - 1/2^n$. The first distinguisher makes one decryption and one encryption queries. The second distinguisher makes only one encryption.

3.1 Two-query Distinguisher

This distinguisher is similar to the one used in [CS06] to show that MEM is not secure against nonce repeating adversary. The difference is that the one in in [CS06] made two encryption queries with the same nonce and we make one decryption and one encryption queries with the same nonce.

The distinguisher is as following:

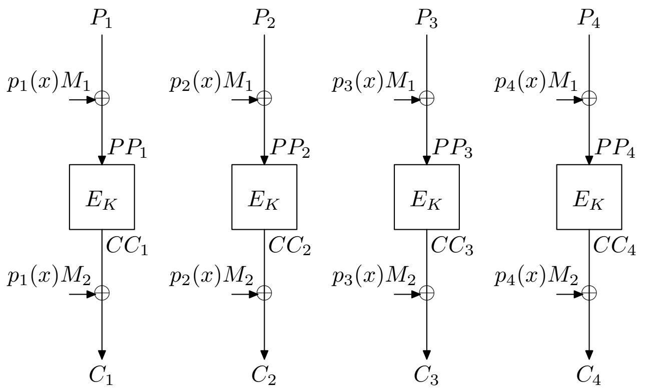

Fig. 2. Enciphering a four-block message $P_1P_2P_3P_4$ under MEM. Set $M_1 = E_K(P_1 \oplus P_2 \oplus P_3 \oplus P_4 \oplus E_K(N))$ and $M_2 = E_K(CC_1 \oplus CC_2 \oplus CC_3 \oplus CC_4 \oplus E_K(xE_K(N)))$.

1. Make a decryption query $(N^s, C_1^s, C_2^s, C_3^s, C_4^s)$ and get $(P_1^s, P_2^s, P_3^s, P_4^s)$;
2. Make an encryption query $(N^t, P_1^t, P_2^t, P_3^t, P_4^t)$ and get $(C_1^t, C_2^t, C_3^t, C_4^t)$, where $N^s = N^t$, $P_1^s = P_1^t$, $P_2^s = P_2^t$, $P_3^s \neq P_3^t$, and $P_3^s \oplus P_4^s = P_3^t \oplus P_4^t$.
3. Calculate $X_1 = p_1(x)^{-1}(C_1^s \oplus C_1^t)$ and $X_2 = p_2(x)^{-1}(C_2^s \oplus C_2^t)$.
4. If $X_1 = X_2$, then return 1, else return 0.

When the distinguisher queries $\mathbf{E}_K(\cdot,\cdot), \mathbf{D}_K(\cdot,\cdot)$,

$$M_2^s = p_1(x)^{-1}(CC_1^s \oplus C_1^s) = p_2(x)^{-1}(CC_2^s \oplus C_2^s)$$

and

$$M_2^t = p_1(x)^{-1}(CC_1^t \oplus C_1^t) = p_2(x)^{-1}(CC_2^t \oplus C_2^t).$$

Notice that $CC_1^s = CC_1^t$ and $CC_2^s = CC_2^t$, we get that

$$M_2^s \oplus M_2^t = p_1(x)^{-1}(C_1^s \oplus C_1^t) = p_2(x)^{-1}(C_2^s \oplus C_2^t).$$

So the probability of $X_1 = X_2$ is 1.

When the distinguisher queries $\$(\cdot,\cdot), \$(\cdot,\cdot)$, then C_1^t and C_2^t are two independently random strings. So the probability of $X_1 = X_2$ is $1/2^n$.

From the above analysis, the advantage of the distinguisher is $1 - 1/2^n$.

3.2 One-query Distinguisher

This distinguisher only makes one encryption query. Notice that when the message length is $m = n + 3$ blocks, $p^{n+2}(x) = p^{n+3}(x) = 1 + x$. We make an encryption query of $(N, P_1, P_2, \cdots, P_{m+3})$, where $P_1 = P_2 = ... = P_{n+3} = 0^n$, and get $(C_1, C_2, \cdots, C_{n+3})$. If $C_{n+2} = C_{n+3}$ then return 1, else return 0.

When the distinguisher queries $\mathbf{E}(\cdot,\cdot)$, we always have $C_{n+2} = C_{n+3}$. When the distinguisher queries $\$(\cdot,\cdot)$, the probability of $C_{n+2} = C_{n+3}$ is $1/2^n$.

From the above analysis, the advantage of the distinguisher is also $1 - 1/2^n$.

Acknowledgment

The authors would like to thank Debrup Chakraborty for providing their paper. It's a great pleasure to discuss your work with you.

References

[BRW04] Mihir Bellare, Phillip Rogaway, and David Wagner. The EAX mode of operation. In Bimal Roy and Willi Meier, editors, *Fast Software Encryption 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 389–407. Springer-Verlag, 2004.

[CS06] Debrup Chakraborty and Palash Sarkar. A new mode of encryption secure against symmetric nonce respecting adversaries, extended version of the FSE'06 paper. Cryptology ePrint Archive, Report 2006/062, 2006. `http://eprint.iacr.org/`.

[HR03] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In D. Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 482–499. Springer-Verlag, 2003.

[HR04] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In Tatsuaki Okamoto, editor, *The Cryptographers' Track at RSA Conference – CT-RSA 2004*, volume 2964 of *Lecture Notes in Computer Science*. Springer-Verlag, 2004.

[Jou03] Antoine Joux. Cryptanalysis of the EMD mode of operation. In L. R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 1–16. Springer-Verlag, 2003.

[KVW04] Tadayoshi Kohno, John Viega, and Doug Whiting. CWC: A high-performance conventional authenticated encryption mode. In Willi Meier Bimal Roy, editor, *Fast Software Encryption 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 408–426. Springer-Verlag, 2004.

[LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. In M. Yung, editor, *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer-Verlag, 2002.

[MV02] David A. McGrew and John Viega. The security and performance of the galois/counter mode (GCM) of operation. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Advances in Cryptology – INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355. Springer-Verlag, 2002.

[RBBK01] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryptiona. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 196–205, 2001.

[Rog02] Phillip Rogaway. The EMD mode of operation (tweaked, wide-blocksize, strong PRP), 2002. `http://eprint.iacr.org/2002/148.pdf`.

[Rog04a] Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology – ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer-Verlag, 2004.

[Rog04b] Phillip Rogaway. Nonce-based symmetric encryption. In Bimal Roy and Willi Meier, editors, *Fast Software Encryption 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 348–359. Springer-Verlag, 2004.

[WFW05] Peng Wang, Dengguo Feng, and Wenling Wu. HCTR: A variable-input-length enciphering mode. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *SKLOIS Conference on Information Security and Cryptology, CISC 2005*, volume 3822 of *Lecture Notes in Computer Science*, pages 175–188. Springer-Verlag, 2005.