# Symmetric Nonce Respecting Security Model and the MEM Mode of Operation

Peng Wang[1], 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 encryption mode of operation proposed by Chakraborty and Sarkar, which was claimed to be secure against symmetric nonce respecting adversaries. We first compare this security model with two similar models and then show that MEM is not secure under symmetric respecting attacks. One attack needs one decryption and one encryption queries, and the other only needs one encryption query.

**Keywords:** Blockcipher, tweakable blockcipher, modes of operation, nonce-based encryption, security model.

## 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, authenticity or both. Recently, Chakraborty and Sarkar [2] proposed a new security model in which the adversary is *symmetric nonce respecting* and the MEM (Mask Encrypt Mask) mode, a *nonce-based* encryption mode of operation, which was claimed to be secure in this model.

Suppose the underlying blockcipher is

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

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

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

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 decryption algorithms in an encryption scheme respectively, which is just MEM in section 3. Let $D_K$ be the inverse of $E_K$.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 280–286, 2006.

### 1.1 Symmetric Nonce Respecting Adversaries

The *nonce-based* symmetric encryption [10] is a syntax for an encryption scheme where the encryption process is a deterministic algorithm, which surfaces an initial vector. The initial vector which is supplied by the user and not by the encryption algorithm is usually a *nonce* — a value, like a counter, used at most once within a session. This syntax was advocated by Rogaway, Bellare, *et al.* [12,11], and first used in the OCB mode [12,10]. In a nonce-based encryption scheme, the encryption algorithm is $\mathbf{E} : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{M}$, where $\mathcal{K}$ is a key space, $\mathcal{N}$ is a nonce space and $\mathcal{M}$ is a message space. We often write $\mathbf{E}(K, N, M)$ as $\mathbf{E}_K(N, M)$ or $\mathbf{E}_K^N(M)$.

**IND$-SNR.** 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 of generality, we also assume that the adversary does not make *pointless* query, such as as a decryption query of $(N, C)$ after getting it as an answer to an encryption query, etc. IND$-SNR is a reasonable model in certain scenarios [2].

If any symmetric nonce respecting adversary cannot distinguish $\mathbf{E}_K(\cdot,\cdot)$ and $\mathbf{D}_K(\cdot,\cdot)$ from that of a *random tweakable permutation* and its inverse, we say that $\mathbf{E}$ is secure against symmetric nonce respecting attacks. Note that all the adversaries in this paper can only use reasonable resources, such as polynomial time and queries. Indistinguishability means that the advantage of the adversary is negligible. Or equivalently [2], this kind of adversary cannot distinguish $\mathbf{E}_K(\cdot,\cdot)$ and $\mathbf{D}_K(\cdot,\cdot)$ from $\$(\cdot,\cdot)$ and $\$(\cdot,\cdot)$, where $\$(N, P)$ returns a random string of length $|P|$. If $\approx$ denotes indistinguishability, we can write it as

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

We denote this security model as IND$-SNR.

**IND$-SSTB.** Without the symmetric nonce respecting restriction, the IND$-SNR security model is exactly that of strong secure *tweakable blockcipher* [7]. More specifically [3,4], $\mathbf{E}$ is an strong security tweakable blockcipher, if for any adversary making no pointless queries

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

Dedicated strong secure tweakable blockcipher constructions, such as CMC [3], EME [4], HCTR [13] etc. are of course secure against symmetric nonce respecting adversaries. We denote this security model as IND$-SSTB.

**IND$-CCA.** The other similar security model is IND$-CCA [11], i.e. the chosen ciphertext security model for nonce based encryption scheme. In this model, the adversary is nonce respecting when makes an encryption query and

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