Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation

Jaechul Sung[1], Sangjin Lee[1], Jongin Lim[1], Wonil Lee[1], and Okyeon Yi[2]

[1] Center for Information Security Technologies(CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, KOREA
{sjames, sangjin, jilim, nice}@cist.korea.ac.kr
[2] Information Security Technology Division, ETRI, Taejon, KOREA
oyyi@etri.re.kr

Abstract. In [1], they gave the notions of security for the symmetric encryption and provided a concrete security analysis of the XOR, CTR, and CBC schemes. Among the three schemes, the CTR scheme achieves the best concrete security in their analysis. In this paper, we propose the new schemes, CTR-OFB and CTR-CFB, which have the security as same as that of the CTR scheme on the point of the concrete security analysis and achieve higher resistance against some practical attacks than the CTR scheme.

Keywords : Modes of Operation, Concrete Security, Pseudorandom Function Family, Symmetric Encryption Schemes.

1 Introduction

The DES has four modes of operation in [11]. The four modes are the ECB, CBC, CFB, and OFB. Since DES modes of operation were introduced, many other modes of operation for block ciphers have been suggested and analyzed. Moreover modes of operations for block ciphers received much attention lately, partly due to an announcement by NIST that they are considering an update to their list of standardized. In [12] several modes of operation were suggested, such as the ABC, CTR, IACBC, ICPM, OCB, XCBC, and etc.

S.Goldwasser and S.Micali was the first to introduce the formal notions of security for encryption [7]. They presented two notions of security for asymmetric encryption, semantic security and polynomial security, and proved them equivalent with respect to polynomial-time reductions. M.Bellare et al.[1] presented the four notions of security for symmetric encryption in the framework of concrete security under the attack assumptions of chosen-plaintext attack(CPA) and chosen-ciphertext attack(CCA) :

1. Left-or-Right indistinguishability (LOR)
2. Real-or-Random indistinguishability (ROR)

3. Find-then-Guess security (FTG)
4. Semantic security (SEM)

They proved the first two notions are security preserving under the any attack assumption and the last two notions are also security preserving. Furthermore the first two notions are the stronger notions of security than the last two notions. Therefore showing an encryption scheme LOR or ROR secure implies tight reductions to all other notions but showing an encryption scheme FTG secure or SEM secure does not. So, if the bounds are equal, it is better to demonstrate security with respect to one of the first two notions, since that immediately translates into equally good bounds for the other notions. With the notions of security, especially left-or-right indistinguishability(LOR), they proved the concrete security analysis of the XOR, CTR, and CBC Schemes.

The counter(CTR) mode was originally introduced by W.Diffie and M.Hellman in 1979 [6]. Recently H.Lipmaa, P.Rogaway, and D. Wagner suggested the CTR mode in standardizing AES modes of operation [12]. The CTR mode has significant efficiency advantages, which can be preprocessed because of the independence of message blocks and easy to random-access. Furthermore the CTR mode gives the better concrete security than the XOR and CBC schemes [1].

In this paper we define new modes of operation for block ciphers. The new modes of operation are counter-based-OFB(CTR-OFB) mode and counter-based-CFB mode(CTR-CFB), which provide the concrete security as same as that of CTR mode. Although the CTR scheme changes the input bits of the underlying function serially, our scheme can randomize some input bits. So this can have more resistant against the SQUARE-type attacks [5, 8] and the conventional differential attack with low hamming weight differential than the CTR scheme. Also our new schemes provide the better concrete security than the OFB and CFB schemes, which achieve the same concrete security as the CBC scheme does.

This paper is organized as follows. In Section 2 we give some preliminary definitions, the notions of security, and some results of [1]. In Section 3 and 4 we propose the new modes of operations and prove the concrete security. In Section 5 we summarize our conclusions.

2 Preliminaries

In this section we describe some relevant definitions. Our treatment follows that of M.Bellare, K.Kilian, P.Rogaway [2], and M.Bellare, A.Desai, E.JokiPii, and P.Rogaway [1].

In [1], they considered the four definitions of security for symmetric encryption under the two attack assumptions of chosen-plaintext attack(CPA) and chosen-ciphertext attack(CCA). Here we will only consider the notion of the left-or-right indistinguishablity(LOR) under the CPA model, which gives the other three notions with comparable bounds.

We define that $a \leftarrow A(x_1, x_2, \ldots)$ denote the experiment of running A on inputs $x_1, x_2, \ldots$ if $A(\cdot, \cdot, \ldots)$ is any probabilistic algorithm. Let $\Pi = (\mathsf{K}, \mathsf{E}, \mathsf{D})$ be

an encryption scheme, where algorithm K is the key generator, E is the encryption algorithm, and D is the decryption algorithm.

The approach to concrete security is via parameterization of the resources of the adversary A. Let t be A's running time, q_e be the number of encryption oracle queries, and μ_e be the amount of the ciphertext A sees in response to its oracle queries.

In the LOR sense adversary is allowed queries of the form (x_0, x_1) where x_0, x_1 are equal length messages. Consider the two different games. In the first, each query is responded to by encrypting the left message. In the second, it is right message. In formal definition, the left-or-right oracle is defined by $\mathsf{E}_k(LR(\cdot,\cdot,b))$, where $b \in \{0,1\}$, to take input (x_0, x_1) and do the following:

If $b = 0$, it computes $C \leftarrow \mathsf{E}_K(x_0)$ and return C.
If $b = 1$, it computes $C \leftarrow \mathsf{E}_K(x_1)$ and return C.

Now we can define the LOR-CPA as the following.

Definition 1. *[1] Let* $\mathsf{SE} = (\mathsf{K}, \mathsf{E}, \mathsf{D})$ *be a symmetric encryption scheme. Let* $b \in \{0,1\}$ *and* $k \in N$. *Let* A_{cpa} *be an adversary has access to the oracle* $\mathsf{E}_K(LR(\cdot,\cdot,b))$. *Consider the following experiment :*

Experiment $\mathbf{Exp}^{lor-cpa-b}_{\mathsf{SE},A_{cpa}}(k)$
$K \leftarrow \mathsf{K}(k)$
$d \leftarrow A^{\mathsf{E}_k(LR(\cdot,\cdot,b))}_{cpa}(k)$
Return d

Define the advantages of the adversary via

$$\mathbf{Adv}^{lor-cpa}_{\mathsf{SE},A_{cpa}}(k) = \Pr[\mathbf{Exp}^{lor-cpa-1}_{\mathsf{SE},A_{cpa}}(k) = 1] - \Pr[\mathbf{Exp}^{lor-cpa-0}_{\mathsf{SE},A_{cpa}}(k) = 1].$$

Define the advantage functions of the scheme as follows. For any t, q_e, μ_e,

$$\mathbf{Adv}^{lor-cpa}_{\mathsf{SE}}(k, t, q_e, \mu_e) = \max_{A_{cpa}}\{\mathbf{Adv}^{lor-cpa}_{\mathsf{SE},A_{cpa}}(k)\}.$$

If a reasonable adversary cannot obtain the significant advantage, we consider an encryption scheme to be good. In the similar way we can define the LOR-CCA with the decryption oracle. For details, see [1].

We will consider the symmetric encryption schemes based on finite pseudorandom functions(PRFs) or permutations(PRPs) [2]. Let $Rand^{l\to L}$ be the family of all functions from $\{0,1\}^l$ to $\{0,1\}^L$ and $Perm^l$ be the family of all permutations on $\{0,1\}^l$. We will not define PRFs and PRPs for detail. The following implies the relation of the advantage between PRFs and PRPs.

Proposition 1. *[1] For any permutation family* P *with length* l,

$$\mathbf{Adv}^{prf}_{P}(t, q) \leq \mathbf{Adv}^{prp}_{P} + \frac{q^2}{2^{i+1}} \ .$$

Now we will see the concrete security of the symmetric encryption schemes, i.e., the XOR, CTR, and CBC schemes, using RFs(random functions), RPs(random permutations), PRFs, and PRPs. Let a function family F be input length l, output length L, and key-length k. To specify the function we will use $f = F_K$. The followings are specified the XOR, CTR, and CBC schemes respectively. The message x to be encrypted is regarded as a sequence of L-bit blocks, $x = x_1 \cdots x_n$, and let r be the nonce and addition is modulo 2^l.

- **The XOR scheme : XOR$[F]$ = (K-XOR, E-XOR, D-XOR)**
  The key generation algorithm K-XOR just outputs a random k-bit key K for the underling function family F, thereby specifying a function $f = F_K$ of l-bits to L-bits. Define $\mathsf{E}\text{-XOR}_K(x) = \mathsf{E}\text{-XOR}^{F_K}(x)$ and $\mathsf{D}\text{-XOR}_K(z) = \mathsf{D}\text{-XOR}^{F_K}(z)$, where :

function E-XOR$^f(x)$	**function** D-XOR$^f(z)$
$r \leftarrow \{0,1\}^l$	Parse z as $r\|\|y_1 \cdots y_n$
for $i = 1, \cdots, n$	**for** $i = 1, \cdots, n$
do $y_i = f(r+i) \oplus x_i$	**do** $x_i = f(r+i) \oplus y_i$
return $r\|\|y_1 y_2 \cdots y_n$	**return** $x = x_1 x_2 \cdots x_n$

- **The CTR scheme : CTR$[F]$ = (K-CTR, E-CTR, D-CTR)**
  The key generation algorithm K-CTR is the same as the XOR scheme, meaning just outputs a random k-bit key K for the underling function family F. Define $\mathsf{E}\text{-CTR}_K(x, ctr) = \mathsf{E}\text{-CTR}^{F_K}(x, ctr)$ and $\mathsf{D}\text{-CTR}_K(z) = \mathsf{D}\text{-CTR}^{F_K}(z)$, where :

function E-CTR$^f(x, ctr)$	**function** D-CTR$^f(z)$
for $i = 1, \cdots, n$	Parse z as $ctr\|\|y_1 \cdots y_n$
do $y_i = f(ctr+i) \oplus x_i$	**for** $i = 1, \cdots, n$
$ctr \leftarrow ctr + n$	**do** $x_i = f(ctr+i) \oplus y_i$
return $(ctr, ctr\|\|y_1 y_2 \cdots y_n)$	**return** $x = x_1 x_2 \cdots x_n$

- **The CBC Scheme: CBC$[F]$ = (K-CBC, E-CBC, D-CBC)**
  The key generation algorithm K-CBC is the same as the XOR scheme, meaning just outputs a random k-bit key K for the underling permutation family F(The CBC Scheme is required that $l = L$) . Define $\mathsf{E}\text{-CBC}_K(x) = \mathsf{E}\text{-CBC}^{F_K}(x)$ and $\mathsf{D}\text{-CBC}_K(z) = \mathsf{D}\text{-CBC}^{F_K}(z)$, where :

function E-CBC$^f(x)$	**function** D-CBC$^f(z)$
$y_0 \leftarrow \{0,1\}^l$	Parse z as $y_0\|\|y_1 \cdots y_n$
for $i = 1, \cdots, n$	**for** $i = 1, \cdots, n$
do $y_i = f(y_{i-1} \oplus x_i)$	**do** $x_i = f^{-1}(y_i) \oplus y_{i-1}$
return $y_0\|\|y_1 y_2 \cdots y_n$	**return** $x = x_1 x_2 \cdots x_n$

Let us see the concrete security of the schemes. We first summarize the security of the XOR scheme.

Theorem 1. *[1]* **[The Concrete Security of the XOR Scheme]**

(*i*) **(The Lower Bound on Insecurity of XOR using a RF)**
Let $R = Rand^{l \to L}$. *Then, for any* t, q_e, *and* μ_e, *such that* $\mu_e q_e / L \leq 2^l$,

$$\mathbf{Adv}^{lor-cpa}_{XOR[R]}(\cdot, t, q_e, \mu_e) \ \geq 0.316 \ \cdot \frac{\mu_e \cdot (q_e - 1)}{L \cdot 2^l}.$$

(*ii*) **(The Upper Bound on Insecurity of XOR using a RF)**
Let $R = Rand^{l \to L}$. *Then, for any* t, q_e, μ_e,

$$\mathbf{Adv}^{lor-cpa}_{XOR[R]}(\cdot, t, q_e, \mu_e) \ \leq \ \frac{\mu_e \cdot (q_e - 1)}{L \cdot 2^l}.$$

(*iii*) **(Security of XOR using a PRF)**
Suppose F *be a PRF family with input-length* l *and output-length* L. *Then, for any* t, q_e, *and* $\mu_e = qL$,

$$\mathbf{Adv}^{lor-cpa}_{XOR[F]}(\cdot, t, q_e, \mu_e) \ \leq \ 2 \cdot \mathbf{Adv}^{prf}_{F}(t, q) \ + \ \frac{\mu_e \cdot (q_e - 1)}{L \cdot 2^l}.$$

The CTR scheme is the stateful version of the XOR scheme. This scheme achieves the better security than that of the XOR. The adversary has no advantage in the ideal case.

Theorem 2. *[1]* **[The Concrete Security of the CTR Scheme]**

(*i*) **(Security of CTR using a RF)**
Let $R = Rand^{l \to L}$. *Then, for any* t, q_e, *and* $\mu_e \leq L2^l$,

$$\mathbf{Adv}^{lor-cpa}_{CTR[R]}(\cdot, t, q_e, \mu_e) \ = \ 0.$$

(*ii*) **(Security of CTR using a PRF)**
Suppose F *be a PRF family with input-length* l *and output-length* L. *Then, for any* t, q_e, *and* $\mu_e = min(qL, L2^l)$,

$$\mathbf{Adv}^{lor-cpa}_{CTR[F]}(\cdot, t, q_e, \mu_e) \ \leq \ 2 \cdot \mathbf{Adv}^{prf}_{F}(t, q).$$

Although in the CBC scheme $l = L$ is required and each F_k should be a permutation, we will still consider the case that F is a pseudorandom function family($l = L$). Also we will see the case that F is a pseudorandom permutation family.

Theorem 3. *[1]* **[The Concrete Security of the CBC Scheme]**

(*i*) **(The Lower Bound on Insecurity of CBC using a RF)**
Let $R = Rand^{l \to l}$. *Then, for any* t, q_e, *and* μ_e, *such that* $\mu_e \ \leq \ l2^{\frac{l}{2}}$,

$$\mathbf{Adv}^{lor-cpa}_{CBC[R]}(\cdot, t, q_e, \mu_e) \ \geq \ 0.316 \cdot \ \left(1 - \frac{2}{2^{l/2}}\right) \cdot \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

(*ii*) **(The Upper Bound on Insecurity of CBC using a RF)**
Let $R = Rand^{l \to l}$. Then, for any t, q_e, and μ_e,

$$\mathbf{Adv}^{lor-cpa}_{CBC[R]}(\cdot, t, q_e, \mu_e) \ \leq \ \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

(*iii*) **(Security of CBC using a PRF)**
Suppose F be a PRF family with input-length l and output-length l. Then, for any t, q_e, and $\mu_e = ql$,

$$\mathbf{Adv}^{lor-cpa}_{CBC[F]}(\cdot, t, q_e, \mu_e) \ \leq \ 2 \cdot \mathbf{Adv}^{prf}_{F}(t, q) \ + \ \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

(*iv*) **(The Lower Bound on Insecurity of CBC using a RP)**
Let $RP = Perm^l$. Then, for any $t, q_e (= \mu_e/l)$, and $\mu_e (\leq \ l2^{\frac{l}{2}})$,

$$\mathbf{Adv}^{lor-cpa}_{CBC[RP]}(\cdot, t, q_e, \mu_e) \ \geq \ 0.316 \cdot \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

(*v*) **(The Upper Bound on Insecurity of CBC using a RP)**
Let $RP = Perm^l$. Then, for any t, q_e, and μ_e,

$$\mathbf{Adv}^{lor-cpa}_{CBC[RP]}(\cdot, t, q_e, \mu_e) \ \leq \ \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

(*vi*) **(Security of CBC using a PRP)**
Suppose F be a PRP family with length l. Then, for any t, q_e, and $\mu_e = ql$,

$$\mathbf{Adv}^{lor-cpa}_{CBC[F]}(\cdot, t, q_e, \mu_e) \ \leq \ 2 \cdot \mathbf{Adv}^{prf}_{F}(t, q) \ + \ \frac{q^2}{2^{l+1}} \ + \ \left(\frac{\mu^2}{l^2} - \frac{\mu}{l}\right) \cdot \frac{1}{2^l}.$$

In the above theorems we can see that the CTR scheme has the best security in a random function model. This also gives the best concrete security in a pseudorandom function model. The CTR model has no collision on the inputs of the function f. Since the function f is in a random function, the attacker have no information to distinguish in the LOR sense. However the XOR and CBC scheme may have an collision on input of f by the birthday paradox, this can leak some information to distinguish. This motivates our schemes. Our scheme pursue the CTR scheme to achieve the perfect concrete security in the random function model under the LOR sense.

3 The CTR-OFB and CTR-CFB Schemes

In the previous section we considered that the CTR mode has the best concrete security in the LOR-CPA sense. This comes from the collision-freeness on the input of the function f. Here we propose the new schemes, the counter-based OFB scheme and CFB scheme, which we call the CTR-OFB scheme and CTR-CFB scheme respectively.

Now we define our schemes. Let a function family F be input length l, output length L, and key-length k. To specify the function we will use $f = F_K$. The message x to be encrypted is regarded as a sequence of l-bit blocks, $x = x_1 \cdots x_n$. Let r be the nonce with v-bit, addition is modulo 2^{l-v}, and ctr be the $(l-v)$-bit integer. The notation $a||b$ means the concatenation of a and b, and $lsb_j(a)$ takes j bits of a from 0 to $j-1$ bit position.

- **The CTR-OFB scheme :**
  CTR-OFB$[F]$ = (K-**CTR-OFB**, E-**CTR-OFB**, D-**CTR-OFB**)
  The key generation algorithm K-CTR-OFB is the same as the XOR scheme, meaning just outputs a random k-bit key K for the underling function family F. Define E-CTR-OFB$_K(x, ctr)$ = E-CTR-OFB$^{F_K}(x, ctr)$ and D-CTR-OFB$_K(z)$ = D-CTR-OFB$^{F_K}(z)$, where :

function E-CTR-OFB$^f(x, ctr)$	**function** D-CTR-OFB$^f(z)$
$v_0 = r \leftarrow \{0,1\}^v$ and $y_0 = v_0 \|\| ctr$	Parse z as $y_0 \|\| y_1 \cdots y_n$
for $i = 1, \cdots, n$	Parse y_0 as $v_0 \|\| ctr$
do $y_i = f(v_{i-1} \|\| ctr + i) \oplus x_i$	**for** $i = 1, \cdots, n$
$v_i = lsb_v(f(v_{i-1} \|\| ctr + i))$	**do** $x_i = f(v_{i-1} \|\| ctr + i) \oplus y_i$
$ctr \leftarrow ctr + n$	$v_i = lsb_v(f(v_{i-1} \|\| ctr + i))$
return $(ctr, y_0 \|\| y_1 y_2 \cdots y_n)$	**return** $x = x_1 x_2 \cdots x_n$

- **The CTR-CFB scheme :**
  CTR-CFB$[F]$ = (K-**CTR-CFB**, E-**CTR-CFB**, D-**CTR-CFB**)
  The key generation algorithm K-CTR-CFB is the same as the XOR scheme, meaning just outputs a random k-bit key K for the underling function family F. Define E-CTR-CFB$_K(x, ctr)$ = E-CTR-CFB$^{F_K}(x, ctr)$ and D-CTR-CFB$_K(z)$ = D-CTR-CFB$^{F_K}(z)$, where :

function E-CTR-CFB$^f(x, ctr)$	**function** D-CTR-CFB$^f(z)$
$r \leftarrow \{0,1\}^v$ and $y_0 = r \|\| ctr$	Parse z as $y_0 \|\| y_1 \cdots y_n$
for $i = 1, \cdots, n$	Parse y_0 as $r \|\| ctr$
do $y_i = f(lsb_v(y_{i-1}) \|\| ctr + i) \oplus x_i$	**for** $i = 1, \cdots, n$
$ctr \leftarrow ctr + n$	**do** $x_i = f(lsb_v(y_{i-1}) \|\| ctr + i) \oplus y_i$
return $(ctr, y_0 \|\| y_1 y_2 \cdots y_n)$	**return** $x = x_1 x_2 \cdots x_n$

The above schemes are conter-based and give the concrete security as same as the CTR scheme. We will see this in the following section. Also the CTR-OFB scheme can be preprocessed because of the independence of the message block. So we can see that our scheme have the same security of the CTR scheme on the concrete security point of view.

The CTR-OFB scheme is similar to the OFB scheme and the CTR-CFB scheme is also similar to the CFB scheme. However, since the OFB and CFB schemes achieve the same concrete security as the CBC scheme does, our new schemes have the better concrete security than the OFB and CFB schemes.

The modes of operation for symmetric encryption are generally using block ciphers. It is well known that block ciphers are difficult to be constructed to

attain PRFs or PRPs. So we should see a scheme not only on the theoretical point of view but also on the practical point of view.

For the most powerful known attacks on block ciphers are Differential Cryptanalysis(DC) [3, 4] and Linear Cryptanalysis(LC) [9, 10]. For the CTR scheme we know that inputs of f are using serially. This may give an easy way to construct to the chosen plaintext pairs with the low hamming weight differential. If the underlying block ciphers have crucial weakness in this attack, the CTR scheme is easy to attack. However for our schemes inputs of f are the concatenation of randomized v bits and $l - v$ bit counter. This make difficult to construct the plaintext pairs having low hamming weight. Also the randomization of the input bits of the underlying function in the CTR-OFB and CTR-CFB schemes also give the higher resistance against the SQUARE-type attacks [5, 8] than that of the CTR scheme.

4 Security Analysis of the CTR-OFB and CTR-CFB Schemes

Here we will see the concrete security of the our proposed schemes. We will use the same notations in section 2. For our scheme the function family F is with the input length l, output length L, and key length k. The following theorem give the concrete security of the CTR-OFB schemes.

Theorem 4. [The Concrete Security of the CTR-OFB Scheme]

(i) **(Security of CTR-OFB using a RF)** *Let $R = Rand^{l \to L}$. Then, for any t, q_e, and $\mu_e \leq L2^{l-v}$,*

$$\mathbf{Adv}^{lor-cpa}_{CTR-OFB[R]}(\cdot, t, q_e, \mu_e) \;=\; 0.$$

(ii) **(Security of CTR-OFB using a PRF)** *Suppose F be a PRF family with input-length l and output-length L. Then, for any t, q_e, and $\mu_e = min(qL, L2^{l-v})$,*

$$\mathbf{Adv}^{lor-cpa}_{CTR-OFB[F]}(\cdot, t, q_e, \mu_e) \;\leq\; 2 \cdot \mathbf{Adv}^{prf}_{F}(t, q).$$

Proof. The proof of (ii) can be achived as the same way of [1]. So we need only to prove (i).
Let (P_i, Q_i) be the oracle queries of the adversary A, each consisting of a pair of equal length messages. Let n_i be the number of blocks in the i-th query. We denote $P_i = p^i_1 \cdots p^i_{n_i}$ and $Q_i = q^i_1 \cdots q^i_{n_i}$. Let $r_i \in \{0,1\}^v$ be the nonce associated to (P_i, Q_i) as chosen at random by the oracle, for $i = 1, \cdots, q_e$. Let be the orcle answers such that $(r_i||ctr, y^i_1, \cdots, y^i_{n_i}) \to O(P_i, Q_i)$, $i = 1, \cdots, q_e$.

In answering the i-th query, the oracle applies the underlying function f to the n_i strings either $r_i||ctr+1, lsb_v(p^i_1 \oplus y^i_1)||ctr+2, \cdots, lsb_v(p^i_{n_i-1} \oplus y^i_{n_i-1})||ctr+n_i$ or $r_i||ctr+1, lsb_v(q^i_1 \oplus y^i_1)||ctr+2, \cdots, lsb_v(q^i_{n_i-1} \oplus y^i_{n_i-1})||ctr+n_i$.

Let D be the following event, defined for either game : $r_i||ctr+1, lsb_v(p^i_1 \oplus y^i_1)||ctr+2, \cdots, lsb_v(p^i_{n_i-1} \oplus y^i_{n_i-1})||ctr+n_i$ and $r_i||ctr+1, lsb_v(q^i_1 \oplus y^i_1)||ctr+2,$

$\cdots$, $lsb_v(q^i_{n_i-1} \oplus y^i_{n_i-1})||ctr + n_i$ have no same value for $i = 1, \cdots, q_e$. We define $\Pr_0[\cdot]$ to be the probability of an event in game 0 and $\Pr_1[\cdot]$ to be the probability of an event in game 1.

Claim 1. $Pr_0[D] = Pr_1[D] = 1$ for $\mu_e \leq L2^{l-v}$

Proof : In any case we know that the input string does not have the same value since the counter bits are different. So the probability of each game is 1.

Claim 2. $Pr_0[A = 1|D] = Pr_1[A = 1|D]$

Proof : Given the event D, we have that, in either game, the function f is evaluated at a new point each time. Thus the output is randomly and uniformly distributed over $\{0,1\}^L$ and each block is a message block XORed with a random value. So we have $Pr_0[A = 1|D] = Pr_1[A = 1|D]$.

Now we compute the advantage of A as follows :

$$\begin{aligned}\mathbf{Adv}^{lor-cpa}_{CTR-OFB[R]}(\cdot, t, q_e, \mu_e) &= Pr_1[A = 1] - Pr_0[A = 1] \\ &= Pr_1[A = 1|D] \cdot Pr_1[D] + Pr_1[A = 1|\bar{D}] \cdot Pr_1[\bar{D}] - \\ &\quad Pr_0[A = 1|D] \cdot Pr_0[D] - Pr_0[A = 1|\bar{D}] \cdot Pr_0[\bar{D}]\end{aligned}$$

By Claim 1 and 2, we have $\mathbf{Adv}^{lor-cpa}_{CTR-OFB[R]}(\cdot, t, q_e, \mu_e) = 0$.

In the similar way, we can prove the following theorem, which gives the concrete security of the CTR-CFB schemes.

Theorem 5. [The Concrete Security of the CTR-CFB Scheme]

(*i*) **(Security of CTR-CFB using a RF)**
Let $R = Rand^{l \to L}$. Then, for any t, q_e, and $\mu_e \leq L2^{l-v}$,

$$\mathbf{Adv}^{lor-cpa}_{CTR-CFB[R]}(\cdot, t, q_e, \mu_e) = 0.$$

(*ii*) **(Security of CTR-CFB using a PRF)**
Suppose F be a PRF family with input-length l and output-length L. Then, for any t, q_e, and $\mu_e = min(qL, L2^{l-v})$,

$$\mathbf{Adv}^{lor-cpa}_{CTR-CFB[F]}(\cdot, t, q_e, \mu_e) \leq 2 \cdot \mathbf{Adv}^{prf}_F(t, q).$$

Proof. This proof is as same as the proof of Theorem 4.

5 Conclusion

In this paper we propose the new modes of operation, the CTR-OFB and CTR-CFB scheme. Each scheme have the perfect concrete security on the sense of [1] as same as the CTR mode do. The CTR scheme have the inputs of f serially. However our schemes can randomize some input bits of the f. We may think that this makes the attack difficult to analyze the scheme on the practical attack point of view, for example, the differential cryptanalysis with low hamming weight differential and the SQUARE-type attacks.

The CTR mode can be preprocessed because of the independence of message blocks and are easy to random-access. The CTR-OFB scheme also can be preprocessed. But it does not permit random-access.

References

1. M. Bellare, A. Desai, E. JokiPii, and P. Rogaway, *A Concrete Security Treetment of Symmetric Encryption : Analysis of the DES Modes of Operation*, Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997. The revised version is available at *http://www-cse.ucsd.edu/users/mihir*.
2. M. Bellare, J. Kilian, and P. Rogaway, *The Security of the Cipher Block Chaining Message Authentication Code*, Advanced in Cryptology - CRYPTO'94, LNCS 839, pp. 341–358, Springer-Verlag, 1994.
3. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Advances in Cryptology - CRYPTO'90, LNCS 537, pp. 2–21, Springer-Verlag, 1991.
4. E. Biham and A. Shamir, *Differential cryptanalysis of the full 16-round DES*, Advances in Cryptology - CRYPTO'92, LNCS 740, pp. 487–496, Springer-Verlag, 1992.
5. J. Daeman, L. Knudsen, and V. Rijmen, *The Block Cipher Square*, Fast Software Encryption 1997, LNCS 1636, pp. 46–59, Springer-Verlag, 1997.
6. W. Diffie and M. Hellman, *Privacy and Authentication : An introduction to Cryptography*, Proceedings of the IEEE, 67(1979), pp. 397–427, 1979.
7. S. Goldwasser and S. Micali, *Probabilistic Encryption*, Journal of Computer and System Sciences, Vol.28, pp. 270–279, April 1984.
8. Stefan Lucks, *The Saturation Attack - a Bait for Twofish*, Fast Software Encrption 2001, 2001, to appear.
9. M. Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology - EUROCRYPT'93, LNCS 765, pp. 386–397, Springer-Verlag, 1994.
10. M. Matsui, *The first experimental cryptanalysis of the Data Encryption Standard*, Advances in Cryptology - CRYPTO'94, LNCS 839, pp. 1–11, Springer-Verlag, 1994.
11. National Bureau of Standards, *DES modes of operation*, FIPS-Pub.46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., December 1980.
12. National Institute of Standards and Technology, *AES Mode of Operation Development Effort*, *http://csrc.nist.gov/encryption/modes*.

Appendix : The figures of the CTR-OFB and CTR-CFB Schemes

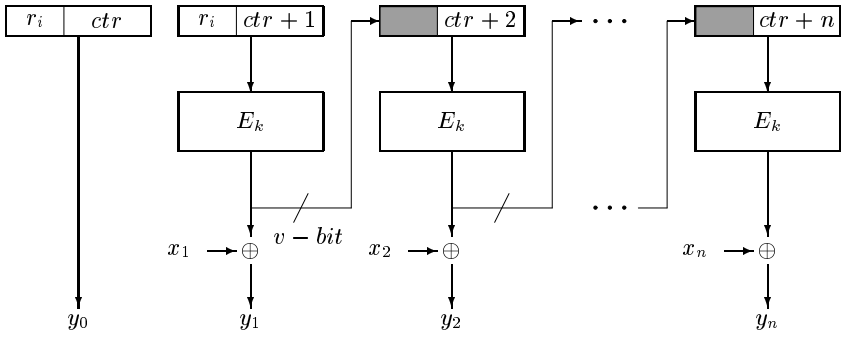

Fig. 1. The CTR-OFB Scheme

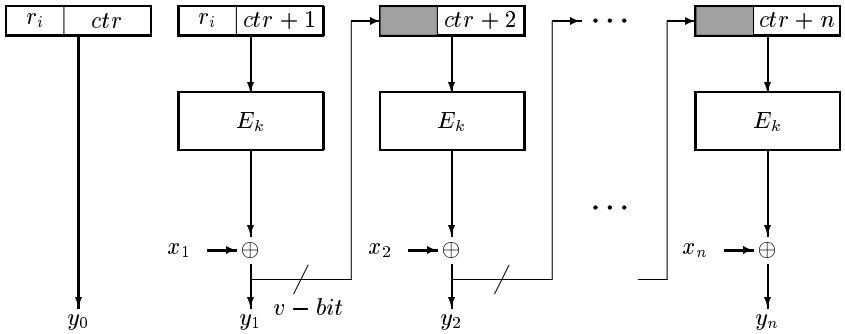

Fig. 2. The CTR-CFB Scheme