Provable security of CFB mode of operation with external re-keying

Vadim Tsypyschev[1] and Iliya Morgasov[2]

[1]Infocrypt, Russia
[2]Infocrypt, Russia
[1]tsypyschev@yandex.ru, [2]morgasov@infocrypt.ru

Abstract

In this article the security of the cipher feedback mode of operation with regular external serial re-keying aiming to construct lightweight pseudo-random sequences generator is investigated. For this purpose the new mode of operation called Multi-key CFB, MCFB is introduced, and the estimations of provable security of this new mode in the LOR-CPA model are obtained. Besides that, the counterexample to well-known result of Abdalla–Bellare about security of encryption scheme with external re-keying is obtained.

Keywords: Multy-key CFB, external serial re-keying, provable security

1 Introduction

This article arose from an attempt to build a lightweight pseudo-random sequence generator. To build such a generator, it is natural to use regular re-encryption of the original random sequence by a lightweight block cipher (for example, Magma) in a mode with good mixing of the original sequence (CFB, OFB, CBC). Due to author's precedency, the CFB mode was chosen.

In addition, it is natural to use a regular update of the initial random key, for which it is reasonable to follow the recommendations of [7] and choose an external key update using a key generator. In these recommendations, two types of external generators are proposed: serial and parallel. It is appropriate to choose a serial key generator for use in a pseudo-random sequences (PRS) generator, since it provides security for previously encrypted messages when the current state of the generator is compromised [3] (so called *forward* security).

Hereafter n is the block size, k is the key size. Since Magma is supposed to be used, $k = \tau \cdot n$, $\tau = 4$, are assumed for definiteness.

The serial key generator is an automaton with one internal state. Initially, the initial state K_1^* is randomly and equiprobably generated, which is used to generate the encryption key K_1^{Enc} as the output of the generator, as well as to generate the next state K_2^*. Herewith, the initial state is overwritten and becomes inaccessible to the adversary. The process is then repeated.

Let's introduce notation. In what follows, without further explanation, we will use generally accepted terms and notation.

$$Const_1 = Vec_n(0) \| \cdots \| Vec_n(\tau - 1);$$
$$Const_2 = Vec_n(\tau) \| \cdots \| Vec_n(2\tau - 1).$$

Let's denote by λ the empty string. For our purpose it is convenient to formulate especially the procedure of ECB enciphering:

```
$ECB_K(String)$
$Output = \lambda$
$j = \lceil |String|/n \rceil$
for $i = \overline{0, j-1}$ do
    $Output = Output \| E_K(MSB_n(String << ni))$
endfor
return $Output$
```

Here and hereafter MSB_n denotes the n most significant bits (leftmost bits) of the bit string, and $<< l$ denotes the left shift of the bit string by l bits filling the rightmost l bit by zeros.

```
Serial Key Generator $\mathcal{SG}$
$K \leftarrow_{\$} \{0,1\}^k$
$K_1^* \leftarrow K$
for $i = \overline{1, \infty}$ do
    $K_i^{\mathsf{Enc}} \leftarrow ECB_{K_i^*}(Const_1)$
    $K_{i+1}^* \leftarrow ECB_{K_i^*}(Const_2)$
endfor
```

For convenience, let's introduce procedure:

```
$Update\mathcal{SG}(K)$
$K^{\mathsf{Enc}} \leftarrow ECB_K(Const_1)$
$K \leftarrow ECB_K(Const_2)$
return $(K^{\mathsf{Enc}}, K)$
```

The CFB (Cipher Feedback) encryption mode has been standardized in the [5, 9] documents. Encryption according to this mode looks like this:

```
$CFB_{K,IV}(String)$
$j = \lceil |String|/n \rceil$
$Output = \lambda$
$Chain = IV$
for $i = \overline{1, j}$ do
    $C_i = E_K\,(Chain) \oplus MSB_n(String << ni)$
    $Chain = C(i)$
    $Output = Output \| C(i)$
endfor
return $Output$
```

The issues of CFB mode security were considered in the papers [2, 6]

Thus, the proposed generator of pseudo-random sequences has the form:

```
PRNG($\mathcal{SG}$,CFB) with external rekeying
Seeding
    $K \leftarrow_{\$} \{0,1\}^k$
Initialization
    $K_1^* \leftarrow K$
$Output \leftarrow \lambda$
$Output_0 \leftarrow Vec_n(0)\|\cdots\|Vec_n(m-1)$
Working
for $i = \overline{1,M}$ do
    $(K_i^{\mathsf{Enc}}, K_{i+1}^*) \leftarrow Update\mathcal{SG}(K_i^*)$
    $IV \leftarrow_{\$} \{0,1\}^n$
    $Output_i \leftarrow CFB_{K_i^{\mathsf{Enc}},IV}(Output_{i-1})$
    $Output \leftarrow Output\|Output_i$
endfor
return $Output$
```

So, the sequence obtained as a result of encryption in the CFB mode with regular key exchange is considered as a single pseudo-random sequence, and, accordingly, the question arises about the quality of such a PRS. It is proposed to evaluate the quality of the proposed PRS by assessing the strength of the generator as an encryption scheme.

To assess the strength of the proposed generator 1 as an encryption scheme, one could use the result [1, Theorem 4.1], however, this Theorem seems to be not quite true, and for this reason the security estimates below are obtained directly for the PRS generator $PRNG(\mathcal{SG}, CFB)$. Reasons why we don't concern the result of Abdalla–Bellare as truthful will be explained below.

The further presentation is structured as follows: first, the mode of using block ciphers Multy-key CFB, MCFB is introduced, as a model of the generator proposed above. For the introduced mode, security estimates are consequently obtained with using a random key generator and with using random functions as cipher conversions. Then, based on above, an estimate of the strength of the MCFB mode is obtained when using random key generation and a pseudo-random family of encryption functions. The final estimate is obtained from the previous one by moving on to consider the MCFB mode with a serial generator and pseudo-random cipher conversions.

Let $M \in \mathbb{N}$ be the number of segments encrypted with the same key, which are hereinafter referred to as *sections*, and let $m \in \mathbb{N}$ be the size of the partition.

Under the scheme encryption $\mathcal{E} = (\mathcal{G}, E)$ we mean a set of a key generation algorithm and a set of encryption functions indexed by keys. Usually a block cipher algorithm is a triplet $(\mathcal{G}, E, D)$ — a set of key generation, encryption, decryption algorithms. But, since the decryption function is not used in CFB mode, it is proposed to omit it.

The set of all random functions $\mathcal{RF}^{n,n}$ and an arbitrary family of pseudorandom functions E are considered below as sets of encryption functions. In this case, for convenience, the function itself is understood as a key indexing a random function.

As key generators either a random generator $\mathcal{RG}$,or the serial generator $\mathcal{SG}$ are considered. The random generator is choosing a key from a given key set (either the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$, or the set $\{0,1\}^k$) randomly equiprobable and regardless of previous choices.

Let n, k be the length of the block and the length of the key of the encryption algorithm, respectively. Let X, Y be the plaintext and ciphertext alphabets, respectively. Then the mode $MCFB^{ext}_{m,M}(\mathcal{G},\mathcal{F})$ with $\mathcal{G}$ key generator and $\mathcal{F}$ encryption functionset with external rekeying is described as follows:

```
$MCFB^{ext}_{m,M}(\mathcal{G},\mathcal{F})$
Input
$X_i, i = \overline{1, mM}$
Working
for $i = \overline{0, mM-1}$ do
    if $i \pmod{m} = 0$ do
        $K_i \leftarrow_{\$} \mathcal{G}$
        $Chain_i \leftarrow_{\$} \{0,1\}^n$
    endif
    $Y_i \leftarrow X_i \oplus \mathcal{F}_{K_i}(Chain_i)$
    $Chain_{i+1} \leftarrow Y_i$
endfor
return $Y_i, i = \overline{1, mM}$
```

2 Preliminaries

The adversary $\mathcal{A}$ is understood as a probabilistic algorithm designed to reveal the cryptographic parameters of a cryptoscheme. As a rule, the adversary turns to the Oracle to calculate the secret data.

The reference of the adversary to the oracle will be denoted by $\mathcal{A}^{O(\cdot)}$, where the dot marks the values of the variables transmitted to the oracle.

Definition 2.1. *The family of pseudorandom functions (Pseudorandom Family, PRF) is the set $F = \{F_K \mid K \in \texttt{keys}F\}$, $F_K : \{0,1\}^l \to \{0,1\}^L$ indexed by the elements of the key set $\texttt{keys}F$.*

If $\mathcal{A}$ is an arbitrary adversary, then the advantage of the observer $\mathcal{A}$ in distinguishing the family F from the family of random functions $\mathcal{RF}^{l,L}$ is the quantity

$$\mathbf{Adv}^{prf}_F(\mathcal{A}) = \mathbf{Pr}\left(K \leftarrow_{\$} \texttt{keys}F \mid \mathcal{A}^{F_K(\cdot)} = 1\right) - \mathbf{Pr}\left(R \leftarrow_{\$} \mathcal{RF}^{l,L} \mid \mathcal{A}^{R(\cdot)} = 1\right)$$

where the probability is taken over all choices of keys, random functions, and adversary $\mathcal{A}$ internal variables.

Insecurity of the F family is a quantity

$$\mathbf{InSec}^{prf}(F; t, q) = \max_{\mathcal{A}} \mathbf{Adv}^{prf}_F(\mathcal{A})$$

where the maximum is taken over all adversaries, which are executed with time complexity t and with the number of queries to the oracle q.

If $\mathbf{InSec}^{prf}(F;t,q) \leq \epsilon$*, then* F *is* $(t,q,\epsilon) - \mathtt{PRF}$*-secure.*

By time complexity we shall mean the execution time of experiments $K \leftarrow_{\$} \mathtt{keys}F; v \leftarrow \mathcal{A}^{F_K(\cdot)}$ *and* $R \leftarrow_{\$} \mathcal{RF}^{l,L}; v \leftarrow \mathcal{A}^{R(\cdot)}$ *as well as the execution time of the* $\mathcal{A}$*'s code in some fixed RAM model, including the calculation time of* F_K *and responses to queries to the oracle.*

Definition 2.2. *The Pseudorandom permutation family (PRP)* $\{E_K \mid K \in \mathtt{keys}E\}$ *is the set of permutations* $E_K : \{0,1\}^l \to \{0,1\}^l$ *indexed by keys* $K \in \mathtt{keys}E$*.*

If $\mathcal{A}$ *is an arbitrary adversary, then the advantage of the adversary* $\mathcal{A}$ *in distinguishing between* E *and a random permutation is defined as*

$$\mathbf{Adv}_E^{prp}(\mathcal{A}) = \mathbf{Pr}\left(K \leftarrow_{\$} \mathtt{keys}E \mid \mathcal{A}^{E_K(\cdot)} = 1\right) - \mathbf{Pr}\left(P \leftarrow_{\$} \mathcal{P}^l \mid \mathcal{A}^{P(\cdot)} = 1\right)$$

where the probability is taken over all possible choices of keys, random permutations, and the adversary's $\mathcal{A}$ *internal variables. It is assumed that the adversary cannot access the reverse permutations* $E_K^{-1}(\cdot), P^{-1}(\cdot)$*.*

The insecurity of family E *is the value*

$$\mathbf{InSec}^{prp}(E;t,q) = \max_{\mathcal{A}} \mathbf{Adv}_E^{prp}(\mathcal{A}),$$

where the maximum is taken over all adversaries executing with time complexity t *with number of queries to oracle* q*.*

If $\mathbf{InSec}^{prp}(E;t,q) \leq \varepsilon$*, then the family* E *is called* $(t,q,\varepsilon) - \mathtt{PRP}$*-secure.*

Statement 2.3 ([6])**.** *Let* E *is a PRP-family over* $\{0,1\}^l$*. Then*

$$\mathbf{InSec}^{prf}(E;t,q) \leq \mathbf{InSec}^{prp}(E;t,q) + \binom{q}{2} \cdot \frac{1}{2^l}$$

The security of the $MCFB^{ext}$ symmetric cipher scheme is discussed below with respect to the left-or-right indistinguishability model in a chosen-plaintext attack (LOR-CPA). The LOR-CPA security model is studied in detail in [4]. In particular, this paper explores how the LOR-CPA model relates to other symmetric encryption security models.

Informally, the attack in the LOR-CPA model is represented by a game between an active adversary (left-right distinguisher) D_{lr} and an encryption oracle $\mathcal{E}_{K,b}$ with key K and bit $b \in \{0,1\}$.

In each round, observer D_{lr} selects two plaintexts m_i^0 and m_i^1, $|m_i^0| = |m_i^1|$, and passes them to $\mathcal{E}_{K,b}$. The oracle returns $c_i = \mathsf{Enc}_K(m_i^b)$. The cases $b = 0$ and $b = 1$ are called left and right, respectively. The observer D_{lr} publishes bit e as his guess about the value of b.

The advantage $\mathbf{Adv}(D_{lr})$ of the adversary D_{lr} is defined as in the statistical test, that is, as the difference between the output probabilities $e = 0$ in each of the two cases: $b = 0$ and $b = 1$.

Definition 2.4 (LOR indistinguishability)**.** *Let* $\mathcal{E} = (\mathcal{G}, E)$ *be a symmetric encryption scheme. Let's define the function* $lr(b, x_0, x_1) = x_b$*. Then for an arbitrary adversary* $\mathcal{A}$ *its advantage over the LOR-CPA security of* $\mathcal{E}$ *is defined as*

$$\mathbf{Adv}_{\mathcal{E}}^{lor-cpa}(\mathcal{A}) = \mathbf{Pr}\left(K \leftarrow \mathcal{G} \mid \mathcal{A}_{E_K}(lr(0,\cdot,\cdot)) = 0\right) - \mathbf{Pr}\left(K \leftarrow \mathcal{G} \mid \mathcal{A}_{E_K}(lr(1,\cdot,\cdot)) = 0\right)$$

LOR-CPA insecurity of scheme $\mathcal{E}$ *is defined as*

$$\mathbf{InSec}_{\mathcal{E}}^{lor-cpa}(\mathcal{E}; t, q_{\mathcal{E}}, \mu_{\mathcal{E}}) = \max_{\mathcal{A}} \mathbf{Adv}_{\mathcal{E}}^{lor-cpa}(\mathcal{A})$$

where the maximum is taken over all adversaries, executing with time complexity t with not greater than $q_{\mathcal{E}}$ queries to oracle using totally $\mu_{\mathcal{E}}$ bits.

If $\mathbf{InSec}^{lor-cpa}(\mathcal{E}; t, q, \mu) \leq \varepsilon$, then we shall say that the scheme $\mathcal{E}$ is (t, q, μ, ε)-LOR-CPA-secure.

Let us define, further, the security of the sequential key generator. In general, the generator is defined as follows: let $\mathcal{F} : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ be a PRF-family indexed by keys from the set $\mathcal{K} = \{0,1\}^k$. Then

```
$\mathcal{SG}[\mathcal{F}]$
Algorithm $\mathcal{K}$
    $K \leftarrow_{\$} \{0,1\}^k$
    return $K$
Algorithm $\mathcal{N}$
    $Out \leftarrow \mathcal{F}(K, 0)$
    $K \leftarrow \mathcal{F}(K, 1)$
    return $(Out, K)$
```

Let's define also experimemts:

```
Experiment $\mathbf{Exp}^{prg-real}_{\mathcal{SG},M,\mathcal{A}}$
$St_0 \leftarrow \mathcal{K}$
$s \leftarrow \lambda$
for $i = \overline{1, M}$ do
    $(Out_i, St_i) \leftarrow \mathcal{N}(St_{i-1})$
    $s \leftarrow s \| Out_i$
endfor
$g \leftarrow \mathcal{A}(s)$
return $g$
```

and

```
Experiment $\mathbf{Exp}^{prg-rand}_{\mathcal{SG},M,\mathcal{A}}$
$s \leftarrow \{0,1\}^{k \cdot M}$
$g \leftarrow \mathcal{A}s$
return $g$
```

Then

Definition 2.5.

$$\mathsf{Adv}^{\mathrm{prg}}_{\mathcal{SG},M,\mathcal{A}} = \Pr\left[\mathbf{Exp}^{prg-real}_{\mathcal{SG},M,\mathcal{A}} = 0\right] - \Pr\left[\mathbf{Exp}^{prg-rand}_{\mathcal{SG},M,\mathcal{A}} = 0\right]$$

$$\mathbf{Insec}^{prg}_{\mathcal{SG},M}(t) = \max_{\mathcal{A}}\{\mathsf{Adv}^{\mathrm{prg}}_{\mathcal{SG},M,\mathcal{A}}\}$$

where the maximum is taken over all adversaries executing with time complexity t.

Time complexity is understood as the time of execution of two experiments and the execution of the adversary's code in some fixed RAM model.

The following result is true [1, Theorem 2.5]:

Statement 2.6.

$$\mathbf{Insec}^{prg}_{\mathcal{SG}[\mathcal{F}],M}(t) = \mathbf{Insec}^{\mathsf{PRF}}(\mathcal{F}; t + \log_2 M, 2)$$

3 Strength of External MCFB Mode with Random Key Generator and Random Encryption Functions

Consider a symmetric encryption scheme $MCFB^{ext}$ over a set of random functions $\mathcal{RF} : \{0,1\}^n \to \{0,1\}^n$ with a random key generator $\mathcal{RG}$. Such generalized symmetric encryption mode will be denoted $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF})$.

Definition 3.1. *Let's call by a collision in the $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF})$ mode a couple of ticks (i,j), $0 \le i \le j \le mM - 1$, in which $(chain_i, F_i(chain_i)) = (chain_j, F_j(chain_j))$. We denote the collision in ticks (i,j) by $col(i,j)$.*

Statement 3.2. *If there is a collision in the $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF})$ mode then the adversary D_{lr} is able to distinguish between the results of encryption of the left and right plaintexts, that is, win the LOR-CPA game.*

Proof. Note that the adversary certainly knows all the values of $chain_i$, $i = \overline{0, mM-1}$, since these are either initial vectors or directly observed ciphertext. So, let (i,j) collide in the $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF})$ mode. Then

$$F_i(chain_i) = F_j(chain_j)$$

Hence,

$$Y_i \oplus Y_j = X_i \oplus X_j = chain_{i+1} \oplus chain_{j+1}$$

Choosing bit e such that

$$m_i^e \oplus m_j^e = chain_{i+1} \oplus chain_{j+1}$$

adversary D_{lr} wins the LOR-CPA game. □

It is assumed above that the equality $m_i^0 \oplus m_j^0 = m_i^1 \oplus m_j^1$ is impossible with reasonable behavior of the adversary. Probability of fulfillment of this equality under a random equiprobable and independent choice of values $m_i^0, m_i^1, m_j^0, m_j^1$ will be discussed below in the next work.

Statement 3.3. *Denote by $(Chain, \mathcal{F}) = (chain_0, F_0(chain_0)), \ldots, (chain_{mM-1}, F_{mM-1}(chain_{mM-1}))$ set of sequences , arising during the operation of the symmetric encryption mode $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF}^{n,n})$ over the set of all random functions $\mathcal{RF}^{n,n}$.*

Denote by C the set of those that contain at least one collision. Then

$$|C| \le M \cdot \binom{m}{2} \cdot 2^{2mMn-n} + \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{2mMn-2n}$$

Proof. Note that the set of mM cycles of operation of the $MCFB^{ext}_{m,M}(\mathcal{RG},\mathcal{RF})$ mode is naturally divided into M sections by m cycles:

$$\begin{array}{lll} 0, & \ldots, & m-1, \\ & \ldots & \\ tm, & \ldots, & (t+1)m-1 \\ & \ldots & \\ (M-1)m, & \ldots, & mM-1 \end{array}$$

Herewith on each of the sections the same enciphering function is used.

We divide the set C into two classes. Denote by

$$C_I = \{col(i,j) \in (Chain, \mathcal{RF}) \mid i - \mathtt{Res}(i,m) = j - \mathtt{Res}(j,m)\}$$

that is, the set of collisions that occurred on segments of length m within the same section with obviously identical cipher conversions $F_i = F_j$.

Denote by

$$C_{II} = \{col(i,j) \in (Chain, \mathcal{RF}) \mid i - \mathtt{Res}(i,m) \neq j - \mathtt{Res}(j,m)\}$$

the set of collisions, which took place in the ticks belonging to the different sections.

The $\mathtt{Res}(i,m)$ denotes above the residue from division of i by m.

Then $C = C_I \cup C_{II}$, $|C| \leq |C_I| + |C_{II}|$.

Further, in the set C_I, the locations of collisions can be chosen in $M \cdot \binom{m}{2}$ ways.

There will be exactly $2^{(mM-1)n}$ ways to choose the sequence $(chain_0, F_0(chain_0)), \ldots, (chain_{mM-1}, F_{mM-1}(chain_{nm-1}))$ under chosen location of collision.

To substantiate this, we note that a collision will take place for any choice of cipher conversion. Due to the randomness of functions from the set $\mathcal{RF}^{n,n}$, the elements of the sequence $chain_0, \ldots, chain_{mM-1}$ are chosen randomly, equiprobably and independently of each other and run through the entire set of vectors $\{0,1\}^{mMn}$, whence, taking into account the collision, there will be $2^{(mM-1)n}$ of them.

Then

$$|C_I| \leq M \cdot \binom{m}{2} \cdot 2^{(mM-1)n} \cdot 2^{mMn}$$

In the set C_{II}, collision locations can be chosen in $\binom{M}{2} \cdot \binom{m}{2}$ ways. The number of ways to choose the left coordinates of the sequence $(Chain, \mathcal{RF}^{n,n})$ in this case is $2^{(mM-1)n}$.

Further, due to the randomness of the choice of functions from the set $\mathcal{RF}^{n,n}$, the elements of the form $F_l(chain_l)$ are chosen randomly, equiprobably and independently of each other and of the elements of the sequence $chain_0, \ldots, chain_{mM-1}$. Therefore, the number of ways to choose the right coordinates of the sequence $(Chain, \mathcal{F}^{n,n})$ does not depend on the choice of the left coordinates and is equal to $2^{(mM-1)n}$.

Hence,

$$|C_{II}| \leq \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{2(mM-1)n}$$

□

Statement 3.4. *Scheme of symmetric enciphering $MCFB^{ext}_{m,M}(\mathcal{RG},\mathcal{RF}^{n,n})$ over the set of random functions $\mathcal{RF}^{n,n}$ is $(t, q, \varepsilon^{MCFB^{ext}}_{m,M,n,q})$-LOR-CPA-secure, herewith*

$$q = mM,$$

$$\varepsilon_{m,M,n,q}^{MCFB^{ext}} = M \cdot \binom{m}{2} \cdot 2^{-n} + \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{-2n}$$

Proof. Denote by P_b the probability distributions arising from the execution of the LOR-CPA game with bit b. Then

$$\mathbf{Adv}_{\mathsf{D}_{lr}} = \mathbf{P}_0(e = 0) - \mathbf{P}_1(e = 0)$$

In the absence of a collision, each value $o_i = F_i(chain_i)$, $F_i \in \mathcal{F}^{n,n}$, is chosen randomly, equiprobably and independently of $c_0, \dots, c_{i-1}$, $m_0^b, \dots, m_i^b$. Therefore, the collision probability in round i does not depend on bit b, and we have:

$$\mathbf{P}_0(C) = \mathbf{P}_1(C)$$

Denote this value by $\mathbf{P}(C)$.

Note further that in the absence of a collision, the adversary chooses $e = 0$ equally likely for $b = 0$ and $b = 1$. Hence,

$$\mathbf{P}_0(e = 0 \mid \bar{C}) = \mathbf{P}_1(e = 0 \mid \bar{C})$$

Therefore, the expression for the advantage of the adversary D_{lr} can be represented as:

$$\begin{gathered} \mathbf{Adv}_{D_{lr}} = \\ = \mathbf{P}_0(e = 0 \mid C)\mathbf{P}_0(C) + \mathbf{P}_0(e = 0 \mid \bar{C})\mathbf{P}_0(\bar{C}) - \\ -\mathbf{P}_1(e = 0 \mid C)\mathbf{P}_1(C) - \mathbf{P}_1(e = 0 \mid \bar{C})\mathbf{P}_1(\bar{C}) = \\ = \mathbf{P}(C) \left(\mathbf{P}_0(e = 0 \mid C) - \mathbf{P}_1(e = 0 \mid C)\right) \le \mathbf{P}(C) \end{gathered}$$

It remains to take into account the fact that the set of all sequences of the form $(chain_i, F_i(chain_i))$, $i = \overline{0, mM-1}$, has cardinality 2^{2mMn} due to the fact that $\mathcal{RF}^{n,n}$ is the set of all random functions, and use Statement 3.3

Note that the time t can be chosen arbitrarily.

□

4 Counterexample to result by Abdalla–Bellare

Let's remember that according to [2, Theorem 1],

$$\mathbf{InSec}(CFB_m(\mathcal{RG}, \mathcal{RF}^{n,n})) = \binom{m}{2} \cdot 2^{-n}.$$

Hence, according to Statement 3.4,

$$\mathbf{InSec}(MCFB_{m,M}^{ext}(\mathcal{RG}, \mathcal{RF}^{n,n})) \le M \cdot \mathbf{InSec}(CFB_m(\mathcal{RG}, \mathcal{RF}^{n,n})) + \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{-2n},$$

or, more accurately,

$$\mathbf{InSec}(MCFB_{m,M}^{ext}(\mathcal{RG}, \mathcal{RF}^{n,n})) = M \cdot \mathbf{InSec}(CFB_m(\mathcal{RG}, \mathcal{RF}^{n,n})) + \Pr[C_{II} \setminus C_I].$$

Obviously,

$$0 < \Pr[C_{II} \setminus C_I] \le \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{-2n}.$$

Now we can discuss our discrepancies with the result of [1, Theorem 4.1]. As applied to our case, assuming $\mathcal{G} = \mathcal{RG}$ in the indicated theorem, we obtain that, according to their results, it should be:

$$\mathbf{InSec}(MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF}^{n,n})) = M \cdot \mathbf{InSec}(CFB_m(\mathcal{RG}, \mathcal{RF}^{n,n})).$$

Thus, [1, Theorem 4.1] does not contain the second term from the previous Statement 3.4, which reflects the cross-correlation of sections, the accumulation of material and the transition of quantity into quality, and not at all because it is proved in the indicated Theorem that it cannot be maybe.

Herewith both results are obtained in the same LOR-CPA model [1, page 15] : *Several (polynomial-time equivalent) defnitions for security of a symmetric encryption scheme under chosen-plaintext attack were given in [2]. We use one of them, called left-or-right security.*

Thus, we consider that the previous Statement 3.4 is a counterexample to [1, Theorem 4.1]

In our opinion, the reason for the erroneousness of this theorem lies in the method of hybrid experiments, which is used in the proof. More precisely, the reason is that the method of hybrid experiments is applicable only when the nature of the object under study allows its division into sub-objects and the reduction of the study of the original object to the study of a set of unrelated sub-objects within the framework of the security model used. Obviously, the method of hybrid experiments is applicable in the ROR-CPA model (real-or-random indistinguishibility under chosen plaintext attack), but, as the counterexample above shows, the method of hybrid experiments is not applicable in the LOR-CPA model, since it is obviously not able to capture the correlation between subobjects into which the original object is split.

As the topic of our next work we shall concern the correctness of [1, Theorem 4.1] under framework of ROR-CPA security model.

5 Strength of External MCFB Mode with Random Key Generator and Pseudo-Random Encryption Functions

Statement 5.1. *Let $\mathcal{F} : \{0,1\}^n \to \{0,1\}^n$ is (t', q', ε')-*PRF*-secure family of pseudo-random functions, $q' \leq m$. Then $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{F})$ is a (t, q, ε)-LOR-CPA-secure scheme of symmetric encryption. Herewith $q = q' \cdot M$, $t = Mt' + \mathrm{o}(t')$,*

$$\varepsilon = 2M\varepsilon' + \varepsilon^{MCFB^{ext}}_{m,M,n,q}$$

Proof. The proof is carried out in exactly the same way as the proof of [2, Theorem 1].

The main idea of the proof is that if for the mode $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{F})$ there exists a left-right distinguisher for the mode with a random generator over the set of pseudo-random functions, better than the distinguisher under above bounds, then it can be used to construct a distinguishing algorithm between the set of pseudo-random functions $\mathcal{F}$ and the set of all random functions.

Let D_{lr} is the left–right distinguisher between enciphering schemes $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{F})$ and $MCFB^{ext}_{m,M}(\mathcal{RG}, \mathcal{RF})$, such that

$$\mathsf{Adv}^{\mathrm{lor-cpa}}_{D_{lr}}(n) > 2M\varepsilon' + \varepsilon^{MCFB^{ext}}_{m,M,n,q}$$

Based on it, we construct a distinguisher D_{prf} of M–sets of functions from $\mathcal{F}$ and $\mathcal{RF}$, respectively:

```
$\mathsf{D}_{prf}$
$Seeding$
    $b \leftarrow\!\!\$\, \{0,1\}$
    $\{f_1, \dots, f_M\} \leftarrow\!\!\$\, \mathcal{RF}$
$Working$
for $j = \overline{1, M}$ do
    for $i = \overline{1, q'}$ do
        $\mathsf{D}_{lr} \xrightarrow{m_i^0; m_i^1} \mathsf{D}_{prf}$
        $\mathsf{D}_{prf} \xrightarrow{m_i^b} \mathcal{CFB}(\mathfrak{F}_{f_j})$
        $\mathcal{CFB}(\mathfrak{F}_{f_j}) \xrightarrow{c_i} \mathsf{D}_{lr}$
    endfor
endfor
$\mathsf{D}_{lr} \xrightarrow{e} \mathsf{D}_{prf}$
$\mathsf{D}_{prf}: \quad e^* \leftarrow (e \neq b)$
$\mathsf{D}_{prf} \xrightarrow{e^*}$ Output
```

Here $\mathcal{CFB}(\mathfrak{F}_{f_j})$ is an oracle simulating the operation of the CFB mode with the encryption function f_j. For each pair of values i, j, this oracle, and, accordingly, the oracle $\mathfrak{F}_{f_j}$, is accessed only once, that is, the distinguisher D_{prf} produces exactly Mq' calls to the oracle simulating the $\{f_1, \dots, f_M\}$ family of functions in a time not exceeding $M \cdot t'$.

For $G \in \{\mathcal{RF}, \mathcal{F}\}$ denote by $\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(G)$ the advantage of the corresponding distinguisher in the LOR-CPA game against the mode encryption $MCFB_{m,M}^{ext}(\mathcal{RG}, G)$, and through $\Pr_G$ the corresponding probability distribution.

Then the advantage of the adversary D_{prf} is as follows:

$$\mathsf{Adv}_{\mathsf{D}_{\mathsf{PRF}}} = \Pr\nolimits_{\mathcal{F}}[e^* = 0] - \Pr\nolimits_{\mathcal{RF}}[e^* = 0]\,.$$

Further,

$$\Pr\nolimits_G[e^* = 0] = \Pr\left[e^* = 0 \,\middle|\, \{f_1, \dots, f_M\} \leftarrow\!\!\$\, G,\ e^* \leftarrow \mathsf{D}_{\mathsf{PRF}}^{\{f_1,\dots,f_M\}}\right] =$$

$$= \Pr\left[e = b \,\middle|\, b \leftarrow\!\!\$\, \{0,1\},\ \{f_1, \dots, f_M\} \leftarrow\!\!\$\, G,\ e \leftarrow \mathsf{D}_{lr}^{\mathcal{MCFB}^{\rceil\S\sqcup}(\mathfrak{F})_{\{f_1,\dots,f_M\},b}}\right].$$

Therefor $b, \{f_1, \dots, f_M\}$ are chosen independently and equiprobably, parameter b is chosen first, we have:

$$\Pr\nolimits_G[e^* = 0] = \frac{1}{2} \sum_{b \in \{0,1\}} \Pr\left[\mathsf{D}_{lr}^{\mathcal{MCFB}^{\rceil\S\sqcup}(\mathfrak{F})_{\{f_1,\dots,f_M\},b}} = b \,\middle|\, \{f_1, \dots, f_M\} \leftarrow\!\!\$\, G\right] =$$

$$= \frac{1}{2}\left(\Pr\left[\mathsf{D}_{lr}^{\mathcal{MCFB}^{]\S\sqcup}(\mathfrak{F})\{f_1,\dots,f_M\},0} = 0 \,\middle|\, \{f_1,\dots,f_M\} \leftarrow_{\$} G\right]\right.$$

$$\left. +1 - \Pr\left[\mathsf{D}_{lr}^{\mathcal{MCFB}^{]\S\sqcup}(\mathfrak{F})\{f_1,\dots,f_M\},1} = 0 \,\middle|\, \{f_1,\dots,f_M\} \leftarrow_{\$} G\right]\right) =$$

$$= \frac{1}{2} + \frac{1}{2}\mathsf{Adv}_{\mathsf{D}_{lr}}(G).$$

According to assumption,

$$\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{F}) > \varepsilon.$$

According to Statement (3.4),

$$\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{RG}) \le \varepsilon_{m,M,n,q}^{MCFB^{ext}}.$$

Hence,

$$\mathsf{Adv}_{\mathsf{D}_{\mathsf{PRF}}} = \frac{1}{2}\left(\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{F}) - \mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{RG})\right) > \frac{1}{2}(\varepsilon - \varepsilon_{m,M,n,q}^{MCFB^{ext}}) = M \cdot \varepsilon'.$$

On the other hand, due to the independence of the choice of the functions $f_1, \dots, f_M$,

$$\mathsf{Adv}_{\mathsf{D}_{\mathsf{PRF}}} \le M \cdot \mathbf{InSec}^{\mathsf{PRF}}(\mathcal{F}; t', q') = M \cdot \varepsilon'.$$

It is contradiction with choice of D_{lr}.
The Statement is proven. □

6 Strength of External MCFB Mode with Serial Key Generator and Pseudo-Random Encryption Functions

Statement 6.1. *Let $\mathcal{F} : \{0,1\}^n \to \{0,1\}^n$, $\mathcal{G} : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$. Let $MCFB_{m,M}^{ext}(\mathcal{RG}, \mathcal{F})$ is a (t, q, ε)-LOR-CPA-secure encryption scheme with $q = mM$.*

Then $MCFB_{m,M}^{ext}(\mathcal{SG}[\mathcal{G}], \mathcal{F})$ is a $(t + \log_2 M, q, \varepsilon')$-LOR-CPA-secure symmetric encryption scheme. wherein

$$\varepsilon' = 2M\mathbf{Insec}^{\mathsf{PRF}}(\mathcal{G}; t + \log_2 M, 2) + \varepsilon.$$

Proof. The proof is carried out in exactly the same way as the proof of Statement 5.1.

Let D_{lr} be the left-right distinguisher of $MCFB_{m,M}^{ext}(\mathcal{SG}[\mathcal{G}], \mathcal{F})$ and $MCFB_{m,M}^{ext}(\mathcal{RG}, \mathcal{F})$ encryption schemes, such that

$$\mathsf{Adv}_{D_{lr}}^{\mathrm{lor-cpa}} > 2M\mathbf{Insec}^{\mathsf{PRF}}(\mathcal{G}; t + \log_2 M, 2) + \varepsilon$$

Based on it, we construct the distinguisher D_{prg} of sequential and random key generators:

```
$\mathsf{D}_{prg}$

Seeding
  $b \leftarrow_{\$} \{0,1\}$
  $\{K_1, \dots, K_M\} \leftarrow_{\$} \{0,1\}^k$
Working
for $j = \overline{1, M}$ do
  for $i = \overline{1, m}$ do
      $\mathsf{D}_{lr} \xrightarrow{m_i^0; m_i^1} \mathsf{D}_{prg}$
      $\mathsf{D}_{prg} \xrightarrow{m_i^b} \mathcal{CFB}(\mathfrak{F}_{K_j})$
      $\mathcal{CFB}(\mathfrak{F}_{K_j}) \xrightarrow{c_i} \mathsf{D}_{lr}$
  endfor
endfor
 $\mathsf{D}_{lr} \xrightarrow{e} \mathsf{D}_{prg}$
$\mathsf{D}_{prg}$ :  $e^* \leftarrow (e \neq b)$
 $\mathsf{D}_{prg} \xrightarrow{e^*}$ Output
```

Here $\mathcal{CFB}(\mathfrak{F}_{K_j})$ is an oracle simulating the operation of the CFB mode with the encryption function $\mathcal{F}_{K_j}$. For each pair of values i, j, this oracle, and, accordingly, the oracle $\mathfrak{F}_{K_j}$, is accessed only once, that is, the distinguisher D_{prg} produces exactly q queries to the oracle simulating the family of functions $\{\mathcal{F}_{K_1}, \dots, \mathcal{F}_{K_M}\}$ in a time not exceeding t.

For $G \in \{\mathcal{SG}[\mathcal{G}], \mathcal{RG}\}$ denote by $\mathsf{Adv}^{\mathrm{lor-cpa}}_{\mathsf{D}_{lr}}(G)$ the advantage of the corresponding distinguisher in the LOR- CPA game against the encryption mode $MCFB^{ext}_{m,M}(G, \mathcal{F})$, and through Pr_G the corresponding probability distribution.

Then the advantage of the adversary D_{prg} is as follows:

$$\mathsf{Adv}_{\mathsf{D}_{\mathsf{PRG}}} = \mathrm{Pr}_{\mathcal{SG}[\mathcal{G}]}\left[e^* = 0\right] - \mathrm{Pr}_{\mathcal{RG}}\left[e^* = 0\right].$$

Further,

$$\mathrm{Pr}_G[e^* = 0] = \mathrm{Pr}\left[e^* = 0 \;\middle|\; \{K_1, \dots, K_M\} \leftarrow_{\$} G,\ e^* \leftarrow \mathsf{D}_{\mathsf{PRG}}^{\{K_1,\dots,K_M\}}\right] =$$

$$= \mathrm{Pr}\left[e = b \;\middle|\; b \leftarrow_{\$} \{0,1\},\ \{K_1, \dots, K_M\} \leftarrow_{\$} G,\ e \leftarrow \mathsf{D}_{lr}^{\mathcal{MCFB}^{\rceil\S\sqcup}(\mathfrak{F})_{\{K_1,\dots,K_M\},b}}\right].$$

Since $b, \{K_1, \dots, K_M\}$ are chosen independently and equiprobably, parameter b is chosen first, we have:

$$\mathrm{Pr}_G[e^* = 0] = \frac{1}{2} \sum_{b \in \{0,1\}} \mathrm{Pr}\left[\mathsf{D}_{lr}^{\mathcal{MCFB}^{\rceil\S\sqcup}(\mathfrak{F})_{\{K_1,\dots,K_M\},b}} = b \;\middle|\; \{K_1, \dots, K_M\} \leftarrow_{\$} G\right] =$$

$$= \frac{1}{2}\Bigg(\mathrm{Pr}\left[\mathsf{D}_{lr}^{\mathcal{MCFB}^{\rceil\S\sqcup}(\mathfrak{F})_{\{K_1,\dots,K_M\},0}} = 0 \;\middle|\; \{K_1, \dots, K_M\} \leftarrow_{\$} G\right]$$

$$+1 - \Pr\left[\mathsf{D}_{lr}^{\mathcal{MCFB}^{\rceil\S\sqcup}(\mathfrak{F})_{\{K_1,\ldots,K_M\},1}} = 0 \,\middle|\, \{K_1,\ldots,K_M\} \leftarrow_{\$} G\right]\Bigg) =$$

$$= \frac{1}{2} + \frac{1}{2}\mathsf{Adv}_{\mathsf{D}_{lr}}(G).$$

According to the assumption

$$\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{SG}[\mathcal{G}]) > \varepsilon'.$$

According to the condition of the Statement,

$$\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{RG}) \leq \varepsilon.$$

Hence,

$$\mathsf{Adv}_{\mathsf{D}_{\mathsf{PRG}}} = \frac{1}{2}\left(\mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{SG}[\mathcal{G}]) - \mathsf{Adv}_{\mathsf{D}_{lr}}^{\mathrm{lor-cpa}}(\mathcal{RG})\right) > \frac{1}{2}(\varepsilon' - \varepsilon) = M \cdot \mathbf{Insec}^{\mathsf{PRF}}(\mathcal{G}; t + \log_2 M, 2).$$

From the other side of view, according to [1, Theorem 2.5],

$$\mathsf{Adv}_{\mathsf{D}_{\mathsf{PRG}}} \leq M \cdot \mathbf{Insec}^{\mathsf{PRF}}(\mathcal{G}; t + \log_2 M, 2).$$

We got a contradiction with the choice of D_{lr}.
The Statement has been proven.

□

7 Summary

Let us now combine the results of Statements 3.4,5.1,6.1.

Theorem 7.1. *Let $\mathcal{F} : \{0,1\}^n \to \{0,1\}^n$, $\mathcal{G} : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$. Then for arbitrary time complexity t $MCFB_{m,M}^{ext}(\mathcal{SG}[\mathcal{G}], \mathcal{F})$ is a $(t + \log_2 M, mM, \varepsilon)$-LOR-CPA-secure symmetric encryption scheme. wherein*

$$\varepsilon = 2M\mathbf{Insec}^{\mathsf{PRF}}(\mathcal{G}; t + \log_2 M, 2) + 2M\mathbf{Insec}^{\mathsf{PRF}}(\mathcal{F}; t/M, m) + M \cdot \binom{m}{2} \cdot 2^{-n} + \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{-2n}.$$

Corollary 7.2. *Let $E = \{E_K \mid K \in \{0,1\}^k\}$ is a block cipher. Then for arbitrary time complexity t $MCFB_{m,M}^{ext}(\mathcal{SG}[E], E)$ is a $(t + \log_2 M, mM, \varepsilon)$-LOR-CPA-secure symmetric encryption scheme. wherein*

$$\varepsilon = 2M\mathbf{Insec}^{\mathsf{PRF}}(E; t + \log_2 M, 2) + 2M\mathbf{Insec}^{\mathsf{PRF}}(E; t/M, m) + M \cdot \binom{m}{2} \cdot 2^{-n} + \binom{M}{2} \cdot \binom{m}{2} \cdot 2^{-2n}.$$

Corollary 7.3. *Let $E = \{E_K \mid K \in \{0,1\}^k\}$ is a block cipher, $k = 4n$. Then for arbitrary time complexity t $PRNG(\mathcal{SG}, CFB)$ (1) is a $(t + \log_2 M, 4 \cdot M, \varepsilon)$-LOR-CPA-secure symmetric encryption scheme. wherein*

$$\varepsilon = 2M\mathbf{Insec}^{\mathsf{PRF}}(E; t + \log_2 M, 2) + 2M\mathbf{Insec}^{\mathsf{PRF}}(E; t/M, 4) + \frac{6M}{2^n} + \frac{3M(M-1)}{2^{2n}}.$$

References

[1] Michel Abdalla, Mihir Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-Keying Techniques”, *Lecture Notes in Computer Science*, ASIACRYPT 2000, **1976**, ed. Tatsuaki Okamoto, Springer-Verlag, Berlin, Heidelberg, 2000 https://cseweb.ucsd.edu/~mihir/papers/rekey.pdf.

[2] Ammar Alkassar, Alexander Geraldy, Birgit Pfitzmann, and Ahmad-Reza Sadeghi, “Optimized self-synchronizing mode of operation”, *Lecture Notes in Computer Science*, FSE; 2000, **2355**, ed. Mitsuru Matsui, Springer, Berlin, Heidelberg, 2001, ISBN: 3-540-43869-6.

[3] M. Bellare and B. Yee, “Forward security in private key cryptography”, *Cryptology ePrint Archive*, **Report 2001/035**, IACR, 2001 http://eprint.iacr.org/2001/035.

[4] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, “A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation”, 38th Symposium on Foundations of Computer Science (FOCS), 1997, 394—403.

[5] “DES Modes of Operation”, *Federal Information Processing Standards Publication*, **81 (FIPS PUB 81)**, NIST, December 2, 1980.

[6] Mark Wooding,, “New proofs for old modes”, *Cryptology ePrint Archive*, **Report 2008/121**, IACR, 2008 https://ia.cr/2008/121.

[7] “Re-keying Mechanisms for Symmetric Keys”, *Request for Comments*, **8645**, ed. S. Smyshlyaev, Internet Research Task Force (IRTF), August 2019.

[8] *GOST 34.12–2012 Cryptographic Protection for Information Processing Systems. Government Standard of the Russian Federation. Government Committee of the RF for Standards*, 2012, In Russian.

[9] *GOST 34.13–2015 Cryptographic Protection for Information Processing Systems. Government Standard of the Russian Federation. Government Committee of the RF for Standards*, 2015, In Russian.