

IMPROVED BLOCK CIPHER COUNTER MODE OF OPERATION SCHEMES

by

IVAN GORBENKO

Kharkov National University of Radioelectronics, Ukraine

and

SERGIY GOLOVASHYCH

Kharkov National University of Radioelectronics, Ukraine

E-mail: serg_golov@mail.ru

Abstract The main goals of presented research were the analysis of the base block cipher protectability from cryptanalytic attacks in standard modes of operation and the ways to increase the stream modes of operation security. We also paid special attention to the problem of the gamma overlapping. Therefore, we selected the counter mode as a basis for the new perspective modes, and investigated its property for the case of multiple encryption restarts with the same key. As result of our research, we are proposing two new schemes of modes of operation. They have advanced security.

Keywords: Cryptography / block ciphers / modes of operation / Counter mode (CTR) / known plaintext attacks / gamma period / gamma overlapping.

1. INTRODUCTION

Modern computer systems are often used for processing, storing and transferring restricted information. These information systems have certain safety requirements and should maintain confidentiality. The easiest way of solving this problem in open systems is using cryptography.

One of the essential components of the modern cryptographic security systems is the symmetric ciphers. They are divided into two classes: stream ciphers and block ciphers.

The block ciphers are more widespread in open computer systems, but the classical stream ciphers usually are hardware implementation oriented, secret and used in special-purpose communication systems.

The block cipher can be considered as key-dependent permutation on a set of binary vectors corresponding to separate blocks. For the purpose of weakness elimination of permutation ciphers, for block ciphers several modes of operation were designed. They are intended for processing a large amount of information. These modes actually define the schemes of stream ciphering on basis of a block cipher.

The most effective classes of cryptanalytical attacks on block ciphers are “known plaintext” and “chosen plaintext” attacks. They assume that cryptanalyst knows the plaintext that corresponds to the intercepted cryptogram or can control the data input of the cipher respectively. As a

result of this the security of block cipher-based stream cipher depends on both the block cipher security and the properties of the mode of operation scheme.

The main goals of our research were the analysis of the base block cipher protectability from cryptanalytic attacks in standard modes of operation and the ways to increase the stream modes of operation security. We also paid special attention to the problem of the gamma overlapping; therefore, we selected the counter mode as a basis for the new perspective modes. The counter mode is a unique mode of operation, which has the “fixed period” and the “random access” properties. We investigated its property for the case of multiple encryption restarts with the same key. As result of our research, we are proposing two new schemes of modes of operation. They have advanced security.

2. NOTATION

In the article we used following notation:

E – block cipher encryption: $O_i = E_K(I_i)$; D – block cipher decryption: $I_i = D_K(O_i)$; G – generator of “synchronization sequences”;

K – secret key for block cipher;

I_i – input block to base block cipher;

O_i – output block from base block cipher;

Γ_i – one block of encryption gamma;

M_i – one block of plaintext (message);

C_i – one block of cryptogram;

IV – initialization vector; S_i – internal state of stream cipher;

n – bit-size of base cipher block;

m – bit-size of gamma-output block;

r – bit-size of feedback.

According to the NIST Sp. Pub. №800-38A [1], it is specified 5 modes of operation (and see also [2,3,4,5]). The first of them (ECB) is a pure block cipher; all other modes define stream ciphers. Let’s consider each of them and analyze the possibility to extract the base cipher input and output values from the known plaintext and cipher text. If this is possible for some mode then the class of known plaintext attacks is applicable to this mode.

3. THE OUTPUT FEEDBACK MODE

On all following layouts of modes of operation the encryption transformation is presented at the left and the decryption is at the right. The Output Feedback (OFB) mode defines synchronous stream cipher (Figure 1).

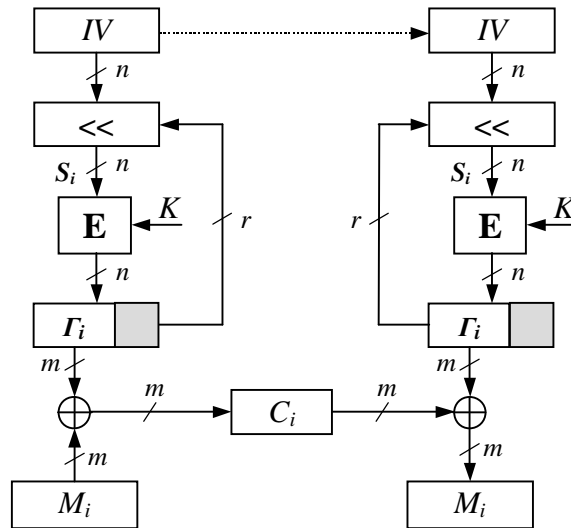


Figure 1. The Output Feedback Mode

The next block of gamma is determined by one or a few of the preceding blocks of gamma. As we can see from the expressions the output of base cipher can be obtained as XOR of cryptogram and known plaintext blocks, but input of base cipher at current step equal to its previous output.

Known plaintext attack ($m = r = n$):

$$I_i = O_{i-1}, \quad O_i = C_i \oplus M_i, \quad I_0 = IV$$

Therefore, the OFB mode doesn't protect the base cipher from known plaintext attacks.

4. THE CIPHER FEEDBACK MODE

The Cipher Feedback (CFB) mode defines self-synchronized stream cipher (Figure 2).

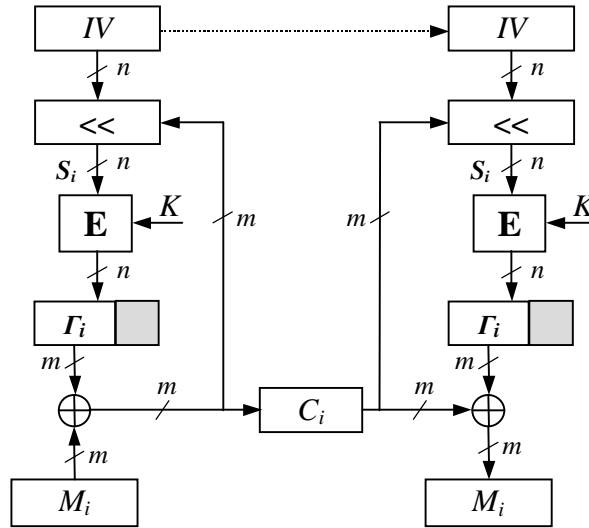


Figure 2. The Cipher Feedback Mode

The next block of gamma is determined by one or a few preceding blocks of cryptogram. The output of the base cipher, as before, can be obtained as XOR of cryptogram and known plaintext blocks, and input of the base cipher at current step is the previous cryptogram block.

Known plaintext attack ($m = n$):

$$I_i = C_{i-1}, \quad O_i = C_i \oplus M_i, \quad I_0 = IV$$

Therefore, the CFB mode doesn't protect base cipher from the known plaintext attacks too.

5. THE CIPHER BLOCK CHAINING MODE

The Cipher Block Chaining (CBC) mode (Figure 3) utilizes the scheme that is the inverse to CFB mode therefore it has similar property. The input of the base cipher can be obtained as XOR of the previous cryptogram block and the current plaintext block, but the output of the base cipher corresponds to the cryptogram block. So the CBC mode also doesn't protect base cipher from the known plaintext attacks.

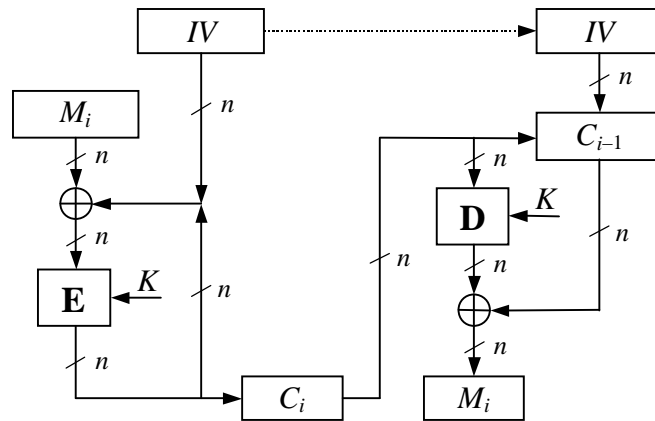


Figure 3. The Cipher Block Chaining Mode

Known plaintext attack:

$$I_i = C_{i-1} \oplus M_i, \quad O_i = C_i$$

6. THE COUNTER MODE

The last standard mode is the Counter (CTR) mode. The layout that is shown on the Figure 4 describes the CTR mode with the secret synchronization sequence. The same scheme is utilized at the 2nd mode of GOST 28147-89. The blocks of gamma are produced by means of the base block encryption of corresponding blocks of the synchronization sequence. The synchronization sequence (S) is produced from the encrypted initial vector (IV) using some recurrent generator (G). In the easiest case the generator G can be defined as the simple n -bit-length summary counter with fixed increment value (W). We shall call this value *the one-step "weight" value*. The module of such generator is equal to the n -th power of two.

In the same way as the OFB mode, the base cipher output can be obtained as XOR of cryptogram and known plaintext. Its input values can't be obtained, but the differences between them are known and potentially it can be used for mounting some differential attack. Therefore, the Counter mode also doesn't protect base cipher from the known plaintext attacks.

Known **plaintext** **attack** $(m = n)$: $I_i = ?$, $\forall i: \Delta I_{i,i+1} = W$, $O_i = C_i \oplus M_i$

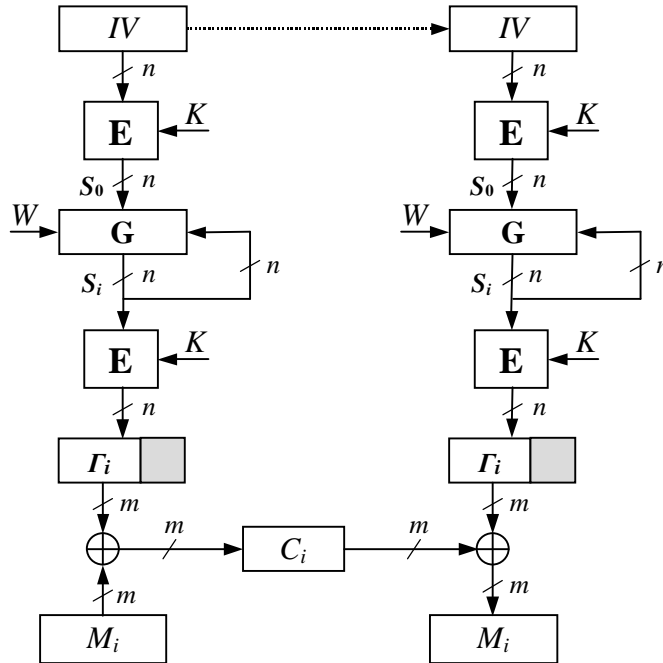


Figure 4. The Counter Mode

7. “FIXED STEP COUNTERS” Let’s consider internal structure of the generator G. As it was mentioned above, in the simplest case it can be simple summary counter with fixed increment value (W). It is quite enough to produce suitable synchronization sequence, because the single requirement for that sequence is to have no repetition on a given length. Such generator can be described by the next recurrent expression:

$$S_i = (S_{i-1} + W) \bmod 2^n,$$

where S_i – internal state at step i ;
 W – one step “weight” value.

We call such generator the “Fixed Step Counter”, because its parameter W is fixed within the bounds of one sequence.

As we can see from the following expression:

$$S_i = (S_0 + W \times i) \bmod 2^n,$$

the difference between any pair of the elements is fixed and can be expressed from the parameter W . Potentially this property can be used for the differential cryptanalysis, especially when the W is known.

We can divide Fixed Step Counters on two classes by usage period of step “weight” value (W):

1. **Constant public parameter W** (in this case, the parameter W is a part of the mode).
2. **Variable (session) secret parameter W** (it changes together with IV at each session).

Let’s consider the periodic properties of each of them.

7.1. Period of Fixed Step Counters Let’s consider the rules of step “weight” value selecting. Let’s assume that message length is always limited by L_{max} blocks, and make use of following notations: the required quantity of binary digits for representing value L_{max} denoted by small letter l , the period of generator denoted by capital letter T . Moreover, the value of l must be at the least four times less than block-bit-length n .

$$T = 2^n / (W, 2^n), \quad l = \lceil \log_2 (L_{max} + 1) \rceil, \quad l \leq n/4$$

7.1.1. Constant Public “Weight”

If the used value of parameter W is odd, then the period of binary counter is maximum and equal to the transformation module. For the first case the step “weight” value is constant and public, therefore parameter W may be any odd number with a respective width. In that case, an assaulter knows parameter W and can calculate the difference between any pair of counter states S_i .

$$W = 2 \times x + 1 \Rightarrow (W, 2^n) = 1 \Rightarrow T = 2^n$$

The difference is calculated at the ring of natural numbers by the module n -th power of two.

Assaulter knowledge: $\Delta S_{i,j} = W \times (j - i) \bmod 2^n$. **7.1.2. Variable (Session) Secret “Weight”**

In the second case, the parameter W is secret; therefore, it must be generated randomly. It must also satisfy to some requirements in order to provide a period that is larger than L_{max} .

The period of the counter is inversely proportional to the greatest common divisor of the module and increment value W . We propose next very simple procedure to form parameter W :

1. Generate a random n -bit-length number.

$$R \leftarrow \text{RANDOM}$$

2. If the $n-l$ least significant bits are zero, then set the least significant bit to one.

$$R = x \times 2^{n-l} + y$$

$$W \leftarrow \begin{cases} R, & y > 0 \\ R \vee 1, & y = 0 \end{cases} \Rightarrow T > L_{\max}$$

The number is produced by this way can be used as secret parameter W .

In the second case, the assaulter knows only that the differences between generator states S_i located at on the same distance are equal. This considerably decreases the assaulter known information in comparison to the first case.

Assaulter knowledge: $\forall i, j, t: \Delta S_{i, i+t} = \Delta S_{j, j+t}$.7.2. **Gamma**

Overlapping Let's consider the problem of gamma overlapping.

The **gamma overlapping** term we shall use for designation of the event that consists of a block repetition within one of the sequences of encryption gamma or at least two blocks repetition in any pair of different sequences, produced by the same key.

For the task simplification, consider the counter mode construction where the encryption-gamma utilizes the full output block of base cipher. In this case, taking into consideration that the block encryption is bijective mapping we may replace the gamma overlapping problem by the synchronization sequence overlapping problem and may consider only generator G accordingly.

As stated above blocks repetition within of one sequence can be prevented by appropriate selection of W parameter.

Now let's consider the overlapping event of two synchronization sequences for both case of counter mode building.

7.2.1. Gamma Overlapping Event for Constant Step “Weight” For the first case when the step “weight” value is constant, we have following situation (Figure 5). If two different synchronization sequences i and j have at least one (not last) common element than all elements following to them coincide in pairs. In that way *the overlapping event depend from the sequences start points only.*

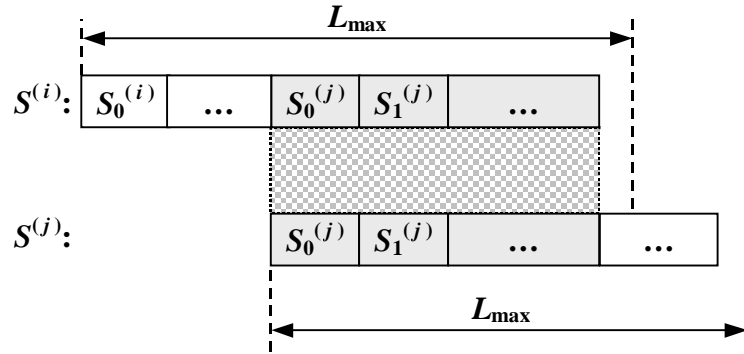


Figure 5. Gamma overlapping event for Constant step “weight”

Gamma overlapping condition:

$$\left| S_0^{(i)} - S_0^{(j)} \right| \leq W \times (L_{\max} - 2)$$

Overlapping probability for one pair of sequences:

$$P_{1\max} = \frac{2 \times L_{\max} - 3}{2^n} \cong 2^{-(n-l-1)}$$

Overlapping probability for multitude sequences:

$$P_{\max} = P_{1\max} \times (N^2 - N) / 2$$

From the overlapping probability expressions, we derive expressions for Allowable number of cipher restarts without key change:

$$N_A \approx \sqrt{2 \times P_A / P_{1\max}} = \sqrt{2^{n-l} \times P_A}$$

where P_A – allowable overlapping probability.

7.2.2. Gamma Overlapping Event for Variable Step “Weight” For the second case when the step “weight” value is variable, we have another situation (Figure 6). The one pair coincidence of not last elements isn’t enough for the overlapping event occurs. Distances to the elements of next coincident pair depend from the correlation between step “weight” values used for the sequences producing. In order to overlapping event is possible

the distances between elements of the nearest coincident pairs must be less than L_{\max} . In that way the overlapping event depends from both the sequences start points and the correlation between step “weight” values.

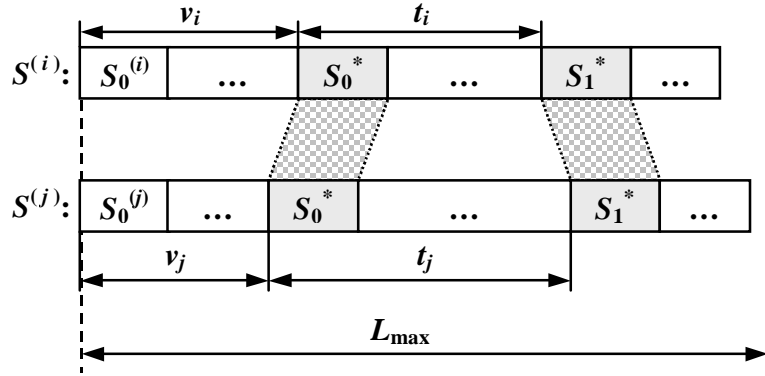


Figure 6. Gamma overlapping event for Variable step “weight”

Gamma overlapping condition:

$$\left\{ \begin{array}{l} S_{v_i}^{(i)} = S_{v_j}^{(j)} = S_0^* \\ S_{v_i+t_i}^{(i)} = S_{v_j+t_j}^{(j)} = S_1^* \\ (v_i + t_i) \leq L_{\max} \\ (v_j + t_j) \leq L_{\max} \\ t_i \neq 0, \quad t_j \neq 0 \\ S_0^* = S_1^* \end{array} \right. \Rightarrow \left\{ \begin{array}{l} t_j \times W_j - t_i \times W_i \equiv 0 \pmod{2^n} \\ v_j \times W_j - v_i \times W_i \equiv \Delta S_0^{(i,j)} \pmod{2^n} \\ (v_i + t_i) \leq L_{\max}, \quad (v_j + t_j) \leq L_{\max} \\ t_i \neq 0, \quad t_j \neq 0 \end{array} \right.$$

where t_i – minimum number of steps between repeated states;

v_i – minimum number of steps to first repeated state;

$\Delta S_0^{(i,j)}$ – initial states difference:

$$\Delta S_0^{(i,j)} = (S_0^{(i)} - S_0^{(j)}) \pmod{2^n}. \text{Gamma overlapping condition 1:}$$

$$\left\{ \begin{array}{l} t_j \times W_j - t_i \times W_i \equiv 0 \pmod{2^n} \\ 0 < t_i \leq L_{\max}, \quad 0 < t_j \leq L_{\max} \end{array} \right. \text{1st condition fulfillment probability:}$$

$$P'_{1\max} = L_{\max}^2 / 2^n \text{Gamma overlapping condition 2:}$$

$$\begin{cases} v_j \times W_j - v_i \times W_i \equiv \Delta S_{i,j}^{(0)} \pmod{2^n} \\ 0 \leq v_i < L_{\max}, \quad 0 \leq v_j < L_{\max} \end{cases} \text{2nd condition fulfillment probability:}$$

$$P_{1\max}'' = (L_{\max} + 1)^2 / 2^n \text{ Overlapping probability for one pair of sequences:}$$

$$P_{1\max} \cong \frac{1}{2} \times \left(\frac{3}{4} \times \frac{L_{\max}^2}{2^n} \right)^2 \cong \frac{1}{4} \times \frac{L_{\max}^4}{2^{2n}} \cong 2^{-(2n-4l+2)} \text{ Overlapping probability}$$

for multitude sequences:

$P_{\max} = P_{1\max} \times (N^2 - N) / 2$ From the overlapping probability expressions, we derive expressions for Allowable number of cipher restarts without key change:

$$N_A \approx \sqrt{2 \times P_A / P_{1\max}} = 2^{n-2l+1} \times \sqrt{2 \times P_A},$$

where P_A – allowable overlapping probability.

In the Table 1, the estimated values of upper bounds of the gamma overlapping probability for one pair of sequences ($P_{1\max}$) and the allowable number of cipher restarts with same key (N_A) are presented. Taking into account the limitation on the value l , which must be at most a quarter of the value n we can see that the overlapping probability of one pair of sequences for the case of variable W is significantly smaller than for the case of constant W .

Table 1. Upper bounds of the gamma overlapping properties

Counter type	$P_{1\max}$	N_A
<i>Constant</i> step “weight”	$2^{-(n-l-1)}$	$\sqrt{2^{n-l} \times P_A}$
<i>Variable</i> step “weight”	$2^{-(2n-4l+2)}$	$2^{n-2l+1} \times \sqrt{2 \times P_A}$

7.2.3. Gamma Overlapping for IP-Traffic Encryption by Counter Mode To illustrate considerable difference of overlapping probability between these two variants of counter mode, consider the example of the gamma overlapping properties calculation for the case of IP-traffic encryption.

$$\begin{aligned} \text{Block length } n &= 128 \text{ bit} & \text{1 day} &= 2^{16,4} \text{ sec.} \\ \text{Min. packet size} &= 28 \text{ byte,} & \text{Max. packet size} &= 2^{16} \text{ byte} \\ L_{\max} &= (2^{16} \cdot 8) / 128 = 2^{12} \text{ blocks} & l &= 12 \end{aligned}$$

We assumed the each packet is a separate message with individual session parameters. It is used following notation: subscript *CSW* means the *Constant Step “Weight”* and subscript *VSW* means the *Variable Step “Weight”*.

We performed calculation of overlapping probability for two most widespread cases of transfer rate: 100 Mbps and 1 Gbps. For shown results we assumed that all packets have maximal size, but P_{CSW} -values can be slightly less if we accept model with minimal packet size. As you can see the absolute value of binary logarithm of overlapping probability for the Variable step “weight” in two and half times more then for the Constant step “weight”.

The upper bounds of the gamma overlapping probability:

$$\begin{aligned}
 P_{CSW} &\approx 2^{-115} \times N^2 : & 100 \text{ Mbps} : & P_{CSW} \approx 2^{-67} \times D^2 \\
 & & 1 \text{ Gbps} : & P_{CSW} \approx 2^{-60} \times D^2 \\
 P_{VSW} &\approx 2^{-210} \times N^2 : & 100 \text{ Mbps} : & P_{VSW} \approx 2^{-162} \times D^2 \\
 & & 1 \text{ Gbps} : & P_{VSW} \approx 2^{-155} \times D^2
 \end{aligned}$$

where D – days number in one key usage period.

The allowable number of cipher restarts:

$$N_{A, CSW} \approx 2^{58} \times \sqrt{P_A}$$

$N_{A, VSW} \approx 2^{105,5} \times \sqrt{P_A}$ So the Variable “weight” counter has two advantages under the Constant “weight” counter:

- 1) the step “weight” value is unknown for assaulter;
- 2) the gamma overlapping probability for the case of multi-session key usage is incomparably smaller.

The main drawback of the Variable step “weight” counter is the two times increasing of the session initialization vector.

8. CONSTRUCTION PRINCIPLES OF SECURE STREAM CIPHERING MODES

Now consider the ways of security improving of stream modes of operation. As was shown above the all standard modes of operation allow application of the known plaintext attack to their base block cipher. And also synchronous OFB mode doesn't guarantee the some lower bound of gamma's period.

On purpose to eliminate the mentioned defects of the standard modes of operation, we have defined three design principles of construction stream modes with advanced security:

- Gamma's period must always satisfy some lower bound (T_{min}) independently from used key and initialization vector.
- The state change function (same as the gamma output function) must be non-linear and key dependent.
- The cipher must hide self internal state, i.e. the states' space must exceed the gamma-output block space.

Common structure of "secure" stream cipher, which satisfies mentioned principles, is presented on Figure 7.

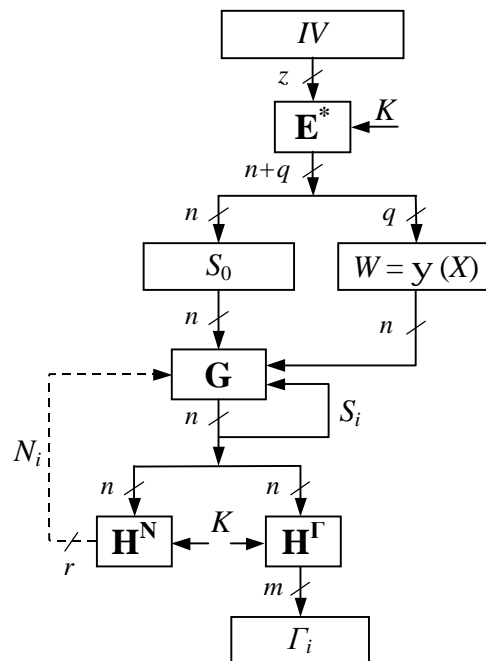


Figure 7. Common structure of "secure" stream cipher

At Figure 7 are used following additional symbols:

N_i – number of steps to the next state $i+1$;

G_i – gamma-output block;

ψ – "weight"-selection function;

E^* – init encryption function;

H^N – keyed feedback function;

HG – keyed gamma-output function. **9. “DYNAMIC STEP COUNTER”** In concordance with these principles we propose the new construction of stream modes. We called it the “Dynamic Step Counter”. It has following analytical description:

$$\begin{aligned}
 S_{i+1} &= (S_i + W \times N_i) \bmod 2^n \\
 N_i &= f_K(S_i), \quad 0 < N_i < 2^r, \quad r + m \leq n \\
 W &= 2^{n/2} + 2^{n/4+1} + 1 \quad (\text{for } r = n/2) \\
 (W, 2^n) &= 1 \Rightarrow 2^{n-r} < T \leq 2^n
 \end{aligned}$$

where S_i – internal state at step i ;
 W – one step “weight” value;
 N_i – number of elementary W -increments on the step i ;
 f_K – a non-linear key-depended feedback function.

This construction based on the simple Counter with constant step “weight” but the number of elementary incrementations by W -value is different on each step and depends from the previous state. In other words we can say that the incrementation value changes dynamically on each step proportionally to W -value. This incrementation value is secret and mustn’t leak out from the cipher.

The zero output value for f_K -function is forbidden. This function may utilize a part of the base cipher output. The W -value must be coprime to counter module, in that case, the period of internal states is variable, but it is always bounded by the presented range.

The most optimal length of feedback function is half of the base cipher block length ($r = n/2$), because it is directly proportional to the assaulter vagueness and inversely proportional to the lower bound of period.

Assaulter vagueness: $N_i = ?$

For simplification of this mode implementation we propose to use the rare W -value with only three unit bits. In such case the multiplication can be replaced by a few additions.

The synchronization sequence generator built according to such scheme has guaranteed lower bound of period and hides the differential property of base cipher input sequence.

Now let’s consider the modes’ schemes constructed on the basis of the “Dynamic step counter”.

9.1. Strengthened Stream Ciphering Mode The scheme of strengthened stream ciphering mode is presented on the Figure 8. It is constructed according to the given above design principles. It scheme define synchronous stream cipher with half block output. The base cipher output block is divided on two non-overlapped parts of equal length. One half of it is used as gamma-output and another – as the feedback (or N_i -vector).

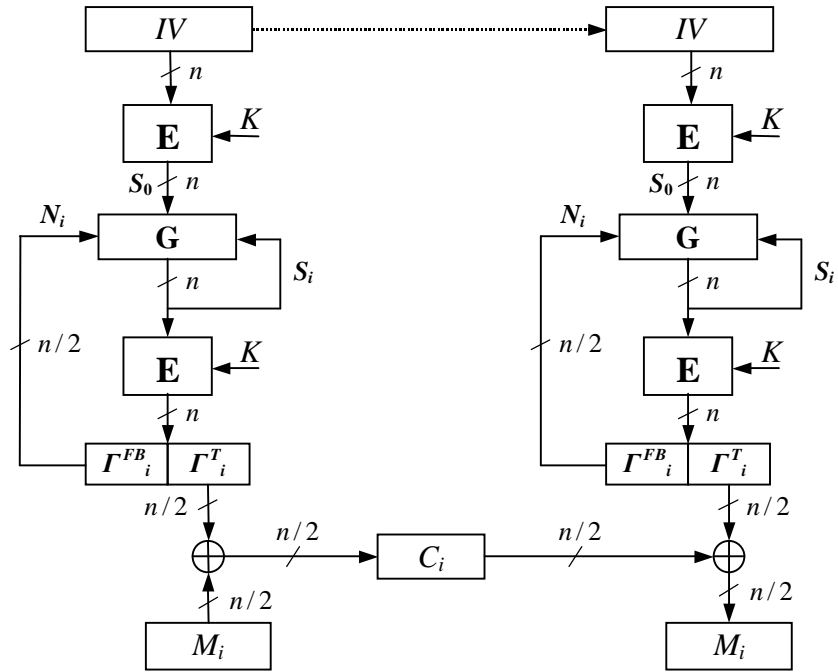


Figure 8. Strengthened stream ciphering mode

We can view this mode as combination of the Counter mode and the Output Feedback mode (CTR+OFB).

The initial internal state is hid by initial encryption of initialization vector (IV). Further states' hiding is provided by the "Dynamic step counter" utilization. This scheme has guaranteed lower bound of the internal states' period.

9.2. Strengthened Stream Ciphering and Authentication Mode

The last scheme (Figure 8) can be modified for ciphering and authentication tasks performing simultaneously (Figure 9).

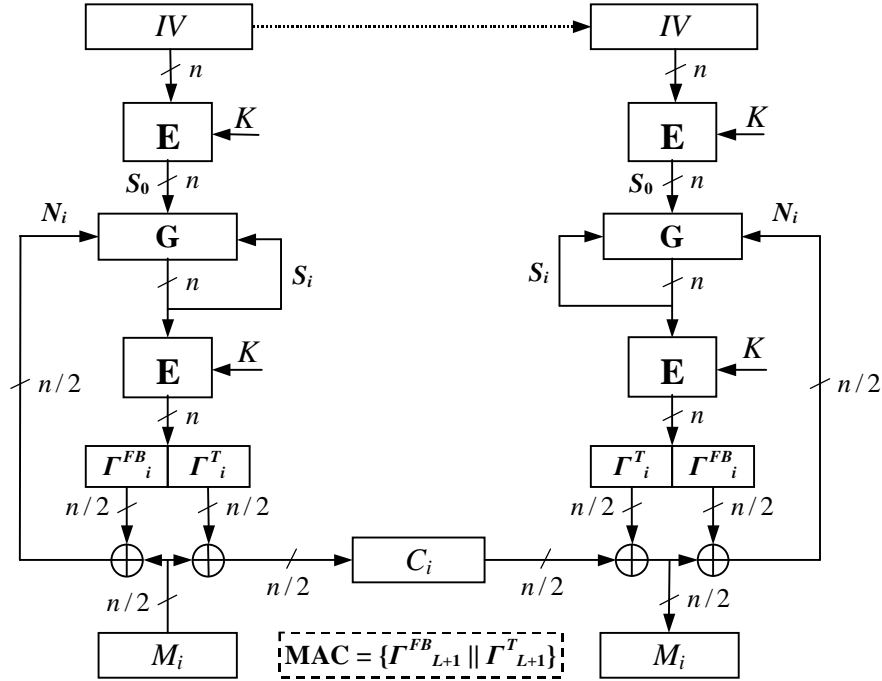


Figure 9. Strengthened stream ciphering and authentication mode

Shown scheme defines strengthened stream ciphering and authentication mode. This mode is similar to previous mode but has one distinction – the feedback value N_i depends on the message block too. As a result the current internal state depends on all processed plaintext blocks.

We can view this mode as combination of the Counter mode and the Cipher Feedback mode (CTR+CFB). After processing all message blocks the cipher internal state (S_i) depends linearly on the last block and non-linearly on all other message blocks (M_i), encryption key (K) and initialization vector (IV). In order to get Message Authentication Code (MAC) it is necessary to perform yet one blank encryption. The obtained base cipher output block or its part can be used as MAC.

10. CONCLUSIONS

Now let's summarize the all presented results.

1. In standard modes of operation (excluding CTR) the base block cipher is vulnerable to known plaintext attacks.

2. In the Counter mode the synchronization sequence has fixed known differential property and therefore the base block cipher is potentially vulnerable to differential cryptanalysis attack.
3. In the OFB mode the minimal gamma period depends on the base block cipher properties and therefore it doesn't guarantee any lower bound.
4. The Counter mode with session step "weight" value has increased security and can be recommended for encryption of information with the random access requirement and strict limitation to gamma overlapping in the case of multi-session key usage. Both proposed schemes of improved "counter mode" utilize "dynamic step" principle and protect base block cipher from known plaintexts and differential attacks. Their performance is practically equivalent to the performance of standard Counter mode with half block size output. The implementation of "Dynamic Step Counter" for 128-bit block-size requires about 10 non-paralleled micro operations on the 32-bit Intel Architecture (for comparison – the standard Counter mode requires 4 non-paralleled micro operations).

11. REFERENCES

1. *Morris Dworkin*. Recommendation for Block Cipher Modes of Operation. Methods and Techniques. NIST Special Publication 800-38A, 2001.
2. FIPS 81, «DES modes of operation», Federal Information Processing Standards Publication 81, U.S. Department of Commerce / National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.
3. ANSI X3.106, «American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation», American National Standards Institute, 1983.
4. ISO 8732, «Banking – Key management (wholesale)», International Organization for Standardization, Geneva, Switzerland, 1988 (first edition).
5. ISO/IEC 10116, «Information processing – Modes of operation for an n -bit block cipher algorithm», International Organization for Standardization, Geneva, Switzerland, 1991 (first edition).