



Advanced Research Workshop
Gdansk 2004



Improved Block Cipher Counter Mode of Operation Schemes

Kharkov National University of Radioelectronics

Ukraine

***Dr. Ivan Gorbenko,
Dr. Sergiy Golovashych***

Goals and objectives

1. Analyze the protectability of the base block cipher from cryptanalytical attacks in standard modes of operation.
2. Evaluate the gamma overlapping probability in the counter mode for the case of multiple messages encryption using the same key.
3. Define the ways to increase the security of standard modes of operation.
4. Propose the schemes of advanced counter mode of operation.

Notation

E – block cipher encryption: $O_i = \mathbf{E}_K(I_i)$

D – block cipher decryption: $I_i = \mathbf{D}_K(O_i)$

G – generator of “synchronization sequences”

K – secret key for block cipher

I_i – input block to block cipher

O_i – output block from block cipher

Γ_i – one block of encryption gamma

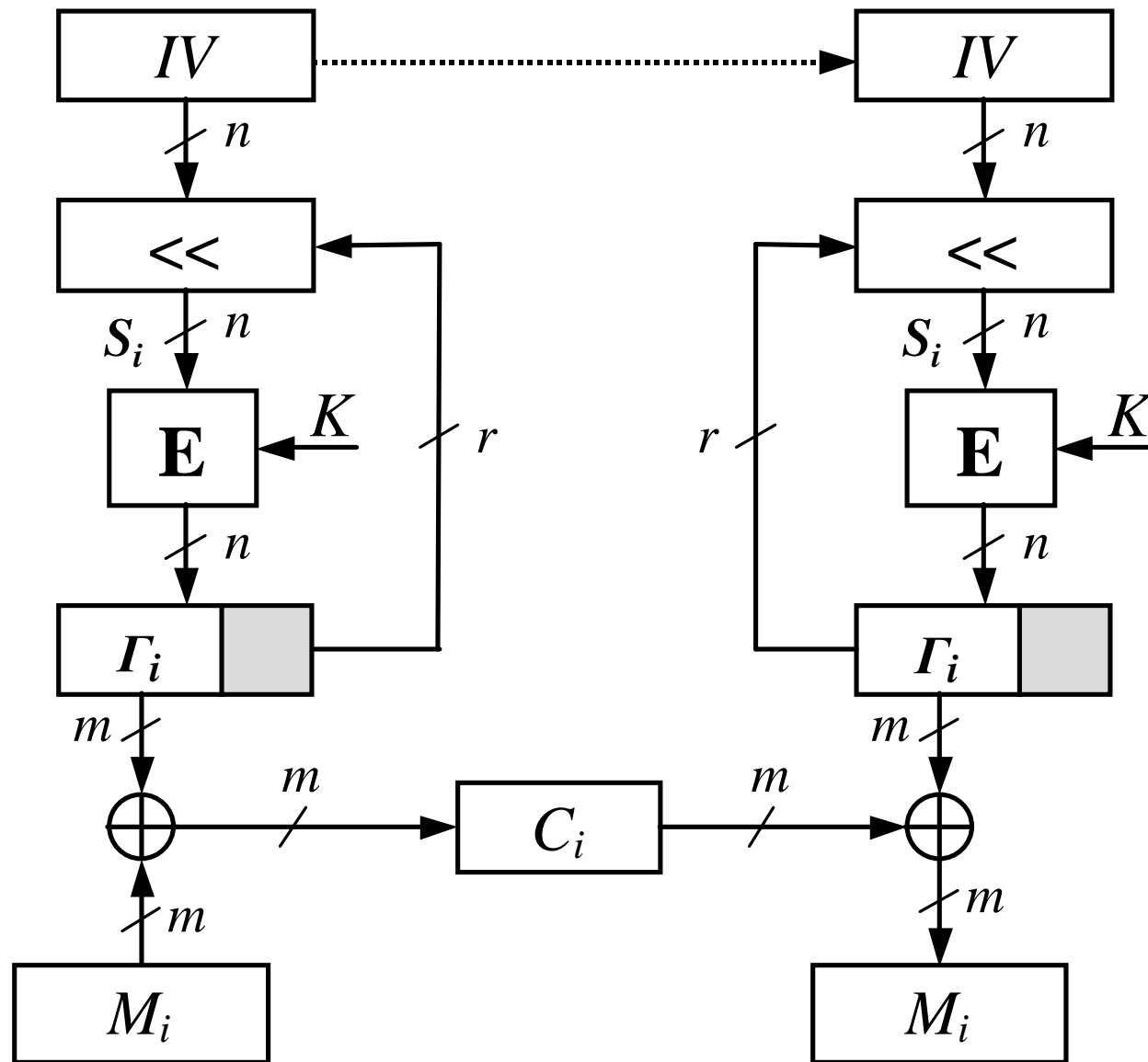
M_i – one block of plaintext (message)

C_i – one block of cryptogram

IV – initialization vector

S_i – internal state of stream cipher

Output Feedback mode (OFB)



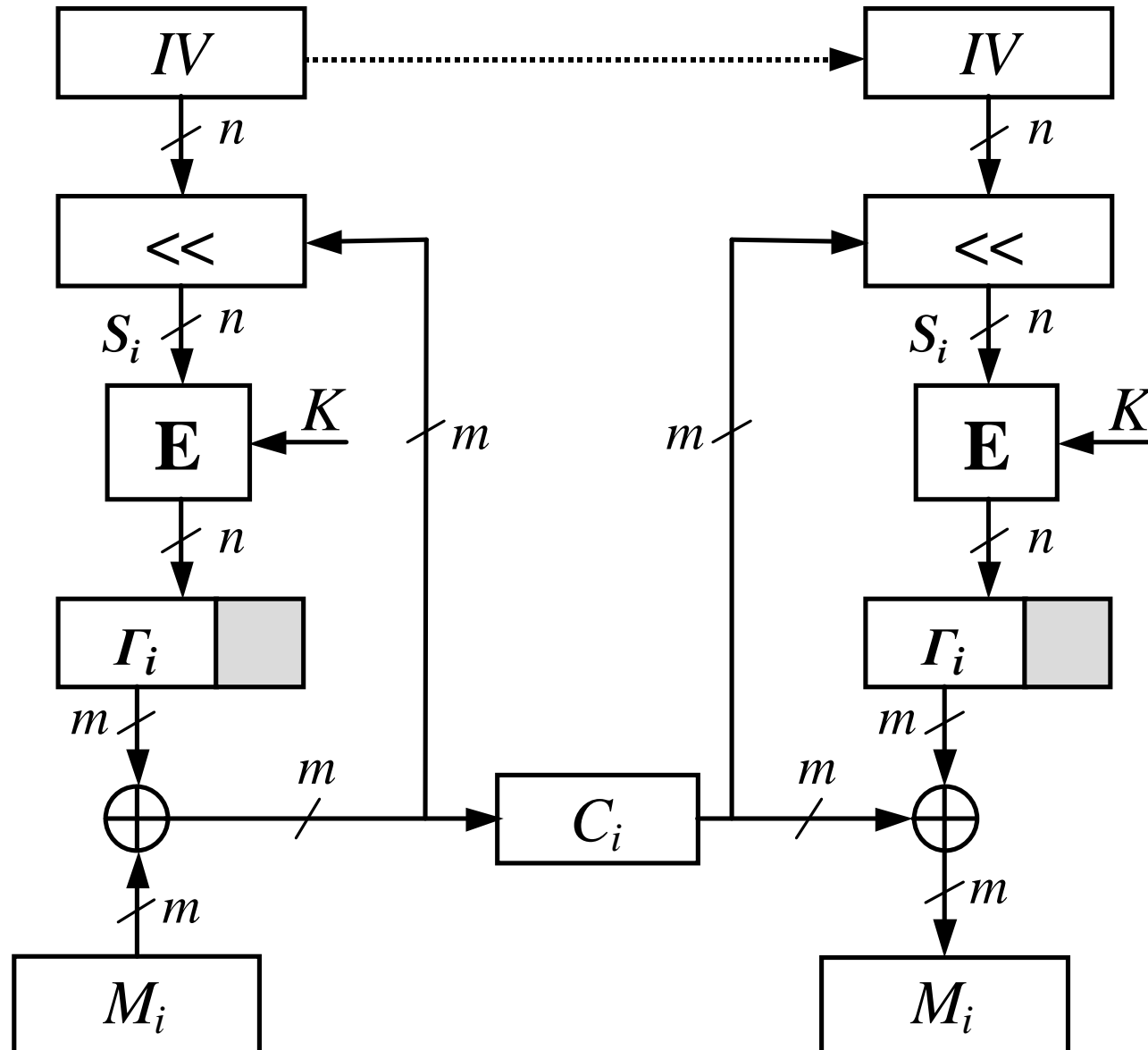
Known plaintext attack ($m = r = n$):

$$I_i = O_{i-1}$$

$$O_i = C_i \oplus M_i$$

$$I_0 = IV$$

Cipher Feedback mode (CFB)



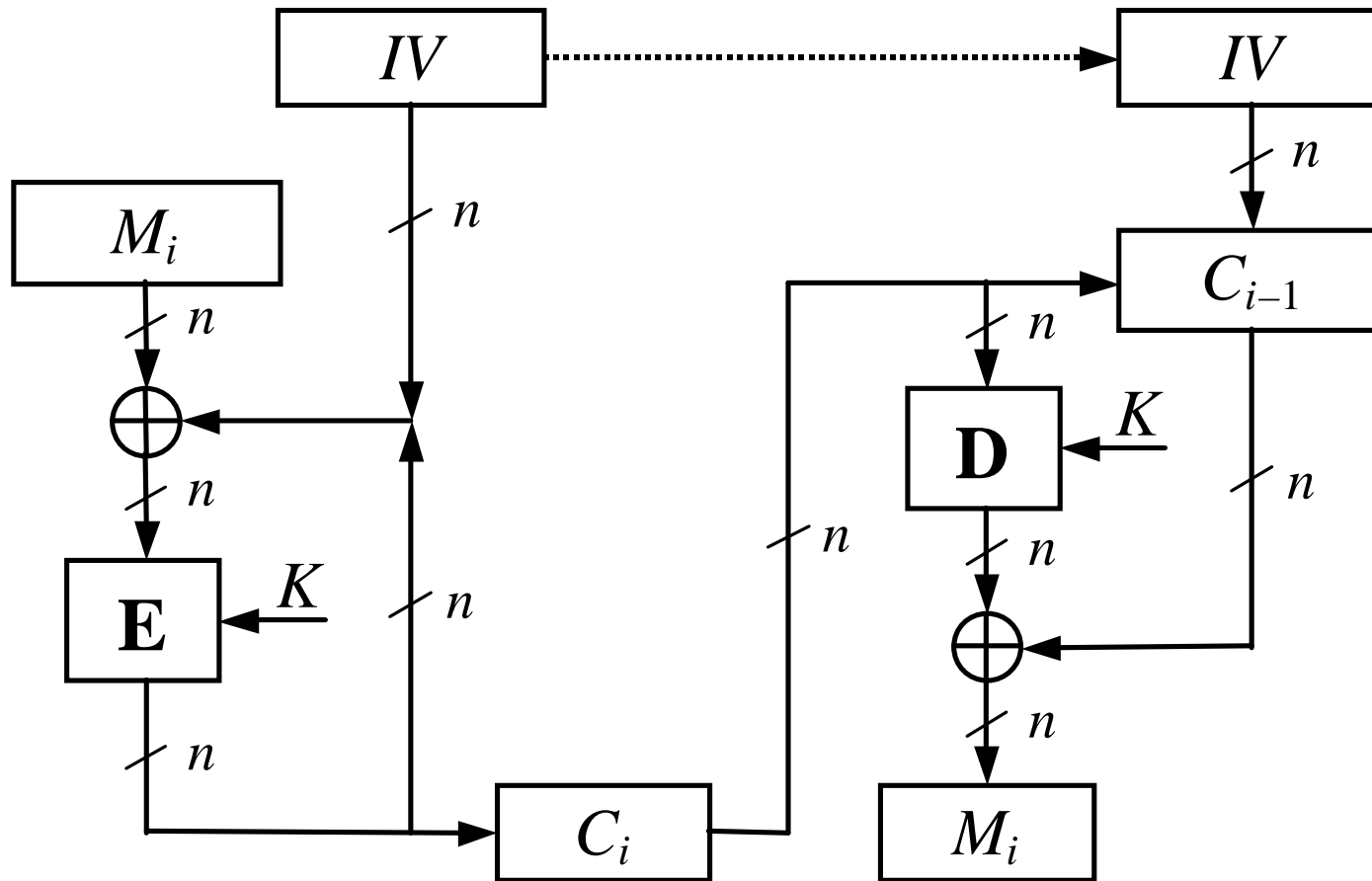
Known plaintext attack ($m = n$):

$$I_i = C_{i-1}$$

$$O_i = C_i \oplus M_i$$

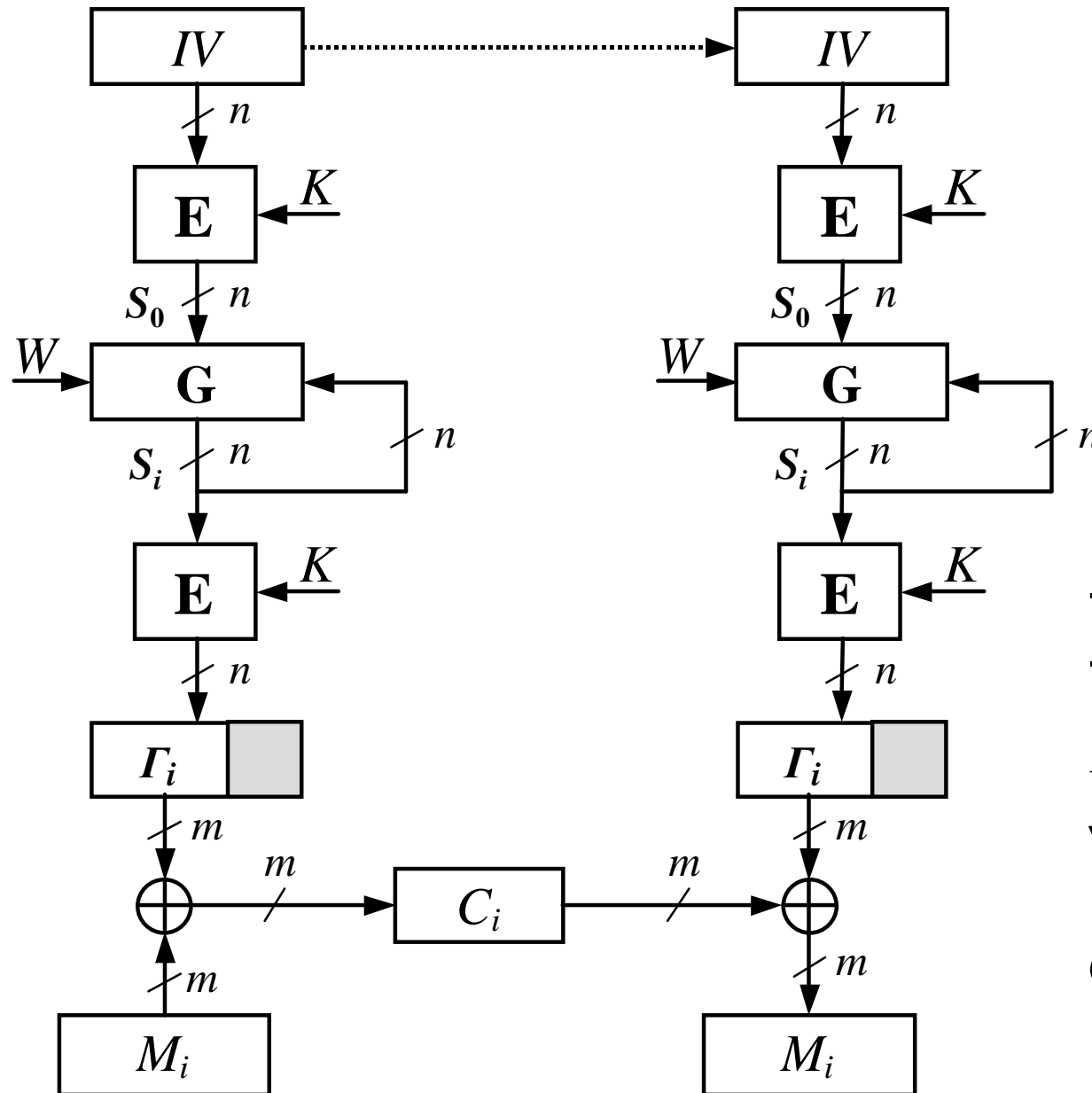
$$I_0 = IV$$

Cipher Block Chaining mode (CBC)



Known plaintext attack: $I_i = C_{i-1} \oplus M_i$, $O_i = C_i$

“Counter” mode (CTR)



Known plaintext attack ($m = n$):

$$I_i = ?$$

$$\forall i: \Delta M_{i,i+1} = W$$

$$O_i = C_i \oplus M_i$$

“Fixed Step Counters”

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

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

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

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

- 1. With constant public W**
- 2. With variable (session) secret W**

Period of Fixed Step Counters

1. Constant public “weight”

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

Assaulter knowledge: $\Delta S_{i,j} = W \times (j - i) \bmod 2^n$

2. Variable (session) secret “weight”

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

1. $R \leftarrow \text{RANDOM}, \quad R = x \times 2^{n-l} + y$

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

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

Gamma Overlapping Event

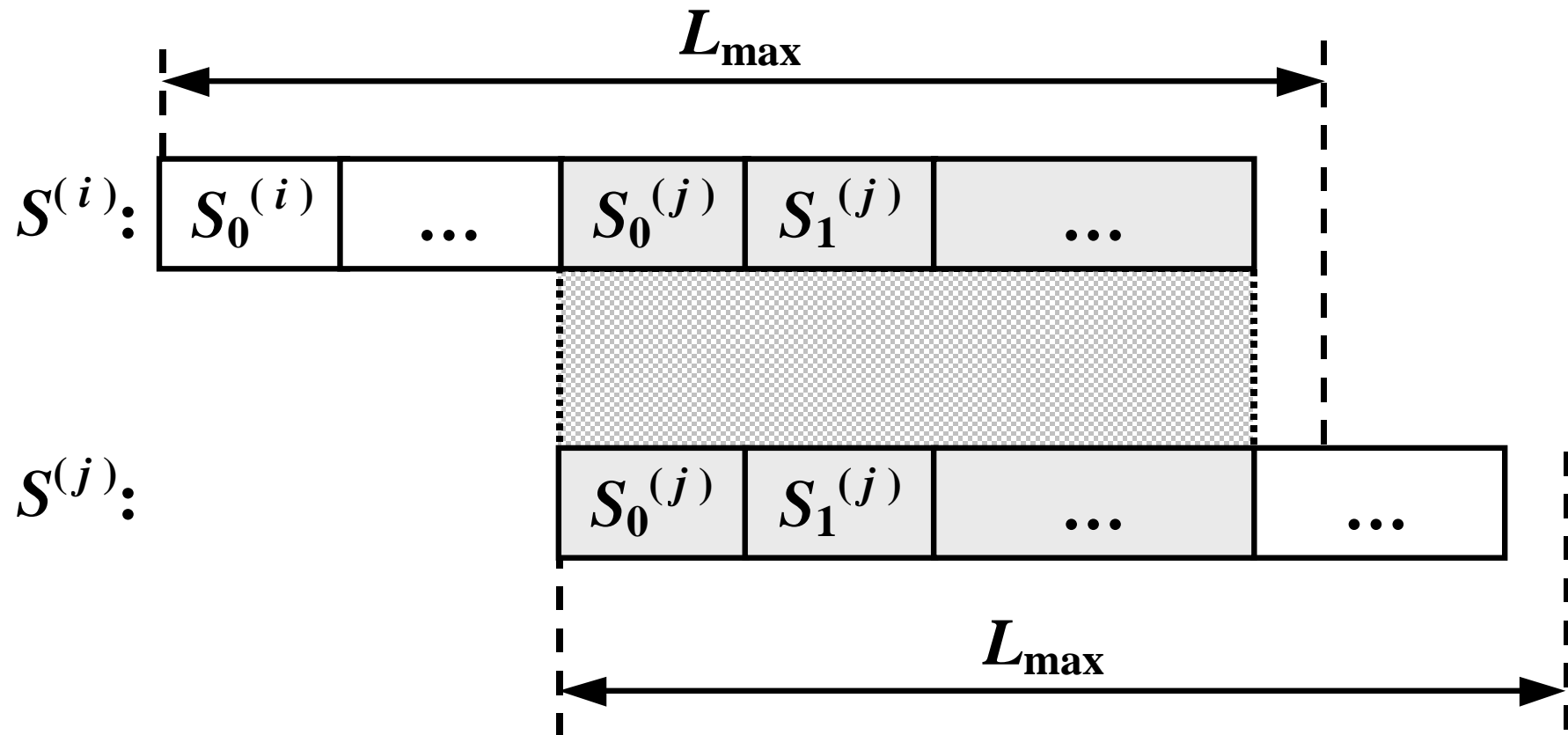
The event that consist in:

- **blocks repetition inside of one sequence of encryption gamma**

or

- **at least two blocks repetition in any pair of different sequences, produced by the same key.**

Gamma overlapping event for Constant step “weight”



Gamma overlapping for Constant step “weight”

Gamma overlapping condition:

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

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:

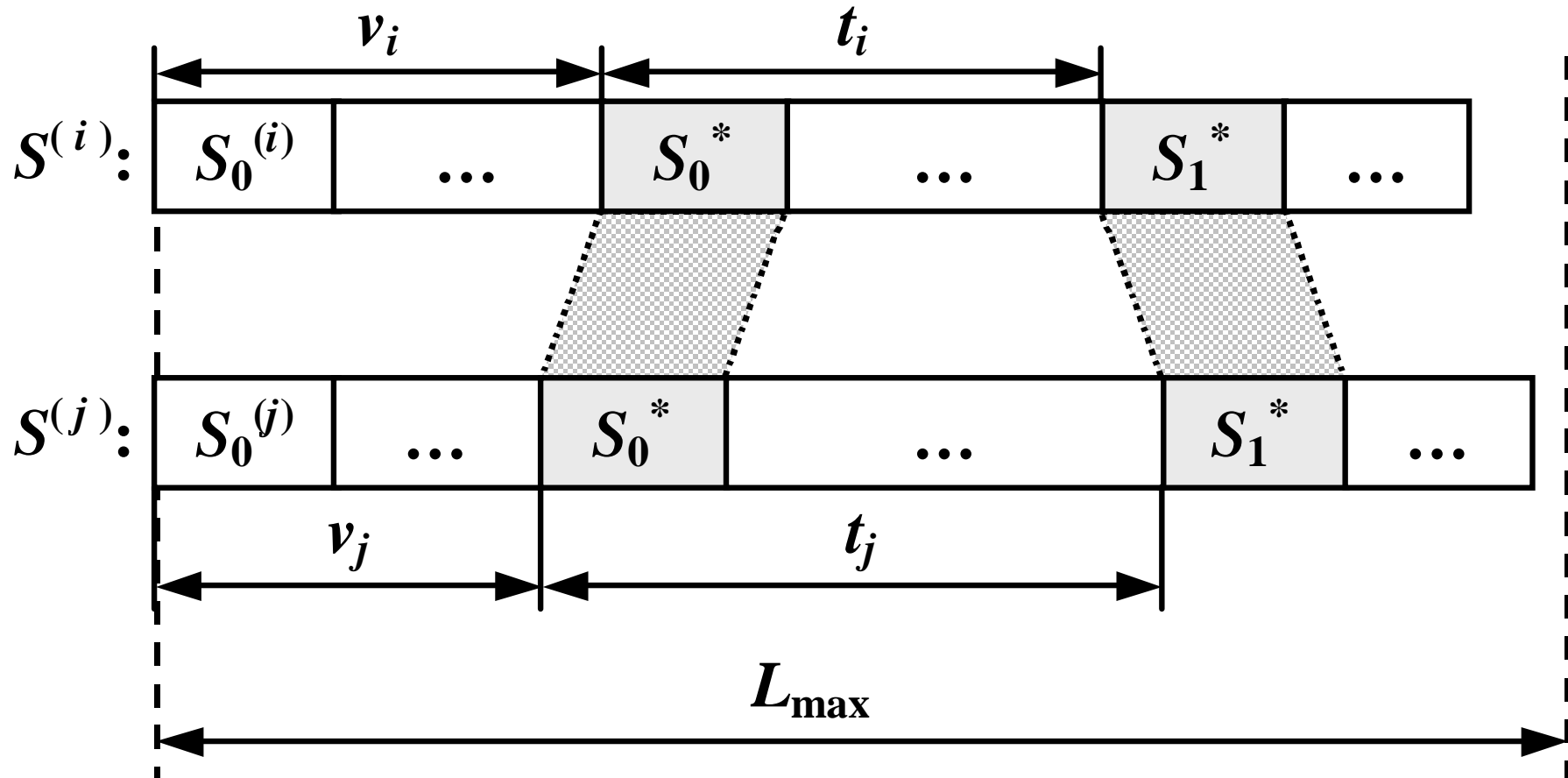
$$P_{\max} = P_{1\max} \times (N^2 - N) / 2$$

Allowable number of cipher restarts with same key:

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

(P_A – allowable overlapping probability)

Gamma overlapping event for Variable step “weight”



Gamma overlapping for Variable step “weight”

Gamma overlapping condition:

$$\left\{ \begin{array}{l} S_{v_i}^{(i)} = S_{v_j}^{(j)} = S_0^* \\ S_{v_i+t_i}^{(i)} = S_{v_j+t_j}^{(j)} = S_1^* \\ (v_i + t_i) \leq L_{\max} \\ (v_j + t_j) \leq L_{\max} \\ t_i \neq 0, \quad t_j \neq 0 \\ S_0^* = S_1^* \end{array} \right.$$

Gamma overlapping for Variable step “weight”

Gamma overlapping condition:

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

t_i – minimum number of steps between repeated states

v_i – minimum number of steps to first repeated state

$\Delta S_0^{(i,j)} = (S_0^{(i)} - S_0^{(j)}) \pmod{2^n}$ – initial states difference

Gamma overlapping for Variable step “weight”

$$\text{Gamma overlapping condition 1: } \begin{cases} t_j \times W_j - t_i \times W_i \equiv 0 \pmod{2^n} \\ 0 < t_i \leq L_{\max}, \quad 0 < t_j \leq L_{\max} \end{cases}$$

1st condition fulfillment probability: $P'_{1 \max} = L_{\max}^2 / 2^n$

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

2nd condition fulfillment probability: $P''_{1 \max} = (L_{\max} + 1)^2 / 2^n$

Gamma overlapping for Variable step “weight”

Overlapping probability for one pair of sequences :

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

Overlapping probability for multitude sequences:

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

Allowable number of cipher restarts with same

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

(P_A – allowable overlapping probability)

Gamma overlapping probability for one pair of sequences

Constant step “weight” : $P_{1\max} \cong 2^{-(n-l-1)}$

Variable step “weight” : $P_{1\max} \cong 2^{-(2n-4l+2)}$

Allowable number of cipher restarts with same key

Constant step “weight” : $N_A \approx \sqrt{2^{n-l} \times P_A}$

Variable step “weight” : $N_A \approx 2^{n-2l+1} \times \sqrt{2 \times P_A}$

(P_A – allowable overlapping probability)

Gamma overlapping for IP-traffic encryption by counter mode (example)

Block length $n = 128$ bit 1 day = $2^{16,4}$ sec.

Min. packet size = 28 byte, Max. packet size = 2^{16} byte

$$L_{\max} = (2^{16} \cdot 8) / 128 = 2^{12} \text{ blocks} \quad \text{P} \quad l = 12$$

$$P_{CSW} \approx 2^{-115} \times N^2 : \quad 100 \text{ Mbps} : \quad P_{CSW} \approx 2^{-67} \times D^2$$

$$1 \text{ Gbps} : \quad P_{CSW} \approx 2^{-60} \times D^2$$

$$P_{VSW} \approx 2^{-210} \times N^2 : \quad 100 \text{ Mbps} : \quad P_{VSW} \approx 2^{-162} \times D^2$$

$$1 \text{ Gbps} : \quad P_{VSW} \approx 2^{-155} \times D^2$$

(D – days number in one key usage period)

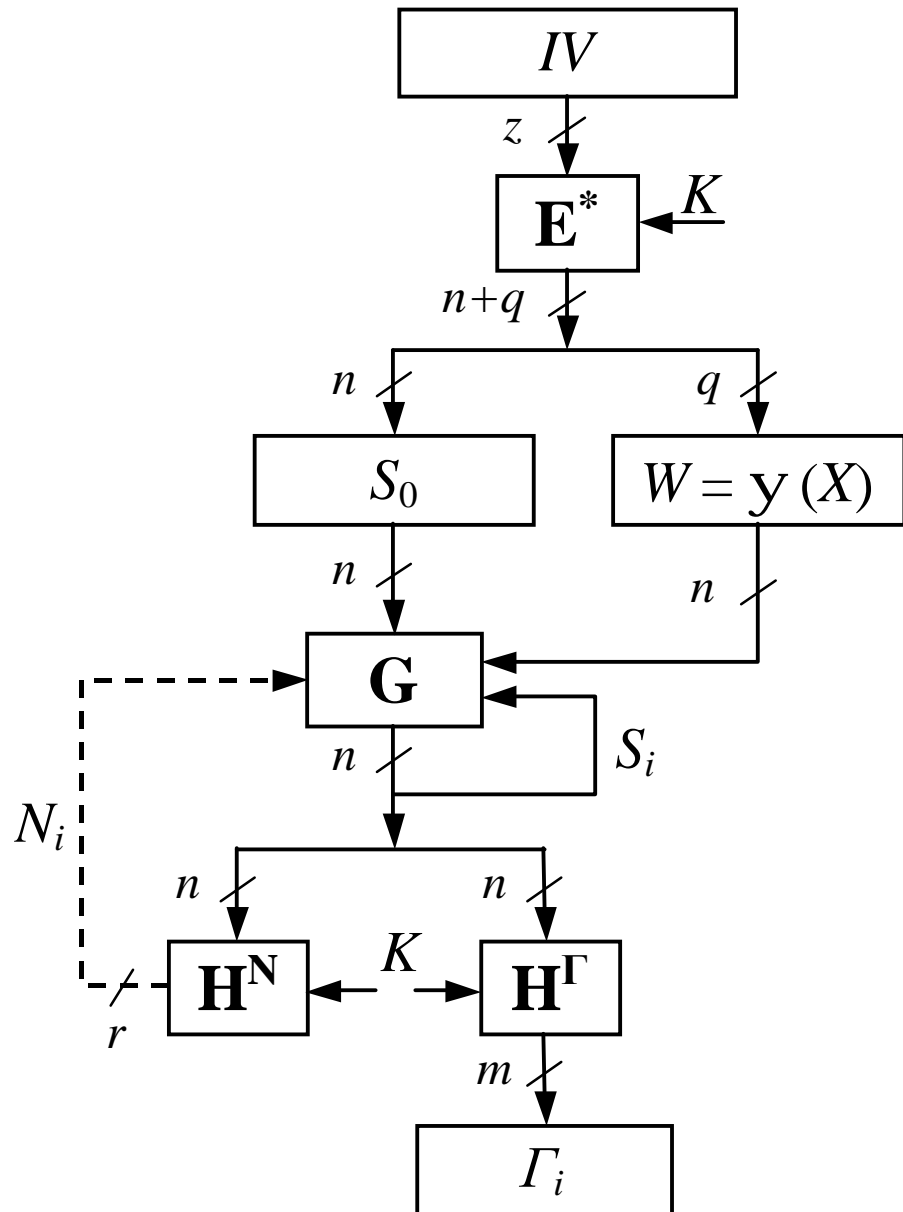
$$N_{A, CSW} \approx 2^{58} \times \sqrt{P_A}$$

$$N_{A, VSW} \approx 2^{105,5} \times \sqrt{P_A}$$

Construction principles of secure stream ciphering modes

- 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 mode



Notation

IV – initialization vector

K – secret key

W – weight of one step

S_i – current state

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 – feedback function

H^G – gamma output function

“Dynamic Step Counter”

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

$$N_i = f_K(S_i), \quad 0 < N_i < 2^r, \quad r + m \leq n$$

$$W = 2^{n/2} + 2^{n/4+1} + 1 \quad (\text{for } r = n/2)$$

$$(W, 2^n) = 1 \quad \Rightarrow \quad 2^{n-r} < T \leq 2^n$$

where S_i – internal state at step i

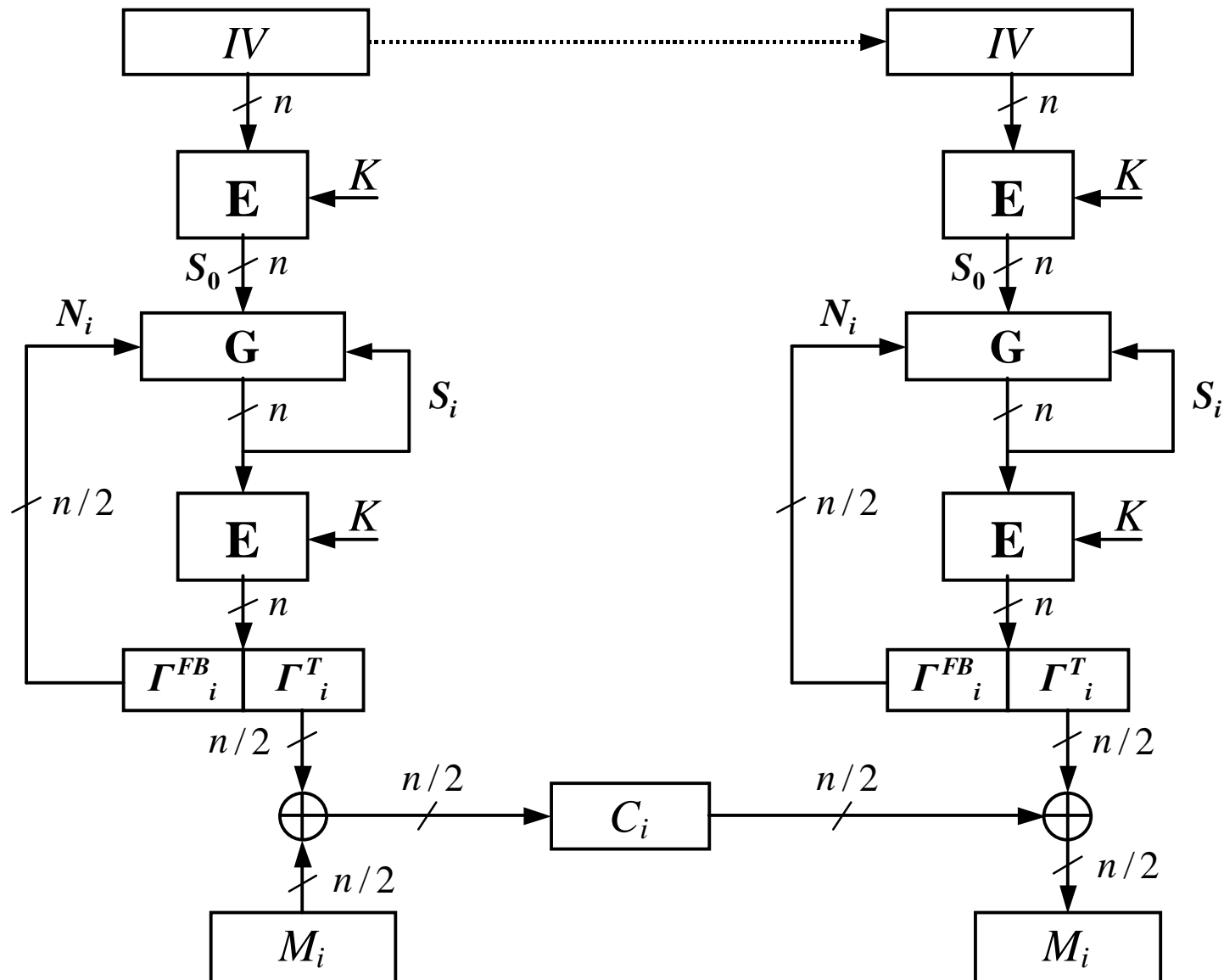
W – one step “weight” value

N_i – number of W -incrementations at step i

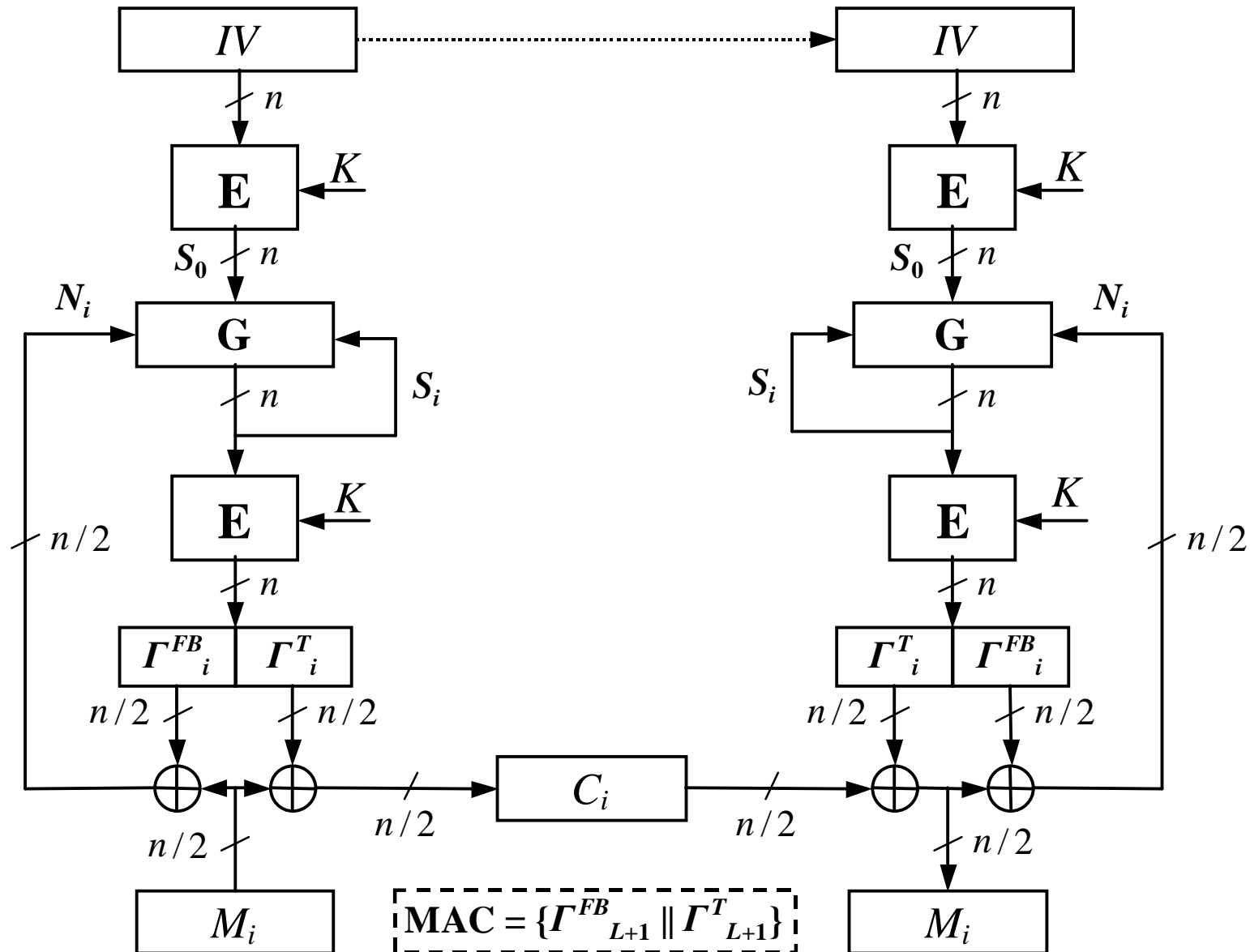
Assaulter vagueness:

$$N_i = ?$$

Strengthened stream ciphering mode (CTR+OFB)



Strengthened stream ciphering and authentication mode (CTR+CFB)



Conclusion

1. In most of standard modes of operation (excluding CTR) the base block cipher is vulnerable to known plaintext attacks.
2. In the CTR mode the base block cipher is potentially vulnerable to the differential cryptanalysis attack.
3. In the OFB mode the minimal gamma period depends on the base block cipher properties.
4. The CTR mode with session step “weight” value can be recommended for encryption an information with the random access requirement and strict limitation to gamma overlapping in the case of multi-session key usage.
5. Both proposed schemes of improved “counter mode” utilize “dynamic step” principle and allow to protect base block cipher from known plaintexts and differential attacks. Their performance is practically equivalent to performance of the standard Counter mode with half block size output.