Security Code

On Efficiency of Block Encryption by Improved Key Schedule

Fomichev V.M.
Koreneva A.M.

Introduction

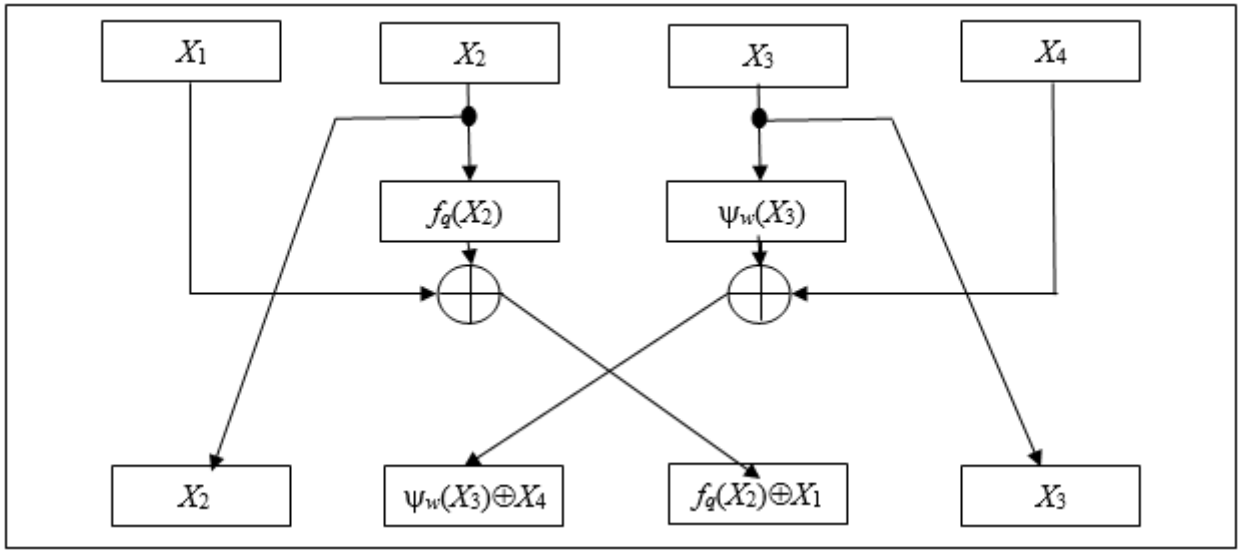
- Approach to construction of block encryption algorithm with higher efficiency compared with GOST 28147-89;

- Increasing of efficiency by 2 – 2,6 times by reducing number of encryption rounds to 12 – 16;

- Improved key schedule for algorithm based on generalized Feistel network with using GOST 28147-89 combining function.

- Estimation of encryption speed must be made more precise by modern software tools.

Block encryption network based on shift register of length 4



Encryption: $T\,g_{q_r,w_r}\ldots g_{q_2,w_2}\;g_{q_1,w_1}(X_1,X_2,X_3,X_4)=(Y_1,Y_2,Y_3,Y_4)$, q_i,w_i – keys for round $i=1,\ldots,r$.

Decryption: $T\,g_{q_1,w_1}\,T^2\ldots T^2\,g_{q_{r-1},w_{r-1}}\,T^2\,g_{q_r,w_r}(Y_1,Y_2,Y_3,Y_4)=(X_1,X_2,X_3,X_4)$.

Permutation T: $T(Z_1,Z_2,Z_3,Z_4)=(Z_3,Z_1,Z_4,Z_2)$.

Round permutation $g_{q,w}$: $g_{q,w}(X_1,X_2,X_3,X_4)=(X_2,\ \psi_w(X_3)\oplus X_4,\ f_q(X_2)\oplus X_1,\ X_3)$.

Combine functions f_q and ψ_w are defined on the next slide.

Mixing properties of round permutation $g_{q,w}$

Combine functions: $f_q=T_z(S_{8,4}(X_2 \boxplus q))$; $\psi_w=T_z(S_{8,4}(X_3 \boxplus w))$,

$\boxplus$ – addition modulo 2^{32};
T_z – left 11 bits cyclic shift for *z=left*;
T_z – right 11 bits cyclic shift for *z=right*;
$S_{8,4}=(S_1,\ldots,S_8)$ – *s*-boxes of GOST 28147-89;

M – mixing matrix of round permutation $g_{q,w}$;
M' – mixing matrix of permutation $(g_{q,w})^{-1}$;
exp$M$ (expM')– exponents of M (of M');
r – recommended lower bound for number of rounds.

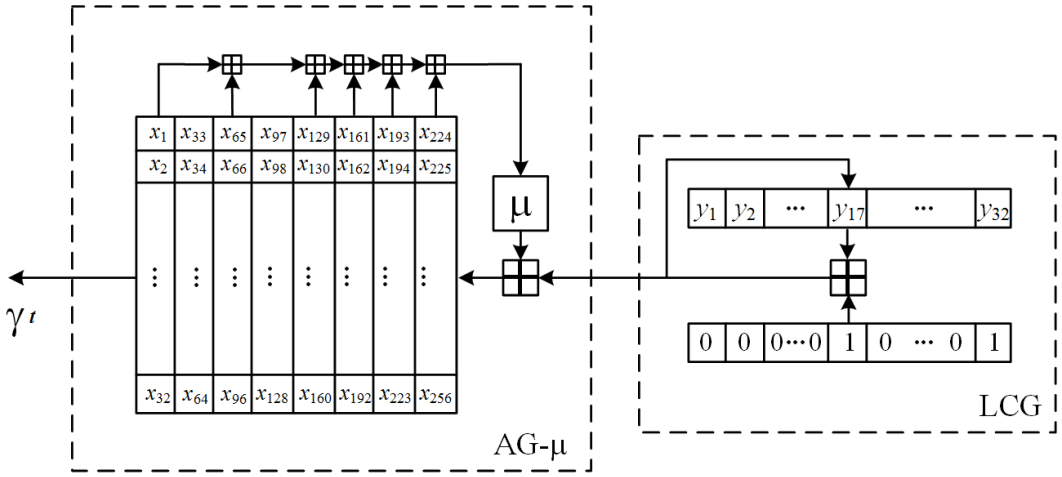
Table 1 – Values of exp$M$, expM', r

	f_q for *z=left*	f_q for *z=right*
ψ_w for *z=left*	8, 8, 15	7, 7, 13
ψ_w for *z=right*	7, 7, 13	7, 6, 12

Note: To counter meet-in-the-middle attack it is enough that for any $l \in \{1,\ldots,r\text{-}1\}$ full mixing will be achieved after l encryption rounds or after r-l decryption rounds. Hence, number of encryption rounds must be at least 12.

Generator *G* of round keys

Generator *G*:



Transformation of *G* states:

$$(X_{0,t+1},X_{1,t+1},\ldots,X_{7,t+1})=(X_{1,t},\ldots,X_{7,t},f^{\mu}(X_{0,t},X_{1,t},\ldots,X_{7,t})\boxplus Y_{t+1}),$$

$$f^{\mu}(X_{0,t}, X_{1,t}, \ldots, X_{7,t})=\mu\left(\left(\sum_{j=0}^{7} a_j X_j\right) \bmod 2^{32}\right),$$

$a_1,\ldots,a_7\in\{0,1\}$, $a_1+\ldots+a_7>0$, $a_0=1$.

Properties of sequence $\{\gamma_t\}=b_{32}(X_{0,t})$, $t=0,1,\ldots$, $b_{32}(X)$ – binary 32-bit notation for $X\in Z_m$, $m=2^{32}$:

- Length of the sequence $\{\gamma_t\}$ period is a multiple of 2^{32}.
- For γ_t all 256 bits of initial state are sufficient for choose $a_0,\ldots,a_7$ and certain transformation μ, $t\geq 16$.

Encryption key: initial state of *G*;

Encryption key length: $128+32k$ bits, $k\in\{0,1,2,3\}$, integers $X_{0,0},\ldots,X_{3-k,0}$ equals 0.

Set of round keys: determinate non-regular selection from $\{\gamma_t\}$, $t<100$.

Recommended parameters and Advantages

Recommended parameters

- Size of input block: 128 bits
- Combining functions:
  $f_q(X_2)=T_{\text{right}}(S_{8,4}(X_2 \boxplus q))$ and
  $\psi_w=T_{\text{right}}(S_{8,4}(X_3 \boxplus w))$,
  $S_1,\ldots,S_8$ – s-boxes of GOST 28147-89.
- Order of key set: $2^{128+32k}$, $k \in \{0,1,2,3,4\}$.
- Number of encryption rounds: from 12 to 16 with corresponding key schedule.

Advantages

- 2-2,6 times reduction of encryption rounds number (compared with GOST 28147-89) by improved key schedule.
- Ability to set encryption key length is equal to $128+32k$ bits, $0 \le k \le 4$.
- Increased block size (compared with GOST 28147-89) with ability to use combine functions of GOST 28147-89.
- A slight difference between encryption and decryption algorithms.

Thank you!