Software encryption: new 64-bit block cryptoscheme

A.Moldovyan N.Moldovyan V.Izbash

Abstract

There are considered new fast software encryption function and some its cryptographical properties. It has been shown that the probability of the selection of two equivalent keys is very low. Crypto-robustness of this cipher has been evaluated on the basis of its probabilistic model.
Key words: software-oriented cipher, block encryption, pseudo-probabilistic cryptoscheme

1 Introduction

Cryptographical methods allow solving the crucial problems of data automated processing protection. They assure high level of data protection and provide possibility of efficient control of information integrity and authentication. Modern encryption methods guarantee practically absolute data protection. There are known many ciphers securing high cryptoresistibility level, however, majority of them (for example, DES, FEAL, IDEA) are hardware-oriented.

Mass application of cryptographical methods is restrained by the fact that the use of specialized encrypting hardware requires substantial financial expenses. Increasing productivity of serial microprocessors and penetration of computer technologies in communication and information systems allows one to solve the last problem on the basis of the software-oriented ciphers.

Recently several software encryption functions based on data-dependent selection of the current key elements has been proposed [1, 2].

In such ciphers there is used an initialization subsystem which generates a long secondary encryption key [3].

In present paper there is considered a new software encryption block cryptoscheme based on local pseudorandomness.

2 Encryption function

Cryptoscheme described below uses a 1024-byte key $\{Q_h\}$, where Q_h is a 32-bit word $(h = 0, 1, 2, \ldots, 255)$. It is supposed that this key depending on the password is generated by the initialization subsystem. Encryption function is based on operations $\oplus$ (xor), $+$ $(mod\ 2^{32})$, and $-$ $(mod\ 2^{32})$ as well as on pseudorandom selection of the key elements. Below there are used the following notations

$$j = (i-1)\ mod\ 4, \quad a_j = (X_{i-1}\ div\ 256^j)\ mod\ 256,$$
$$b_j = (Y_i\ div\ 256^j)\ mod\ 256,$$

and $\quad Q(x) = Q_x$.

ENCRYPTION ALGORITHM

INPUT: 64-bit date block $T = A\|B$ represented as concatenation of two 32-bit words.

1. Set parameter $p = 3$, counter $i = 1$, and initial values of the variables X and Y: $X_0 = A$ and $Y_0 = B$.

2. Transform the variable Y: $Y_i = Y_{i-1} + Q(a_j)\ mod\ 2^{32}$.

3. Transform the variable X: $X_i = X_{i-1} \oplus Q(b_j)$ and increment i.

4. Transform Y: $Y_i = Y_{i-1} \oplus Q(a_j)$.

5. Transform X: $X_i = X_{i-1} - Q(b_j)\ mod\ 2^{32}$ and increment i.

6. Transform Y: $Y_i = Y_{i-1} - Q(a_j)\ mod\ 2^{32}$.

7. Transform X: $X_i = X_{i-1} \oplus Q(b_j)$ and increment i.

8. Transform Y: $Y_i = Y_{i-1} \oplus Q(a_j)$.

9. Transform X: $X_i = X_{i-1} + Q(b_j)\ mod\ 2^{32}$ and increment i.

10. If $i < 4p$ then increment i and jump to step 2, otherwise STOP.

OUTPUT: 64-bit ciphertext block $C = X_{12} \| Y_{12}$.

Program implementing this algorithm provides the conversion speed about $70/r$ Mbit/s for microprocessor Intel 486/100, its size being about 2 Kbytes. Parameter p assigns the necessary number of encryption passages.

Encrypting some initial data blocks T_0 many times the sequences $\{T_j\}$ have been constructed for different keys $\mathbf{Q}: T_j = E(T_{j-1})$, where E is encryption function and $j = 1, 2, 3, \ldots$. Numerous sequences $\{T_j\}$ have been checked with several spectral and compaction tests which have shown the bit distribution is pseudorandom. Analyzing long sequences $\{T_j\}$ we have not succeeded to find any periods for $j \leq 10^{11}$.

A distinguishing feature of the described cipher is its use of the data-dependent selection of the key area elements. The selection is not predetermined and can be characterized as a "pseudorandom" one. Encryption of some input data block T can be described by the following generalized formula:

$$C = E(T, Q_{h_1}, Q_{h_2}, \ldots, Q_{h_{8p-1}}, Q_{h_{8p}}), \tag{1}$$

where $\{Q_{h_e}\}$, $e = 1, 2, \ldots, 8p-1, 8p$, is a set of the key area elements used while encrypting. Generation of the current set $\{Q_{h_e}\}$ depends on both input message and key area. There are possible only $N_T = 2^{64}$ different input data blocks, but for given key area the number of different sets $\{Q_{h_e}\}$ equals $L^{8p} = 2^{64p}$ ($L = 256$ is the key area length in 32-bit words).

3 Some properties

For given key any block encryption function defines a permutation of a set of N_T numbers 0,1,2,...,$2^b - 1$, where b is the input data block length in bits. The keys **Q** and **K** are equivalent ones if they define the same permutation.

One-round ($p = 1$) encryption function has the following property.

Theorem. *For both arbitrary set of indexes* $\{h_e\}$ *and arbitrary key* **Q** *there exists unique input data block* $T = A\|B$ *defining the respective set of key elements* $\{Q_{h_e}\}$.

Indeed, for given **Q** an input block defines the set of indexes $h_1, h_2, \ldots, h_8$:

$$A \ mod \ 2^8 = h_1, \tag{2}$$

$$Y_1 \ mod \ 2^8 = h_2, \qquad (Y_1 = B + Q_{h_1} \ mod \ 2^{32}) \tag{3}$$

$$(X_1 \ div \ 2^8) \ mod \ 2^8 = h_3, \qquad (X_1 = A \oplus Q_{h_2}) \tag{4}$$

$$(Y_2 \ div \ 2^8) \ mod \ 2^8 = h_4, \qquad (Y_2 = Y_1 \oplus Q_{h_3}) \tag{5}$$

$$(X_2 \ div \ 2^{16}) \ mod \ 2^8 = h_5, \qquad (X_2 = X_1 - Q_{h_4} \ mod \ 2^{32}) \tag{6}$$

$$(Y_3 \ div \ 2^{16}) \ mod \ 2^8 = h_6, \qquad (Y_2 = Y_2 - Q_{h_5} \ mod \ 2^{32}) \tag{7}$$

$$(X_3 \ div \ 2^{24}) \ mod \ 2^8 = h_7, \qquad (X_3 = X_2 \oplus Q_{h_6}) \tag{8}$$

$$(Y_4 \ div \ 2^{24}) \ mod \ 2^8 = h_8, \qquad (Y_4 = Y_3 \oplus Q_{h_7}) \tag{9}$$

For given $\{h_e\}$ and $\mathbf{Q}$ the values A and B are unknowns. It is easy to show that this system of equations has unique solution. One can solve equations (1)-(8) by turns starting from (1).

Corollary 1. *For given* $\mathbf{Q}$ *every block* T *defines unique set of indexes.*

Corollary 2. *If equivalent keys* $\mathbf{Q}$ *and* $\mathbf{K} \neq \mathbf{Q}$ *exist, then* $Q_j \neq K_j$ *for* $j = 0, 1, 2, \ldots, 255$.

Indeed, if there exists such index e for which $Q_e = K_e$, then we can select T' defining the set of indexes $\{e, e, e, e, e, e, e, v\}$, where $Q_v \neq K_v$. Such index v exists because $\mathbf{K} \neq \mathbf{Q}$. We get $E(T',\mathbf{Q}) \neq E(T',\mathbf{K})$.

Let us consider blocks T' and T'' defining sets of indexes $\{h'_1, h'_2, \ldots, h'_8\}$ and $\{h''_1, h''_2, \ldots, h''_8\}$, where

$$\begin{cases} h'_i = h''_i, & \text{if} \quad i = 1, 2, \ldots, 6 \\ h'_i \neq h''_i, & \text{if} \quad i = 7, 8. \end{cases}$$

For these input blocks T' and T'' the last condition is valid for arbitrary key. Considering encryption function one can obtain

$$[E(T') \oplus E(T'')] \; mod \; 2^{32} = Q_{h'_7} \oplus Q_{h''_7} = \delta_{h'_7 h''_7},$$

$$\{[E(T') \; div \; 2^{32}] - [E(T'') \; div \; 2^{32}]\} \; mod \; 2^{32} = Q_{h'_8} - Q_{h''_8} = \Delta_{h'_8 h''_8}.$$

It is possible to select different pairs T' and T'' and to construct sets of differences $\{\Delta_{ij}\}$ and $\{\delta_{ij}\}$ for all couples of indexes ij. The following corollary is evident.

Corollary 3. *For equivalent keys the sets of differences* δ_{ij} *and* Δ_{ij} *are composed from the same elements.*

The last corollary is of great practical importance. It shows that for one-round encryption function the probability to select two equivalent key is negligible. For randomly chosen key $\mathbf{Q}$ we have set $\{\Delta_{ij}\}$ containing 256^2 elements. The probability to find n given 2^{32}-bit numbers in this set can be estimated by formula

$$P < 256^{-2n}.$$

For $n = 6$ we have $P < 10^{-30}$, but for equivalent key there are fixed $n = 256$ of differences. Thus, for one-round encryption function the probability P of the selection of two equivalent keys is very low. For $p \geq 2$ it is difficult to estimate directly the probability P. This can be made on the basis of the general properties of permutations. Let us suppose that one-round encryption for two different keys **Q** and **K** defines permutations α and β, respectively. For p-round encryption these keys define permutations α^p and β^p, correspondingly. For some $\alpha \neq \beta$ one can get $\alpha^p = \beta^p$. This means that for p-round scheme the keys became equivalent though they are not equivalent for $p = 1$.

The order of permutation γ (denoted by $|\gamma|$) is the minimal natural number n satisfying equality $\gamma^n = \epsilon$, where ϵ is the identical permutation. Thus, for any permutation α we have $\alpha^{|\alpha|} = \epsilon$. Let us consider relations between orders $|\alpha|$ and $|\beta|$ for permutations α and β which satisfy condition $\alpha^p = \beta^p$. Below there are used the following notations: (m, n) is the greatest common divisor of numbers m and n; $m|n$ ($m \not| n$) denotes that m divide (do not divide) n;

It is known:

(1) if $(m, n) = d$, then $(m/d, n/d) = 1$;

(2) if $(m, n) = 1$, then there exist such integers x and y that $mx + ny = 1$;

(3) if $m|n$ and $n|m$, then $m = n$.

For primary p there are possible the following cases.

Case 1. $p||\alpha|$ and $p||\beta|$. We get the following implications:

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{|\alpha|/p} = (\beta^p)^{|\alpha|/p}) \Longrightarrow (\alpha^{|\alpha|} = \beta^{|\alpha|}) \Longrightarrow$$

$$\Longrightarrow (\beta^{|\alpha|} = \epsilon) \Longrightarrow |\beta|||\alpha|,$$

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{|\beta|/p} = (\beta^p)^{|\beta|/p}) \Longrightarrow (\alpha^{|\beta|} = \beta^{|\beta|}) \Longrightarrow$$

$$\Longrightarrow (\alpha^{|\beta|} = \epsilon) \Longrightarrow |\alpha|||\beta|.$$

Hence $|\alpha| = |\beta|$.

Case 2. $p \not| |\alpha|$ and $p \not| |\beta|$. Let us assume r and t are such natural numbers (they exist) that $0 < r < p, \quad 0 < t < p$,
and $p|(|\alpha| + r), \quad p|(|\beta| + t)$. Then

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{(|\alpha|+r)/p} = (\beta^p)^{(|\alpha|+r)/p}) \Longrightarrow (\alpha^{|\alpha|+r} = \beta^{|\alpha|+r}) \Longrightarrow$$

$$\Longrightarrow (\alpha^r = \beta^{|\alpha|+r}) \Longrightarrow ((\alpha^r)^p = (\beta^{|\alpha|+r})^p) \Longrightarrow (\alpha^{pr} = \beta^{p|\alpha|+pr}) \Longrightarrow$$

$$\Longrightarrow (\beta^{pr} = \beta^{p|\alpha|+pr}) \Longrightarrow (\beta^{p|\alpha|} = \epsilon) \Longrightarrow |\beta||p|\alpha|),$$

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{(|\beta|+t)/p} = (\beta^p)^{(|\beta|+t)/p}) \Longrightarrow$$

$$\Longrightarrow (\alpha^{p|\beta|} = \epsilon) \Longrightarrow (|\alpha||p|\beta|).$$

Since p is a prime, then $|\beta||p|\alpha| \Longrightarrow |\beta|||\alpha|$ and $|\alpha||p|\beta| \Longrightarrow |\alpha|||\beta|$. Hence $|\beta| = |\alpha|$. Thus, $r = t$ and $\beta^{|\alpha|} = \epsilon$. Now we get

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{(|\alpha|+t)/p} = (\beta^p)^{(|\alpha|+t)/p}) \Longrightarrow (\alpha^{|\alpha|+t} = \beta^{|\alpha|+t}) \Longrightarrow$$

$$\Longrightarrow (\alpha^t = \beta^t).$$

Since $(p, t) = 1$, there exist such integers k and s that $pk + ts = 1$. Then we have

$$\alpha = \alpha^{(pk+ts)} = \alpha^{pk}\alpha^{ts} = (\alpha^p)^k(\alpha^t)^s = (\beta^p)^k(\beta^t)^s =$$

$$= \beta^{pk}\beta^{ts} = \beta^{pk+ts} = \beta.$$

Thus, in case 2 we have obtained $\alpha = \beta$

Case 3. $p||\alpha|$ and $p \not|\beta|$). In this case we get

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{|\alpha|/p} = (\beta^p)^{|\alpha|/p}) \Longrightarrow (\alpha^{|\alpha|} = \beta^{|\alpha|}) \Longrightarrow$$

$$\Longrightarrow (\beta^{|\alpha|} = \epsilon) \Longrightarrow |\beta|||\alpha|.$$

Since $p||\alpha|$ and $(|\beta|, p) = 1$, we get $|\beta||(|\alpha|/p)$ therefore $p|\beta|||\alpha|$. On the other hand there exists such integer n that $p|(|\beta| + n)$. Then

$$(\alpha^p = \beta^p) \Longrightarrow ((\alpha^p)^{(|\beta|+n)/p} = (\beta^p)^{(|\beta|+n)/p}) \Longrightarrow (\alpha^{|\beta|+n} = \beta^n) \Longrightarrow$$

$$\Longrightarrow (\alpha^{p|\beta|+pn} = \beta^{pn} = \alpha^{pn}) \Longrightarrow (\alpha^{p|\beta|} = \epsilon) \Longrightarrow |\alpha||p|\beta|.$$

From $p|\beta|||\alpha|$ and $|\alpha||p|\beta|$ one can conclude $|\alpha| = p|\beta|$.

Case 4. $p \not|\alpha|$ and $p||\beta|$. This case is analogous to the case 3 and one can get $|\beta| = p|\alpha|$.

Thus, the equality $\beta^p = \alpha^p$ implicate: either $\alpha = \beta$, or $|\alpha| = |\beta|$, or $|\alpha| = p|\beta|$, or $|\beta| = p|\alpha|$. Hence, if $|\alpha| \neq |\beta|$, $|\alpha| \neq p|\beta|$, and $|\beta| \neq p|\alpha|$, then $\alpha^p \neq \beta^p$.

Analogous consideration of the case $\alpha^{p^k} = \beta^{p^k}$, where p is a prime, shows that there are potentially possible the following equalities

$$\alpha = \beta, \quad |\alpha| = |\beta|, \quad |\alpha| = p|\beta|, \quad |\alpha| = p^2|\beta|, \ldots, |\alpha| = p^k|\beta|;$$

$$|\beta| = p|\alpha|, \quad |\beta| = p^2|\alpha|, \ldots, |\beta| = p^k|\alpha|.$$

These relations between orders $|\alpha|$ and $|\beta|$ show that the probability of the selection of two equivalent keys is very low for p-round $(p = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17 \ldots)$ encryption function described in Section 2.

4 Robustness evaluation

There are possible only $N_T = 2^{64}$ different input data blocks, but for given key area the number of different sets $\{Q_{h_e}\}$ equals $L^{8p} = 2^{64p}$ ($L = 256$ is the key area length in 32-bit words). Such repetitions can take place due to the possible presence of some equal elements at different sites of the key area. Taking into account results of Section 1 one can conclude that probability of the generation of two equal sets $\{Q_{h_e}\}$ corresponding to input blocks $T' \neq T''$ is very low for arbitrary p. Robustness of the cryptosystem under consideration is conditioned mainly by the complexity of the $\{Q_{h_e}\}$ set repetition recognition regardless of the complexity of the solution of the equation (1) or of the system of such equations.

Some preliminary estimations can be obtained on the basis of the probabilistic model of the cipher under discussion. Let us assume the following:

1. Key elements Q_{h_e} are selected randomly.

2. To calculate a set $\{Q_{h_e}\}$ it is sufficiently to recognize two pairs (T', C') and (T'', C'') corresponding to sets of the used key elements for which indexes $h_{4p}, h_{4p+1}, \ldots, h_{8p}$ are the same.

3. The solution of the respective system of two equations (1) is not a complex problem.

The minimal known plaintext size V_{min} which is necessary for cryptanalysis can be estimated by the following formula corresponding to the 0.5 probability of the observation of a $h_{4p}, h_{4p+1}, \ldots, h_{8p}$ subset repetition:

$$V_{min} = N_1 = \sqrt{P_1^{-1}} = L^{2p} \qquad (blocks), \tag{10}$$

where P_1 is the probability to observe a given subset $h_{4p}, h_{4p+1}, \ldots, h_{8p}$ when encrypting gives input data block. For $p = 2(3)$ we have $V_{min} > 10^9(10^{14})$ *blocks*. Let us suppose that cryptanalyst is able to obtain and to process so large texts. To meet a true repetition one has to check

on the average about $C_{N_1}^2/2$ of different pairs (T, C). The complexity of this procedure is

$$R_{min} > R_0 \cdot C_{N_1}^2/2 \approx (R_0/4) \cdot N_1^2 = (R_0/4) \cdot L^{4p}, \qquad (11)$$

where R_0 is some average number of operations which are to be executed while checking one system. For $R_0 = 2$ *operations* and $p = 2(3)$ we have $R_{min} > 10^{19}(10^{28})$ *operations*.

References

[1] Moldovyan A.A., Moldovyan N.A., Moldovyan P.A. Effective software-oriented cryptosystem in complex PC security software// Comput. Sci. J. of Moldova. 1994. V. 2. No 3. P. 269 - 282.

[2] Moldovyan A.A., Moldovyan N.A. Fast software encryption system based on local pseudorandomness// Comput. Sci. J. of Moldova. 1995. V. 3. No 3(9). P. 252 - 262.

[3] Moldovyan A.A., Moldovyan N.A. Fast Software Encryption Systems for Secure and Private Communication//12th Intern. Conf. on Computer Communic. (ICCC'95). Seoul, Korea, Aug. 21-24, 1995. Proceed. P. 415-420.

A.Moldovyan, N.Moldovyan, V.Izbash Received July 30, 1996

A.Moldovyan, N.Moldovyan
Institute of Modelling and Intellectualization
of Complex Systems,
5, Prof. Popov str., St-Petersburg,
197376, Russia
Phone: 7(812)2340415; fax 7(812)2349093
e-mail: sovetov@imics.spb.su

V,Izbash
Institute of Mathematics,
Academy of Sciences of Moldova,
5, Academiei str., Kishinev,
2028, Moldova
e-mail: 24gal@math.moldova.su
phone: (373–2) 73-80-29