# Conference Record

IEEE/AFCEA

# EUROCOMM 2000

## Information Systems for Enhanced Public Safety and Security

**Advanced wireless communications & information systems for:**

- Police
- Military
- Public Safety
- Border Control
- Crime Prevention
- Penal Systems
- Law Enforcement
- Civilian Air Control
- Rescue Agencies
- Fire Departments
- Central Government
- Local Government

Sponsored by

AFCEA

IEEE
Networking the World™

IEEE COMMUNICATIONS SOCIETY

Technically Co-Sponsored by

ITG INFORMATIONSTECHNISCHE GESELLSCHAFT IM VDE

# On the Design of Error Detection and Correction Cryptography Schemes

N. V. Patsei, P. P. Urbanovich
BY- Minsk, Belarussian State Technological University,
E-mail: pat@psdn.belpak.minsk.by

*Abstract*--**The paper introduces the method of modifying cryptography encryption and decryption units which includes circuitry of checks that operations has been performed without errors. This technique based on addition to storage devices error correction codes and modulo check of arithmetic and logic units operations. The example of cryptoscheme development are presented in graph.**

## I. Introduction

The defects and errors can be found practically everywhere: the threats in models, architecture, algorithms and protocols, in practical hardware and software implementation and configuration setup, in user interface, procedures, and also in other parts of cryptosystems.

It is important to ensure that the encryption and decryption operations are performed accurately. However because of storage elements and also because of origin any violation of normal function of logical or arithmetic operations the result of transformation can be incorrect. Thus, as a rule, errors can be detected only after algorithm termination and the repetition encryption/decryption operations are required or sometimes errors remain undetectable. The indicated defects reduce the device operational reliability because of failures of storage devices and units of information conversion.

One known technique is simply to feed the input data to two different and independent encryption units at the first site, and compare the final result of each unit to the other. If they both are identical then it is assumed that both encryption units performed correctly, if they differ it is possible to assume that at least one unite is in error, and the encryption process is repeated again in each encryption unit. Similarly, performed the decryption data process. Disadvantages of such units are doubling of the encryption and decryption hardware and, besides this the error will be detected only after encryption/decryption completion that increase detection and error-correction time.

There is also known improved DES unit [1], with internally circuitry of checks that the encryption or decryption has been performed without error. In the improved DES unit, data check bits that correspond to the input data which has been expanded are exclusive NORed with key check bits that corresponded to the key, and a result of the first exclusive ORing to identify any errors in the operation of the basic DES unit. Also, a check selection function is performed on the result of the first exclusive ORing. A result of the check selection function is exclusive NORed with data check bits for another part of the input data to yield input data for input to the expanding function for a next iteration. The improved DES unit also checks for accuracy in processing an input key by permuted choicing the input key, key shifting a result of the permuted choicing, and checking a result of the key shifting against key check bits which correspond to the input key and bypass the permuted choicing and key shifting functions.

In the next section the example of the proposed error-detection/correction cryptoscheme is presented.

## II. Exploiting error-detection/correction for cryptography schemes

Partly based on the technique described above [1], we offered a method of fault tolerance ensuring cryptography transformation by introduction of error correction circuits for store and check schemes of main algorithm operations and with smaller quantity of the redundant equipment. Let consider this method on the GOST 28147-89 cryptoscheme example [2].

As shown in Fig.1 the control units for arithmetic and logic operations, units of error-checking (or encoders/decoders), additional stores for information checking of a key storage (*X*), unit of substitution (*K*) and main stores (*N*) are entered into the cryposcheme.

During recording each data word of store is supplemented with checking (control) bits, which are previously formed on the basis of the used correcting code [3] or by encoders (*CD*) and written in appropriate additional stores. Error-detection and correction, incipient in information bits, is possible at data read-out with the help of check bits and equipment of decoding (*DC* or *CD/DC*). Besides, the computation check of main arithmetic and logic operations is implements in the scheme through methods of a control based on properties of comparison (modulo control) with the help of control units' (*check* units fig. 1) [4].

The offered device of cryptography transformation contains except of standard memory elements (stores) X, K, $N_{1\text{-}6}$ appropriated by them $X_r$, $K_r$, $N_{1\text{-}6r}$ $r$-bits additional stores (the number of bits in additional stores is determined by power of the used correcting code). In write mode, parallel with information entering in stores their check bits are calculated and recorded in appropriate additional stores. Contents of stores and additional stores appropriate to them, entering in error-checking units which correct errors during information read-out. Essentially, the filling of the main and additional stores represents information and check parts of the systematic correcting code *(32+r, 32)*, with $t$ error-correcting capability, and correction unit – noise combating encoder.

For a control of the congruence $2^{32}$ addition in summator $Cm_1$, the items as well as sum, entered in control unit. The adding control unit operates on the basis of a control modulo $p$ method. Let's signified items as *A* and *B*, and their sum as

$A+B=C$. For a control it is expedient to go on from the binary input information representation to new scale of notation with nonagenary $q=2^s$. The control codes can be compute by bit splitting into groups on $s$ bits with the subsequent addition modulo $p=(2^s \pm 1)/m$ of these groups, where $m$ and $s$ - some whole positive numbers $(s \geq 2)$. This process of convolution [3] it is possible to present as:

$$r_A^{'} \equiv \sum_{i=1}^{32/s} a_i (\bmod p); \tag{1}$$

$$r_B^{'} \equiv \sum_{i=1}^{32/s} b_i (\bmod p); \tag{2}$$

$$r_C^{'} \equiv \sum_{i=1}^{32/s} c_i (\bmod p), \tag{3}$$

Where $a_i$, $b_i$ and $c_i$ - binary representation of numbers in a system nonagentary $2^s$, $r_A^{'}$, $r_B^{'}$, $r_C^{'}$ - control codes for *A*, *B* and *C* correspondingly.

The *C* control code is discovered through control codes of items (1), (2) and (3), namely:

$$r_C \equiv \left[r_A^{'} + r_B^{'} - \alpha\right](\bmod p), \tag{4}$$

$$\begin{cases} \alpha = 0 \ , \ A+B<2^{32} \\ \alpha = 1 \ , \ A+B \geq 2^{32} \ . \end{cases}$$

Then control unit checks the correspondence of convolutions $r_C^{'}$ and $r_C$. At their coincidence the operation is executed correctly. In case of an incongruity of convolutions the signal about an error is exhibited (error flag turn on), and operation iterates again. Simple enough obtaining of control codes without the considerable time consumption is the main advantage of the given method.

Circular shift control unit realizes the control of circular shift on eleven steps in the side of high bits (according to algorithm) in the R register.

Let's enter the following designations. Let value before shifts be *D* and after circular shifts - $\bar{D}$. In appropriate way we shell designate their control codes: $r_D$ and $r_{\bar{D}}$. Then:

$$r_D \equiv \sum_{i=1}^{32/s} d_i (\bmod p), \tag{5}$$

$$r_{\bar{D}} \equiv \sum_{i=1}^{32/s} \bar{d}_i (\bmod p) ; \tag{6}$$

$r_{\bar{D}}^{'}$ - is computed per eleven times of appropriations fulfillment:

$$\begin{cases} r'_{\bar{D}} \equiv \bar{r}_D + d_{k_s} \bmod(2^s - 1), & (7) \\ \bar{r}_D \ = \ r_D^{'} \ , & (8) \end{cases}$$

where the first value of $\bar{r}_D$ is shifted control code $r_D$, $d_{k_s}$ - high bit of the control code $r_D$. The control unit of circular shift checks correctness of circular shift fulfillment by matching $r_{\bar{D}}^{'}$ and $r_{\bar{D}}$. At an incongruity of control codes the error signal is given.

The control unit of summator Cm$_2$ modulo two, with items and result of addition designated as *E*, *F* and *G* $(G = E \oplus F)$ accordingly, compare values $r_G$ (control code *G*) and $r_\oplus$, calculated as follows:

$$r_G \equiv \sum_{i=1}^{32/s} g_i (\bmod p) , \tag{9}$$

$$r_\oplus \equiv r_{E+F} + \bar{\bar{r}}_{E \wedge F} (\bmod p); \tag{10}$$

here $r_{E+F}$ - control code of the sum *E* and *F*, $\bar{\bar{r}}_{E \wedge F}$ - inversion of the control code of logical multiplication *E* and *F* with shift of the code to the left on one bit. At an incongruity of control codes $r_G$ and $r_\oplus$ the error signal is given.

The principle of control unit addition modulo $(2^{32}-1)$ functioning differ from operation of the control unit modulo $2^{32}$ (4) in calculation of value:

$$r_C \equiv \left[r_A^{'} + r_B^{'}\right](\bmod p), \tag{11}$$

for $A+B \geq 2^{32}$ and $A+B > 2^{32}$.

## III. Conclusion

The offered method make no influence on algorithm functioning. However advantage of the given method scheme development consists in increase of hardware fault tolerance, and consequently, in a functioning reliability and obtaining of correct results from the point of algorithm implementation view. Really, the redundant schemes of checks allow to neutralize both the memory elements failures influence at reading/recording and errors in different arithmetic and logic operations units (even during transformations fulfillment), as against in unit [1]. Frequently errors originating in the devices, remain undetected, in case of detection they are difficulty enough localized and lead to throughput degradation in two and more times, that is eliminated by the offered method.

## References

[1] United States Patent №5432848, Int. CL. H04K 1/00, H04L 9/06 (1995).

[2] GOST 28147-89. *Data reduction system. Protection cryptography. Algorithm of cryptography transformation.*

[3] Richard E. Blahut *Theory and practice of error control codes*. Addison-wesley PC, (1984 ).

[4] Saveliev A. *The applied theory of digital automats*.-Moscow:, (1987).

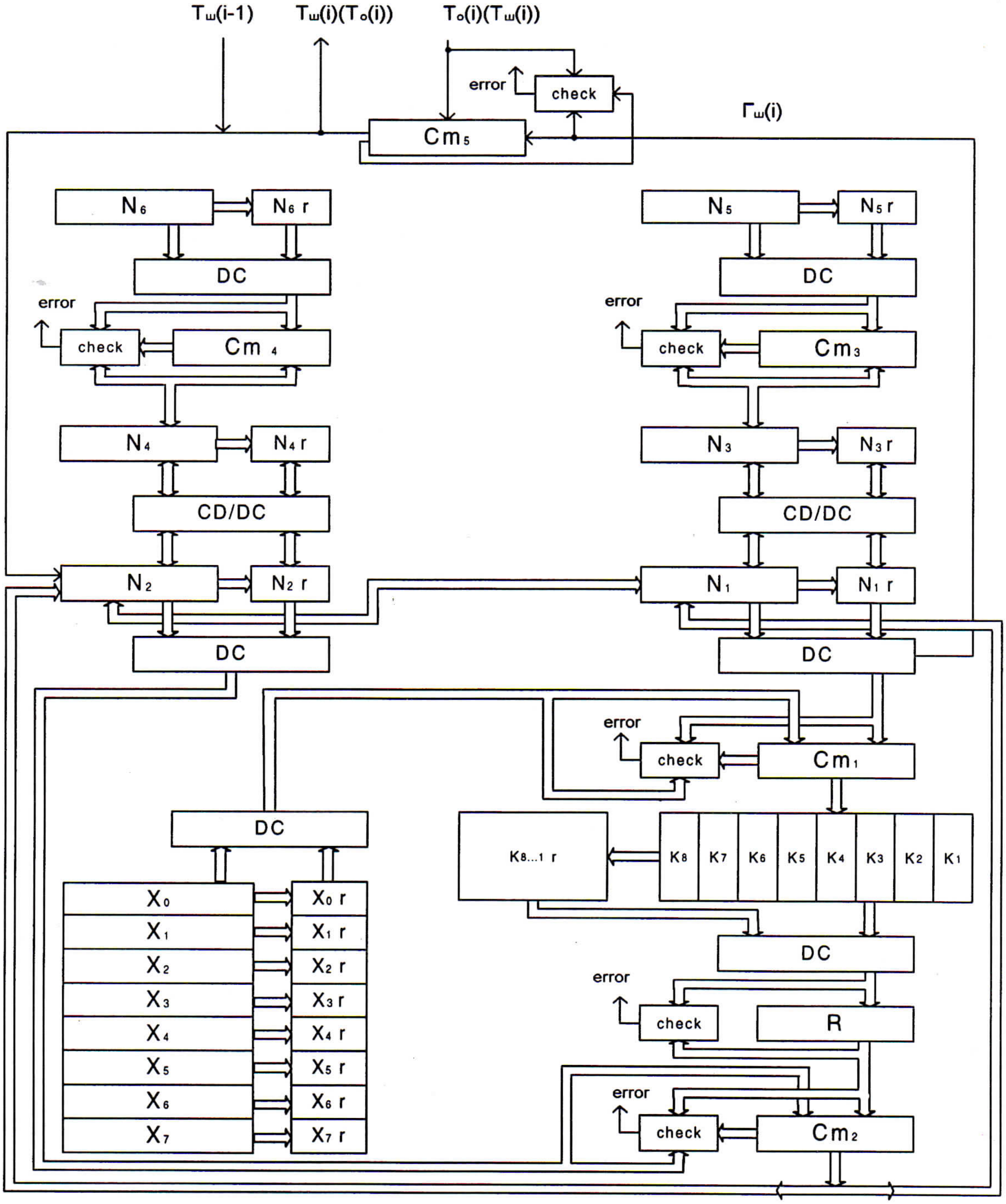

Figure 1. GOST 28147-89 cryptoscheme with error-detection and correction circuity.