Технические науки и современное производство

ENCRYPTION BASED ON MULTIVARIATE REPRESENTATION OF VIRTUAL KEY BANDS SAMPLE SPACES

Kotenko V.V., Rumyantsev K.Ye.,
Polycarpov S.V., Levendyan I.B.
Taganrog State University of Radioengineering , Taganrog, Russia

Implementation of key bands virtual sample spaces strategy based on multivariate performance of sample spaces takes a special place among possible variants of given strategy implementation. First of all, it speaks opening possibility of different mathematical model using. In this case multivariate performance is a collection of virtualization procedures $VIR_j(K_{nd}(i))$, each of them is considered to be a separate measurement. From these positions process of virtual key $K_V^M(t)$ creation can be represented as initial key in some M-dimensional space simultaneously on all to his(its) measurements virtualization with the subsequent unification of virtualization results into some function of this space which will represent a virtual key:

$$K_V^M(t) = UNIF(K_V^j(t)), \quad (1)$$

$$K_V^j(t) = VIR_j(K_{nd}(i)), \quad (2)$$

Where UNIF(.) - unification procedure;

$VIR_j(.)$ - virtualization procedure defining j-measurement;

$K_{nd}(i)$ - initial key formed on the basis of given key data K_d;

$K_V^j(t)$ - projection of virtual key onto j-measurement;

The unfolded key is formed by obtained virtual key devirtualization:

$$K_r^M(i) = DVIR_M(K_V^M(t)). \quad (3)$$

Expressions (1) - (3) define common algorithm of unfolded key creation at multivariate performance of key bands virtual sample spaces. The concrete definition of the given algorithm is carried out by unification procedure definition . Variants of such concrete definition are represented by expressions (4) and (5)

$$K_r^M(i) = DVIR_M\left(\sum_{j=1}^{M}(K_V^j(t))\right), \quad (4)$$

$$K_r^M(i) = DVIR_M\left(\prod_{j=1}^{M}K_V^j(t)\right). \quad (5)$$

Software implementation of the algorithms given in expressions (4), (5) allowed software encryption complex creation, which opens a possibility of absolute undeciphering capability support. Experimental researches of the complex confirm its significant potential possibilities. Given results are obtained during researches at Russian Federation Education Ministry grant T02-03.1-816 support.

The bibliographic list
1. Kotenko V.V., Polycarpov S.V. The strategy of key bands virtual sample spaces creation at information protection problem solving//Information Security Problems . 2002. №2. p 47-52.

ENCRYPTION WITH PARALLEL COMPLICATING VIRTUAL SAMPLE SPACES OF KEY BANDS

Kotenko V.V., Rumyantsev K.Ye.,
Polycarpov S.V., Levendyan I.B.
Taganrog State University of Radioengineering , Taganrog

Possibility of absolute undeciphering capability support which is opened by key bands sample spaces virtualization strategy [1] defines an urgency of further researches in the given direction. Results, obtained in nowadays, show that one of given strategy implementation variants is parallel complicating of virtual sample spaces. Parallel complicating in this case is virtual key creation and its devirtualization simultaneously on M independent channels. Thus, unfolded key is formed by unification of used channels devirtualization results. Thus, the algorithm of work key creation may be represented as

$$K_V^j(t) = VIR_j(K_{nd}(i)) \quad (1)$$

$$K_V^j(t) = VIR_j(K_{nd}(i)) \quad (2)$$

где

UNIF (.) – unification procedure;

VIR_j (.) – j-channel virtualization procedure;

$DVIR_j$ (.) – j-channel devirtualization procedure;

$K_V^j(t)$ – channel virtual key;

$K_{nd}(i)$ – initial key formed on given key data K_d basis

Order of virtual sample space complicating in this case is determined by number of parallel-way-used channels j. The reduced algorithm is common. Its concrete definition is made by unification procedure choice. It is necessary to underline, that here opens wide action field for researcher. For example adding and multiplying of channels devirtualization results can be used as this procedure. In first case unrolled key creation algorithm becomes as represented in expression (3), in the second case - in expression (4)

$$K_r^M(i) = \prod_{j=1}^{M} DVIR_j(K_V^j(t)) : \quad (3)$$

$$K_r^M(i) = \sum_{j=1}^{M} DVIR_j(K_V^j(t)) \quad (4)$$

Implementation of given algorithms allowed creation of encryption software complex which opens possibility of absolute undeciphering capability providing. The re-