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-

searches spent in direction of given complex perfecting yield reassures results, representing scientific and practical interest. 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 KEY BANDS VIRTUAL SAMPLE SPACES SEQUENTIAL COMPLICATING

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

The urgency of absolute undeciphering capability providing problem solution in modern conditions is determined by increase of information technologies role. Recently defined progress was planned in this direction. So, in [1] the strategy of the given problem solution on a basis of key bands sample spaces virtualization was offered. The subsequent researches allowed to receive a number of given strategy implementation variants. One of such variants is an encryption based on sequential complicating of key bands virtual sample spaces. Its basis is made with recurrent algorithm (1) of virtual key creation :

$$K_V^j(t) = VIR_j(DVIR_{j-1}(K_V^{j-1}(t))),\ j = 1...N \quad (1)$$

where

$VIR_j(\,.\,)$ – virtualization procedure;

$DVIR_j(\,.\,)$ – devirtualization procedure;

j – order of complicating level .

The obtained algorithm assumes multiple sequential virtualization and devirtualization of key band. Thus on each virtualization step virtual key obtained on the previous step devirtualization result appears as an initial key. The entry condition $DVIR_0(K_V^0(t))$ of given algorithm operation is the initial key $K_{nd}(i)$, formed on given key data K_d basis:

$$DVIR_0(K_V^0(t)) = K_{nd}(i). \quad (2)$$

The unfolded key $K_n^N(i)$ is formed by devirtualization of virtual key obtained on a finite N step of complicating:

$$K_n^N(i) = DVIR_N(K_V^N(t)) \quad (3)$$

On the given approach basis the set of encryption modes with virtual key sequential complicating, opening possibility of absolute undeciphering capability providing was obtained. Their implementation allowed creation of software complex of encryption possessing unique possibilities. Experimental researches showed high reliability and efficiency of the complex.

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.

QUANTUM CRYPTOGRAPHY PROTOCOL BB84 EFFICIENCY RESEARCH WITH CODING ONE-PHOTON STATUSES ON POLARIZATION

Khairov I.Ye., Rumyantsev K.Ye.,
Novikov V.V., Trotsuk E.V.
Taganrog State University of Radioengineering , Taganrog, Russia

In nowadays the enhanced attention to confidential information transmission systems all over the world is devoted. One of the most perspective and newest direction in the field of cryptography is quantum cryptography. As show researches in the given area, the combination of quantum cryptography methods of private key allocation and classical methods of encryption will allow to create fundamentally protected systems of confidential information transmission.

One of quantum cryptography protocols which is most spread now is BB84 protocol. In the given protocol one-photon statuses may be modulated on polarization or on a relative phase. Each of these modulation methods has the advantages and lacks. In particular, polarizing modulation is most preferable at data transfer on open optical channel while modulation on a relative phase may be used in fibre-optical communication systems.

In this work efficiency of quantum cryptography protocol BB84 with coding one-photon statuses on polarization is researched. With this purpose was developedt software complex for computer which allows taking into account both parameters of transmitting and reception units, and parameters of quantum data link. At photons sequence generating on transmitting unit in model two situations are possible:

1) The amount of photons of optical impulse duration is strictly fixed. The given situation allows to estimate efficiency of the protocol at ideal one-photon or multiphoton laser usage.

2) The amount of photons for duration of optical impulse is accidentally and is subordinate to Poisson law with given average $\bar{n}$. Thus generation of pseudorandom numbers n, having Poisson distribution with average $\bar{n}$, was carried out using method offered by Caen. During simulation the analysis of this algorithm [1] was spent. The sequence of random variables generated thus has expectation and a dispersion distinguished from value $\bar{n}$ on the 100-th long of percent. It confirms legitimacy of offered algorithm usage under law of Poisson random numbers generation .

As parameter of the photoreception unit its quantum efficiency describing probability of optical into electrical signal conversion used. Given parameter, along with