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 :

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

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:

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

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

$$K_n^N(i) = DVIR_N(K_V^N(t)) \tag{3}$$

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