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 noise properties od photo-recieving equipment, is one of defining efficiency of all communication system.

At simulation optical radiation quantum data link losses with absorption and scattering of radiation were taken into an account. Also, situation with presence in the channel of intercepting agent was modelled. Thus two situations were researched:

1) Interception and generation by the malefactor of all photons for optical impulse duration. The given situation allows to model real communication systems.

2) Selection of only one photon for impulse duration. This situation allows to estimate quantum cryptography efficiency protocol at malefactor with the ideal equipment, permitting to realize unauthorized data acsess presence .

Thus, spent researches allowed to estimate efficiency of quantum cryptography protocol BB84 at polarizing modulation usage.

The bibliographic list:

1. Radio-electronic technologies of information safety: Collection of scientific articles / Under. edition. K.E.Rumjantseva. - Taganrog: TSURE, 2002. - With. 145-155.

ANALYSIS of KEY SEQUENCE METHODS CREATION In MULTI-USER QUANTUM COMPUTER NETWORKS

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

The rough development of quantum computers and the technologies connected to them in the recent times reduced to appearance of some revolutionary achievements, capable significantly speed up scientific and technical progress. The quantum cryptography concerns to such an achievements.

Key generation by quantum cryptography methods is carried out immediately during transmission of single photons on a data link. Reliability of these methods is founded on fundamental laws of quantum physics firmness.

Quantum cryptography systems originally were used for communication of separate pairs users. However development and research of similar methods for communication of a great many of users is actual. Researches in the given direction are actively carried on both foreign and domestic centres of science.

As researches have shown known methods of private key allocation use tree-like topology of the network or ring with necessity of additional channels of information interchange usage. In particular, methods of quantum cryptography can be used at passive optical network construction containing the central network controller, connected by a passive optical beam splitter with set of network users. In this scheme quantum behaviour of an optical beam splitter is used. Accordingly, each user will be provided with a unique arbitrary selected bits subset.

Other quantum-cryptography system contains a quantum link with a set of sites including transmitting and reception units, connected with a quantum data link. Transmitting unit generates the light signal representing a sequence of photons, for allocation through the quantum channel. Receiver of the message accepts the light signal radiated by the transmitter and measures quantum statuses of this signal. The given method of optical network organization uses ring topology; however its main virtue is that each of users may be the initiator of data exchange.

Thus. private key allocation method development problem between a great many sequentially located users without additional channels of information interchange is actual. In thw work new method of optical network organization in which there is an allocation of private key with usage of quantum cryptography is offered. The given method is based on a principle measurement - repeated sending off and applicable in systems with modulation on polarization.

Researches also showed, that at immediate usage of given method, exchange process of is characterized by the big percent of errors. However, with introduction to the considered network of subsystem synchronization between polarizing analyzers of users, given method will correspond to protocols used for data exchange between several users.

The given optical network of private key allocation by methods of quantum cryptography can also be applied to network with ring topology.

Main problem of practical implementation of the similar optical network is support of exact synchronization of polarizing analyzers turns of great many sequentially the located users. As the probability of polarized photon passing through the analyzer is proportional to cosine of a corner between direction of polarization and an axis of the analyzer, inaccuracy of synchronization may make units of degrees.

ФАЗОВЫЕ ПЕРЕХОДЫ МЕТАНА ПРИ ИЗМЕНЕНИИ ТЕРМО-ДИНАМИЧЕСКИХ ПАРАМЕТРОВ ГОРНОГО МАССИВА

Беспятов Г.А.
Кузбасский Государственный Университет, Кемерово

Для построения математической модели фазовых превращений метана примем во внимание, что образование метана в период накопления торфяника и постепенного погребения его под наносы последующих отложений происходило при температурах 150-300^{o}C, когда сорбционная способность угля была близка к нулю. В дальнейшем, в процессе инверсии и понижении температуры, часть метана сорбировалась углем, часть оставалась в свободном состоянии как в трещинах и микропорах угля, так и в коллекторах вмещающих пород. Дальнейшее изменение термодинамических параметров угленосной толщи влекло за собой переход свободного газа в гидратированное состояние. Образование гидратов метана происходит либо при низких температурах (t=12-14 ^{o}C) при $P = 10$МПа, либо при высоком гидростатическом давлении, большем чем в современных условиях. Например, для равновесного состояния гидрата метана [1]