УДК 004.056.55

PROSPECTS OF QUANTUM TECHNOLOGIES IMPLEMENTATION IN SECURITY OF E-BANKING SYSTEMS IN UKRAINE

S. O. Gnatyuk, V. M. Kinzeryavyy, S. V. Prystavko, E. V. Didych

National aviation unevercity

SergiyGnatyuk@meta.ua

Проаналізовано поточну ситуацію щодо інформаційної безпеки систем електронного банкінгу. Розглянуто найпоширеніші проблеми захищеності, що можуть виникнути. Показано як квантові технології дають змогу вирішити проблеми безпеки систем дистанційного банківського обслуговування. Також описано перспективи впровадження квантових технологій у системи електронного банкінгу України для підвищення рівня інформаційної безпеки.

This article describes the analysis of current situation with information security in e-banking systems. Here are considered the most common security problems which may arise. And is shown how quantum technologies can solve such security problems of e-banking systems. Also here are described prospects of implementation quantum technologies in e-banking systems in Ukraine to enhance information security.

Introduction

Providing security is the main objective for any system despite its complexity and purpose. This can be any social system, any biological organism or any information system. Nowadays we can see information technologies almost in every human activity. Computers are serving for banking systems support, controlling nuclear reactors, controlling flights, satellites and space ships. Therefore people require high level of liability of such systems. Computer felony or other non legitimate actions can break the activity of organizations all over the world. There are difficulties which put limitation on reacting to such threats [1]:

- There is no perfect laws in this branch of activity;
- There are no certified systems of information processing (OS, SCDB and other).

Cryptography has the purpose of providing information security. Classical cryptography is divided into two branches regarding how it works with encryption keys. There are symmetric and asymmetric crypto systems.

Recent years we can observe increased interest to quantum cryptography [2]. This is very “young” science. But it has been rapidly developed for the last 25 years from simple hypothesizes to practical experiments and very promising results. Now we can see concrete solutions which quantum cryptography gives us in solving problems of information security. Quantum technologies in prospect can be used in banking institutions in Ukraine to provide secured data transmission.

E-banking security analysis

Nowadays every banking institution uses different automatic systems of information procession. This systems deal with information which is very critical and important for banks (i.e. this can be client’s data-files, numbers of client’s credit cards, signed agreements with partners). Usually such information refers to confidential information [3].

Such information is real money for banks. Computer systems are using this information for making payments, money transfers and other operations. And banking organizations are responsible before their clients for providing security of such types of information against unauthorized access. The loss of this information can make a great damage and can undermine the reputation of the organization [3]. Thus organization will lose its profits.

One of the most rapidly developing banking services is on-line banking and exchange of electronic data. This service allows customers to have access to their bank accounts through the internet, thus allowing them to make money transfers, different payments or purchasing some goods. This is very convenient service, because you can do any operation without leaving your home or working place. Providing this service put very strong requirement on protection of the transferred information. Everyone knows that transferring data through the Internet is very risky. Thus the more the service of on-line banking is used the more accidents of stealing the confidential information will appear. Statistics shows us how much money banks lose every year from hacking computer systems (i.e. stealing or decrypting passwords). Numbers are stunning: from 170 million to 41 billion dollars per year.

There are two main problems when talking about on-line banking service. First is secure key distribution. Encryption keys must be delivered to users with the minimum probability of stealing or intercepting them. Second problem is verification of legitimate users. While making e-payments customer signs his e-document that second party (bank) can recognize that this document was really sent by the customer. To solve these tasks classical cryptography [1; 2] is used. More precisely, different methods of data encryption and digital signature are used now in on-line banking systems to ensure protection of the confidential user’s data while transferring it. The problem is that such methods do not provide sufficient level of information security. The intercepted encrypted data can be easily restored by the unauthorized user if he has enough computing resources (this is not a problem with today's highly developed computer systems). The main goal is enhancing security of key distribution and user's verification. This can be done by using quantum cryptography technologies.

Main objectives

This article has several objectives:

- Definition of problems and vulnerabilities of e-banking systems in Ukraine;
- Analysis of possibilities to enhance information security of e-banking by using quantum technologies;
- Comparison of existing quantum technologies and showing their advantages over classical system which are used now in banks.

Ability of quantum technologies

Quantum cryptography technologies can help enhance security of key distribution and data protection in on-line banking. These are Quantum Key Distribution (QKD) [5; 6], Quantum Secure Direct Communication (QSDC) [7; 8] and Quantum Digital Signature (QDS) [9].

QKD is one of the most developing methods of information security based on quantum mechanics. Its main advantage is the possibility of detection of the interference within the system. Another advantage is the possibility of eavesdropping detection. This property follows from the basic theorem of quantum mechanics and no cloning theorem which says that any measurements of quantum states within the channel, inevitably leads to the changes in the system. Quantum mechanics establishes a set of negative rules stating things that cannot be done. For example [5]:

1. Every measurement perturbs the system.
2. One cannot determine simultaneously the position and the momentum of a particle with arbitrary high accuracy.
3. One cannot measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
4. One cannot draw pictures of individual quantum processes.
5. One cannot duplicate an unknown quantum state.

QKD uses following features:

- Authentication;
- Error checking;
- Privacy amplification.

There are also systems for d-level systems [6]. QKD system can be combined with the encryption system based on classical cryptography with absolute strength so that the entire system will have theoretical information strength. The QKD systems also have shortcomings. These are high price of such systems, afrerpulsing effect, and difficulty of realization for d-level systems. QKD has advantages over other methods of key distribution described in [5] such as:

- Classical information-theoretic scheme;
- Classical public-key cryptography;
- Classical computationally secure symmetric-key cryptographic scheme;
- Trusted couriers' method.

QKD combined with the encryption algorithm based on classical cryptography can be used in online banking for the key distribution purpose. The encryption key will be created using quantum technologies which exclude any interception or system violation by the third party. Such keys have greater strengthen before their classical analogs. Thus total strengthen of the entire system will increase. Then banking institution and customer can securely exchange their private information.

Another way of using QKD is inside bank network. It will be used to limit access to the key-generator module. This follows from the fact that it is not secure to send private encryption keys for internal payment systems. Because in some cases the program module of generation encryption keys can be built into the software which bank provides to its customer. And having access to such module third party can disclose the algorithm of key's generation. Therefore modules for generation of bank's encryption keys and user's encryption keys are divided and are placed in different locations. Using QKD we can limit number of people who has access to the software module of encryption key generation.

QSDC requires use of quantum superdense coding, ERP-pairs, GHZ-triplets (and other) for sending messages between users without encryption and key distribution [8]. Usually transfer of qubit blocks is used. This allows detection any measurement or violation before the data exchange starts. One and the most important advantage of the QSDC systems is high level of information security [7; 8]. Here we can talk almost about totally secured system. To the shortcomings of QSDC systems we can refer:

- need of large sizes of memory;
- vulnerability to "man-in-middle" attacks;
- complexity of practical realization of QSDC systems.

QSDC system in prospect can be used in banking activity. This method requires the presence of direct channel between two parties. Thus, there appear some limitations on using QSDC technology. But still it can be applied to provide information security in banking activity. For example, for the transfer secret information between headquarter and branches. Or QSDC systems ban be used between geographically divided SEP-servers and ensuring the data replication between databases. We can also use QSDC system in connection central servers of CPS client-bank and common center of encryption keys certification. Using QSDC systems we can have totally secured channel for transferring data. Thus nobody will be concerned about the loss of any secret data.

Another quantum technology is QDS [9]. QDS security is based on fundamental principles of quantum physics [10]. QDS scheme allows a sender (Alice) to sign a message in such a way that the signature can be validated by a number of different people, and all will agree either that the message came from Alice or that it has been tampered with. To accomplish this task, each recipient of the message must have a copy of Alice's "public key," which is a set of quantum states whose exact identity is known only to Alice. Quantum public keys are more difficult to deal with than classical public keys: for instance, only a limited number of copies can be in circulation, or the scheme becomes insecure. However, in exchange for this price, we achieve unconditionally secure digital signatures. Quantum digital signature scheme is absolutely secure, even against powerful quantum cheating strategies. This scheme is somewhat cumbersome, but the underlying principles suggest novel research directions for the field of quantum cryptography. While quantum public keys are more limited than classical public keys, they remain more powerful than private keys, and the existence of an unconditionally secure quantum digital signature scheme suggests an as-yet unrealized potential for quantum public key cryptography.

Classical digital signature schemes can be created out of any one-way function. Similarly quantum digital signature scheme is based on a quantum analogue of a one-way function [9] which, unlike any classical function, is provably secure from an information-theoretic standpoint, no matter how advanced the enemy's computers. QDS is also applicable to usage in on-line banking. Using QDS we obtain more secured algorithm of generation our e-signature. Then if customer sing any of his electronic documents using QDS method bank will ensures enhanced and more secured method of validation of the sender and exclude the possibility of violation of the document by a third party.

Conclusion

Thus, after such analyses we can see that usage of quantum technologies can solve the problem of low-level information security in electronic systems which nowadays are used in banking institutions. Thus, it is a good idea to use quantum technologies for providing information security in the electronic banking systems in Ukraine. We hope that in the nearest future we will see that Quantum Key Distribution systems, Quantum Secure Direct Communication systems, and Quantum Digital Signature systems will be providing high level of information security in banking institution in our country.

There are also other quantum technologies such as Quantum Stenography, Quantum Secret Sharing, Quantum Bit Commitment, Quantum Coin Tossing, and Quantum Gambling. The progress of their research and development has been just started. But with such rapid development of quantum cryptography which we can see in XXI century we can see the usage of such systems in e-banking technologies in the nearest future.

There also exist threats were even quantum cryptography cannot help. These are usage of non-certified devices for information security, mistakes which can be made on the projecting faze of security system, and human factor.

REFERENCES

1. *Грездов Г. Г.* Современные методы криптографической защиты информации (обзор по материалам открытой печати) / Г. Г. Грездов. — К., 2002. — 32 с.
2. *Gisin N.* Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. — 2002. — V. 74. — Pp. 145—195.
3. *Задірака В. К.* Методи захисту банківської інформації: підруч. / В. К. Задірака, О. С. Олексюк, М. О. Недашковський. — К. : Вища шк., 1999. — 261 с.
4. *Smart N.* Cryptography: An Introduction (3rd edition). — McGraw Hill, 2009. — 433 p.
5. *SECOQC* White Paper on Quantum Key Distribution and Cryptography. — Preprint: http:// www. arxiv.org/abs/quant-ph/0701168v1. — 2007. — 28 p.
6. *Cerf N.J., Bourennane M., Karlsson A., Gisin N.* Security of quantum key distribution using d-level systems // Physical Review Letters. — 2002, № 12. — V. 88, — Art. 127902.
7. *Wojcik A.* Eavesdropping on the «Ping-Pong» Quantum Communication Protocol // Physical Review Letters. — 2003. — Vol. 90, № 15. — 157901.
8. *Deng F.-G.* Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block / F.-G. Deng, G.L. Long, X.-S. Liu // Physical Review A. — 2003. — V. 68, № 4. — 042317.
9. *Wang J., Zhang Q., Tang C.* Quantum signature scheme with single photons // arXiv:quant-ph/0511224v1.
10. *Nielsen M., Chuang I.* Quantum Computation and Quantum Information. — Cambridge University Press. — 2000. — 676 p.

Стаття надійшла до редакції 6.10.09.