Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):1-4
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

MODIFIED ONE TIME PAD

Maksim Iavich, Zura Kevanishvili
Caucasus University, European School

ABSTRACT

Theoretically, quantum computers will be able to solve quickly the problems that classical computers would solve for thousands of years. This technology can change our world. A typical user will not need a quantum computer for a long time, maybe never. But using quantum computer it is possible to break all existing crypto systems. American mathematician Peter Shore invented a quantum algorithm that can factorize a large number into two simple factors very quickly. Unfortunately, classical computers make it very slowly. Classical computers can do it by sorting out all the combinations, but it will take million years. Safety of modern cryptographic algorithms is based on this weakness of classical computers, for example RSA. RSA BSAFE encryption technology is used approximately by five hundred million users in the world. RSA BSAFE is a validated cryptography library offered by RSA scheme. As we can wee RSA is the mostly used crypto system and it can be considered one of the most common public key cryptosystems that is developing together with development of Internet. Breaking RSA is a global problem and it can lead to breaking almost all the products in the world

One Time Pad (OTP) cipher is an example of a system with absolute cryptographic stability, this is system with perfect secrecy. It is considered one of the simplest cryptosystems. The biggest problem of one-time pad cypher is that it has one-time key. If the key is used to encrypt more than one message, the cypher is not secure.

In the article is offered the new modified variation of OTP, that is safe against quantum computer attacks.

Introduction.

Quantum computer is a computing device that uses quantum superposition and quantum entanglement phenomena to transmit and process data. Although the appearance of transistors, classical computers and many other electronic devices is associated with the development of quantum mechanics and condensed matter physics, the information between the elements of such systems is transferred in the form of classical quantities of ordinary electric voltage.

A fully-fledged universal quantum computer is still a hypothetical device. The very possibility of fully-fledged universal quantum computer needs the serious development of quantum theory in the field of many particles and complex experiments.

Developments in this field are related to the latest discoveries and achievements of modern physics.

Theoretically, quantum computers will be able to solve quickly the problems that classical computers would solve for thousands of years. This technology can change our world. A typical user will not need a quantum computer for a long time, maybe never. But using quantum computer it is possible to break all existing crypto systems.

In the 90s of the last century, the American mathematician Peter Shore invented a quantum algorithm that can factorize a large number into two simple factors very quickly. Unfortunately, classical computers make it very slowly. Classical computers can do it by sorting out all the combinations, but it will take million years. Safety of modern cryptographic algorithms is based on this weakness of classical computers, for example RSA.

RSA crypto-system with the key of length four thousand bits is considered safe from classical computers attacks, but it is vulnerable against attack of quantum computers [1,2].

To date, almost all valuable information that is transmitted over the Internet, is encrypted using RSA. This includes banking transactions, secret negotiations, and even your correspondence in social networks. Decipher all this with the help of classical computers is almost impossible.

Many products on various platforms in different areas use RSA encryption.

Now cryptosystem RSA is used by almost every commercial product, the number of which increases very quickly. RSA system is also widely used in from Microsoft, Apple, Novell and Sun operating systems also use RSA. RSA algorithm is used also in hardware; it is used in network cards, smart cards and Ethernet. RSA is used in cryptographic hardware also.

RSA algorithm is a part of the protocols protected Internet communications, like S / MIME, SSL and S / WAN.

RSA BSAFE encryption technology is used approximately by five hundred million users in the world. RSA BSAFE is a validated cryptography library offered by RSA scheme. As we can wee RSA is the mostly used crypto system and it can be considered one of the most common public key cryptosystems that is developing together with development of Internet.

As we see breaking RSA is a global problem and it can lead to breaking almost all the products in the world [3].

2. OTP

Vernam Cipher is a symmetric encryption system invented in 1917 by AT & T employee Gilbert Vernam.

This cipher is a kind of cryptosystem of one-time pad crypto systems. It uses boolean function "Exclusive OR"(xor). The Vernam cipher is an example of a system with absolute cryptographic stability, this is system with perfect secrecy. It is considered one of the simplest cryptosystems [4,5].

To get the cypher in one-time pad, message is xored with they key.

c= m xor k

For decryption cypher is xored with the message

m= x xor k

The biggest problem of one-time pad cypher is that it has one-time key. If the key is used to encrypt more than one message, the cypher is not secure.

Here we show the example where 2 messages are encrypted with the same key:

c1= m1 xor k

c2 = m2 xor k

if we calculate c1 xor c2 we get following:

c1 xor c2 = m1 xor k xor m2 xor k

c1 xor c2 = m1 xor m2

As we see cyphers can leak information about messages, if the messages are encrypted with the same key.

One-time pad is secure against attacks of quantum computers, so the biggest problem is the key distribution.

3. Modified scheme

Encryption: each letter in the message is xored with the corresponding letter in the key, so m[i] is xored with k[i] and like that is got the i-th letter of cypher.

Where m is the message and k is the key.

Afterwards m[i] is xored with the corresponding letter in the key, but in the inversed order, let us define the received number as x. So we add x random numbers to after i-th symbol in the cypher.

Decryption: The first symbol of the cipher is xored version of the first letter of the text and the first letter of the key. Thus this symbol can be reversed by being xored with the first letter of the key back into a letter of the text. Next the same symbol is being xored with the last letter of the key. The received number is the amount of pseudo random numbers present after that letter before the next letter of the message. These numbers are erased and the same process is then repeated for each letter of the cipher text until no more letters are left to decrypt.

5. Conclusion

In the new crypto system, we do not have already one-time key problem, the system is secure against quantum computers attacks, but must be mentioned that the scheme does not have perfect secrecy.

Must be carried out the work on the reducing of cypher’s size.

Acknowledgement. The work was conducted as a part of joint project of Shota Rustaveli National Science Foundation and Science & Technology Center in Ukraine [№ STCU-2016-08]

REFERENCES

1. Gagnidze A.G., Iavich M.P., Iashvili G.U., Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36
2. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems," Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20
3. Bernstein D.J. (2009) Introduction to post-quantum cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg
4. Bennett, Charles H., et al. "Quantum Cryptography." Scientific American, vol. 267, no. 4, 1992, pp. 50–57. JSTOR, JSTOR, www.jstor.org/stable/24939253.
5. Gu, B., Zhang, C., Cheng, G. et al. Sci. China Phys. Mech. Astron. (2011) 54: 942. https://doi.org/10.1007/s11433-011-4265-5
6. Kocher P.C. (1996) Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz N. (eds) Advances in Cryptology — CRYPTO '96. CRYPTO 1996. Lecture Notes in Computer Science, vol 1109. Springer, Berlin, Heidelberg
7. Boneh D. (1998) The Decision Diffie-Hellman problem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science, vol 1423. Springer, Berlin, Heidelberg
8. Dominic Mayers, Quantum Key Distribution and String Oblivious Transfer in Noisy Channels, Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, p.343-357, August 18-22, 1996