SECRET KEY EXTRACTION OVER UNAUTHENTICATED PUBLIC CHANNELS

Saša Adamović
Singidunum University

Marko Šarac
Singidunum University

Dalibor Radovanović
Singidunum University

Tijana Radojević
Singidunum University

Abstract

This paper discusses the possibility of secret key extraction over unauthenticated public channels. Starting from theoretical foundations of the concept perfectly developed by Claude E. Shannon cryptographic system analyzes the specific solutions for secret keys extraction over public channels. Comparative analysis includes a quantum protocol BB84 and Maurer protocol based on common satellite distribution of correlated random sequences. BB84 protocol is designed for quantum key distribution (QKD) to replace the asymmetric protocol requires two communication channels. The first is a one-way quantum channel, and the other two-way public channel. There was great similarity between these two protocols. Maurer's protocol is in its first stage is performed differently than in the first phase of the BB84 protocol. Instead of one-way quantum channel introduces the satellite, which broadcasts a bad copy of the original random binary number generated by satellite. The remaining three phases of BB84 protocol are identical to other stages Maurer protocol. We showed that an eavesdropper shares minuscule mutual information with legitimate communicators, thereby supporting security against eavesdroppers. This paper presents a simulation of Maurers protocol and discussed some of the quantitative indicators that are very important for practical applicability of this method.

Keywords: *secret keys, protocol, public shannel, key distribution*

INTRODUCTION

In professional systems, cryptographic protection is an essential process of every information system. The goal of any organization is to protect the confidential information stored in databases and various communication channels. One of the implied conditions for success and performance is its ease of use.

In cryptographic systems is not enough for cryptographic algorithm is secret, because it is very easy to compromise, but that really should depend on the secrecy of cryptographic key. There have been numerous symmetric crypto systems that are enabled. But he remained an unsolved problem, and that the exchange or distribution cryptographic keys between people who want to communicate. 1976th In W. Diffie and M. Hellman published protocol for establishing a secret key between people who do not share any pre-shared secret information. This idea has been applied in asymmetric algorithms that use two keys: public and private encryption for decryption.

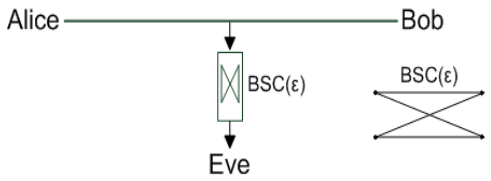


Fig. 1. *Symmetric cryptosystem*

SYMMETRICAL BINARY COMMUNICATION CHANNELS

1978th Csiszar and Korner was noted that the binary symmetric communication channel with noise can have power in the field of cryptographic key distribution. Binary symmetric (BSC) channel is a digital system in which the value of transmission error has a constant value p, equal to zero (0) and unit (1). In the case of an error output bit is a complementary input.

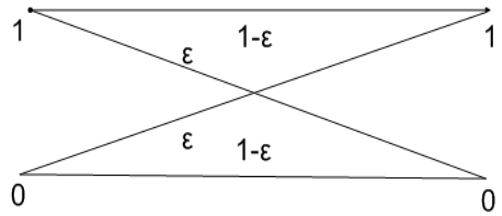


Fig. 2. *Binary symmetric channel*

In their paper "Broadcast channels with confidential messages", presented to the broadcast channel with a lower limit on the secrecy capacity **Cs (PYZlX) ≥ max [I (X, Y)-I (X, Z)].**

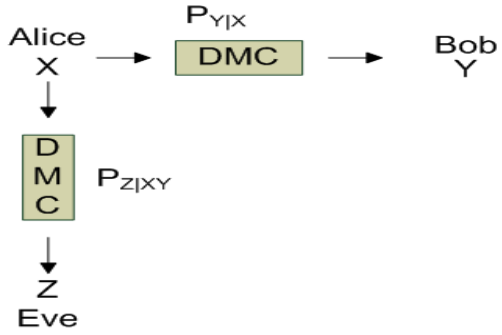


Fig. 3. *Broadcast Channel*

Csiszar and Korner were presented a scenario in which the secret transfer is possible only if the legitimate users are connected to a channel that has less noise (error) of channel eavesdroppers (Eve), which is not always an accurate assumption. U. Maurer 1993rd year, adding to the quantum protocols, proposed a protocol in which Alice and Bob can have two less correlated lower than it has Eve, and yet still manage to establish a shared key. To make this possible, Maurer has designed a special scenario in which Alice and Bob receive sequences of correlated random signals nekontrolabilnog sources and introduced the distillation phase of the advantages which Alice and Bob achieve advantage over Eve and added to the other two methods in the no-cloning of quantum protocols .

QUANTUM PROTOCOL BB84

The application of quantum cryptography is quantum key distribution key (QKD), that serves as a substitute asymmetric protocols. One of most quantum protocol is BB84. It includes two communication channels. The first is a one-way quantum channel, and the other is a two-way public channel.

The first phase of the protocol is one-way quantum channel. According to the Heisenberg uncertainty principle, the bit that Alice sends no one can accept with probability greater than 75%. The probability that the receiver chooses which base is chosen, and Alice is 50%. In this case, the probability that Bob will receive the correct bit is 1 Otherwise, if Bob has chosen the wrong base, there is still a 50% probability to be received will be interpreted correctly. It follows the budget:

P = 0.5 * 1 + 0.5 * 0.5 = 0.75 = 75%

Following so far described of the protocol Alice and Bob have bit strings of equal length but not the same bite in the same places. Eva now can have certain knowledge about these sequences, but Alice and Bob can determine the upper limit on the amount of that information.

The two-way public channel, there are two components of the protocol. The first phase of the harmonization of information (Information Reconciliation), and other privacy amplification (Privacy Amplification).

The first phase of the protocol for compliance information or error-correction protocol, whereby it is assumed that Alice has the right, and Bob the damaged array. The protocol is reduced to a series of harmonization of Bob's with Alice's. At the beginning of this stage Alice and Bob share a string of n blocks, then compare the parities. The blocks have different parities binary search to find a different bit. In this case, Bob will be inverted.

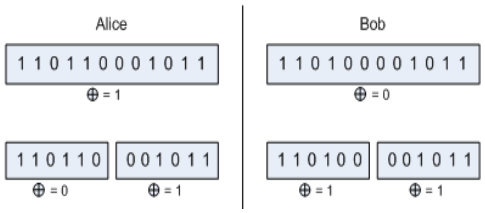


Fig. 4. *Reconciliation information*

Based on the assessment of errors in communication Alice and Bob know the upper limit of k bits that could be known Eve out of n bits in their equivalent key. The second phase of Fig. 5. in two-way protocol is to enhance privacy. This phase is a method that ensures the end of this phase a secret string that can be undertaken

through public communication into a very short range and the final secret key.

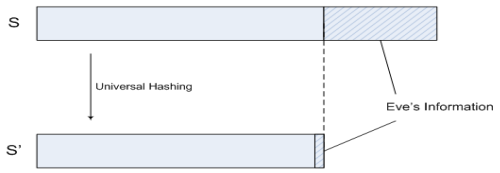


Fig. 5. *Privacy amplification*

If the length of the series but which Eve has t bits of information make a universal hash function of the length r, then the resulting row length of r Eva has less than **r = H2 (S l S)** - with bits of information, where **S = ntR** (security factor). Hash function can be known Eve, but must be used once.

UELI MAURER - SATELLITE SCENARIO

U. Maurer 1993rd The proposed protocol in which Alice and Bob can have two less correlated lower than it has Eve, and yet still manage to establish a shared key. The aim of the protocol is that Alice and Bob establish a secret string that will be known only to them or shared symmetric secret key.Taj be used as a series of one-time encryption key (One Time Pad). Satellite protocol scenario is possible even when the channel error Evinog ε less than Alice's error (α) and Bob's channels (β). Scenario is possible only if Eve's error ε = 0 (ideal access to satellite), or if Alice and Bob can not receive broadcast series.

Satellite scenario has four stages. In the first stage of Alice, Bob and Eve receive their initial series from satellites through a binary symmetric channel (BSC). All the strings are different, but there is a degree of corelation among them.

Sequences all of length N, but not exactly the same and represent an imperfect copy originals to anyone who is not known.

$$p(a_i \neq s_i) = \varepsilon_A$$
$$p(b_i \neq s_i) = \varepsilon_B$$
$$p(e_i \neq s_i) = \varepsilon_E$$

If Eve's error is less than Alice's and Bob, Alice and Bob have no advantage over Eve and can not immediately enter the third and fourth phase of the protocol.

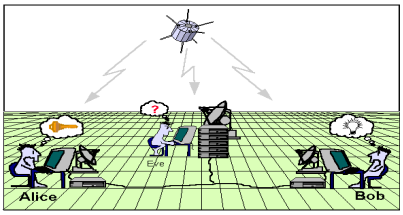


Fig. 6. *The first phase of the satellite scenario*

The second phase of the distillation of advantages. Distillation is the process of generating benefits ahead of Eve, thanks to the authenticity of the channel.

The protocol is implemented as follows. Alice and Bob share their sequences in pairs and determine the parity of each pair. Couples in which the parity is different is rejected, and in which the same shall be retained only the first bit. Bits that are discarded are a number that goes to the next step. Exponential compression flow series, Alice and Bob receive the benefit.

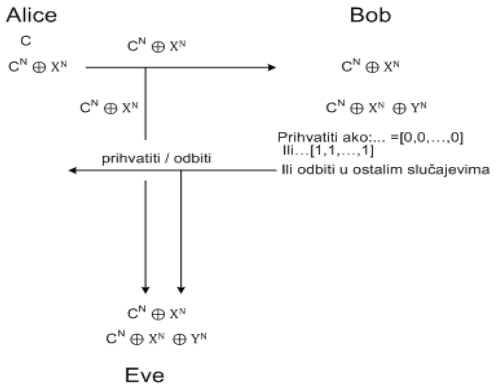


Fig. 2. *The first phase of the satellite scenario*

The third phase of the protocol is the harmonization of information and troubleshooting. After n iterations of the protocol of distillation of the advantages of Alice's and Bob's range are still different. The aim of the protocol for the harmonization of information is that the probability p (A≠ B) is less than some pre - specified value.

The fourth phase of the protocol is to enhance the privacy in which to eliminate the information Eve universal hashing Fig. 5.

COMPARATIVE ANALYSIS

If the established secret key used to encrypt (One Time Pad), quantum cryptography provides provable security against an attacker with unlimited computing power and infinite memory.

Table 2: COMPARATIVE ANALYSIS

A comparative analysis of protocols for distributing public keys kriptoloških channels	
Quantum protocol (BB84)	**Ueli Maurer (Satellite scenario)**
Provable security is valid for an active attacker on the quantum and the classical passive channel.	Provable security is valid only for passive attacker.
Alice and Bob must be linked to the public and the quantum channel.	For Satellite scenario requires only the public channel.
Expensive equipment which limits widespread use.	Very difficult setting that requires nekontrolabilni source of randomness.
Protocol parameters easily measurable.	The main setting is a protocol error. Error eavesdroppers, can not be measured.
The range is limited.	Range unlimited.

SOFTWARE SIMULATION OF SATELLITE SCENARIOS

For the purpose of the work written in the Java programming language simulation Maurer Protocol (Satellite scenario). Practical tests and test results will be further analyzed and illustrated in another paper.

Currently the results from the simulations indicate that it is necessary to have initial sequences of length 29 300 bits to generate a secret (the key) to control noise (errors).

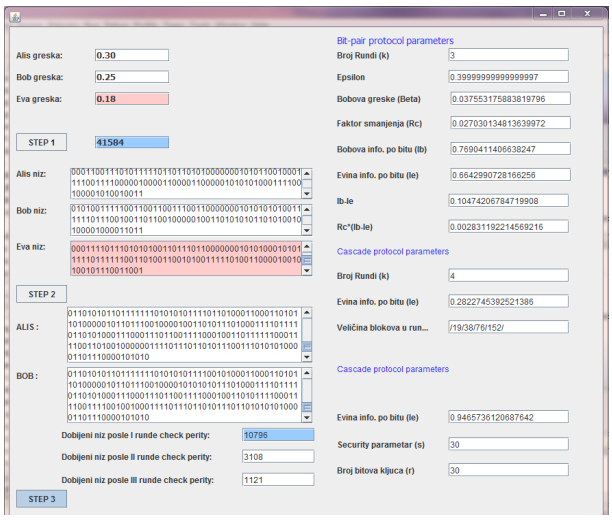


Fig. 2. *Software simulation (Java SE)*

CONCLUSION

The paper discussed the possibilities for distribution kriptoloških keys. We analyzed some of the methods (QKD) taken from quantum cryptography. It was found that the security of such systems depends on the individuality of errors when receiving the initial series. It is possible to establish a secret key on which the bug has arbitrarily little information (<0.5 per bit). That any two parties who want to establish a secret key must be connected to public channel. That is based on comparative analysis Maurers protocol resistant only to passive eavesdroppers, and if the two parties communicate, share a little secret of the previous, the system becomes resistant to the active eavesdroppers.

Our results suggest that the performance of today's PC and the high cost of equipment is not sufficient for full use features cryptographic mechanisms.

The experimental results demonstrate the need for additional hardware rather than software solutions. The need for studying and developing methods of cryptography is higher than that applied to computers, computer networks, and with them, and databases as the only form of archiving data and control among the people.

The importance of this area has several dimensions such as political, military, economic, social, ethical, and so on.

REFERENCES

[1] C. Shannon, Communication Theory of Secrecy Systems, Bell Systems Internal publications

[2] D. Knuth, The Art of Computer Programming, Vol 2 Seminumerical algorithms, Addison-Wesley1998.

[3] U. Maurer, Secret Key Agreement by Public Discussion, IEEE Trans. INFORM. Theor. 39 (1993) 733-742.

[4] C. H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984, pp 175-179.

[5] I. Csiszar, J. Koerner, Broadcast channels with confidential messages, IEEE Trans.Inform. Theor. 24 (1978) 339-348.