Math-Net.Ru

Общероссийский математический портал

G. B. Marshalko, V. I. Rudskoy, Распределение ключей. Эпизод 1: квантовая угроза, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 2, 99–110

DOI: <https://doi.org/10.4213/mvk324>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.12

26 апреля 2023 г., 16:29:05

Key distribution. Episode 1: Quantum menace

G. B. Marshalko, V. I. Rudskoy

Technical committee for standardisation "Cryptography and security mechanisms" (TC 26), Moscow

Получено 28.XI.2019

Abstract. We study the possibility of applying related key attacks to cryptographic devices with hybrid key systems, when a session key is generated from a long-term «classical» key and a key generated via quantum key distribution (QKD). For the simplest system that XORs quantum key and long-term key we study the impact of compromising the «quantum» part. We show that for many QKD systems the probability of a quantum key recovery by an attacker is close to 1. This leads to the increase of success probability when applying related key attack. Therefore we propose to use key derivation functions for key update.

Keywords: QKD, quantum key distribution, related key attack, Magma, Kuznyechik, attacks on QKD systems, block cipher, key derivation

Распределение ключей. Эпизод 1: квантовая угроза

Г. Б. Маршалко, В. И. Рудской

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), Москва

Аннотация. Изучается возможность применения атак со связанными ключами к средствам криптографической защиты информации с гибридными ключевыми системами, в которых сеансовый ключ строится по долговременному ключу и ключу, вырабатываемому протоколом квантового распределения ключей (КРК). Для случая покоординатного сложения по модулю 2 квантового и долговременного ключей исследуется влияние компрометации квантового ключа на безопасность системы. Показано, что для многих систем КРК вероятность восстановления квантового ключа злоумышленником близка к 1. Это приводит к увеличению вероятности успеха при применении атаки со связанными ключами. Поэтому предлагается для обновления ключей использовать функции выработки производных ключей.

Ключевые слова: ККС, квантовое распределение ключей, атака со связанными ключами, Магма, Кузнечик, атаки на ККС, блочный шифр, выработка производных ключей

1. Introduction

Traditionally, it is desirable to obtain information-theoretic security proof for quantum key distribution protocols, which implies an assessment of the statistical distance between the uniform distribution and the distribution of key bits. The following three types of attacks are generally considered (in the order of increase of the eavesdropper capabilities).

- Individual attacks in which the eavesdropper makes independent measurements of photon states transmitted between legitimate users.
- Collective attacks in which it is assumed that the eavesdropper has quantum memory and has the ability to store measurement results for further processing.
- Coherent attacks in which the eavesdropper is assumed to have the broadest range of capabilities, including adaptive attacks (depending on the results of previous measurements).

Under this approach, encryption using the obtained keys should also be secure from the information-theoretical point of view. From a practical viewpoint, this leads to the need to use the Vernam cipher, which, however, does not allow to achieve an acceptable rate of information processing, since it is limited by the speed of key generation by quantum cryptographic key distribution systems (QKD systems).

So in the majority of existing systems QKD are often integrated with the existing cryptographic devices. In such cases the encryption key of the cryptographic device is periodically updated by means of keys generated by the QKD system.

If the above mentioned Vernam cipher is used for updating the cryptographic device key (bitwise addition of the quantum key with the cryptographic device key), it is also possible to achieve the information-theoretic security in case of compromising the cryptographic device key or the quantum key. In each of these two cases the compromised (known) key is encrypted using another key, and this prevents the attacker from identifying the key used directly for information encryption.

Taking into account that up to now the assessment of practical security of the QKD systems remains questionable (first of all, regarding the attacks on the technical implementation of the QKD), it is assumed that in case of quantum keys compromising the mentioned approach allows to keep the security of the cryptographic devices at the «initial» level.

At the same time, for some existing encryption algorithms the proposed approach may lead to the possibility of related keys attacks implementation. Therefore it is important to study this possibility for Russian standardized encryption algorithms in case of successful implementation of an attack on the quantum component. We study the possibility of application of related key attacks on block ciphers, including those defined by the standard GOST R 34.12-2015, as well as assess their effectiveness depending on the parameters of attacks on the technical implementation of the QKD systems.

The paper is organised as follows. In section 1 we recall the general model for related-key attacks on block ciphers. Sections 3 and 4 describe existing results on application of related key attacks on block ciphers, standardized in GOST R 34.12-2015. In Section 5 we assess the efficiency of a related key attack on the Magma cipher in case when the secret key is obtained through a bitwise addition of a classical key with a compromised quantum key. In section 6 we review the existing practical attacks on QKD systems, which could lead to quantum key compromise. In section 7 we propose the use of key derivation function in order to provide security in case of a quantum key compromise.

2. Related key attacks on block ciphers

One of the well-known principles of cryptanalysis is the so-called «Kerckhoffs's principle», which was formulated as follows: «It must not be required to keep the system secret, and it must be able to fall into the hands of the enemy without harm». In modern cryptanalysis this principle is commonly interpreted as follows: the attacker cannot decipher the ciphertext even if he has complete information on the cipher but have no information on the key used. In probabilistic model «no information» condition is formalized by modeling encryption key as a sample from the uniform distribution on the set of all possible keys.

In practical implementations of cryptographic devices the volume of the data processed with one key is often essentially limited for a number of reasons. Thus to process big volumes of data a periodic change of encryption keys is made. Hence the attacker has a set of ciphertexts encrypted with different keys, and the number of these keys may be rather large. In this case, we are dealing with a multikey attack model, and the mentioned above probabilistic condition may be reformulated as follows: the encryption keys are sampled independently and equiprobably from the set of keys and do not depend on the attacker.

A related key attack on encryption algorithms was proposed in [2]. In

the related key attack it is assumed that the attacker works in a multikey model, i. e. has data encrypted with different keys. At the same time, the exact values of the keys are unknown to the attacker, but the attacker has information on some dependencies between these keys. Let's assume that the encryption is performed with the set of keys

$$(K_1, \dots, K_m), \quad K_i \in V_k, \quad i = 1, \dots, m,$$

where V_k is the key set. Let's call mapping $R: V_k^m \rightarrow \{0, 1\}$ by m -arity predicate, which is associated with its satisfiability set

$$I_R \subseteq V_k^m, \quad I_R = \{\bar{x} \in V_k^m \mid R(\bar{x}) = 1\}.$$

In general, the related key model assumes that the attacker knows that the predicate for the set of keys $(K_1, \dots, K_m)$ is satisfied, i. e. $R(K_1, \dots, K_m) = 1$. Besides, the predicate itself and the satisfiability set are chosen by the attacker or are known to him. A special case is the so-called functional predicates:

$$R(K_1, \dots, K_m) = \begin{cases} 1, & K_i = f_i(K_1), \quad i = 2, \dots, m, \\ 0 & \text{otherwise,} \end{cases}$$

where $f_i: V_k \rightarrow V_k$, $i = 2, \dots, m$, are predefined or known functions, so the functional relations between the analyzed encryption keys is known (or chosen). In turn, a particular case of a functional relation between keys is the differential relation which is often used in related keys differential attacks. In this case, it is assumed that

$$f_i(x) = x \oplus \Delta_i, \quad i = 1, \dots, m,$$

where $\oplus$ is a bitwise XOR in V_k . The values Δ_i are set by the attacker (or known to him).

Suppose that the encryption system uses a hybrid scheme for obtaining encryption keys K_i^H by adding a long-term key K^* with the keys K_i^Q distributed via QKD system, i. e. $K_i^H = K^* \oplus K_i^Q$, $i = 1, \dots, m$. If the QKD system has been compromised, then keys $K_1^Q, \dots, K_m^Q$ are known to the attacker. In this case the encryption keys K_i^H are not known to the attacker because the long-term key is unknown. However, the attacker has information on the differences between the encryption keys:

$$K_i^H = K^* \oplus K_i^Q = K_j^H \oplus K_j^Q \oplus K_i^Q = K_j^H \oplus \delta_{ij},$$

where all

$$\delta_{ij} = K_i^Q \oplus K_j^Q, \quad i, j = 1, \dots, m,$$

are known to the attacker. So we fall into the situation of a differential functional relation between the keys described above, which may lead to a significant reduction in the security of encryption algorithms.

3. Related key attacks for Magma

Related key attacks on GOST 28147-89 (Magma) was considered in [4,5]. In [4] the method of determining the key using the enhancement of the differential attack – the related-key boomerang attack – was proposed.

The related-key «boomerang» attack uses four plaintext/ciphertext pairs, where each of the ciphertexts is obtained by encryption of the corresponding plaintext on its own key. The basic attack of [4] uses four encryption keys with the following relation:

$$K_1, \quad K_2 = K_1 \oplus \Delta_1, \quad K_3 = K_1 \oplus \Delta_2, \quad K_4 = K_1 \oplus \Delta_1 \oplus \Delta_2.$$

The attack recovers 31 bits of the first round key with time complexity of about 2^{12} encryptions and the same number of adaptive chosen plaintexts. The paper also suggests generalizations of the basic attack which recovers 192 bits of the key (6 round keys out of 8), while the remaining 64 bits are proposed to be determined by a brute force search. In this case, the attack complexity is about 2^{71} encryptions, and the data complexity is 2^{28} pairs of chosen plaintexts. The generalized attack requires a set of 14 related keys.

In [5] a combination of differential and boomerang attacks was proposed. The boomerang attack described in [4] is used to recover the first two round keys. For further recovery of round keys it was proposed to use the differential attack with related keys. The attack requires 12 related keys to be mounted. In the worst-case scenario the complexity of the attack is 2^{62} encryptions, and the data complexity does not exceed 2^{43} chosen text pairs.

4. Related key attacks for Kuznyechik

The analysis carried out in [7,8] did not reveal any related key attacks for the full round Kuznyechik cipher, primarily due to its complex key schedule. Hence it is now believed that the related key attacks are not applicable to this algorithm.

5. Dependencies between attack success rate and the number of related keys

In many cases the application of related-key attacks assumes that the relation between the keys used is set by the attacker. However, in the situation described above when the QKD system is compromised, the relation between the keys is known to the attacker, but is not set by him.

Further we assume that the number of plaintexts encrypted under each key is sufficient to mount the attacks from [4, 5] and plaintexts are known to the attacker. Thus we need only assess the success rate of the attack in the considered scenario.

The value

$$\delta_{ij} = K_i^Q \oplus K_j^Q$$

is the sum of the two keys generated from the QKD system, which are generated by a random bit generator. Thus, the values in general may be considered as uniformly distributed (but dependent: for example, $\delta_{ij} \oplus \delta_{jk} \oplus \delta_{ik} = 0$).

Then, when mounting the related-key attack, the following problem arises. Suppose that we need to use m related keys $(K_1, \dots, K_m)$ to perform the attack. The relation is defined by the differential functional predicate, i.e.

$$K_i = K_1 \oplus \Delta_i, \quad i = 2, \dots, m,$$

where the values Δ_i are known to or defined by the attacker, depending on the cryptanalytic algorithm. We need to estimate the number of encryption keys M : K_j^H , $j = 1, \dots, M$, such that among them there is a subset with the necessary relation between the keys: $R(K_{j_1}^H, \dots, K_{j_m}^H) = 1$ with the required probability. Such model arises from the fact that even in case of a quantum key compromise the attacker can only observe the quantum key bits values, but can't force them to desired values, as shown in the next section.

Let's consider the simplest case, when an attack requires two keys: K_1 and $K_2 = K_1 \oplus \Delta$. The whole key set is divided into a set of key pairs with the difference Δ . Now the key set can be divided into two disjoint classes, such that if one of the keys of the pair lies in the first class, the other one lies in the second one. At the same time, the number of encryption keys K_j^H in each class will be the same on average due to the uniform distribution of encryption keys and equal cardinality of classes. Then the estimation of the probability of finding a key pair K_1 and $K_2 = K_1 \oplus \Delta$

among K_j^H is essentially the problem of estimating the probability of a collision in two samples.

It is known from the generalized «birthday paradox» that the probability of collision in two subsets of N elements, where the subset sizes are equal to $\tau_1\sqrt{N}$ and $\tau_2\sqrt{N}$ may be estimated as

$$1 - e^{-\tau_1\tau_2}$$

when $N \rightarrow \infty$. Then, assuming

$$\tau_1\sqrt{N} \approx \tau_2\sqrt{N} \approx \frac{M}{2},$$

we get that the probability of guessing the key pair K_j^H , satisfying the required relation is

$$P_2 = 1 - e^{-\frac{M^2}{4N}},$$

where $N = 2^k$ is the cardinality the key set.

Now consider the related-key boomerang attack, where four related keys are used:

$$K_1, K_2 = K_1 \oplus \Delta_1, K_3 = K_1 \oplus \Delta_2, \text{ and } K_4 = K_1 \oplus \Delta_1 \oplus \Delta_2.$$

As before, the key set can be divided into 4 disjoint classes of equal size, and the estimate of the probability of finding the four related keys can be obtained through the estimate of the probability of 4-multicollision. In [3] Wagner proposed an efficient algorithm for solving the problem, which gives us the correspondence between the desired probability and the amount of data needed. As a result this allows us to correlate the number of related keys available to the attacker with the probability that there exists a subset with the required property, and hence, to evaluate the success rate of the attack.

In classical assumptions, when keys are assumed to be uniformly and independently distributed, the attacker acts under the assumption that the keys are related. Therefore, the attack success rate includes a factor that corresponds to the probability of this assumption being fulfilled which is equal to

$$2^{-k(r-1)}$$

when using r keys. This factor makes the overall success rate of the attack almost zero.

In the case of a compromised QKD system, when the differences between the keys are known and uniformly distributed, and when the attack

applicable to one particular relation predicate is known (as in the above attacks for the Magma cipher), the number of encryption keys required for the attack is quite large: to achieve success rate close to 1 for an attack with two related keys the attacker needs (recall that $k = 256$ for Magma) about

$$\sqrt{N} = \sqrt{|V_k|} = 2^{128}$$

encryption keys. For an attack with four related keys:

$$(|V_k|)^{\frac{3}{4}} = 2^{196}.$$

Hence if the attacker has a small number of encryption keys, the estimated success rate is almost the same as under the classical assumptions.

6. Practical attacks on quantum key distribution systems

In this section we will briefly review some known practical attacks exploiting implementation weaknesses of optical modules of QKD systems. We focus mostly on systems implementing widely studied BB84 and CV QKD systems. Our goal is to to assess a posterior probability of the quantum key bits, or, in other words, the probability that the eavesdropper knows the quantum key after the attack. It should be noted that in order to provide information-theoretic security of the quantum key the privacy amplification techniques should be performed after error correction. This is usually done by means of 2-universal hash functions family [14]. That means that quantum key, which is possibly eavesdropped, is loaded into the cryptographic device after some functional transformation. Since the procedures of error correction and privacy amplification of the key are determined, it is sufficient to estimate such probability P for the raw (before error correction) key.

6.1. Photon-number splitting attack

One of the main problems for QKD systems is to implement a single-photon source in practice. In the majority of implementations weak coherent (laser) pulses are used, which means that source emits multi-photon pulses with non-zero probability. In this case, Eve has the ability to split the beam in order to intercept part of the photons in the pulse without affecting others and store them in quantum memory. After legitimate users announce their bases, Eve can measure the stored photon(s) and get the raw key bit.

In [15] a thorough study is performed. The probability for eavesdropper to get a correct key depends on the transmission efficiency of a quantum channel η , mean photon number μ and the fraction of the pulses containing one photon κ . The probability of correct key guessing for Eve as a function of disturbance D which is introduced for the information channel between the legitimate users is described as

$$P(D) = \frac{1 - e^{-\mu}(1 + \mu) + (1 - \kappa)\mu e^{-\mu}[1/2 + \sqrt{D(1 - D)}]}{1 - e^{-\mu}(1 + \mu\kappa)}.$$

The probability depending on the parameters could be up to 1, which means that the eavesdropper knows the whole key.

6.2. Detector laser damage

In [16] an attack based on high voltage laser damage of photodetectors was proposed. In the worst case the attacker is able to get the full control over the process of quantum key generation by destroying detectors. That means the probability P could be equal to 1 in this attack.

6.3. Trojan horse attack

In this type of attack, the eavesdropper irradiates the laser of the encoding module and receives information about the coding of the photon by analysing the reflected signal. In [1] the practical application of the attack for two QKD systems is shown. The research suggests that it is possible to correctly determine the key bit with a probability $P > 0.99$.

6.4. Bright illumination attack

This type of attack may be used against avalanche photo detectors [13]. During the attack, the photo detector is irradiated by a powerful beam of light, which leads to the transition of the detector from Geiger mode to linear mode. As a result an eavesdropper can carry out a meet-in-the-middle attack by measuring the photons sent by initiator and inducing, according to the measurement, the response of the corresponding photodetector on the receiver side. As a result, an eavesdropper receives full information about the key being transmitted, $P = 1$.

6.5. Time shift attack

In order to minimize the effect of dark readings in a number of systems the photon detectors activate only after receiving synchronization signals. The

possibility of an attack arises from the fact that the detection efficiency profiles of photon detectors are not the same. In this case, an eavesdropper can measure photons, and then change the synchronization signal to activate the receiver's detector according to his measurements in order to control detection efficiency according to her measurements. In the worst case, an eavesdropper can get all the information about the key [10].

6.6. Wavelength attack

Many of QKD systems implement beam splitter on the receiver side. The imperfectness of the beam splitter's wavelength dependent optical property could be exploited by the eavesdropper. The study [11] suggests that after measuring the photon the eavesdropper resends it to the receiver at the wavelength depending on the measured state and optical properties of the beam splitter. In the worst case the eavesdropper could get all the information about the key.

7. On the possibility of related key attack and countermeasures

The review presented in the previous clause suggests that many of practical attacks on QKD make it possible for the eavesdropper to obtain the full knowledge of quantum key. At the same time the main problem with the implementation of related key attack from the attacker's viewpoint is the impossibility of imposing desired keys to legitimate subscribers. Even when the eavesdropper is able to get full control over optical parts of the legitimate users, the process of encoding photons on sender side is beyond his control. As a result, after the application of the key correction and privacy amplification procedures, the eavesdropper will not be able to impose the keys with the specified ratios. As a result, even if the raw key is compromised, the eavesdropper will be able to expect the related keys to appear only with the specified probability.

At the same time, the considered practical attacks allow the eavesdropper to detect the appearance of related keys, which increases the success rate of the attack, and, in general, reduces the security of the cryptographic device. Hence it is reasonable to use methods of key derivation that exclude the possibility of considered attacks.

The most effective countermeasure is the use of the key derivation functions, for example, defined by the recommendations for standardization [6, 17]. The key derivation functions $\text{kdf}(S, T, L, P \dots)$ described in [6] con-

sist of two stages. At the first stage, an intermediate key $K^{(1)} = \text{kdf}^{(1)}(T, S)$ is produced, which is obtained by hashing of the original secret key S with salt T , which is supposed to be uniformly sampled from some set and, in general, is known to the attacker. At the second stage, the derived keys $K^{(2)} = \text{kdf}^{(2)}(K^{(1)}, L, P, \dots)$ are generated from the intermediate key using the cryptographic transformations, where L is the length of the key sequence produced, and P is additional information.

In order to provide the security of cryptographic device in case of the QKD system compromise, it is proposed to use the key derivation function, where the keys obtained as a result of the quantum protocol are used as salt K_i^Q and the long-term key of a cryptographic device K^* is used as the secret key.

As a result of this approach, even in the case of compromising the quantum keys K_i^Q , the keys produced by $K_i^H = \text{kdf}(K^*, K_i^Q, L, P, \dots)$ are computationally indistinguishable from the uniform independent sample from the keyspace, according to [9].

8. Conclusion

We have studied the possibility of applying related-key attacks to hybrid cryptographic devices which use QKD for updating the long-term key in case of quantum channel compromise.

For the key update method which consists in bitwise XOR of quantum and long-term key we show the increase of success rate of the related-key attack compared to the classical assumptions.

A variant of the key update method based on standardized key derivation functions, which excludes the possibility of application of the considered attacks, is proposed.

References

- [1] Stiller B., Khan I., Jain N., Jougnet P., Kunz-Jacques S., Diamanti E., Marquardt Ch., Leuchs G., *Quantum hacking of continuous-variable quantum key distribution systems: realtime Trojan-horse attacks*, Optical Soc. America Tech. Digest (online), paper FF1A.7, 2015.
- [2] Biham E., "New types of cryptanalytic attacks using related keys", *J. Cryptology*, **7**:4 (1994), 229–246.
- [3] Wagner D., "A generalized birthday problem", CRYPTO'02, Lect. Notes Comput. Sci., **2442**, 2002, 288–304.
- [4] Rudskoy V., *On zero practical significance of «Key recovery attack on full GOST block cipher with zero time and memory»*, 2011, <http://eprint.iacr.org/2010/111>.
- [5] Pudovkina M.A., Khoruzenko G.I., "Attacks on full block cipher GOST 28147-89 with 2 or 4 related keys", *Prikladnaya Diskretnaya Matematika*, **3** (2010), 29–30 (in Russian).

- [6] “Recommendation for standardization R 1323565.1.022-2018. Information technologies. Cryptographic data protection. Key derivation functions” (In Russian).
- [7] Alekseev E., Goncharenko K., Marshalko G., “Provably secure counter mode with related-key-based internal re-keying”, *J. Comput. Virol. Hack. Tech.*, 2020, <https://doi.org/10.1007/s11416-020-00357-9>.
- [8] Ishchukova E.A., Krasovskiy A.V., Polovko I.Yu., “Analysis of the cipher Kuznyechik by the related keys method”, *Sovremennye naukoemkie tekhnologii*, **5** (2018), 85–90 (in Russian).
- [9] Bellare M., “New proofs for NMAC and HMAC: Security without collision resistance”, *CRYPTO 2006, Lect. Notes Comput. Sci.*, **4117**, 2006, 602–619.
- [10] Qi B., Fung C., Lo H. et al., *Time-shift attack in practical quantum cryptosystems*, 2005, quant-ph/0512080.
- [11] Li H., Wang S., Huang J. et al., “Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources”, *Phys. Rev. A*, **84**:6 (2011), 062308.
- [12] Weier H., Krauss H., Rau M. et al., “Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors”, *New J. Physics*, **13** (2011), 073024.
- [13] Lydersen L., Skaar J., Makarov V., “Tailored bright illumination attack on distributed-phase-reference protocols”, *J. Modern Optics*, **58** (2011), 680–685.
- [14] Gilbert G., Hamrick M., Thayer F.J., *Privacy amplification in Quantum Key Distribution: Pointwise bound versus average bound*, 2001, <https://arxiv.org/abs/quant-ph/0108013v1>.
- [15] Williamson M., Vedral V., “Eavesdropping on practical quantum cryptography”, *J. Modern Optics*, **50**:13 (2003), 1989–2011.
- [16] Bugge A.N., Sauge S., Ghazali A.M.M., Skaar J., Lydersen L., Makarov V., “Laser damage helps the eavesdropper in quantum cryptography”, *Phys. Rev. Lett.*, **112**:7 (2014), 070503.
- [17] “Recommendation for standardization R 50.1.113-2016. Information technologies. Cryptographic data protection. Cryptographic algorithms to accompany the usage of digital signature and hash function” (In Russian).