RESEARCH ARTICLE | JUNE 23 2020

On applying pseudorandom number generators in quantum cryptography with coherent states

A. S. Avanesov; D. A. Kronberg

AIP Conf. Proc. 2241, 020026 (2020)
https://doi.org/10.1063/5.0011486

On Applying Pseudorandom Number Generators in Quantum Cryptography with Coherent States

A.S.Avanesov[1, 2] and D.A.Kronberg[1, 2, 3, 4, a)]

[1)] *Steklov Mathematical Institute of Russian Academy of Sciences, ul. Gubkina 8, Moscow 119991, Russia*
[2)] *Moscow Institute of Physics and Technology, Institutski per. 9, Dolgoprudny 141701, Russia.*
[3)] *Russian Quantum Center, 100 Novaya St., Skolkovo, Moscow 143025, Russia*
[4)] *Quantum Communications Center of NTI, NUST MISIS, 119049, Russia*

[a)] *Corresponding author: dmitry.kronberg@gmail.com*

Abstract. We consider the use of pseudorandom number generators in quantum cryptography. They can be used in two ways: for basis choice according to pseudorandom sequence shared between Alice and Bob and for setting the pseudorandom phase for each coherent state to make worse the performance of some attacks. We propose this technology for the situations where the use of classical cryptographic methods like AES is satisfactory for the legitimate users.

INTRODUCTION

Quantum cryptography allows us to distribute keys with guaranteed security. Though it is frequently said that security of the distributed keys is unconditional, actually there are suggested some assumptions like availability of random number generators for legitimate users and the correct work of protocol devices according to specifications. Besides, the achieved key generation rates do not allow practical usage of these keys in the one-time pad regime. Therefore, it is common to use classical cipher algorithms, such as AES (see Fig. 1). Consequently, the final cryptosystem loses theoretical security.

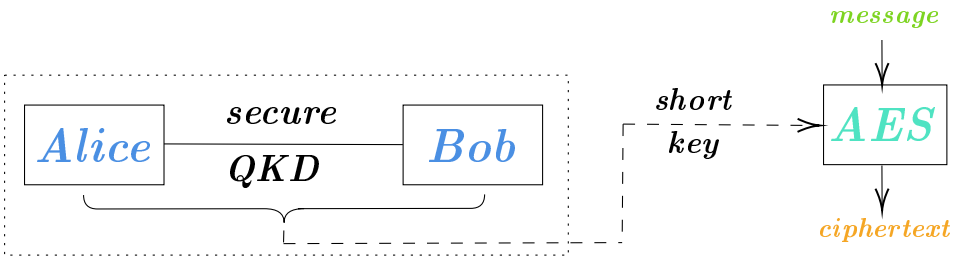

FIGURE 1. The scheme of ordinary QKD with AES cipher.

We propose a way to increase the key rate by using the methods of classical cryptography that preserves the important advantage of quantum cryptography, namely the time-independent security of the keys.

PSEUDORANDOM BASIS CHOICE

First, let us consider a quantum key distribution protocol based on symmetric coherent states with pseudorandom basis choice [1]. Like coherent state-based BB84 [2], it uses symmetric coherent states and single-photon detectors after the interferometer on the receiver side, but the number of bases is high and legitimate users use pseudorandom sequence for basis choice.

Like Y-00 [3] with PSK, it uses symmetric coherent states and pseudorandom basis choice, but the states within each basis are less distinguishable (i.e. the intensity is lower or the phase difference within each basis is not π), and we use single-photon avalanche detectors instead of homodyne detection.

Our only assumption about Eve is that she cannot calculate the seed of pseudorandom sequence before the end of communication session which takes no more than several minutes. After the session, the protocol becomes close to B92 [4]: Eve cannot get full information from nonorthogonal states even knowing the right basis for each position.

Fifth International Conference on Quantum Technologies (ICQT-2019)
AIP Conf. Proc. 2241, 020026-1–020026-3; https://doi.org/10.1063/5.0011486
Published by AIP Publishing. 978-0-7354-2000-7/$30.00

The reason why we need many bases is unambiguous state discrimination (USD) attack [5], when Eve extracts full information from the signal with some success probability or blocks the pulse otherwise.

Without knowing pseudorandom sequence, Eve sees the ensemble of symmetric coherent states at each position, and the success probability of unambiguous discrimination for Eve is very low for high number of bases [6], so she cannot make proper decision.

Once the state arrived to Bob, he can make a measurement in a basis specified by the pseudorandom sequence, so he always knows the right basis, and sometimes obtains inconlusive results just because of nonorthogonality of the states.

If Eve has perfect quantum memory, she can make a proper measurement right after the computation of pseudorandom sequence, and her information is close to the Holevo value [7] of the original states. But if we additionaly assume decoherence in Eve's quantum memory, the states within each basis can be chosen more distinguishable. Then key generation rate becomes higher, because the probability of conclusive results at receiver side increases, but Eve still gets low information, because her states become worse by the time of measurement.

This approach requires computational assumption about Eve, thus such protocols are not information-theoretically secure, but it still provides better security than any classical scheme with pseudorandomness (like stream cipher), because Eve cannot get full information from the key even after performing all computations.

Despite the aforementioned assumption of eavesdropper abilities, the proposed schemes have an important advantage over the classical protocols. Indeed, if Eve was unsuccessful in her attempt to obtain the key during the session period, she is not able to obtain any additional information about the key later.

QKD PROTOCOLS MODIFIED WITH PSEUDORNADOMNESS

Similar modifications with pseudorandom phase can be adopted to other QKD protocols.

In COW protocol Alice encodes each informational bit by the sequence of two coherent states [8]. The pair $|\alpha\rangle|0\rangle$ corresponds to bit 0, and bit 1 is encoded by $|0\rangle|\alpha\rangle$. Alice also sends two non-empty pulses $|\alpha\rangle|\alpha\rangle$ as a decoy. On the receiver side, the incoming signal is splitted in two parts. The first one is sent to the detector, where the time of arrival of the signal is measured. The second part is sent to the delayed interferometer, where Bob measures the coherence between two successive non-empty pulses. The modification can be the follows: Alice choose different phases for each of the transmitted states and the pseudorandom generator can be used to set these phases, so the knowing of the seed of pseudorandom sequence allows to Bob align his interferometer well. This modification makes it difficult to perform an attack, where Eve tries to distinguish between vacuum state and non-empty pulse as she does not know the chosen phases. Though the efficiency of the proposed protocol is restricted by the assumption that Eve is not able to calculate the seed of pseudorandom sequence during the session time.

The pseudorandom choice of the phases of transmitted states can be adopted in the case of DPS protocol [9]. In the initial scheme, Alice sends the train of coherent states of the form $|\pm\alpha\rangle$. The informational bits are encoded by relative phases of successive pulses. The phase shift 0 correspond to bit 0 and bit 1 is encoded by the phase shift π. Bob measures the relative phase by the delayed interferometer. The usage of the pseudorandom generator allows Alice to prepare the train of states of the form $|\pm\alpha e^{i\varphi_t}\rangle$ without decreasing the key rate. Bob knows the seed of the pseudorandom sequence, so he can align his interferometer. The modified protocol should act better in the case of the attack where Eve uses the same measurement scheme as Bob or in the case of active beamsplitting attack [10].

Finally, we discuss the modification of B92 protocol with strong reference state [11]. Here, Alice sends the weak signal state and reference state of high intensity. The information is encoded by the relative phase between these pulses. On the receiver side, the reference state is splitted in two parts. The first one has the same intensity as signal state and interferes with it. The second one is used to control the decrease of intensity in the communication channel. Again, the usage of the pseudorandom generator allows to choose different phase for each transmitted state and reconcile the choice between Alice and Bob.

In all of the considered protocols, the usage of several phases in the state generation makes some attacks (like sequentioal attack [12] or USD attack [5]) far less effective. Therefore, it is possible to use the higher intensity for transmitted signals, though we can not use the pulses of arbitrary high intensity because of the possibility of beamsplitter attack.

The general scheme, which includes the coherent-state based protocol with pseudorandom basis choice and the modifications of the protocols listed above, is shown on Fig. 2. Note that this scheme is no worse than the scheme at Fig. 1 because of longer key obtained from QKD system.

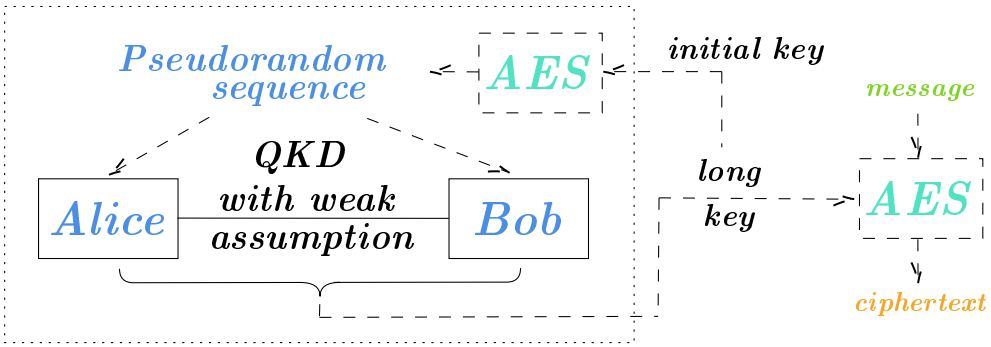

FIGURE 2. The scheme of QKD with pseudorandom generator.

CONCLUSION

In conclusion, we believe that the usage of pseudorandom sequences with the purpose to increase the key generation rate should be considered for existing schemes of quantum cryptography. It is reasonable for all applications, where legitimate users find it acceptable to use classical ciphers like AES.

ACKNOWLEDGMENTS

This work is supported by the Russian Science Foundation under grant 18-71-00074.

REFERENCES

1. A.S. Avanesov, D.A. Kronberg, Coherent-state quantum cryptography using pseudorandom number generators, Quantum Electronics **49** (10) 974-–981 (2019)
2. B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1994)
3. Horace P. Yuen, KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation, arXiv:quant-ph/0311061 (2003)
4. Bennett, C.H. Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121–3124 (1992)
5. Dušek, M., Jahma, M., Lütkenhaus, N. Unambiguous state discrimination in quantum cryptography with weak coherent states. Physical Review A, 62(2), 022306 (2000)
6. Anthony Chefles and Stephen M. Barnett, Optimum Unambiguous Discrimination Between Linearly Independent Symmetric States, Phys. Lett. A **250**, 223 (1998)
7. Holevo, A.S. Some estimates of information transmitted through quantum communication channel, Probl. Peredachi Inf. **9**, 3–11 (1973)
8. Stucki, D., Brunner, N., Gisin, N., Scarani, V., Zbinden, H. Fast and simple one-way quantum key distribution, Applied Physics Letters, **87**, 194108-194108 (2005)
9. Inoue, K., Waks, E., Yamamoto, Y. Differential phase shift quantum key distribution, Phys. Rev. Lett., **89**, 037902 (2002)
10. Avanesov, A.S., Kronberg, D.A., Pechen, A.N. Active Beam Splitting Attack Applied to Differential Phase Shift Quantum Key Distribution Protocol, p-Adic Numbers, Ultrametric Analysis and Applications **10**, 222–232 (2018)
11. Tamaki, K., Lütkenhaus, N., Koashi, M., Batuwantudawe, J. Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse, Phys. Rev. A **80**, 032302 (2006)
12. Curty, M., Zhang, L.L., Lo, H.-K., Lütkenhaus, N. Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states, arXiv:quant-ph/0609094 (2006)