Practical discrete-state QKD with lossy channels: avoiding unambiguous state discrimination attack

K. S. Kravtsov[1,2], I. V. Radchenko[1,2], S. P. Kulik[1], and S. N. Molotkov[3]

[1] *Faculty of Physics, Moscow State University, Moscow, Russia*
[2] *A.M. Prokhorov General Physics Institute RAS, Moscow, Russia*
[3] *Academy of Cryptography, Moscow, Russia; Institute of Solid State Physics, Chernogolovka, Moscow Rgn., Russia; Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow Russia*

(Dated: April 26, 2017)

Many conventional QKD protocols using weak coherent pulses as information carrier are susceptible to unambiguous state discrimination attack, provided loss in the system is large enough. That creates theoretical and implementation difficulties, which have to be overcome in order to guarantee key security. Not all QKD protocols are proven to be protected against this type of attack, bounds for safe loss levels often remain unknown. We advocate for a special protocol design, which eliminates the problem altogether and overly simplifies the security analysis.

Practical QKD systems typically use weak coherent pulses (WCP) as information carriers. As infinite-dimensional quantum systems, those states can always be told apart with a non-zero probability using unambiguous state discrimination (USD). That directly leads to the loss of security in the limit of high channel loss. Namely, Eve can perform USD on every state in the channel and retransmit only successful discrimination results. In this case legitimate users will not be able to detect the attack if overall system efficiency is lower than the probability of successful USD.

Consequently, all popular protocols are susceptible to this type of attack, provided losses are high enough. For some protocols, like WCP-based BB84, the critical loss level is well known [1, 2], which makes this particular one insecure right away even for moderate loss levels, see Fig. 1. For other popular ones, such as DPS [3] and COW [4], it is strictly speaking unknown, but presumably extremely large due to pulse chaining. However, at the expense of generating some errors for legitimate users, the USD probability of success may be drastically increased by splitting these chains into shorter chunks, treating them as independent. For Alice and Bob it results in a particular trade-off between the allowed loss and QBER. To the best of our knowledge, those security bounds haven't been strictly shown/proven, which suggests that the available security proofs are incomplete (at least compared to the proofs for the original single-photon BB84 [5, 6])

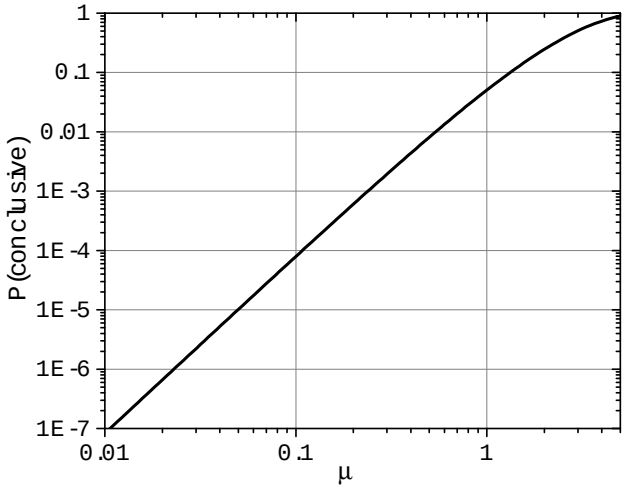

FIG. 1: Success probability of unambiguous discrimination of BB84 WCP states vs. average number of photons in a pulse. For typical $\mu \gtrsim 0.1$ this probability is larger than 10^{-4}, while the probability of detection is only 1/10. Thus, a 30 dB loss is enough to make the system insecure. In most cases this already includes inefficiency of the system itself, so the channel loss must be even substantially smaller.

Special note can be made about decoy state protocols: their original goal was to protect from a photon number splitting attack. This attack, however, is in fact a particular (and severely limited) type of a USD-based one. In a gen-

eral case, USD allows (with some probability) discrimination of coherent states with different average number of photons, i.e. allows to distinguish 'signal' and 'decoy' states, which undermines the whole decoy-state strategy. Again, the critical parameter is channel loss, for which users still can guarantee security. To the best of our knowledge these bounds (potentially, together with QBER) have not yet been found either.

Even with known bounds, security of conventional WCP-based QKD depends on *overall* [12] loss in the system, which is an apparent step back from the original single-photon BB84 setting [7], where there is a single security indicator — the QBER.

In this work we show examples of WCP-based QKD protocols that are not susceptible to USD attacks and advocate for their practical use. Two notable and possibly the only known examples are relativistic QKD [8] and B92 with strong reference pulses [9], where results of unsuccessful USD cannot be hidden in loss, and inevitably produce errors in the raw key. This is possible due to the special time-space protocol structure of the former and the presence of classical reference pulses in the latter.

From theoretical point of view, those two cases are very simple as both assume a binary quantum channel with two non-orthogonal states, namely, coherent states with different phases. Classical capacity of such channel is given by the Holevo bound $\chi = h\left(\frac{1-|\langle\psi_0|\psi_1\rangle|}{2}\right)$ [10], so regardless of strategy, one cannot extract more than χ bits from a pulse on average. Whenever Bob gets a detector click (for simplicity we assume noiseless detectors here), he gets one bit of information. This is possible because Bob performs post-selection — selects only states for those his detector clicked. In conventional protocols Eve can do the same, leaving only those states in the line, which she could successfully measure. She has to block all the other ones, which she can easily do given enough loss in the system. That completely hides her presence in the channel.

To avoid this problem, a protocol should not allow Eve to choose her action based on her measurement result. In the case of the relativistic protocol Eve is forced to make decisions earlier than she can actually try to perform her measurement. If her measurement fails she inevitably produce random clicks in Bob's detector, i.e. the obtained raw key bits will have no correlation between Alice and Bob. In the case of B92, Eve cannot suppress the classical reference, which has to be detected by Bob. However, if she suppresses the quantum part, e.g. with unsuccessful measurement, Bob's detector clicks become uncorrelated with Alice's transmissions. In any case, the inability to post-select fundamentally limits Eve's information by χ per pulse. Since Bob, after his post-selection, obtains 1 bit per each pulse and $\chi < 1$, he always has information advantage that can be distilled into a secret key, completely unknown to Eve.

We understand that such information-based approach to QKD security is internally flawed and cannot compare with a more recent trace-distance based one [11]. However, it suits the purpose of this simple illustration, while a more formal approach may be developed with reasonable efforts.

There is a significant experimental advancement in demonstration of both mentioned protocols. Right now we have a working relativistic QKD system, which is demonstrated to generate keys over 180 m long free-space channel, as well as some proof of concept experiments in realization of B92 with a strong reference.

In conclusion, we describe some QKD security issues connected with the coherent nature of carrier states and the presence of loss in the system. Conventional protocols are to some extent susceptible to this threat, which leads to the requirement of additional security checks implementation. We argue for a more fundamental solution: special protocol design that eliminates the problem altogether. We also show experimental results that prove feasibility of the chosen approach.

[1] A. Chefles, "Quantum state discrimination," *Contemporary Physics*, vol. 41, no. 6, pp. 401–424, 2000.

[2] M. Dusek, M. Jahma, and N. Lutkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A*, vol. 62, p. 022306, 2000.

[3] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, p. 037902, 2002.

[4] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, p. 194108, 2005.

[5] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[6] M. Christandl, R. Renner, and A. Ekert, "A generic security proof for quantum key distribution," 2004, arXiv:quant-ph/0402131.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 1984, pp. 175–179.

[8] I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, "Relativistic quantum cryptography," *Laser Phys. Lett.*, vol. 11, no. 6, p. 065203, 2014.

[9] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 1992.

[10] A. S. Holevo, "Quantum coding theorems," *Russian Math. Surveys*, vol. 53, no. 6, pp. 1295–1331, 1998.

[11] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," 2014, arXiv:1409.3525 [quant-ph].

[12] Even if inefficiency of Bob's setup is accounted by the legitimate users, its contribution to the system loss may be advantageous for Eve, who can, in many cases, retransmit brighter pulses