Quantum cryptography protocols robust against photon number splitting attacks

Valerio Scarani[1] [*] Antonio Acín[1 2] [†] Grégoire Ribordy[1] [‡] Nicolas Gisin[1] [§]

[1] *Group of Applied Physics, University of Geneva*
20, rue de l'Ecole-de-Médecine, 1211 Genève 4, Switzerland
[2] *Institut de Ciències Fotòniques*
Jordi Girona 29, 08034 Barcelona, Spain

Abstract. We describe a new quantum key distribution (QKD) protocol that differs from the BB84 only in the classical sifting procedure: instead of revealing the basis, Alice reveals a pair of non-orthogonal states. The new protocol is as robust as BB84 against optimal individual eavesdropping, and is much more robust than BB84 against the most general photon-number splitting attack, increasing the security of QKD implementations that use weak laser pulses.

Keywords: Quantum key distribution, implementation, multi-photon pulses

The study of quantum key distribution has reached its maturity in the last years. On the theoretical side, proof of the unconditional security of the BB84 and the B92 protocols were found; on the application level, QKD is leaving the realm of academics, and commercial prototypes are available [1]. Everything seems quite nice — but there is a gap. All the most advanced security proofs assume an ideal implementation of the protocol, one that uses single-photon sources. But the experimental realizations, especially the prototypes, use attenuated laser pulses as sources: in this case, a non-negligible fraction of the pulses contain more than one photon. In the year 2000, Lütkenhaus and co-workers realized that the presence of multi-photon pulses has dramatic consequences on the security of the BB84 protocol [2]. They described an attack that has been called *photon-number splitting attack* (PNS): (i) Eve counts the number of photons; (ii) if there is more than one photon in the pulse, she keeps one in a quantum memory and forwards the others on a lossless channel; (iii) when the basis are revealed, she measures the photon she has kept and obtains all the information. The only constraint that Eve is asked to respect, is that the raw detection rate on Bob's side should not decrease. Note that by this attack Eve does not introduce any error: the photons that are forwarded to Bob are untouched.

The PNS provides Eve with tools that do not exist today: the non-demolition measurement of the number of photons, the quantum memory, the lossless line; but these tools may well exist one day; moreover, "realistic" attacks have been studied and found to be rather dangerous. It is thus definitely important to counter the possibility of PNS attacks. The obvious way to go, is to develop single-photon sources: several research groups work in this direction, with encouraging results. In this work, we report on a completely different way of countering the PNS attack.

We start from the following question: why is the PNS so dramatic in the case of BB84? The answer has already been given above: it is because, in the sifting procedure, Eve comes to know the basis in which the state has been encoded; since she has kept a perfect copy, she can deterministically find out the state. Can one do something to avoid this? The answer is yes: one can *modify the sifting phase*, so that Alice does not reveal the basis any longer. What can she reveal then? Suppose she has sent $|+x\rangle$: instead of revealing the basis, which amounts to say "either $|+x\rangle$ or $|-x\rangle$", Alice can reveal "either $|+x\rangle$ or $|+y\rangle$". If Bob has measured in the y basis and found the result $|-y\rangle$, he knows for sure that Alice had sent $|+x\rangle$: this happens on 1/4 of the raw key, so the length of the sifted key is reduced with respect to BB84. However now, Eve (who supposedly has kept a photon) must distinguish between $|+x\rangle$ and $|+y\rangle$, and this cannot be done deterministically.

The full analysis of the robustness of the new protocol against the PNS attacks has been described in Refs. [3]. Fig. 1 summarizes the effect of PNS against this protocol, compared to BB84. This proves that our protocol is much more robust than BB84 against pure PNS attacks, that do introduce any errors. This remains true in the presence of noisy detectors.

We have also studied the optimal individual attack on the new protocol, for an hypothetical single-photon implementation: there is a very tiny advantage over BB84. More complex attacks, and of course ultimately the issue of unconditional security, are still open problems of investigation.

Let us summarize. The new protocol that we propose differs from the BB84 only in the classical sifting phase: the quantum states that are sent are the same as in BB84. Somehow unexpectedly, this simple modification entails no difference for the robustness against individual attacks and a *significant improvement of the robustness against the PNS attacks.* This work throws a new light on the problem of countering the PNS attack: the strength of these attacks can be significantly reduced by using a well-tailored protocol, without any

[*] valerio.scarani@physics.unige.ch
[†] antonio.acin@upc.es
[‡] gregoire.ribordy@physics.unige.ch
[§] nicolas.gisin@physics.unige.ch

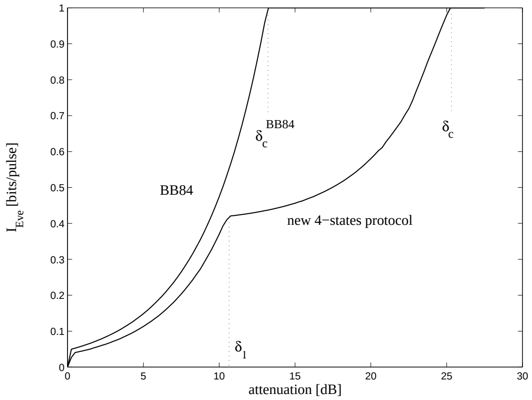

Figure 1: PNS attacks with QBER=0 on the BB84 protocol for $\mu = 0.1$ and on the new protocol for $\mu = 0.2$: Eve's information as a function of the attenuation $\delta = \alpha\ell$.

change of the existing experimental apparatus. As a final word, we want to stress that this work is not a manifest against single-photon sources, that are interesting in themselves, and will be certainly useful for cryptography and for many other applications — just think to Knill-Laflamme-Milburn quantum computation. Rather, we emphasize that existing implementations (even prototypes) of QKD that use attenuated laser pulses as photon sources are possibly more secure than one expected a few years ago.

References

[1] A recent review:
N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002).

[2] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders. Limitations on practical quantum cryptography. Phys. Rev. Lett. **85**, 1330 (2000).
N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. Phys. Rev. A **61**, 052304 (2000).

[3] V. Scarani, A. Acín, N. Gisin, G. Ribordy. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. quant-ph/0211131 (2002).
A. Acín, N. Gisin, V. Scarani. Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks. quant-ph/0302037 (2003).