Security proof of the unbalanced phase-encoded BB84 protocol

Agnes Ferenczi,[1,*] Varun Narasimhachar,[1] and Norbert Lütkenhaus[1]

[1] *Institute for Quantum Computing & Department for Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1, Waterloo, Ontario, Canada*

(Dated: May 18, 2012)

In optical implementations of the phase-encoded BB84 protocol, the bit information is usually encoded in the phase of two consecutive photon pulses generated in a Mach-Zehnder interferometer. In the actual experimental realization, the loss in the arms of the Mach-Zehnder interferometer is not balanced, for example because only one arm contains a lossy phase modulator. Therefore, the amplitudes of the pulses is not balanced, and the structure of the signals and measurements no longer corresponds to the (balanced) ideal BB84 protocol. Hence, the BB84 security analysis no longer applies in this scenario. We provide a security proof of the unbalanced phase-encoded BB84. The resulting key rate turns out to be lower than the key rate of the ideal BB84 protocol. Therefore, in order to guarantee security, the loss due to the phase modulator cannot be ignored.

Quantum key distribution (QKD) provides a way for two distant parties (Alice and Bob) to establish a shared secret key with absolute confidentiality. Many protocols [1] have been suggested to achieve this goal, among which the BB84 protocol [2] is the most well-known example. In the BB84 protocol, Alice randomly chooses between two conjugate bases of a qubit Hilbert space, and encodes the bit value of the key elements in the basis states. She sends these states to Bob through a quantum channel, who measures them randomly in one of the conjugate bases. After having collected enough data, they perform error correction to eliminate the errors in their data, followed by privacy amplification to guarantee the security of the generated key from an eavesdropper (Eve).

In optical implementations, the bit information is usually encoded in a photonic degree of freedom, e.g., in the polarization of photons, or the phase of two consecutive photon pulses. In the phase-encoded protocol, the phase between two consecutive pulses prepared by Alice determine the bit and the basis value of the sent signal. In the actual experimental realization of the phase-encoded BB84 protocol with Mach-Zehnder interferometers (see Fig. 1), the phase modulator, which is in one arm of the interferometer, introduces loss ("unbalanced phase-encoded protocol"). While this does not change the observed error rate in the data, it changes the signal states and the measurements of the protocol. Since this is now a different protocol, the security proofs tailored to the BB84 protocol no longer apply in this scenario.

I. UNBALANCED PHASE-ENCODED PROTOCOL

The setup of the unbalanced phase-encoded protocol with Mach-Zehnder interferometers is shown in Fig. 1. Alice sends photon pulses through a Mach-Zehnder interferometer with a long arm and a short arm, to create the signal states. In the long arm, Alice changes the relative phase φ_A of the two pulses with a phase modulator to imprint the basis and the bit information on the signal. Alice chooses the phases $\varphi_A \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ with equal probability for the 4 signal states. Likewise, the receiver (Bob) detects the signals by means of a Mach-Zehnder interferometer. Bob chooses the phase $\varphi_B \in \{0, \pi/2\}$, which determines the basis of his measurement. Bob chooses each measurement setting with probability 1/2.

The pulses arrive in Bob's detectors in three different time slots, either in the top output port (slots c_1, c_2 and c_3 in Fig. 1) or in the bottom output port (slots d_1, d_2 and d_3 in Fig. 1). Only the middle clicks (slots c_2 and d_2) are used for the key generation. The outside clicks (slots c_1, c_3, d_1 and d_3) are pulses that did not interfere at Bob's second beam splitter. If the signal produces interference (e.g. the detectors click in the middle time slot), then Bob determines the bit value of the incoming signal based on his phase setting.

The lossy phase modulator typically introduces a loss in one of the arms of the interferometer, producing pulses with different amplitudes. We model the lossy phase modulator by a perfect (lossless) phase modulator followed by a beamsplitter with transmissivity $\kappa \leq 1$ that simulates the loss.

II. HARDWARE FIX

One simple way to recover the original BB84 scenario is by manually introducing a beamsplitter with the same transmissivity κ in the shorter arm of the interferometers to compensate for the loss due to the phase modulator. Alternatively, one can replace the first beamsplitter in the interferometer by a biased beamsplitter with transmissivity $\frac{\kappa}{1+\kappa}$. A schematic of these alternatives is shown in Fig. 2.

[*] aferenczi@iqc.ca

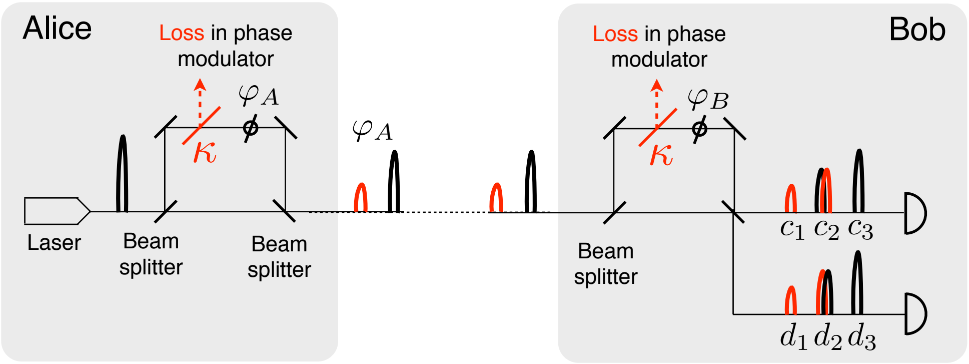

FIG. 1: Alice and Bob use a Mach-Zehnder interferometer to prepare and detect the signal pulses. Only the interfering pulses, which produce clicks in the time slots c_2 and d_2 (black-red and red-black overlapping pulses) are used for the key generation.

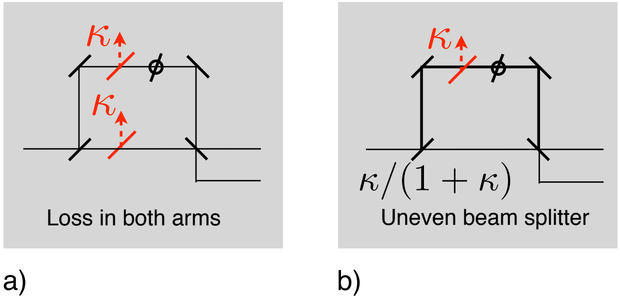

FIG. 2: a) Hardware fix with the same amount of loss introduced in the short arm of the interferometer to compensate for the loss due to the phase modulator, b) Hardware fix with a biased beamsplitter in the interferometer.

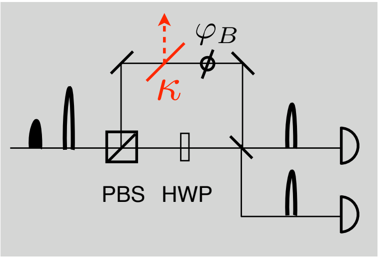

FIG. 3: A variation of the protocol with the pulses encoded in different polarization. Bob places a polarizing beam splitter (PBS) at the entrance of his interferometer, and rotates the polarization in one arm of the interferometer, for example by using a half wave plate (HWP) to cause the desired interference.

III. PBS PROTOCOL

As a slight variation of the protocol, consider Alice encoding her outgoing pulses in different polarization, and Bob replacing his first beamsplitter by a polarizing beamsplitter (see Fig. 3). This causes the two pulses to arrive simultaneously at Bob's second (interfering) beamsplitter. If he also rotates the polarization of the signal in one arm, all signals will interfere.

IV. KEY RATES

We provide a qubit-based security proof of the unbalanced phase-encoded BB84. We use the security approach presented in Refs. [3, 4] to calculate the key rate. This security approach is valid when Eve is restricted to collective attacks, but in many situations, it also holds for the more general coherent attacks. In our security proof we make the conservative assumption that the loss in the phase modulator is under Eve's control. We calculate the key rate using the symmetry approach in Ref. [5] which justifies that the optimal eavesdropping attack has a certain symmetry.

The qubit security proof is then extended to the realistic scenario with optical modes by means of the tagging approach in Refs. [6, 7] in the decoy framework [8–10], and the squashing model in Refs. [11–13]. We simulate a channel using the experimental values in Ref. [14] for channel loss, dark counts, detector efficiency and error correction efficiency, and assume that no double clicks were observed. We also optimize over the mean photon number of the signal pulses leaving Alice. In Fig. 4 the key rates of the unbalanced phase-encoded protocol, the PBS protocol and the hardware fixes for different values of κ are shown.

Generally, the loss in the phase modulator decreases the key rate of the protocols. The performance of the unbalanced phase-encoded protocol coincides exactly with the performance of the hardware fix with an uneven beamsplitter, providing a choice between the hardware fix (requiring a special unsymmetrical beam splitter), and the imporved theory solution presented here. Both of these scenarios, however, outperform the second hardware fix with an additional loss in the short arm.

The key rates of the PBS protocol are higher than the key rates of the unbalanced phase-encoded key for equal loss in the phase modulator, because no signal is lost due to outside clicks. Nevertheless, the loss in the phase modulator decreases the key rates of the PBS protocol.

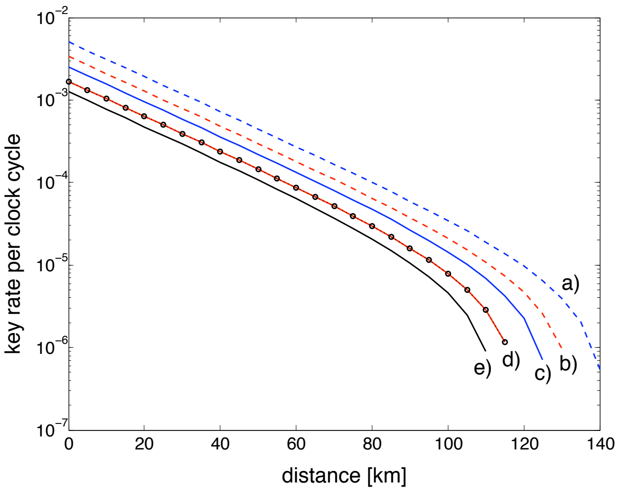

FIG. 4: Plot of the key rates in the realistic scenario. a) Key rate of the PBS protocol with no loss (dashed blue line). b) Key rate of the PBS protocol with $\kappa = 0.5$ (dashed red line). c) Key rate of the unbalanced phase-encoded protocol with no loss ($\kappa = 1$) (solid blue line). d) Key rate of the unbalanced phase-encoded protocol with $\kappa = 0.5$ (solid red line) coinciding with the key rate of the hardware fix with an uneven beamsplitter (black circles). e) Key rate of the hardware fix with additional loss in the short arm (black line).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, 2009.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, dec 1984. IEEE.

[3] I. Devetak and A. Winter. Distillation of secret key entanglement from quantum states. *Proc. of the Roy. Soc. of London Series A*, 461(2053):207–235, 2005.

[4] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501, Aug 2005.

[5] Agnes Ferenczi and Norbert Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85(5):052310, 2012.

[6] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.*, 4(5):325, 2004.

[7] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D*, 2007.

[8] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett*, 91:57901, 2003.

[9] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

[10] X. B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, 2005.

[11] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008.

[12] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78:032302, 2008.

[13] Varun Narasimhachar. Study of realistic devices for quantum key-distribution. Master's thesis, University of Waterloo, 200 University Ave. W., Waterloo, Ontario, Canada, N2L 3G1, 2011.

[14] C. Gobby, Z.L. Yuan, and A.J. Shields. Quantum key distribution over 122km of standard telecom fiber. *Appl. Phys. Lett.*, 84:3762–3764, 2004.