

Quantum key distribution with undefined encoding bases

Nima Rafiei(1), Jan Bogdanski(1), Marek Zukowski(2) & Mohamed Bourennane(1)

1: Department of Physics, Stockholm University, S-10961 Stockholm, Sweden

2: Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdanski, PL-80-952 Gdansk, Poland

Abstract

Security of information is essential. Classical cryptography relies on computational difficulty, and cannot reveal eavesdropping. Quantum cryptography employs quantum laws, and eavesdropping causes detectable errors. Standard quantum protocols fix the set of used states. Eavesdropping attacks take advantage of that. Errors occur, but a part of the key is stolen. If protocol uses weak pulses, photon number splitting attacks are possible, which cause in principle no errors. We present a cryptographic protocol with (random) states known to only sender (the qubit makes around trip). Attacks are in vain, even photon-splitting, or coherent ones. We apply this method also for multiparty secret sharing. The protocol was experimentally demonstrated, thus we have a highly secure method using quantum laws to protect secret information.

Introduction

Quantum cryptography aims to provide an unconditionally secure key distribution (QKD) between two parties, Alice and Bob. Bennett and Brassard (BB84) proposed a quantum key distribution protocol in which Alice and Bob choose randomly between two *known* conjugate (mutually unbiased, complementary) bases and in each basis the information is encoded using two orthogonal quantum states (qubits). The use of a random choice of mutually unbiased bases furthermore implies that if the sender Alice prepares a state in one basis, the outcome of a measurement by Bob or eavesdropper (by convention called Eve) in a conjugate basis will yield a totally random outcome. Since the choice of Alice's basis is unknown to Eve she cannot copy the sent states perfectly (the non-cloning theorem). These features guarantee that any eavesdropping attempt will invariably introduce errors, which can be detected by the legitimate communicating parties. There are many theoretical and experimental works using these principles.

Main achievements

Here we propose a new protocol for QKD. The main idea is that Alice, as she is the sender of the qubit and the final recipient, can impose on it a totally random "offset" phase, known only to her. Thus her qubit is for Bob, as well as for eavesdroppers, in a maximally mixed state, while Alice can undo the offset phase right before the final measurement. Alice and Bob also perform unitary transformations, typical for QKD protocols, on the qubit making a round trip. As in BB84, in a version which uses a specific initial polarization state, they use one of four transformations, which are split to two classes – the two transformations belonging to the same class lead to two orthogonal states; only the information on the class on actions is later revealed – the actual transformations and the offset are never revealed. As our protocol requires only single qubits it is realizable

with the current technologies (and we have performed its first experimental test). We also designed a secret sharing protocol using the same trick.

As the measurement basis of Alice's depends on the offset phase, Eve is totally blind on the final form of the measurement and its result (until it is announced). Thus she gets no knowledge of Alice's coding method whatsoever, and when Alice and Bob exchange publicly some part of their sifted key, they immediately see that they are completely uncorrelated. Thus they abandon the crypto-communication. No action on the qubit, whatsoever, including its replacement, can correlate Eve's strings of data with Alice's. Even the so-called coherent attacks are useless because the offset phases are different for each qubit, and totally unknown for Eve. To put it short: *effective eavesdropping would be equivalent to pinpointing the offset phases for each qubit, and this in turn is equivalent to the possibility of measuring its state.*

One can discuss further the above claim assuming the PNS attack. This is possible for sources that are not perfectly single-photon ones, which is the usual case. In such a case Eve may beam-split the pulses, and keep one photon, while sending the rest to Bob. Thus she has a perfect copy of the qubit sent by Alice. But as the offset phase is unknown to her, there is no way for her to get a deterministic information on the coding of Alice even after Alice reveals *the class of her transformation* (this is in a drastic contrast with the modified BB84 scheme, presented above). But Eve can be even more subtle and after catching the first photon she can wait for the photons returned by Bob (we again assume that there is more than one), and again beam-split them, to keep one more perfect copy, now of the qubit after Bob's encoding transformations. Now, her task would be to compare the two qubits. She knows that if they are in orthogonal states then Bob's *bit* is 1, and if they are the same state then *it* is 0. However, even after Bob and Alice reveal *the classes of their transformations* her situation is unchanged. As she does not have a faintest idea about *the offset phase* she has the

deterministically impossible task of distinguishing whether her two photons are in the same *unknown* state or are in two unknown orthogonal states. E.g., she can try to perform a collective measurement such as the Hong-Ou-Mandel type interference experiment. The photons would exit in into one detector always when they are in the same (polarization) state, but also in 50% of cases when they are in two orthogonal states. Thus her error rate would be 25% exactly as in the case of an intercept-resend attack.

Conclusions

The presented quantum cryptographic scheme is very robust against attacks, and easy to implement in practise. It has also an obvious generalization to a secret sharing scheme.

This work was supported by Swedish Research Council (VR) and Swedish Defence Material Administration (FMV). M.Z. was supported by Wenner Gren Foundations and by the EU programme QAP (Qubit Applications, No. 015858).