Theoretical Computer Science 560 (2014) 27–32

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

The black paper of quantum cryptography: Real implementation problems

Valerio Scarani *, Christian Kurtsiefer

Centre for Quantum Technologies and Department of Physics, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore

ARTICLE INFO

Article history:
Received 31 May 2009
Accepted 7 June 2011
Available online 17 September 2014

Keywords:
Quantum cryptography
Security
Quantum hacking

ABSTRACT

The laws of physics play a crucial role in the security of quantum key distribution (QKD). This fact has often been misunderstood as if the security of QKD would be based *only* on the laws of physics. As the experts know well, things are more subtle. We review the progresses in practical QKD focusing on (I) the elements of trust that are common to classical and quantum implementations of key distribution; and (II) some threats to security that have been highlighted recently, none of which is unredeemable (i.e., in principle QKD can be made secure). This leads us to guess that the field, similar to non-quantum modern cryptography, is going to split in two directions: those who pursue practical devices may have to moderate their security claims; those who pursue ultimate security may have to suspend their claims of usefulness.

1. Introduction

In their seminal 1984 paper [1], Bennett and Brassard argued that some basic laws of physics may prove useful in cryptographic tasks. They considered first the task of *key distribution* between distant partners and noticed that quantum signals are ideal trusted couriers: if the eavesdropper Eve tries to obtain some information, her action cannot remain concealed, because measurement modifies the state or, equivalently, because of the no-cloning theorem. In the second part of their paper, they turned to the task of bit-commitment and proposed a quantum solution relying on entanglement. In 1991, Ekert independently re-discovered quantum key distribution [2]: his intuition was based on entanglement, more specifically on Bell's inequalities. These two works are the milestones of the field, even if precursors for these ideas had been brought up [3].

The fact that security is based on physical laws leads to the hope that quantum cryptography may provide the highest possible level of security, namely security against an adversary with unrestricted computational power; in the jargon, *unconditional security*. Further research vindicated only one of the two conjectures of Bennett and Brassard: key distribution can indeed be made unconditionally secure [4–6], while bit commitment cannot [7]. Most of the subsequent developments in quantum cryptography have therefore been devoted to *quantum key distribution (QKD)*; several review papers are available [8–11].

* Corresponding author.
E-mail addresses: valerio.scarani@gmail.com (V. Scarani), christian.kurtsiefer@gmail.com (C. Kurtsiefer).

http://dx.doi.org/10.1016/j.tcs.2014.09.015
0304-3975/© 2014 Elsevier B.V. All rights reserved.

2. Quantum signals as incorruptible couriers

Even before unconditional security was technically proved, *"security based on the laws of physics"* became the selling slogan of QKD. It's catchy, and it can be understood correctly — but it may also be understood wrongly and has often been explicitly spelled out as "security based *only* on the laws of physics". Of course, a pause of reflection shows that the statement cannot possibly be as strong as that. For instance, the laws of physics do not prevent someone from reading the outcomes of a detector; however, if the adversary has access to that information, security is clearly compromised! But many people were just carried away by the power of the slogan — fair enough, this does not happen only with QKD.

On the wings of enthusiasm, some promoters of QKD also managed to convey the impression that they were presenting *the solution for (almost) every task of secret communication*. This may have impressed some sponsors. However, the main result was to alienate a great part of the community of experts in classical cryptography, who, unfamiliar with quantum physics though they may be, could not fail to spot the overstatement. Fortunately, several experts of QKD, well aware of the real scope of their research, managed to re-establish a constructive dialog. Both the interest and the niche character of QKD are generally admitted today.

In fact, the understanding of the niche character of QKD immediately clarifies the role of the laws of physics as well. The *SECOQC White Paper* of 2007 [12] convincingly argued that *QKD is a form of "trusted courier"* i.e. a potential solution for those tasks, for which a trusted courier may be useful. For instance, if one can guarantee that a one-time pad key has not been revealed during its exchange, then the secret is guaranteed also in the future: this is an advantage over complexity-based schemes [13]. Now, with human couriers, we are fairly familiar. Suppose Alice creates a one-time pad key on her computer, burn it on a DVD and entrust to a human courier Charlie the task of bringing it to Bob. Alice should be confident that

(i) her computer and Bob's are not leaking information, by themselves of through active hacking;
(ii) Charlie is honest at the moment of receiving the key from Alice;
(iii) During his travel from Alice to Bob, Charlie will neither be corrupted nor let information leak out inadvertently.

Replacing Charlie *with quantum couriers, one does not have to worry about (iii) anymore: the laws of physics guarantee it; but they don't guarantee (i) and (ii)*. Indeed, it's pretty obvious that (i) must be enforced also for QKD. As for (ii), a "dishonest" quantum courier would be a quantum signal whose state has not been accurately characterized.

Still, one may think that the danger of (i) and (ii) does not extend beyond caricature examples: "Sure enough, if Eve can see Alice through a window...; sure enough, if the source produces always two photons instead of one... But one can easily check for such blunders". Unfortunately, exactly the opposite is the case: blunders affecting the security through failures of (i) or (ii) may be numerous and very subtle; most of the recent developments in practical QKD have to do with those concerns, as we are going to show in the next section.

Before that, we want to stress an important, though quite obvious, issue: in this paper, we review the development of practical QKD. However, since assumptions (i) and (ii) are common for quantum and classical couriers, classical implementations must be checked as well for similar blunders. In other words, we are by no means implying that QKD would be more problematic than classical cryptography. In fact, QKD does have an advantage over classical methods, namely (iii).

3. All that the laws of physics don't take care of

3.1. Problems at preparation

We begin by examining the need for a careful assessment of the properties of the courier. Here is a list of examples. Note that most of them refer to implementations with weak coherent pulses: probably not because they are much worse than others, but because they have been scrutinized more thoroughly.

1. *Problem:* attenuated laser pulses are not single photons, multi-photon components are important [14]. *Solutions:* adapt the security proofs to take the effect into account [15], or change the protocol [17,16] or of course change the source.
2. *Problem:* successive pulses emitted by a laser are generally not independent, they may have phase coherence [18]. *Solution:* adapt the security proofs (not done at the moment of writing) or actively randomize the phase.
3. *Problem:* in the so-called "plug-and-play" implementations (the ones chosen for several commercial setups), photons do a round trip: Alice's device must receive light, code it and resend it [19]. But then, one must assume that the photons that enter Alice's lab might have been prepared by Eve [20]. *Solution:* add attenuation and active phase randomization, then use a suitable security proof [21].
4. *Problem:* in continuous-variables QKD, if the local oscillator travels between Alice and Bob, the implementation is completely insecure unless Bob monitors the intensity [22]. *Solution:* add a beam-splitter and monitor the intensity.
5. *Problem:* in some implementations, the different letters of the QKD alphabet are prepared by different light sources [23]. Each source may have its own fingerprint: for instance, even if coding is supposed to be in polarization, different sources may have different spectra. Also, minor initial or temperature-dependent differences in the electric driving circuitry of each source may go undetected in normal operation or assembly of the setup, but certainly leave a temporal fingerprint