The black paper of quantum cryptography: real implementation problems

Valerio Scarani, Christian Kurtsiefer
Centre for Quantum Technologies & Department of Physics, National University of Singapore, Singapore
(Dated: May 29, 2009)

The fact that the laws of physics play a role in the security of quantum key distribution (QKD) has often been misunderstood, as if the security of QKD would be based *only* of the laws of physics. The history of practical QKD demonstrates how misleading such a stance may be. An assessment of the latest developments leads us to guess that the field is going to split in two: those who pursue really practical devices will have to moderate their security claims; those who pursue ultimate security will have to suspend their claims of usefulness.

I. 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.

The fact that security is based on physical laws lead 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 [3–5], while bit commitment cannot [6]. Most of the subsequent developments in quantum cryptography have therefore been devoted to *quantum key distribution (QKD)*; several review papers are available [7–10].

II. 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, not all dialog was broken, and both the interest and the niche character of QKD are peacefully 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 [11] convincigly argued that *QKD is a form of "trusted courier"* i.e. a potential solution only for those tasks, for which a trusted courier may be useful. With human couriers, we are fairly familiar. Suppose Alice creates a one-time pad key on your computer, burn it on a DVD and entrust to a human courier Charlie to bring 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) Charlie will not be corrupted during his travel from Alice to Bob.

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 go 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.

III. ALL THAT THE LAWS OF PHYSICS DON'T TAKE CARE OF

A. 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 explicitly to implementations with weak coherent pulses: probably not because they are much worse then others, but because they have been scrutinized more thoroughly.

1. *Problem:* attenuated laser pulses are not single photons, multi-photon components are important [12]. *Solutions:* adapt the security proofs to take the effect into account [15], or change the protocol [13, 14] or of course change the source.

2. *Problem:* successive pulses emitted by a laser are generally not independent, they may have phase coherence [16]. *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 [17]. The photons that enter Alice's lab might have been prepared by Eve [18]. *Solution:* add attenuation and active phase randomization, then use a suitable security proof [19].

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 [20]. *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 [21]. 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 in the transmitted signal. *Solution:* no miracle solution exists, one has to characterize the sources and bound the possible leakage of information.

B. Problems at detection

Let us now review some examples of the problems at the level of detection. One such problem (admittedly, an anecdotal one) was stressed in the very first demonstration experiment presented by Bennett and coworkers [22]: the Pockels cells used to select the bases were driven by high-voltage devices, which made an audible sound depending on the basis or letter selection. Someone said that the device provided "unconditional security against a deaf eavesdropper": a joke... or a prophetic insight in the fate of practical QKD?

1. *Problem:* an example of leakage of classical information explores parasitic properties of detectors. It is known that, upon detection, Silicon avalanche photodetectors emit light due to hot carrier recombination. This light may leak out through the optical channel, revealing which detector has fired [23]. *Solution:* other photo-diodes have been tested and no such back-flashing was detected (of course, these studies rely on the assumption that the devices used to probe for such radiation capture any sensibly accessible wavelength range).

2. *Problem:* in "plug-and-play" systems, as mentioned, Alice's device is open to receive photons, before coding and resending them. The eavesdropper may implement a *Trojan horse attack* to probe Alice's phase modulator: send in light (say at a different wavelength) and collect it back, coded. *Solution:* because the setup involves attenuators, the additional light that is sent in should be quite intense; a proportional detector is then added at the entrance of the setup, which should detect unusually strong signals [24].

3. *Problem:* light fields ('faked states') can be generated which force at least some of the common detectors to produce outcomes resembling those corresponding to the detection of single photons [25]. This may be exploited to implement something similar to a man-in-the-middle attack. *Solution:* depends on the details of the implementation.

4. *Problem:* photodetectors may also be manipulated to change their timing behaviour [26], such that the detection time is partly correlated with the detection outcome. An experimental evaluation of this leakage channel be-

came known as the time-shift attack [27]. *Solution:* check that all the detectors have the same timing statistics.

5. *Problem:* in a similar fashion, communication of detection times (necessary in any scenario with a lossy communication channel) with a too high accuracy may reveal substantial information about the measurement results, just due imbalanced electronic delays and/or detector parameter scatter [28]. *Solution:* do not reveal too many digits of your detection times.

C. A balance

Just as in every field, there have been sheer mistakes in practical QKD: using the wrong security bound, neglecting to authenticate the classical channel, and similar. The problems reviewed above, however, do not belong to that category: each of them has been the object of a *real discovery*.

The positive side of it all is that, once identified, each of those problems can be solved: thanks to these discoveries, the security of implementations has increased over the years. Another good piece of news is that, in spite of serious scrutinizing, there is no hint of a threat that would compromise the security of QKD in an irredeemable way. But there is a negative side to it: before being identified, each of the problems above represented a serious potential breach of security. It is a truism to stress that we may not be aware of similar problems, which have not been discovered yet.

We come to the bottom line of this section. We believe that this state of affairs cannot be simply dismissed with a "there have been examples of *bad design* of the device". At any stage of development, the devices were actually carefully designed; the security claims of the authors were accepted as valid by referees and colleagues. Neither now, nor at any later time, will one be able to guarantee that the devices in use are provably good. And it is certainly not a good idea to close one's eyes, invoke the laws of physics and dump on them a responsibility they cannot possibly bear.

IV. PATHS FOR THE FUTURE

QKD has evolved from the dreams of childhood to the seriousness of maturity. What is the next stage? Sure enough, "only time will tell what we will do in the future" [29]. But the facts sketched above, combined with some tendencies within the QKD community, allow a guess of two directions in which the field may evolve in the coming years.

A. Option 1: reasonable security of a device

Although they do not provide "security based only on the laws of physics", usual QKD devices provide a quite reasonable level of security if implemented with technical competence and without false complacency on their "quantumness". After all, couriers of classical information must also be trusted; once the trust is there, QKD guarantees the incorruptibility of the courier during its travel — a guarantee that classical information cannot offer.

Here we have therefore a *first possible stance*: give up claims of ultimate security, find a competitive edge and try to produce devices than compare favorably with those operating with classical information. It is our impression that, already at the moment of writing, some of main actors in practical QKD are already taking this stance. We leave to those who embark on this path the task of finding where the competitive edge may lie — a superficial collection of claims may suggest that long-distance implementations are one of the goals, but in fact QKD does not seem to be a viable solution in that regime [30].

B. Option 2: device-independent security and its price

Recently, some authors have come up with a new class of QKD protocols that come as close as possible to the claim of "security based only on the laws of physics". The idea was already present in Ekert's 1991 seminal paper [2], but went unnoticed for many years. The key ingredient is that *Bell's theorem is independent of quantum physics*. As a consequence, it is also independent of the details of the physical systems under study (its Hilbert space, its state, the measurements that are performed). Therefore, a protocol that estimates Eve's information through the amount of violation of a Bell-type inequality is "device-independent" [31].

Of course, even the security of device-independent protocols is not based only on the laws of physics; however, it seems that only those requirements are left that are *strictly necessary*: the eavesdropper does not read your data, does not know which measurements you are going to choose, and the like. A comprehensive discussion can be found in Ref. [32]. What we want to highlight here is that this level of security, arguably the most paranoid one can envisage, comes together with very stringent constraints. As an example, we show how *device-independent protocols have an (almost) intrinsic limitation in distance*. This stems from the requirement that the detection efficiency must be high enough to close the so-called detection loophole. Indeed, as soon as the fraction of detected pairs falls below a given threshold, the observed violation of Bell-type inequality could have been created by pre-established

agreement: the devices may just contain computers pre-programmed by the eavesdropper! In an implementation, being impossible to distinguish losses in transmission from losses due to the quantum efficiency of the detector, the threshold gives the value of the tolerable *total* amount of losses.

How much is this threshold? A thorough study of the detection loophole is missing, partly because the classification of Bell's inequalities is a hard task in itself, and partly because the whole issue was considered of limited interest before the idea of device-independent QKD came about. It is known that there is no finite lower bound: there are explicit examples in which the detection loophole can be closed with arbitrarily low efficiency [33]. However, these examples use states of very large dimension d and a number of measurements that is exponential in d. For a QKD protocol to qualify as "practical", the number of measurements and of outcomes must be kept "reasonable". The set of inequalities with few measurements and few outcomes has been studied in great detail (though not in its fullness) and, in those cases, the detection threshold is always found well above 50% [34].

For definiteness therefore, let us take the value of 50% for the threshold of total detection efficiency. InGaAs photodetectors in the telecom wavelength range have efficiencies below 30% even under the most optimistic specifications; none of the implementation using those detectors can therefore be used for device-independent security. Depending on the trust into manufacturer specifications, setups using Silicon-APD may just about reach the threshold on the detector side, but then almost no losses can be tolerated in the channel. Assuming detectors with 100% efficiency [35], fiber-optical transmission channels without any interconnect losses and with the usually quoted (optimistic) attenuation coefficient of 0.18 dB/km would limit a direct QKD link to a distance of 16 km.

This issue of the distance has been presented as an example of how stringent the requirements for device-independent security may be. If we believe that history repeats itself, further scrutiny will lead to identifying further limitations of these very recent protocols. In other words, it may be premature to attach any practical value to device-independent QKD; whence the *second possible stance* that we envisage for the coming years: focus on developing the tools (both theoretical and experimental) required to demonstrate the ultimate level of security, leaving aside, at least temporarily, all claims of usefulness.

V. CONCLUSION

We have reviewed the evidence of the fact that QKD guarantees security based on the laws of physics *provided* the implementation is perfect, or more precisely, provided all the imperfections of the implementation have been characterized and their effect is accounted for. Since a thorough check of all possible leakage channels is impossible, the security of QKD will always be based on some elements of trust. Expressions like "security based only on the laws of physics" or "unconditional security" are unfortunate. They may be convenient among experts, as part of their technical jargon; but when they leak out to larger audiences, they almost invariably convey the wrong message.

Specifically, we argued that the level of trust for usual QKD protocols, like BB84, is not very different from the one demanded of a "trusted courier" carrying classical information. Protocols based on Bell's inequalities minimize the number of elements of trust but come with very stringent requirements. Twenty-five years after BB84, the field seems on the point of splitting in two directions: (i) the development of prototypes optimized for the needs of niche tasks and guaranteeing a "reasonable" level of security; (ii) the quest for demonstrating the most paranoid level of security, decoupled from any claims of practical usefulness.

Acknowledgments

This work is supported by the National Research Foundation and Ministry of Education, Singapore.

[1] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179.* (1984).

[2] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)

[3] D. Mayers, in: *Advances in Cryptology — Proceedings of Crypto '96* (Springer Verlag, Berlin, 1996), p. 343.

[4] H.-K. Lo, H.F. Chau, Science **283**, 2050 (1999).

[5] P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[6] Interestingly, the impossibility of bit commitment also derives from a deep physical law: the fact that the correlations obtained by measuring an entangled state do not arise from a time-ordered chain of events. Here, it implies that Bob cannot be sure that Alice has actually performed her measurement and thus committed to her bit. For the formal proof, see: H.-K. Lo, H.F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[7] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)

[8] M. Dušek, N. Lütkenhaus, M. Hendrych, Progress in Optics **49**, Edt. E. Wolf (Elsevier), 381 (2006)

[9] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, arXiv:0802.4155

[10] H.-K. Lo, Y. Zhao, arXiv:0803.2507

[11] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger, *SECOQC White Paper on Quantum Key Distribution and Cryptography*, quant-ph/0701168

[12] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[13] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[14] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[15] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).

[16] H.-K. Lo, J. Preskill, Quant. Inf. Comput. **8**, 431 (2007).

[17] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, N. Gisin, Appl. Phys. Lett. **70**, 793 (1997)

[18] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[19] Y. Zhao, B. Qi, H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).

[20] H. Häseler, T. Moroder, N. Lütkenhaus, Phys. Rev. A **77**, 032303 (2008).

[21] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, J.G. Rarity, Nature **419**, 450 (2002)

[22] C.H. Bennett, F. Bessette, L. Salvail, G. Brassard, J. Smolin, J. Cryptology **5**, 3 (1992)

[23] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, J. Mod. Opt. **48**, 2039–2047 (2001).

[24] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, Electronics Letters **34**, 2116 (1998)

[25] V. Makarov, D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005)

[26] V. Makarov, A. Anisimov, J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[27] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, Phys. Rev. A **78**, 042333 (2008)

[28] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[29] Freely translated from "L'avenir nous dira ce qu'on va faire dans le futur", a by now famous truism by Swiss soccer tycoon Christian Constantin, Prix Champignac d'Or 2007.

[30] Try the following back-of-the-envelop calculation: Alice creates weak coherent pulses with μ average photon number at a rate R and sends them to Bob over a channel with transmittivity $t = 10^{-\alpha\ell/10}$ where ℓ is the distance and α characterizes the losses. Bob uses a detector with η quantum efficiency. The time Bob needs to detect K bits of data is $\tau = \frac{K}{R\mu t\eta}$ (note that we are considering only the effect of losses and detection: one should add dark counts and of course data processing to extract a secure key). As an example, take $R = 1$MHz, $K = 1$Gb, $\mu = \eta = 0.1$, $\alpha = 0.2$dB/km (fibers) and $\ell = 100$km; then $\tau = 10^7$s $= 115$ days: you are certainly faster walking there. If one goes to $\ell = 500$km (typically the distance at which, again for fibers, quantum repeaters start becoming useful), one finds the awesome value $\tau = 10^{15}$s ≈ 30 million years.

[31] We do not delve here into the detailed sequence of discoveries and claims that lead to device-independent QKD. The most meaningful references are: J. Barrett, L. Hardy, A. Kent, Phys. Rev. Lett. **95**, 010503 (2005); A. Acín, N. Gisin, L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006); A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[32] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scarani, New J. Phys. **11**, 045021 (2009)

[33] S. Massar, Phys. Rev. A **65**, 032121 (2002)

[34] **REFS!!!**

[35] Superconductor-based TES detectors reach close to 100% quantum efficiency and have been used in some QKD experiments: P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S.W. Nam, A.E. Lita, A.J. Miller, J.E. Nordholt, New J. Phys. **8**, 193 (2006). At present, this technology cannot yet be called "practical", due to its cooling requirements.