# 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 28, 2009)

Write

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, called *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].

But what does "unconditional security" actually mean? The expression itself conveys the meaning of "something that can be trusted blindly" and the fact that the security of QKD is "based on the laws of physics" reinforces the same impression. But this cannot be the case. For instance, the laws of physics do not prevent someone from reading the outcomes of a detector; however, if Eve has access to that information, security is clearly compromised! In fact,"unconditional security" has the same meaning in QKD as it has in the usual jargon of cryptography, namely: security can be guaranteed against an eavesdropper with unrestricted computational power, *provided the devices and procedures of the authorized partners Alice and Bob are well characterized.* This paper has been written to emphasize this point.

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

### A. Leakage of quantum information: side channels

In the usual QKD protocols, the laws of physics do not take care of side channels. A side channel is, in short, some component of the real quantum signal that one happens to neglect. For clarity, let us go through the most famous examples of such undesired effects:

1. For some years, at the beginning of QKD, it was believed that attenuated lasers were good practical approximations of single-photon states. Then Lütkenhaus and coworkers stressed that the presence of multi-photon components in a laser pulse opened a serious gap in security [11]. For the specific side channel consisting of the photon number, variations of the protocol have been proposed [12, 13]. Security proofs were later adapted to take into account the effect of this and similar side channels [14].

2. About the same implementation, it was later noticed that the proofs applied only under the assumption of complete phase randomization between successive pulses [15], and did not apply to plug-and-play systems **[Not sure if 'plug-and-play' is a clear reference with everyone or just a markting fad]** because one cannot guarantee which state enters Alice's device [16]. A security proof coping with the latter has since been given [17], while for the first issue the only known solution consists in implementing active phase randomization.

3. Another class of side channels is present in more traditional prepare-and-send implementations, where the different letters of the QKD alphabet are prepared by different light sources: The distinguisgability of the characters is usually not limited to something which maps to a spin-1/2 space like polarization of photons. A spectral fingerprint of different letters due to physically different light sources is an example which is very likely to be present in all systems using independent lasers or LEDs for the different letters.

4. Along the same line, minor initial or temperature-dependent differences in the electric driving circuitry of independent light sources may go undetected in normal operation or assembly of the source, but certainly leave a temporal fingerprint in the transmitted signal, opening a side channel available to an eavesdropper with sufficient technical abilities to extract this information.

5. A particularly serious side channel was discovered at some point for continuous-variable QKD. In the usual implementations, the local oscillator providing the phase reference for the homodyne measurement is sent from Alice to Bob. In this case, security is entirely compromised if the intensity of this beam is not monitored at Bob's side [18].

### B. Leakage of classical information: bad design and hacking

**Is there really a difference between classical and quantum information leaks? If you think this is the case, a short para what you mean by that would perhaps help. I don't see an intrinsic difference in them: Anything which gives you information about the source, be it multiphoton, spectral or classical seems to be the same. Wether you call a timeshift a classical thing or an extension of a Hilbert space seems a bit arbitrary. I also object against the notion of a 'bad design', since it has the flavour that any design which has an unknown channel may be considered a 'bad design' as soon as you learn about it. Desgins where you don't investigate their shortcommings are not necessarily good. Alternative proposal: separate between detector and receiver vulnerabilities?**

1. Perhaps one of the first arrack schemes on detection schemes reported was in the demonstration experiment presented by C. Bennett and coworkers: The pockels cells used for selecting the bases were driven by high-voltage devices, which made an audiable sound depending on the basis or letter selection.

2. **Should be there something on the trojan horse on the 'plug-and-play' systems? The cure against that is also strictly by classical engineering...** A very similar attack scheme with modulator-based QKD systems in a 'plug-and-play' configuration with a roundtrip of optical pulses became known as the trojan horse attack: The state of the modulator imprinting the classical information could be read out by an attacker working with a pulse of different wavelength.

3. An example of leakage of receiver information once the signal has gone 'classical' in a realistic system explores parasitic properties of detectors: At least Silicon avalanche photodetectors are known to emit light due to hot carrier recombination inside the device upon an avalanche triggered by a photoelectron, leading to a leakage of 'classical' information to an eavesdropper through the optical channel [23]. Although it has been reported that this is no problem with direct-bandgap InGaAs detectors for the telecom wavelength range (ref:some of the geneva work on detectors), such 'proofs' rely on the assumption that the devices used to probe for such radiation capure any sensibly accessible wavelength range.

4. Light fields ('faked stages') can be generated which force at least some of the common detectors to outcomes resembling those correpsonding to the detection of single photons [24]. This may be exploited to implement something similar to a man-in-the-middle attack.

5. Lo time-shift (idea: [25], implementation: [10]) Photodetectors may also be manipulated to change their timing behaviour [25], such that information of the detection instant will partly reveal the measurement result in the classcal sifting process. An experimental evaluation of this leakage channel became known as the time-shift attack [10].

6. In a similar fashion, communication of detection times (necessary in any scenario with a lossy communication channel) with a too high accuracy just due imbalanced electronic delays and/or detector parameter scatter may reveal substantial information about the alledgedly secret measurement results [26].

7. Makarov reloaded: saturate and control detectors **I think the basic idea is the same as in the fake state generation, just with a specific application to a complete system with a passive base choice. I would wait with the inclusion of this attack until we have stuff on this on the arxive.**

### C. A balance

We have reviewed the most prominent discoveries of side channels, leakage and hacking in real implementations of QKD. We stressed how, once identified, each of the issues above can be coped with, either by adapting the security proofs or by hardware modifications. In this sense, the security of those implementations has increased in the last years, and the ultimate security of QKD does not seem to be under threat. Before being identified, however, each of the issues above represented a serious potential breach of security.

There has been and still is a temptation to classify some of the open information channels mentioned above as 'bad design/implementation', but this has been recognized as a dangerous attitude in classical cryptography a long time ago (we should have a reference here): A system may only appear as well-designed and thus conceived as secure as long as a particular physical implementation weakness is not known. There is no proof, however, that an implementation is free of a particular weakness of any kind.

The development of QKD has therefore clearly shown that *"unconditional security" and "security based only on the laws of physics" are two distinct notions.* Unconditional security, in its jargon sense, can be and has been proved for many QKD protocols — this is of course remarkable, and would be impossible without quantum physics. However, the application of a security proof to a real device requires an additional level of trust: one must be confident that the leakage of both quantum information (through side channels) and classical information (through bad design or hacking) has been correctly bounded.

In this sense, the notion *unconditionally secure* seems to be a particularly unfortunate jargon, since it insinuates security while it refers only to a particular set of assumptions or conditions, including the one that a system is free of unknown leakage channels wich, once they become kown, will be classified as *bad design.*

## II. PATHS FOR THE FUTURE

Only time will tell what we will do in the future [19]. 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 do provide a quite reasonable level of security. After all, classical devices must be trusted on not leaking too much information out too; and once the trust is there, QKD offers something that classical devices cannot offer. Moreover, thanks to the technological developments of the last years, for some applications QKD devices may also be competitive in terms of reliability, speed, cost...**Do we need this really? This is not a marketing article?** Here we have therefore a first possible stance: give up claims of ultimate security, find a competitive edge and try to produce better devices than those based on classical information processing. This stance implies the admission that QKD is not going to be "the solution for (almost) every secret communication", as it is still presented sometimes. But the niche character of QKD is not new: see for instance the comprehensive analysis of the place of QKD within cryptography given by the *SECOQC White Paper* of 2007 [20].

### 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" [21]. 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... In other words, whenever a Bell-type inequality is violated without sending a signal, the correlations that are created must contain some secrecy (because if a third party had full information, this information would be a local hidden variable).

Therefore, a protocol that estimates Eve's information through the amount of violation of a Bell-type inequality is "device-independent". By definition, this approach takes automatically care of all side channels, because there is no need of specifying anything about the quantum signal anyway. It is also sensitive to hacking strategies in which Eve tries to force a result chosen by herself. For a comprehensive review of the benefits of device-independent QKD as understood today, we refer the reader to Ref. [22]. Here, we want to highlight the remaining level of trust and the price one has to pay for such a general level of security (for the sake of this paper, we assume that "unconditional security" will be proved one day for device-independent protocols, though the issue is still open at the moment of writing).

The *level of trust* is defined by some obvious requirements, namely (i) quantum physics must be correct, (ii) Eve must not have access to the data, (iii) Eve must not have provided the random number generator that makes the choice of setting. These are common to all of QKD. A fourth requirement is less obvious: although, as we said, one does not need to know the details of how the devices operate, one must make sure that (iv) the violation of Bell's inequality is not be due to the exchange of a signal. In principle, one might think that this last requirement can be guaranteed by arranging space-like separated detections. But this is not evident in a black-box scenario: even if the outcomes are perceived as exactly simultaneous, one of them might have been created earlier and just kept in a memory for the convenient amount of time.

Anyway, before even addressing those issues, there is a further crucial concern: one must be sure to observe a *real* violation of Bell's inequalities in the first place. In a black-box scenario and in the presence of an adversary, the *detection loophole* becomes a natural option. Indeed, as soon as the fraction of detected correlations is below the required threshold, the observed violation of Bell-type inequality could have been created by pre-established agreement: the black-box may just contain a computer with a pre-determined program! Furthermore, the detection loophole is not only about the efficiency of the detectors: *all the losses*, and in particular the losses in the transmission, must lie below the threshold. This means that device-independent QKD can in no case be demonstrated over long distances!

**Give numbers, conclude on distances!** If losses of the photons cannot exceed 50% or 3 dB, none of the current implementations using InGaAs photodetectors used for the telecom wavelength range would allow establish any secret key due to their efficiencies below 30% even under the most optimistic specifications. Depending on the trust into manufacturer specifications, Silicon-APD based schemes may just about reach the treshold on the detector side.

Assuming efficient detectors become available (the supraconductor-based TES detectors [**?** ] are of that kind, albeit with limited practicability due to their current cooling requirements), fiber-optical transmission channels without any interconnect losses and with the ususally quoted (optimistic) attenuation coefficient of 0.18 dB/km would limit a direct QKD link to a distance of 16 km.

## III. CONCLUSION

Moderate the claims....

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

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

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

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

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

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

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

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

[19] 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.

[20] 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

[21] 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).

[22] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Mas-

sar, V. Scarani, New J. Phys. **ACCEPTED** (2009)

[23] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, The breakdown flash of Silicon Avalanche Photodiodes - backdoor for eavesdropper attacks? J. Mod. Opt. **48**, 2039–2047 (2001).

[24] V. Makarov and D. R. Hjelme, Faked states attack on quantum cryptosystems, J. Mod. Opt. **52**, 691–705 (2005).

[25] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A **74**, 022313 (2006).

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