# Is the security of quantum cryptography guaranteed by the laws of physics?

Daniel J. Bernstein[1,2]

[1] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands

**Abstract.** It is often claimed that the security of theoretical quantum key distribution (QKD) is guaranteed by the laws of physics. However, this claim is content-free if the underlying definition of theoretical QKD is not actually compatible with the laws of physics. This paper observes that (1) the laws of physics pose serious obstacles to the security of QKD and (2) these laws are ignored in all QKD "security proofs".

**Keywords:** security failures, quantum cryptography, quantum key distribution, side-channel attacks, electromagnetism, gravity, information flow, holographic principle

---

*QKD . . . offers the ultimate security of the inviolability of a law of Nature for key distribution.* —Hughes, Alde, Dyer, Luther, Morgan, and Schauer, 1995 [11]

---

*Quantum cryptography differs from conventional cryptography in that the data are kept secret by the properties of quantum mechanics, rather than the conjectured difficulty of computing certain functions.* —Shor and Preskill, 2000 [22]

---

*Quantum key distribution provides perfect security because, unlike its classical counterpart, it relies on the laws of physics.*
—Christandl, Renner, and Ekert, 2004 [7]

---

*Quantum cryptography solves the problem of key distribution by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the fundamental laws of physics.* —ID Quantique, 2012 [12]

---

This work was supported by the European Commission under Contract ICT-645622 PQCRYPTO; by the Netherlands Organisation for Scientific Research (NWO) under grant 639.073.005; and by the U.S. National Science Foundation under grant 1314919. "Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation" (or, obviously, other funding agencies). Permanent ID of this document: e39346ac8e0f20edb8df3334f8751ac75a600099. Date: 2016.03.26.

## 1 The "provable security" of quantum cryptography

The core advertisement for quantum cryptography—in particular, for quantum key distribution, which I'll focus on—is the claim that its security is guaranteed by the laws of physics. One would expect this claim to be backed by a clearly stated theorem having the following shape:

- "Assume $L$." Here $L$ is a statement of the laws of physics.
- "Assume $P$." Here $P$ states physical actions carried out by Alice and Bob.
- "Then $S$." Here $S$ states a security property: e.g., something about the randomness, from Eve's perspective, of a key shared between Alice and Bob.

This theorem statement would provide a starting point for security auditors to dive into questions of whether the stated $L$ is actually how the real world works; whether the stated $P$ matches what is actually being sold as "quantum key distribution"; whether the proof of the theorem is correct; and whether the stated $S$ actually includes what the users want.

An auditor who attempts to find this security theorem in the literature will easily find papers claiming to present "security proofs" for several different types of quantum cryptography; see, e.g., [8]. However, the theorems in these papers never seem to explicitly hypothesize $L$, the laws of physics.

Is this merely a culture gap—when physicists say "Theorem" they implicitly mean a theorem under certain well-known hypotheses? Or is there an important reason that these papers aren't hypothesizing Newton's law of gravitation, for example, and Maxwell's equations for electromagnetism? Or refinements such as general relativity and quantum electrodynamics?

An auditor who dives more deeply into the "security proofs" won't find Maxwell's equations used anywhere. This justifies omitting Maxwell's equations as a hypothesis, but it also strongly suggests that the secret physical actions taken by Alice and Bob don't involve any electricity or magnetism. How could one possibly prove anything about the effects of electromagnetic actions without invoking the relevant laws of physics? Similarly, Newton's law isn't used anywhere, strongly suggesting that the secret physical actions taken by Alice and Bob don't involve moving any mass around. But then what exactly *are* the secret actions taken by Alice and Bob?

## 2 Abstractions without examples

A closer look shows that the papers don't actually say what physical actions Alice and Bob are hypothesized to be carrying out. Sometimes the papers do specify physical details of, e.g., polarized photons being sent from Alice to Bob via Eve; or entangled pairs of photons being sent from Eve to both Alice and Bob (in so-called "device-independent" QKD; see, e.g., [17]); or photons being sent with particular timing (in "relativistic" QKD; see, e.g., [15]); but there are always many other steps taken by Alice and Bob whose physical details are not mentioned anywhere in any of the "security proofs".

Instead the papers make various abstract hypotheses regarding quantum states. Consider, for example, the following hypothesis from [14]:

> Eve can choose an observable $Z$ and obtains an outcome $E$. We assume that this, together with the public messages exchanged by Alice and Bob, is all information available to her.

Apparently Alice and Bob are supposed to take physical actions that do not interact with Eve's quantum state except through the public interactions specified by the protocol. This begs the question of what those physical actions are supposed to be.

Obviously there are physical actions that Alice and Bob can take in the real world that might look like QKD but that don't actually meet the hypotheses of the QKD "security proofs". In particular, every QKD "security proof" assumes that there are various secret actions by Alice and Bob, actions unobserved by Eve, such as a sizeable fraction of Alice's choices of polarization bases in the BB84 protocol. If Alice and Bob actually leak these secrets to Eve then these hypotheses are false and the QKD "security proofs" say nothing.

Anyone who claims that the security of QKD is guaranteed by the laws of physics is logically forced to argue that these physical actions by Alice and Bob are not actually QKD: the only physical actions that qualify as QKD are those for which the hypotheses of the theorems are satisfied. On the other hand, many authors insist on using the label "QKD" for actions that are obviously outside the scope of the theorems. Sometimes "security" systems that have already been convincingly demonstrated to fail in the real world (see, e.g., [10]) are still sold as "QKD".

To avoid confusion, let's use the name "theoretical QKD" to refer to QKD meeting all of the hypotheses of the theorems. Is it clear that theoretical QKD exists within the laws of physics? Are there any examples of physical actions for Alice and Bob that *do* qualify as theoretical QKD?

Consider the following nightmare scenario for the QKD "security proofs": The hypotheses of theoretical QKD are actually *inconsistent with the laws of physics*. For every sequence of physical actions that Alice and Bob can take, the hypotheses turn out to be false. It is vacuous to claim that the security of theoretical QKD is guaranteed by the laws of physics, since the laws of physics imply that theoretical QKD does not exist. What evidence do we have that the QKD "security proofs" are not in this nightmare scenario?

Part of the job of a mathematician or computer scientist stating a theorem is to verify—or at least plausibly conjecture—that there are examples meeting the hypotheses of the theorem. Vacuous lemmas are occasionally stated as intermediate steps inside proofs by contradiction, but these lemmas are also clearly identified as being vacuous, not as saying anything meaningful.

## 3 The holographic principle

Let me focus specifically on the hypothesis that Alice and Bob are taking various actions unobserved by Eve. This is, as I mentioned above, assumed in every QKD

"security proof". Obviously Alice and Bob have no security against Eve if Eve observes all of their secrets, so one cannot avoid making such a hypothesis.

This hypothesis seems to be flatly contradicted by the "holographic principle". In the words of Brian Greene (quoted in [13]):

> The holographic principle envisions that all we experience may be fully and equivalently described as the comings and goings that take place at a thin and remote locus. It says that if we could understand the laws that govern physics on that distant surface, and the way phenomena there link to experience here, we would grasp all there is to know about reality.

Readers not familiar with the idea that the universe is connected in this way should consider radios as an example of long-distance interaction. Radio communication typically relies on Alice and Bob generating a reasonably strong signal to make the receiver's job easier, but this cooperation is not necessary; by building a very large array of radio receivers, Eve can pick up a very faint radio signal from ten thousand miles away.

In light of Maxwell's equations, how can one justify the notion that Eve is unable to observe secret electromagnetic actions by Alice and Bob? Alice and Bob can try to use a Faraday cage to block their signal, but a Faraday cage does not create a truly isolated environment; it merely applies some scrambling to the signals emitted from that environment. One could hypothesize that Eve *is not observing* the actions by Alice and Bob—perhaps Eve is underfunded, or simply lazy—but this is obviously not "absolute security, guaranteed by the fundamental laws of physics".

It seems that the only way for Alice and Bob to avoid Maxwell's information leak is to avoid any data flow from secrets to electricity or magnetism. But then how are Alice and Bob supposed to control their photon generators, photon detectors, and other QKD equipment?

More importantly, the holographic principle says that the difficulty here is not limited to electromagnetism. *Any* physical encoding of information will be visible to a sufficiently resourceful attacker watching signals on a remote screen.

Well-known examples of signal processing (sonar arrays, radar arrays, X-ray tomography, magnetic-resonance imaging, etc.) all seem to fit the following general rule: Eve's cost for stealing a physically encoded secret grows only polynomially with Eve's distance from the secret. Alice and Bob might try to hide at some reasonable distance from attackers, and from any attacker-controlled equipment, but this only moderately increases the cost of the attack.

QKD is claimed to have information-theoretic security guaranteed by the laws of physics, not depending on "the conjectured difficulty of computing certain functions". Even if holographic signal processing actually has superpolynomial cost, the availability of the holographic signal is enough to contradict the QKD security claims. Eve can carry out all necessary computations at her leisure, retroactively breaking QKD without having to interfere with the protocol execution; this directly contradicts the claims in [24] and [21, page 17] that QKD offers "everlasting security".

Of course, claimed "laws" of physics do not have the same level of certainty as mathematics. Many past "laws" seem inconsistent with experiment and are no longer believed to be accurate: e.g., Newton's law of gravitation is merely a first approximation, failing to take relativistic effects into account. One might speculate that (1) the holographic principle is not true in the level of generality suggested in [9], [23], [4], etc.; (2) the leaks of information to Eve are "merely" through electromagnetic waves, gravity, etc.; and (3) there is some way for Alice and Bob to carry out QKD without triggering any of these leaks of information. In other words, it is conceivable that some law of physics not known today will eventually guarantee the security of some form of QKD not specified today. But these unsupported speculations are very far from justifying the claim that QKD provides "absolute security, guaranteed by the fundamental laws of physics".

## 4 Previous work

There is a huge literature claiming that the security of theoretical QKD is guaranteed by the laws of physics. I am not aware of previous papers clearly and directly raising the possibility that this claim is vacuous—that theoretical QKD is not actually compatible with the laws of physics.

Plaga in [18] pointed out that speculations about nonlinearity of quantum gravity, if correct, could allow Eve to extract information from the data *explicitly communicated* in some QKD protocols. What I am saying is quite different: I am focusing on information leaked from the "secret" portions of QKD protocols, and I am relying on core physical phenomena such as electromagnetism.

More relevant is a paper [19] by Rudolph, which (among other things) questions the "impenetrability/no emanation" hypotheses for theoretical QKD. What I am saying is stronger in three ways. First, Rudolph merely questions the hypotheses, while I am questioning both the hypotheses and the conclusion. Second, regarding details, Rudolph touches upon ways that *some* secrets could leak, and asks whether these leaks can be limited to "an exponentially small amount of useful information", while I am pointing to ways that *all* secrets leak to a sufficiently resourceful attacker. Third, Rudolph says that a "black hole lab" would "presumably" satisfy the hypotheses, while I am not drawing any such line. My impression of the consensus of physicists is that black holes are *not* an exception to the holographic principle.

Brassard stated in [5] that the original prototype implementation of QKD "was unconditionally secure *against any eavesdropper who happened to be deaf*! `:-)`" (italics and smiley in original). This is still an overstatement of the security provided by the implementation. It is clear that the implementation would also have given up all of its secrets to, e.g., a deaf eavesdropper watching the screen of an oscilloscope attached to a small coil of wire. More importantly, Brassard presented this security failure as being specific to one implementation of QKD, not recognizing the possibility of the laws of physics forcing the same fundamental type of security failure to appear in *all* forms of QKD.

A series of papers on "quantum hacking", most recently [10] by Huang, Sajeed, Chaiwongkhot, Soucarros, Legre, and Makarov, have broken the security of various commercial implementations of QKD. All of these attacks follow the theme of Eve interacting physically (passively or actively) with the "secret" computations by Alice and Bob.

QKD proponents generally respond to "quantum hacking" by claiming that these security failures arise from fixable gaps between current practical QKD and theoretical QKD. For example, Scarani and Kurtsiefer in [20], while generally expressing skepticism regarding the security of QKD, also claim that "in principle QKD can be made secure". However, none of these responses have explained *how* theoretical QKD can be achieved within the laws of physics. Any effort to fill this gap would seem to run afoul of the holographic principle.

## 5 Countermeasures

What should Alice and Bob do if the promise of "security guaranteed by the fundamental laws of physics" is a sham—in particular, if physical effects allow a computationally unlimited attacker to steal secrets from an arbitrary distance?

The obvious answer is to study the *cost* of Eve's attack, and to take measures to increase this cost—hopefully beyond anything that Eve can afford. There are several ways to argue that Eve is subject to cost limits:

- Perhaps the lifetime of the universe is limited.
- Perhaps, even in an everlasting universe, the cosmological constant is positive, putting a limit on all computations, as explained in [3]. This constant is generally believed to be around $10^{-122}$.
- Perhaps the space aliens who control most of the resources in the universe are happy that Alice and Bob are secretly arranging climate-change protests, and are not willing to help policewoman Eve see these secrets. Compare [16].

If Eve is limited to cost $C$, then Alice and Bob do not need to aim for the unachievable goal of security guaranteed by the laws of physics; Alice and Bob merely need to be secure against all attacks that cost at most $C$.

Earlier I mentioned that Eve's cost for stealing a physically encoded secret seems to grow only polynomially with Eve's distance from the secret. However, this polynomial also seems to depend heavily on the choice of encoding mechanism. Alice and Bob can and should choose technologies for encoding their secrets with the goal of making this polynomial as large as possible. For example, one might guess that the following steps help:

- Store and process secrets inside a modern 14nm Intel CPU, rather than using older, less efficient chip technology. Presumably consuming less energy for the same computation will reduce the amount of signal visible to Eve, increasing Eve's cost for recovering the secrets.
- Hide the secrets by adding shields and by generating extra noise. A Faraday cage theoretically leaks information but seems to make the information more difficult to intercept and decipher.

- Mask the secrets, for example by encoding bit 0 as a random even-weight 4-bit string and encoding bit 1 as a random odd-weight 4-bit string.
- Apply more sophisticated mathematical encodings, such as "secret-key cryptography" and "public-key cryptography".

Of course, guessing is not the same as systematically studying the actual impact on attack cost. The premier venue for scientific papers analyzing the costs of attackers learning secrets from (passive and active) physical effects, and analyzing the costs of users defending themselves against these attacks, is the "Cryptographic Hardware and Embedded Systems" (CHES) conference series. CHES has run every year since 1999 and attracted more than 400 attendees in 2015.

I can easily be accused of bias—I've served on the CHES program committee every year since 2008 (looking mainly at the costs for users)—but I don't think anyone can dispute the need for this type of research. Competent attackers take advantage of not merely the information that we declare as public but also all of the information they can see through every available side channel. We have to take the same perspective, taking account of all aspects of how secrets are embedded into the real world, if we want to build information-protection systems that society can afford to use but that the attackers find infeasible to break.

The QKD literature doesn't try to argue that QKD will produce improvements within the traditional chart of $(x, y) = (\text{user cost}, \text{attack cost})$. Instead the QKD literature tries to dodge cost questions by claiming that QKD inhabits a magical realm beyond the top of the chart—security "guaranteed by the laws of physics". Unfortunately, this claim is not justified anywhere in the literature, and it seems very difficult to justify, in light of what the laws of physics actually say.

## References

[1] — (no editor), *Proceedings of IEEE information theory workshop on theory and practice in information theoretic security, Awaji Island, Japan, October 2005*, 2006. See [5].

[2] Ahmed Ali, John Ellis, Seifallah Randjbar-Daemi (editors), *Salamfestschrift: a collection of talks from the Conference on Highlights of Particle and Condensed Matter Physics, ICTP, Trieste, Italy, 8–12 March 1993*, World Scientific Series in 20th Century Physics, 4, World Scientific, 1993. See [9].

[3] Raphael Bousso, *Positive vacuum energy and the N-bound*, Journal of High Energy Physics **11** (2000), 038. URL: https://arxiv.org/abs/hep-th/0010252. Citations in this document: §5.

[4] Raphael Bousso, *The holographic principle*, Reviews of Modern Physics **74** (2002), 825–874. URL: https://arxiv.org/abs/hep-th/0203101. Citations in this document: §3.

[5] Gilles Brassard, *Brief history of quantum cryptography: a personal perspective*, in [1] (2006), 19–23. URL: https://arxiv.org/abs/quant-ph/0604072. Citations in this document: §4.

[6] Ran Canetti, Juan A. Garay (editors), *Advances in cryptology—CRYPTO 2013—33rd annual cryptology conference, Santa Barbara, CA, USA, August 18–22, 2013, proceedings, part I*, Lecture Notes in Computer Science, 8042, Springer, 2013. See [24].

[7] Matthias Christandl, Renato Renner, Artur Ekert, *A generic security proof for quantum key distribution* (2004). URL: https://arxiv.org/abs/quant-ph/0402131. Citations in this document: §1.

[8] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, John Preskill, *Security of quantum key distribution with imperfect devices*, Quantum Information and Computation **4** (2004), 325–360. URL: https://arxiv.org/abs/quant-ph/0212066. Citations in this document: §1.

[9] Gerard 't Hooft, *Dimensional reduction in quantum gravity*, in [**2**] (1993). URL: https://arxiv.org/abs/gr-qc/9310026. Citations in this document: §3.

[10] Anqi Huang, Shihan Sajeed, Poompong Chaiwongkhot, Mathilde Soucarros, Matthieu Legre, Vadim Makarov, *Gaps between industrial and academic solutions to implementation loopholes in QKD: testing random-detector-efficiency countermeasure in a commercial system* (2016). URL: https://arxiv.org/abs/1601.00993. Citations in this document: §2, §4.

[11] Richard J. Hughes, Douglas M. Alde, P. Dyer, Gabriel G. Luther, George L. Morgan, Martin M. Schauer, *Quantum cryptography*, Contemporary Physics **36** (1995), 149–163. URL: https://arxiv.org/abs/quant-ph/9504002. Citations in this document: §1.

[12] ID Quantique, *Understanding quantum cryptography, version 2.0* (2012). URL: http://marketing.idquantique.com/acton/attachment/11868/f-0060/1/-/-/-/-/Understanding%20Quantum%20Cryptography.pdf. Citations in this document: §1.

[13] Andrew Zimmerman Jones, *Holographic principle* (2016). URL: http://physics.about.com/od/physicsetoh/g/holoprinciple.htm. Citations in this document: §3.

[14] Lluís Masanes, Renato Renner, Matthias Christandl, Andreas Winter, Jonathan Barrett, *Full security of quantum key distribution from no-signaling constraints*, IEEE Transactions on Information Theory **60** (2014), 4973–4986. URL: https://arxiv.org/abs/quant-ph/0606049. Citations in this document: §2.

[15] Sergey N. Molotkov, Sergey S. Nazin, *A simple proof of the unconditional security of relativistic quantum cryptography*, Journal of Experimental and Theoretical Physics **92** (2001), 871–878. URL: https://arxiv.org/abs/quant-ph/0008008. Citations in this document: §2.

[16] Arthur Neslen, *Paris climate activists put under house arrest using emergency laws* (2015). URL: http://www.theguardian.com/environment/2015/nov/27/paris-climate-activists-put-under-house-arrest-using-emergency-laws. Citations in this document: §5.

[17] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Valerio Scarani, *Device-independent quantum key distribution secure against collective attacks*, New Journal of Physics **11** (2009), 045021 (25pp). URL: http://www.unige.ch/gap/quantum/_media/publications:bib:qkddeviceindepfull.pdf. Citations in this document: §2.

[18] Rainer Plaga, *A fundamental threat to quantum cryptography: gravitational attacks*, The European Physical Journal D—Atomic, Molecular, Optical and Plasma Physics **38** (2006), 409–413. URL: http://link.springer.com/article/10.1140/epjd/e2006-00045-y. Citations in this document: §4.

[19] Terry Rudolph, *The laws of physics and cryptographic security* (2002). URL: https://arxiv.org/abs/quant-ph/0202143. Citations in this document: §4.

[20] Valerio Scarani, Christian Kurtsiefer, *The black paper of quantum cryptography: Real implementation problems*, Theoretical Computer Science **560** (2014), 27–32. URL: https://arxiv.org/abs/0906.4547. Citations in this document: §4.

[21] Christian Schaffner, *Quantum cryptography: from key distribution to position-based cryptography (talk slides)* (2015). URL: https://events.ccc.de/congress/2015/Fahrplan/events/7305.html. Citations in this document: §3.

[22] Peter W. Shor, John Preskill, *Simple proof of security of the BB84 quantum key distribution protocol*, Physical Review Letters **85** (2000), 441–444. URL: https://arxiv.org/abs/quant-ph/0003004. Citations in this document: §1.

[23] Leonard Susskind, *The world as a hologram*, Journal of Mathematical Physics **36** (1995), 6377–6396. URL: https://arxiv.org/abs/hep-th/9409089. Citations in this document: §3.

[24] Dominique Unruh, *Everlasting multi-party computation*, in Crypto 2013 [**6**] (2013), 380–397. URL: https://eprint.iacr.org/2012/177. Citations in this document: §3.