Theoretical Computer Science 560 (2014) 1–6

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Preface

This special issue of *Theoretical Computer Science* Section C (TCS-C), together with its companion issue of *Natural Computing* (NACO), marks the 30th anniversary of the BB84 paper [3], which is named after Charles H. Bennett and Gilles Brassard. This paper, which was originally published in the proceedings of a conference that took place in Bangalore, India, in December 1984, significantly advanced the use of quantum effects for cryptographic purposes and thereby launched a novel research field, quantum cryptography.

This issue features the BB84 paper itself, which is therefore published here in a journal *for the first time*. Another historical paper, known as BBB82, was written *two years previously* by Bennett and Brassard, along with Seth Breidbart [4]. This paper, which had been rejected at the time from an important computer science conference, is published for the first time in the companion NACO issue mentioned above.

It is a huge honor for us to edit this joint special issue. We consider the BB84 paper as one of the most important scientific contributions of the last century. It has been a most major step in the creation of a novel research field, quantum information science, which is at the interface between information theory and quantum physics. It had a tremendous impact on both fields individually, as well as on computer science.

In physics, information-theoretic considerations are becoming more and more important for understanding the deepest questions in the foundations of quantum theory. In information theory and in computer science, in contrast to what one may believe based on Shannon's mathematical theory of information, the insight is that the physics of the information carriers cannot be ignored. This fact, together with similar conclusions about Turing's computation theory [17], had led without doubt to a basic change of paradigm.

The birth of quantum cryptography has happened through four major events. First, Stephen Wiesner wrote "Conjugate coding" in 1968, in which the idea of using quantum-mechanical effects for accomplishing cryptographic tasks was suggested for the first time. In that paper, Wiesner not only invented quantum cryptography, but also invented the extremely important notion of oblivious transfer (or more precisely a variant of oblivious transfer known as one-out-of-two oblivious transfer) long before it was reinvented independently by Michael O. Rabin in 1981. Unfortunately, quantum cryptography then went into a long state of "lethargy" because Wiesner's journal submission was rejected and he did not pursue the matter.

Luckily, Wiesner had told his friend Charles H. Bennett about his ideas, which eventually led to several joint papers, including [5], discussed below, but also the much more famous invention of superdense coding [8].

The second major event in the birth of quantum cryptography occurred when Bennett and Gilles Brassard met in 1979 while swimming in San Juan, Puerto Rico (see details of that event in Brassard's historical perspective paper [10]). They then started to discuss various uses of quantum mechanical effects for cryptographic purposes. During the stage that then followed, several papers were written, some of which were published.

The most important among them, by far, became known as BB84, a paper in which two main ideas were developed [3]. The advent of BB84 is thus the third principal event in the birth of quantum cryptography. The two major ideas presented there were: first, using polarized photons for distributing a secret key — now called "quantum key distribution"; and second, using entanglement to attack quantum cryptographic protocols. Furthermore, the notion of quantum coin tossing was pioneered in the BB84 paper.

These contributions are described below in more detail. Mainly due to the first contribution, the invention of quantum key distribution (QKD), the paper received enormous attention, and is by now cited thousands of times; here, in this special issue and its companion in NACO, we celebrate 30 years of BB84. Nevertheless, it should be pointed out that the first official talk about these results took place at the *IEEE International Symposium on Information Theory* in St-Jovite, Québec, Canada, in 1983 [2]. However, the proceedings of that conference contained only one-page abstracts, which was sufficient to lay the basic claims but not give the actual protocols. Consequently, the BB84 QKD protocol was published for the first time in the 1984 Bangalore conference proceedings [3], so that the protocol deserves the "84" in its name.

http://dx.doi.org/10.1016/j.tcs.2014.10.020

The fourth (and last) event in the birth of quantum cryptography happened when physicists became aware of this field and its connection to the foundations of quantum physics. This occurred partially because a first experimental prototype was built in 1989 by Bennett, Brassard and three of their students [1], and much more so because Artur Ekert invented entanglement-based quantum key distribution in 1991. In contrast to BB84, Ekert's protocol [18] is based on the use of non-classical correlations, and eavesdropping is detected by monitoring the extent of violation of a Bell inequality. Even though Ekert's original protocol [18] could be recast in a BB84-like "prepare-and-measure" scenario [7], some subsequent QKD protocols based on entanglement have no such counterparts and are genuinely different from the concept initially envisioned by Bennett and Brassard. In particular, entanglement-based protocols can offer security even if certain components of the devices (e.g., the light sources or the detectors) are corrupted [19].

Quantum cryptography officially started during that second stage of birth, when the first paper in the field of quantum cryptography (where that term was actually coined) was published [5], and when *Sigact News* printed Wiesner's unpublished 1968 manuscript "Conjugate coding" [34]. Next, the idea to use polarized photons for transmitting confidential information surfaced in the aforementioned and until now unpublished paper [4]. This paper got essentially forgotten because two of the authors developed their next idea, namely quantum key distribution [3], which introduced major improvements, both practical and qualitative.

Quantum key distribution was invented when Bennett and Brassard realized that the optimal way to use the photons and the quantum channel is to transmit an arbitrary long *random* secret key, for possible subsequent use as a one-time pad, rather than the secret message itself, as they had proposed in BBB82. Their 1984 paper, "Quantum cryptography: Public key distribution and coin tossing", appeared solely in a (rather obscure) conference proceedings, hence it is appropriate to republish it in this special issue. Note that Brassard has informed us that there is a widespread misconception that the Bangalore conference in which BB84 was presented was an IEEE conference and that the correct citation should include "IEEE Conference". However, the IEEE was merely one of the sponsors and took no part in printing the proceedings, which appeared without any copyright notice.

This paper presents two protocols, both of which show that quantum information carriers can be used to enable cryptographic tasks under substantially weaker assumptions than what is necessary for the corresponding classical schemes.

The first contribution is a proposal for a protocol to securely establish a secret key between two remote parties, connected only by an insecure quantum communication channel as well as what is called a "public channel" in the BB84 paper, and described as a classical channel "susceptible to eavesdropping but not to the injection or alteration of messages" [3].

This result is groundbreaking. The BB84 quantum key distribution protocol is the first proposal for a scheme that provides information-theoretic secrecy *with no need for prior secret keys*, based only on the assumption that a public channel is available (and, of course, that quantum mechanics is correct). This is both of theoretical interest (indeed, it shows that Shannon's pessimistic result that the length of a cryptographic key has to be at least as long as the entropy of the message in order to achieve information-theoretic security is only valid if one is restricted to purely classical communication schemes) as well as of practical importance — in the meantime, various commercial products based on this protocol have become available.

While it was argued that the protocol for quantum key distribution proposed in BB84 is secure, no full proof of this claim was given at the time. Furthermore, practical aspects such as noise or losses in the communication lines were not considered. In fact, this turned out to be a highly challenging task that could only be resolved more than a decade later. However, now we know that the security claims made in BB84 are correct.

Coin tossing. Another topic discussed in the BB84 paper also contains a fascinating result. The paper presents a protocol for coin tossing between two mistrusting parties, connected by a quantum communication channel. As Bennett and Brassard then argued, the protocol is secure under the assumption that an adversary only stores classical information. But the more remarkable aspect of this work is that the protocol can be broken by an adversary who can store and manipulate quantum information carriers. For this, Bennett and Brassard showed a connection to the Einstein–Podolsky–Rosen effect, and therefore to foundational questions related to the completeness of quantum theory. This connection between foundations and applications is striking and obviously had an enormous impact on the field. In addition, Bennett and Brassard's insights were crucial for the further design of two-party protocols beyond coin tossing. Incidentally, the BB84 coin tossing protocol could just as well have been seen as a form of quantum bit commitment (also insecure against entanglement-based attacks, which can be seen as a forerunner of the general no-go theorem [25,23]).

Pre-QKD quantum cryptography for the purpose of transmitting confidential messages started in the earlier-described BBB82 paper, which was rejected from a conference and never published until now. It is titled "Quantum cryptography II: How to re-use a one-time pad safely even if $P = NP$", by Bennett and Brassard, together with Seth Breidbart.

The paper proposes a novel approach to information-theoretic cryptography, exploiting the fundamentally non-classical aspects of quantum information carriers. More specifically, it considers the problem of private communication between two distant parties over an insecure channel. In contrast to conventional communication settings, the two parties are assumed to have means to exchange quantum systems (e.g., photons). A sender is allowed to prepare them in any state (e.g., by choosing their polarization) and the receiver can apply any measurement. It is then argued that, in this setting, it is possible to safely reuse the key in an appropriately adapted one-time-pad encryption scheme. Crucially, the security of this scheme is based solely on physical principles. In particular, no assumptions about the hardness of certain mathematical problems are necessary.

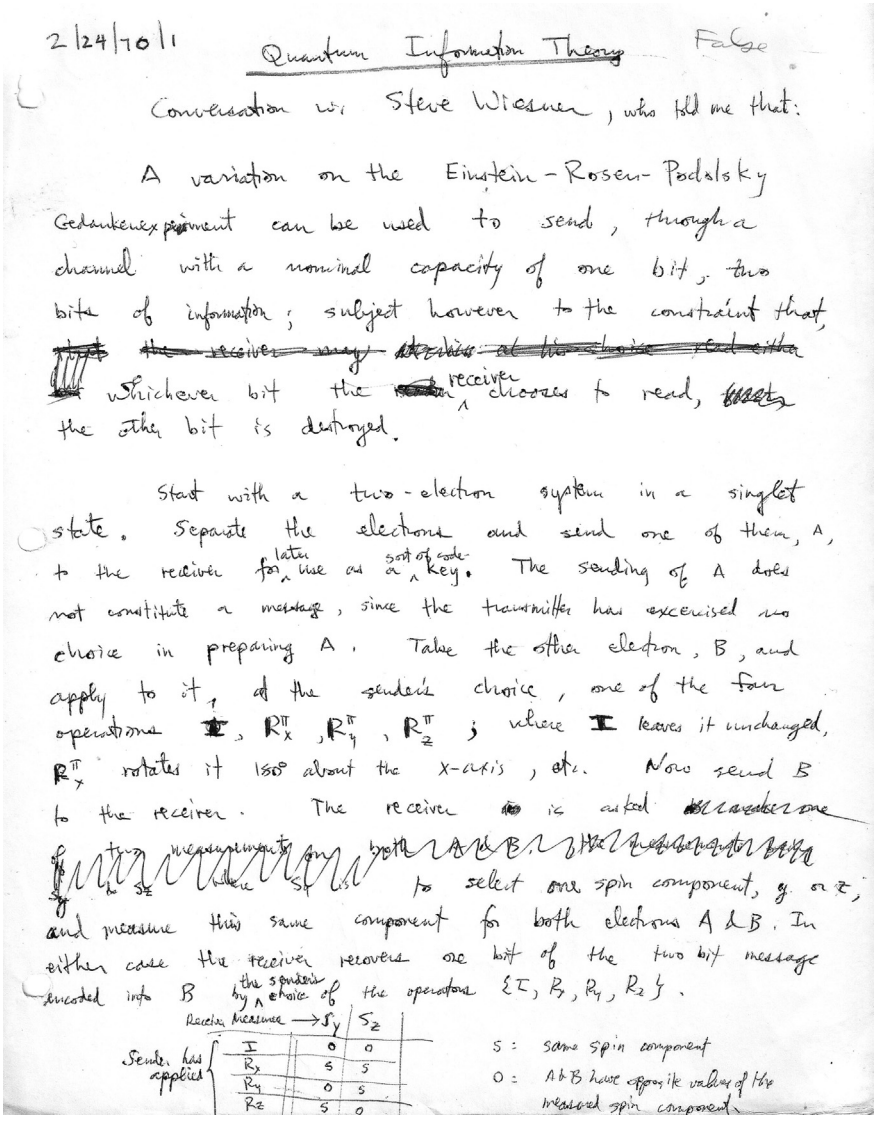

Fig. 1. Notes taken by Bennett while talking to Wiesner on 24 February 1970. The penciled "false" at the top, which Bennett added later, needs some explanation. The note describes what Wiesner at first thought was a simpler implementation of the "multiplexing channel" he had described in his 1968 manuscript [34]. Alice gives Bob one of two maximally entangled qubits, applies a chosen one of the four Pauli operations to the other, then gives it to him also. If Bob is restricted to single-particle measurements, he can recover either one, but not both, of the two bits encoded by Alice. Soon after Bennett took those notes, Wiesner realized that a joint measurement would reveal both bits, which spoils the scheme as a multiplexing channel, but constitutes another uniquely quantum primitive in its own right: the ability to transmit two classical bits by manipulating only one of an entangled pair of qubits. Wiesner explained this technique, now called superdense coding, to many people, and eventually published it with Bennett along with a suggested optical implementation [8]. A high resolution scan in full color is available as supplementary online material. © Charles H. Bennett, reproduced with his permission.

The main contribution of that paper was to introduce a novel paradigm into cryptography, namely the use of quantum physical information carriers to achieve privacy. The work is based on ideas of Wiesner, who proposed to use quantum coding for making unforgeable banknotes [34], yet it proposes, for the first time, the use of quantum communication to send secret messages. For the first time? Maybe not… Actually, Bennett has shared with us the following recollection: "Wiesner was aware as early as the 1970s that his quantum banknote principle could also be applied to eavesdrop-resistant communication, but preferred not to pursue research in this direction for fear of triggering governmental interference". Be that as it may, Wiesner subsequently joined forces with Bennett, Brassard and Breidbart to write Ref. [6], which appeared in the obscure and now-discontinued *IBM Technical Disclosure Bulletin*. This was essentially a translation of BBB82 from academic language into the language of an invention disclosure.

For historical interest, we include as Fig. 1 a facsimile of handwritten notes that Bennett took while talking to Wiesner on 24 February 1970, showing the extent to which Wiesner was ahead of his times. It may even be the first time ever that the words "Quantum Information Theory" were written down.

Written before BB84, it is clear that BBB82 had not only a fundamental impact on cryptography, but also on information theory in general. It shows that information that is represented quantum-mechanically has properties that are fundamentally different from their classical counterparts. Indeed, as shown by Shannon in 1949, such a scheme could not be unconditionally secure with purely classical information carriers. But since BBB82 was not published at the time, this fundamental advantage of quantum carriers over classical ones was communicated subsequently to the scientific community via the BB84 paper, and thus also is commonly attributed to that paper.

Although the main claims in the BBB82 paper are correct, it did not provide a full security proof of the proposed scheme. For this, it would be necessary to consider arbitrary attack strategies of a possible quantum adversary. This would however be clearly beyond the scope of this paper written in 1982, whose goal was to propose a completely novel idea and argue (convincingly) that it works. This paper shows that quantum-mechanical information carriers can be used to realize applications that are (provably) impossible using classical technology. This insight is of tremendous importance in cryptography, information theory, and beyond.

QKD has triggered an enormous research activity over the past decades, culminating in full proofs of security that are applicable to theoretical protocols, and partial proofs of security for practical protocols [24,12,32,26,33,27–29,9,22]. For several reviews, please see [20,31,19]. In parallel, there have been many exciting developments in quantum cryptography beyond QKD, including for example quantum secret sharing, quantum bit commitment, and coin tossing [11,23,25,30,14,21,15,16,13].

For the two companion issues, we invited six leading researchers in the field of quantum cryptography, Charles H. Bennett, Gilles Brassard, Ivan Damgård, Louis Salvail, Valerio Scarani and Alexander (Sasha) Sergienko, to present the papers of their choice (one per author).

Six additional submitted papers were carefully refereed and chosen, and are described here as well. Our choice of which papers should go in each of the two journals was mainly (but not only) based on how well they fit in this *Theoretical Computer Science* journal, versus *Natural Computing*, which is a journal with a broader scope. This (TCS-C) special issue consists of eight papers.

The first paper, “Quantum cryptography: Public key distribution and coin tossing”, by Charles H. Bennett and Gilles Brassard, is the extremely famous historical paper, BB84, described above in detail. The paper was chosen by Bennett and Brassard as one of their two invited papers. It was decided to publish it as a historical paper, thus the original conference paper is published exactly as it was in 1984, except for fresh typesetting and the correction of some typographical mistakes. Furthermore, a scan of the original paper also appears online, accessible from the TCS website.

The second paper, “Secure identification and QKD in the bounded-quantum-storage model”, by Ivan Damgård, Serge Fehr, Louis Salvail and Christian Schaffner, was chosen by Damgård as his invited paper. The paper proposes two identification protocols that are secure under the assumption that an adversary can only store a limited number of quantum bits; one protocol that is using only a weak (human memorizable) password, and an improved protocol that uses a strong password and provides additional security against ‘man in the middle’ attacks.

The third paper, “The black paper of quantum cryptography: Real implementation problems”, by Valerio Scarani and Christian Kurtsiefer, was chosen by Scarani as his invited paper. The main conclusion of this paper is that, similarly to non-quantum modern cryptography, those who pursue practical quantum devices may have to moderate their security claims, and those who pursue ultimate security may have to suspend their claims of usefulness.

The fourth paper, “Public-key cryptography based on bounded quantum reference frames”, by Lawrence M. Ioannou and Michele Mosca, suggests a quantum *public key* cryptography scheme to be used for identification. In their scheme, the sender uses the knowledge of a reference frame as the secret key, and multiple qubits encoding this frame are used as the public key.

The fifth paper, “Quantum key distribution using a two-way quantum channel”, by Marco Lucamarini and Stefano Mancini, presents an improved (in the sense of being more feasible) variant of their own protocol from 2005, along with a partial security analysis.

The sixth paper, “Using quantum key distribution for cryptographic purposes: A survey”, by a very long list of authors,[1] is a good survey paper, by an extraordinarily strong set of researchers. It describes research results achieved within the European SECOQC project, whose aim was to investigate the integration of QKD in existing communication networks. The paper also gives an overview of the challenges related to the further development of cryptographic infrastructure based on quantum technologies.

The seventh paper, “Non-contextual chocolate balls versus value indefinite quantum cryptography”, by Karl Svozil, is a fascinating attempt to present quantum cryptographic protocols that might be stronger than existing ones, as these novel protocols are protected by Bell– and Kochen–Specker type arguments.

The last paper, “Optimal axis compensation in quantum key distribution protocols over unital channels”, by Shun Watanabe, Ryutaroh Matsumoto and Tomohiko Uyematsu, presents a very clear analysis of the various key distribution rates when one or both parties apply unitary operators on their systems in order to compensate for channel errors in six-state and BB84 protocols.

[1] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter and A. Zeilinger.

The companion issue of NACO consists of four papers. The first paper, "Quantum cryptography II: How to re-use a one-time pad safely even if P = NP", by Charles H. Bennett, Gilles Brassard and Seth Breidbart, is the historical paper, BBB82, discussed above. The paper was chosen by Bennett and Brassard as one of their two invited papers. It was decided to publish it as a historical paper, thus the original version (submitted in 1982) is published there with almost no editing, except for the correction of some typographical mistakes and the addition of a few footnotes written in retrospect by the authors.

The second paper, "Entanglement sudden death: A threat to advanced quantum key distribution?", by Gregg Jaeger and Alexander (Sasha) Sergienko, chosen by Sergienko as his invited paper, considers the effect of local noise on a class of entangled states used in entanglement-based quantum key distribution, in order to assess the threat that entanglement sudden death (a sudden and complete loss of entanglement in finite time due to asymptotic dephasing or relaxation) might pose to it.

The third paper, "How to re-use a one-time pad safely and almost optimally even if P = NP", by Ivan Damgård, Thomas Brochmann Pedersen and Louis Salvail, chosen by Salvail as his invited paper, discusses the idea of key recycling using quantum encryption, much as in the aforementioned BBB82 paper. This contribution now provides a *working scheme* of this type, which is very similar to the original proposal, together with a careful security proof. It is thus a very satisfying completion of the work started decades earlier by Bennett, Brassard and Breidbart. Interestingly, Damgård, Pedersen and Salvail were not aware of the prior unpublished art when they published the original conference version of their work (under a different title) in the Proceedings of the Eurocrypt 2004 conference, and they reinvented the idea of reusing a one-time pad independently. Of course, in the journal version of their work, published in the companion NACO special issue, they give due credit to Bennett, Brassard and Breidbart.

The last paper, "Cryptographic encryption scheme based on metastable excited nuclei", by Thomas Durt and Alex Hermanne, presents a novel and highly speculative approach. It proposes to replace the conventional quantum uncertainties (commonly used in QKD) by another type of uncertainty, which characterizes the knowledge of the time at which an unstable nucleus decays.

We are most grateful to the authors for all their submissions and to the reviewers for their thorough and thoughtful reviews. We are especially grateful to Gilles Brassard who, in addition to contributing and refereeing papers, also acted as co-editor for one of the papers. We also thank both Bennett and Brassard for sharing with us fascinating historical facts and for granting us permission to use Fig. 1. Finally, we would very much like to thank Grzegorz Rozenberg, founding editor-in-chief of TCS-C and NACO, for his unstinting support and enlightening advice.

Appendix A. Supplementary material

Supplementary material related to this article can be found online at http://dx.doi.org/10.1016/j.tcs.2014.10.020.

References

[1] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, John Smolin, Experimental quantum cryptography, J. Cryptology 5 (1) (1992) 3–28.
[2] Charles H. Bennett, Gilles Brassard, Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing, in: Proceedings of IEEE International Symposium on Information Theory, St-Jovite, 1983, p. 91.
[3] Charles H. Bennett, Gilles Brassard, Quantum cryptography: public-key distribution and coin tossing, in: Proceedings of International Conference on Computers, Systems and Signal Processing, Bangalore, 1984, pp. 175–179.
[4] Charles H. Bennett, Gilles Brassard, Seth Breidbart, Quantum cryptography II: How to re-use a one-time pad safely even if P = NP, Unpublished manuscript, 1982.
[5] Charles H. Bennett, Gilles Brassard, Seth Breidbart, Stephen Wiesner, Quantum cryptography, or unforgeable subway tokens, in: David Chaum, Ronald L. Rivest, Alan T. Sherman (Eds.), Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 267–275.
[6] Charles H. Bennett, Gilles Brassard, Seth Breidbart, Stephen Wiesner, Eavesdrop-detecting quantum communications channel, IBM Tech. Dis. Bull. 26 (8) (1984) 4363–4366.
[7] Charles H. Bennett, Gilles Brassard, N. David Mermin, Quantum cryptography without Bell's theorem, Phys. Rev. Lett. 68 (1992) 557–559.
[8] Charles H. Bennett, Stephen Wiesner, Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states, Phys. Rev. Lett. 69 (1992) 2281–2284.
[9] Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, Vwani Roychowdhury, A proof of the security of quantum key distribution, J. Cryptology 19 (4) (2006) 381–439.
[10] Gilles Brassard, Brief history of quantum cryptography: A personal perspective, in: Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005, pp. 19–23.
[11] Gilles Brassard, Claude Crépeau, Quantum bit commitment and coin tossing protocols, in: Alfred J. Menezes, Scott A. Vanstone (Eds.), Advances in Cryptology — Proceedings of CRYPTO '90, in: Lecture Notes in Computer Science, vol. 537, Springer, Berlin, Heidelberg, 1991, pp. 49–61.
[12] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, Barry C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. 85 (2000) 1330–1333.
[13] André Chailloux, Iordanis Kerenidis, Optimal quantum strong coin flipping, in: Proceedings of 50th Annual IEEE Symposium on Foundations of Computer Science, 2009, pp. 527–533.
[14] Richard Cleve, Daniel Gottesman, Hoi-Kwong Lo, How to share a quantum secret, Phys. Rev. Lett. 83 (1999) 648–651.
[15] Ivan B. Damgård, Serge Fehr, Louis Salvail, Christian Schaffner, Secure identification and QKD in the bounded-quantum-storage model, in: Alfred Menezes (Ed.), Advances in Cryptology — Proceedings of CRYPTO 2007, in: Lecture Notes in Computer Science, vol. 4622, Springer, Berlin, Heidelberg, 2007, pp. 342–359.
[16] Ivan B. Damgård, Serge Fehr, Louis Salvail, Christian Schaffner, Cryptography in the bounded-quantum-storage model, SIAM J. Comput. 37 (6) (2008) 1865–1890.
[17] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, Proc. R. Soc. A 400 (1985) 97–117.

[18] Artur K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67 (1991) 661–663.
[19] Artur Ekert, Renato Renner, The ultimate physical limits of privacy, Nature 507 (2014) 443–447.
[20] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, Quantum cryptography, Rev. Modern Phys. 74 (2002) 145–195.
[21] Mark Hillery, Vladimír Bužek, André Berthiaume, Quantum secret sharing, Phys. Rev. A 59 (1999) 1829–1834.
[22] Hitoshi Inamori, Norbert Lütkenhaus, Dominic Mayers, Unconditional security of practical quantum key distribution, Eur. Phys. J. D 41 (3) (2007) 599–627.
[23] Hoi-Kwong Lo, H.F. Chau, Is quantum bit commitment really possible?, Phys. Rev. Lett. 78 (1997) 3410–3413.
[24] Hoi-Kwong Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science 283 (1999) 2050–2056.
[25] Dominic Mayers, Unconditionally secure quantum bit commitment is impossible, Phys. Rev. Lett. 78 (1997) 3414–3417.
[26] Dominic Mayers, Unconditional security in quantum cryptography, J. ACM 48 (3) (2001) 351–406.
[27] Renato Renner, Security of quantum key distribution, PhD thesis, Swiss Federal Institute of Technology (ETH), Zurich, 2005, available at arXiv:quant-ph/0512258.
[28] Renato Renner, Nicolas Gisin, Barbara Kraus, Information-theoretic security proof for quantum key distribution protocols, Phys. Rev. A 72 (2005) 012332.
[29] Renato Renner, Robert König, Universally composable privacy amplification against quantum adversaries, in: Proceedings of Second Theory of Cryptography Conference, in: Lecture Notes in Computer Science, vol. 3378, Springer, 2005, pp. 407–425.
[30] Louis Salvail, Quantum bit commitment from a physical assumption, in: Hugo Krawczyk (Ed.), Advances in Cryptology — Proceedings of CRYPTO '98, in: Lecture Notes in Computer Science, vol. 1462, Springer, Berlin, Heidelberg, 1998, pp. 338–353.
[31] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, Momtchil Peev, The security of practical quantum key distribution, Rev. Modern Phys. 81 (2009) 1301–1350.
[32] Peter W. Shor, John Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2000) 441–444.
[33] Kiyoshi Tamaki, Masato Koashi, Nobuyuki Imoto, Unconditionally secure key distribution based on two nonorthogonal states, Phys. Rev. Lett. 90 (2003) 167904.
[34] Stephen Wiesner, Conjugate coding, Manuscript written while participating in the Columbia University student protests of April 1968 and eventually, published in ACM SIGACT News 15 (1) (1983) 78–88.

Tal Mor
Computer Science Department, Technion, Haifa 32000, Israel
E-mail address: talmo@cs.technion.ac.il

Renato Renner
Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
E-mail address: renner@phys.ethz.ch

Available online 18 October 2014