A Brief Review on Quantum Bit Commitment

Álvaro J. Almeida[a,b] Ricardo Loura[c,d]

Nikola Paunković[c,d] Nuno A. Silva[b,e] Nelson J. Muga[b,e]

Paulo Mateus[c,d] Paulo S. André[b,f] Armando N. Pinto[b,e]

[a]Dept of Physics, UAveiro, Portugal
[b]Instituto de Telecomunicações, Aveiro, Portugal
[c]SQIG Instituto de Telecomunicações, IST-TU Lisbon, Portugal
[d]Dept of Mathematics, IST-ULisbon, Portugal
[e]Dept of Electronics, Telecommunications and Informatics, UAveiro, Portugal
[f]Dept of Electrical and Computer Engineering, IST-ULisbon, Portugal

Abstract

In classical cryptography, the bit commitment scheme is one of the most important primitives. We review the state of the art of bit commitment protocols, emphasizing its main achievements and applications. Next, we present a practical quantum bit commitment scheme, whose security relies on current technological limitations, such as the lack of long-term stable quantum memories. We demonstrate the feasibility of our practical quantum bit commitment protocol and that it can be securely implemented with nowadays technology.

Keywords: Quantum Bit Commitment, Quantum Cryptography.

1 Introduction

Bit commitment is a fundamental primitive in cryptography which allows two untrustful parties to do a secure commitment. It consists in two phases: *commitment* and *revealing*. In the commitment phase, the one that commits, Alice, has to choose between a bit value, 0 or 1. After commitment, Alice gives her choice to Bob during the revealing phase. In order to be secure, the protocol must be both binding and concealing. To be binding means that Alice cannot change her choice later in time, in particular during the revealing phase. To be concealing means that Bob cannot learn Alice's commitment before she reveals it to him.

In classical cryptography, the security of bit commitment lies in assumptions of computational complexity such as the difficulty of factoring large numbers [10]. However, with the increase of the computational power and the rise of quantum computers, its security can be broken [39]. In fact, it can be proven that unconditionally secure bit commitment based only on classical resources is impossible [28]. It was also demonstrated that even if Alice and Bob have access to quantum resources, unconditionality secure quantum bit commitment (QBC) is impossible within nonrelativistic physics [33, 29]. As in classical cryptography, QBC schemes must rely on physical assumptions, e.g. the quantum memory that an attacker can use is noisy [40]. The situation changed when it was found that using Minkowsky causality in a relativistic scenario it is possible to build unconditionally secure QBC protocols [19]. This sort of protocols are starting to be implemented nowadays [31, 28].

We review the state of the art of bit commitment schemes, from classical to quantum, and present the main achievements and drawbacks. A practical QBC scheme is also presented and experimentally verified in a back to back case scenario. Finally we present the main conclusions of this work.

2 From Classical Bit Commitment to Unconditionally Secure Relativistic Quantum Bit Commitment

2.1 Review of the State of the Art

The importance of encryption and secrecy in communication is well studied in the mathematical theory of communication from Shannon [38]. In this influential article, Shannon presented what he considered the essential five parts of a communication system: the information source, that produces a message; the transmitter which operates on the message to create a signal that can be transmitted through a channel; the channel which is the medium of transmission of the signal; the receiver which performs the inverse operation done by the transmitter in order to reconstruct the message and the destination, person or machine, to whom or which the message is intended. Due to the need for security in new applications such as electronic bank transactions or the improvement of computer technology, new encryption schemes were created, like the *data encryption standard* (DES) [14] or the *advanced encryption standard* (AES) [1]. Several years before the proposed schemes, Stephen Wiesner had the idea to make quantum banknotes, that was not accepted immediately, giving rise to a complete new level of security in what would be called quantum cryptography [42].

In 1981, Blum presented the notion of bit commitment in his work about coin flipping over telephone [4]. The concept of commitment would be formalized by Brassard et al. only in 1988 [8]. In fact, the first quantum cryptographic protocol, which was proposed in 1984 by Bennett and Brassard, widely known as BB84 [3], was already a preliminary version of a bit commitment protocol, since the idea was to associate the commitments of 0 and 1 with two complementary observables. In a later paper, a QBC protocol, known as BCJL, was claimed by the authors to be unconditionally secure [6]. In that work, the authors presented an argument in which, according to the laws of quantum physics, the participants in the protocol are only allowed to cheat with an arbitrarily small probability. Despite the initial optimism to achieve an unconditionally secure QBC protocol, Mayers [33] and independently Lo and Chau [29], proved a no-go theorem showing that unconditionally secure QBC is impossible unless relativistic effects are used. This impossibility comes from the fact that a cheating strategy using EPR pairs can always be implemented. Thus, different approaches have been presented in order to avoid the no-go theorem [11]. These proposals are based on relaxing some of the assumptions, such as using noisy/bounded quantum memories [40]. Unfortunately none of these attempts achieved more than what classical cryptography itself can provide.

A new classical bit commitment protocol taking advantage of cryptographic constraints imposed by special relativity was proposed by Kent [21]. The author shows that the protocol is unconditionally secure against both classical or quantum attacks. Subsequently, Kent proposed an unconditionally secure QBC protocol that uses quantum and relativistic effects and that requires 4 additional trusted agents [22]. This protocol was recently implemented by two different groups. In one implementation the thrusted agents were separated by more than 9000 km, corresponding to a commitment time of 15.6 ms [31], and in the second implementation the agents were separated by about 20 km, achieving a commitment time of about 60 μs and a cheating probability less than 5.68×10^{-2} [28].

Although not unconditionally secure, an experimental demonstration of a practical QBC protocol whose security is based on current technological limitations was presented by Danan and Vaidman [13]. The technological limitations in question are the lack of non-demolition measurements and long-term stable quantum memories. The protocol is based on BB84 scheme and has the advantages of being relatively simple to implement and of immediate realization using current technology. Quantum non-demolition (QND) measurements are under study basically since the foundation of quantum theory [5]. If Alice was able to perform a non-demolition measurement, she would be able to detect the presence of a photon without destroying it or affecting its polarization state. However, practical QND measurements are still in its preliminary stage. An experimental demonstration of 90% QND measurements in a controlled environment (photons confined in a cavity) was presented, although this type of measurements is more suitable for computational purposes, rather than cryptographic [17]. Even if Alice had access to QND measurements, she would need a stable long-term quantum memory in order to perform the measurements later in time. Advances in quantum-memories technology are also significant and we step from a 2 seconds proposal [32] to a 39 minutes one [36] only in two years. Although notable, current technology allows only noisy memories, usually implemented in optical fibers, increasing the probability to have errors in the system, since the qubit losses increase exponentially with the length of the fiber.

Recently, a two-state version of the protocol presented by Danan and Vaidman [13] was proposed [30]. This paper addresses several issues related to a practical implementation, e.g. modeling of errors due to noise and equipment imperfections, a quantitative analysis of the effects of noise in the system, the optimal cheating strategy or the protocol's security. An experimental implementation based on this work [30] was recently demonstrated [2]. The security of the implementation of this protocol [2] is based on the lack of long-term stable quantum memories.

2.2 Applications

Bit commitment is a building block for several cryptographic primitives, including coin tossing [4, 12, 34], zero-knowledge proofs [7, 23], oblivious transfer [26, 15] and secure two-party computation [27]. In terms of real-world applications it will be useful in a near future. High-speed trading stock market is one example, secure voting or long-distance gambling are other applications [9, 31].

Since the discovery of Mayers in 1997, efforts on bit commitment were put in combining quantum theory with relativity and in theoretical analysis and experimental realizations of practical protocols with noisy/bounded memories [41, 37, 40, 24, 35, 15]. It was shown that if the memory is not ideal but has a finite noise, there are protocols whose security will not be compromised as long as the time difference between the commitment and the opening phase is bigger than some threshold value, determined by the noisy characteristics of the memory used [30]. Regarding protocols based on relativistic effects, Kent has been working in this topic for several years, proposing several protocols for unconditionally secure bit commitment [21, 16, 19, 22, 20].

Nowadays, with the recent experimental demonstrations of unconditionally secure bit commitment [31, 28], a broad range of opportunities is now open for a lot of applications.

3 Experimental Quantum Bit Commitment using Technological Limitations

In Loura et. al [30], the authors have proposed a nonrelativistic two-state QBC protocol whose security relies on current technological limitations. In fact there are some disadvantages of using relativistic bit commitment protocols that makes it worthwhile to continue to study nonrelativistic protocols. First, contrary to relativistic bit commitment, the protocol in Loura et. al [30] uses less equipment and is less costly, making it easier to implement. Second, in relativistic protocols both parties need to be in separated and secure locations and the communication between them needs to be continuous during the entire commitment phase [18]. In particular in the protocol proposed by Kent, 4 thrusted and secure agents are needed, which increases the complexity and cost of the system [22].

Next we present an implementation of the protocol presented in Loura et. al [30]. The protocol has three phases, initialization, commitment and revealing, which run as follows:

1. **Initialization:** Bob generates a random sequence of classical bits, encodes them in one of two states of polarization, $|0\rangle$ or $|1\rangle$ and sends them to Alice. The two states of polarization are not orthogonal, i.e. $\langle 0|1\rangle = \cos(\pi/4)$.

2. **Commitment:** Alice performs the measurements right after receiving a photon from Bob, choosing one of two orthogonal observables, that we called $\hat{C}_0$ and $\hat{C}_1$, on all photons.

3. **Revealing:** Alice reveals her commitment by informing Bob about the observable she measured and the results obtained.

One can define conditional probabilities for the optical contributions ($p_c(r|b)$, with $c, r, b \in \{0, 1\}$) that a result r is obtained when measuring the observable $\hat{C}_c$ on state $|b\rangle$ [30].

- If Alice measures $\hat{C}_0$:

$$\begin{aligned} p_0(0|0) &= 1 - \frac{p}{2} \\ p_0(1|0) &= \frac{p}{2} \\ p_0(0|1) &= 1/2 \\ p_0(1|1) &= 1/2\,. \end{aligned} \tag{1}$$

- If Alice measures $\hat{C}_1$:

$$\begin{aligned} p_1(0|0) &= 1/2 \\ p_1(1|0) &= 1/2 \\ p_1(0|1) &= \frac{p}{2} \\ p_1(1|1) &= 1 - \frac{p}{2}\,. \end{aligned} \tag{2}$$

The parameter p in (1) and (2) traduces the amount of optical noise in a depolarizing channel model of white noise.

In Fig. 1 we present the experimental setup used to implement the two-state QBC described above. On Bob's side, a laser at 1550 nm band was attenuated to generate an average number of photons per pulse much lower than 1. Next,

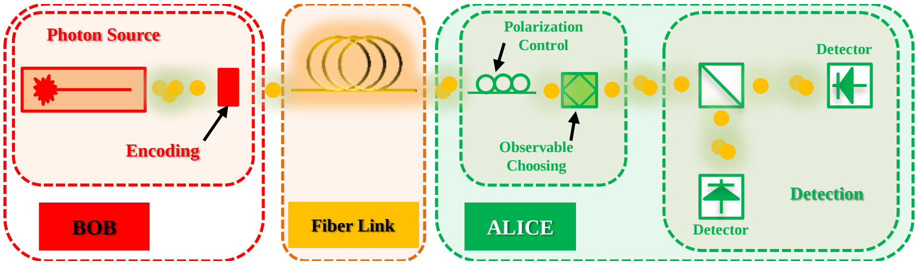

Figure 1: Experimental scheme to implement the two-state QBC protocol.

photons were encoded into polarization and sent through a 1 km long fiber. At the receiver's side, Alice used a polarization controller to compensate for random rotations of polarization inside the optical fiber and performed her commitment. The commitment to an observable was done using a wave plate. Photons were detected using two avalanche photodiodes. The experimental results of the measurement probability obtained in five different runs when measuring $\hat{C}_0$ and $\hat{C}_1$ are shown in Fig. 2. The average measurement probabilities obtained from each observable are presented in Table 1. Note that measurements in equal bases means that the measurement observable coincides with the basis from which the state was prepared and measurements in different bases means that the two are different.

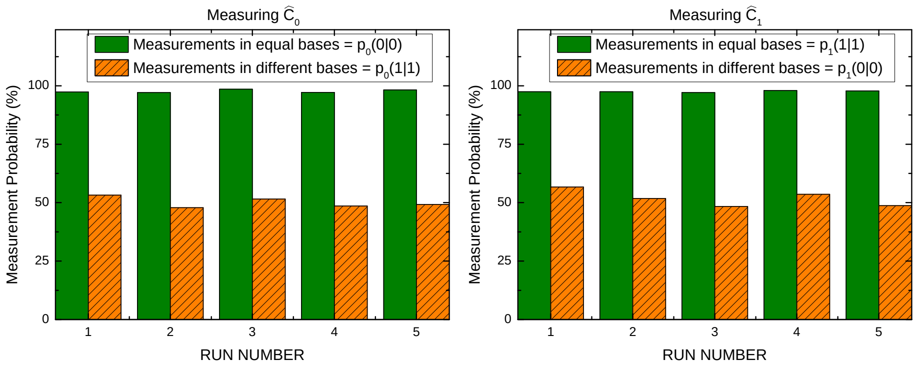

Figure 2: Experimental results for the measurement probability in $\hat{C}_0$ and $\hat{C}_1$, obtained for five different runs.

Table 1: Average measurement probabilities from $\hat{C}_0$ and $\hat{C}_1$.

	Equal bases (%)	Different bases (%)
$\hat{C}_0$	97.69	50.10
$\hat{C}_1$	97.55	51.83

The results obtained are according to theory in (1) and (2), since in the ideal case (where there is no optical noise, $p = 0$), when the measurements are performed in equal bases the success rates (given by $p_0(1|1)$ and $p_1(0|0)$) should be 100%, while for measurements in different bases (given by $p_0(0|0)$ and $p_1(1|1)$) the rates should be 50%. Since the alignment between Bob and Alice is not perfect, we will get wrong detections and consequently a rate lower than 100%, or different from 50%, depending if we are talking about measurements in equal bases or different bases, respectively.

The wrong counts when we are measuring in equal bases will contribute to the quantum-bit error rate (QBER) of the system, which is one of the most important parameters to quantify the quality of the transmission. The overall QBER, including optical and non-optical contributions can be written as [25],

$$\mathrm{QBER} = \frac{\mu t_{\mathrm{link}} \eta P_{\mathrm{opt}} + P_{\mathrm{dark}}}{\mu t_{\mathrm{link}} \eta + 2P_{\mathrm{dark}}} \, . \tag{3}$$

The optical contribution to errors due to rotation of polarization is given by,

$$P_{\mathrm{opt}} = p_0(1|0) = p_1(0|1) = \frac{1-V}{2}, \tag{4}$$

where V is the visibility of the state of polarization. For the non-optical part, the channel contribution from photon absorption is,

$$t_{\mathrm{link}} = 10^{\frac{-\alpha L}{10}}, \tag{5}$$

where α is the fiber attenuation coefficient [in dB/km] and L is the fiber length [in km]. The parameter μ is the average number of photons per pulse and P_{dark} and η are the detectors' dark counts and quantum efficiency, respectively. The success rate (SRATE) in the measurement, i.e., when the measurement basis is equal to the coding basis, can be defined as,

$$\mathrm{SRATE} = 1 - \mathrm{QBER}. \tag{6}$$

In Fig. 3 we show the success rate as a function of the fiber length obtained from (6). From this figure it can be seen that, according to the parameters used and which are presented in Table 2, bit commitment can be securely performed even if the parties are separated through a quantum channel of about 175 km. This is due to the fact that the success rates for the optimal cheating strategy is $\cos^2(\pi/8) = 0.8536$ [30]. Thus, if the errors induced by an honest part (Alice) are identical to the error of a cheating one, the two strategies are indistinguishable and the protocol cannot be performed.

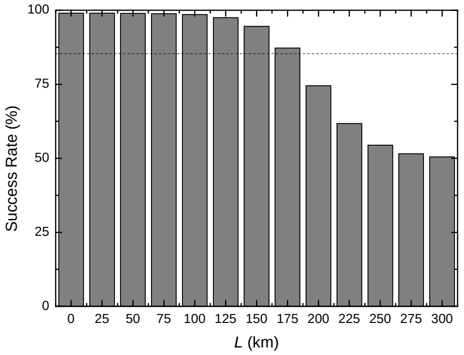

Figure 3: Success rate as a function of the fiber length. The dashed line sets the threshold to secure bit commitment.

Table 2: Parameters used in (6) to plot Fig. 3.

Parameter	Value
μ	0.2
α	0.2 dB/km
η	0.1
P_{dark}	1×10^{-6}
V	0.98

4 Conclusions

We reviewed the state of the art of bit commitment protocol. It was verified that bit commitment is a very important primitive in cryptography and has seen a rapid progress. Nowadays, there are proposals for unconditionally secure bit commitment which are based in special relativity combined with quantum mechanics. Some of these proposals were already implemented experimentally. Regarding the one presented in this work, which is of relatively simplicity of implementation if compared with relativistic options, it was demonstrated that it can be achieved secure QBC. The measurement probabilities when measuring each one of the observables were far above the minimum theoretical security limit of 85.36%. Also, it was shown that it is worthwhile to continue to study non-relativistic QBC protocols while relativistic ones still present some disadvantages. Bit commitment has a lot of applications and can be a serious candidate to a real-world implementation in a near future.

Acknowledgments

This work was supported in part by the FCT - Fundação para a Ciência e a Tecnologia, through the PhD Grants SFRH/BD/79482/2011 and SFRH/BD/79571/2011; the Post Doctoral Grants SFRH/BPD/77286/2011 and SFRH/BPD/96457/2013; by the Conselho de Reitores das Universidades Portuguesas (CRUP) project ‘Ação Integrada E 91/12’ and by the FCT and the Instituto de Telecomunicações under the PEst-OE/EEI/LA0008/2013 program, project “CV-Quantum”.

References

[1] Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. U.S. Department of Commerce, National Institute of Standards and Technology, 2001.

[2] Álvaro J. Almeida, Aleksandar D. Stojanovic, Nikola Paunković, Ricardo Loura, Nelson J. Muga, Nuno A. Silva, Paulo Mateus, Paulo S. André, and Armando N. Pinto. Implementation of a Two-State Quantum Bit Commitment Protocol in Optical Fibers. *submitted to Journal of Optics*, 2015.

[3] C. H. Bennett and G. Brassad. Quantum cryptography: Public-key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, December 1984.

[4] Manuel Blum. Coin flipping by telephone. In Allen Gersho, editor, *CRYPTO*, pages 11–15. U. C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, 1981.

[5] V. B. Braginsky and F. Y. Khalili. Quantum nondemolition measurements: the route from toys to tools. *Rev. Mod. Phys.*, 68:1–11, January 1996.

[6] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 362–371, 1993.

[7] Gilles Brassard. Modern cryptology: A tutorial, 1998.

[8] Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.

[9] Anne Broadbent and Alain Tapp. Information-theoretically secure voting without an honest majority. Cryptology ePrint Archive, Report 2008/266, 2008.

[10] Richard Crandall and Carl Pomerance. *Prime Numbers: A Computational Perspective*. Springer, 2nd edition, August 2005.

[11] Claude Crépeau. *What is going on with Quantum Bit Commitment?* Czech Technical University Publishing House, 1996.

[12] Ivan Damgård and Carolin Lunemann. Quantum-secure coin-flipping and applications. In Mitsuru Matsui, editor, *Advances in Cryptology ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 52–69. Springer Berlin Heidelberg, 2009.

[13] A. Danan and L. Vaidman. Practical Quantum Bit Commitment Protocol. *Quantum Information Processing*, 11(3):769–775, June 2012.

[14] Data Encryption Standard (DES). Federal Information Processing Standards Publication 46-3. U.S. Department of Commerce, National Institute of Standards and Technology, 1999.

[15] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs. An experimental implementation of oblivious transfer in the noisy storage model. *Nature Communications*, 5, March 2014.

[16] Lucien Hardy and Adrian Kent. Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.*, 92:157901, April 2004.

[17] B. R. Johnson, M. D. Reed, A. A. Houck, D. I. Schuster, L. S. Bishop, E. Ginossar, J. M. Gambetta, L. Dicarlo, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf. Quantum non-demolition detection of single microwave photons in a circuit. *Nature Physics*, 6:663–667, September 2010.

[18] A. Kent. Quantum Bit String Commitment. *Phys. Rev. Lett.*, 90(23):237901, June 2003.

[19] A. Kent. Unconditionally secure bit commitment with flying qudits. *New J. Phys.*, 13(11):113015, November 2011.

[20] A. Kent. Quantum tasks in Minkowski space. *Classical and Quantum Gravity*, 29(22):224013, November 2012.

[21] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, August 1999.

[22] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109:130501, September 2012.

[23] Hirotada Kobayashi. General properties of quantum zero-knowledge proofs. In Ran Canetti, editor, *Theory of Cryptography*, volume 4948 of *Lecture Notes in Computer Science*, pages 107–124. Springer Berlin Heidelberg, 2008.

[24] R. Konig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *Information Theory, IEEE Transactions on*, 58(3):1962–1984, March 2012.

[25] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang. Comparison of Four Multi-User Quantum Key Distribution Schemes Over Passive Optical Networks. *Journal of Lightwave Technology*, 23:268, January 2005.

[26] Y.-B. Li, Q.-Y. Wen, S.-J. Qin, F.-Z. Guo, and Y. Sun. Practical quantum all-or-nothing oblivious transfer protocol. *Quantum Information Processing*, 13:131–139, January 2014.

[27] Yehuda Lindell and Benny Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In Moni Naor, editor, *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 52–78. Springer Berlin Heidelberg, 2007.

[28] Yang Liu, Yuan Cao, Marcos Curty, Sheng-Kai Liao, Jian Wang, Ke Cui, Yu-Huai Li, Ze-Hong Lin, Qi-Chao Sun, Dong-Dong Li, Hong-Fei Zhang, Yong Zhao, Teng-Yun Chen, Cheng-Zhi Peng, Qiang Zhang, Adán Cabello, and Jian-Wei Pan. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.*, 112:010504, January 2014.

[29] H.-K. Lo and H. F. Chau. Is Quantum Bit Commitment Really Possible? *Phys. Rev. Lett.*, 78:3410–3413, April 1997.

[30] R. Loura, Á. J. Almeida, P. S. André, A. N. Pinto, P. Mateus, and N. Paunković. Noise and measurement errors in a practical two-state quantum bit commitment protocol. *Phys. Rev. A*, 89(5):052336, May 2014.

[31] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.*, 111:180504, November 2013.

[32] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. J. Twitchen, J. I. Cirac, and M. D. Lukin. Room-Temperature Quantum Bit Memory Exceeding One Second. *Science*, 336:1283–1286, June 2012.

[33] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Phys. Rev. Lett.*, 78:3414–3417, April 1997.

[34] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger. Experimental quantum coin tossing. *Phys. Rev. Lett.*, 94:040501, January 2005.

[35] N. H. Y. Ng, S. K. Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nature Communications*, 3, December 2012.

[36] Kamyar Saeedi, Stephanie Simmons, Jeff Z. Salvail, Phillip Dluhy, Helge Riemann, Nikolai V. Abrosimov, Peter Becker, Hans-Joachim Pohl, John J. L. Morton, and Mike L. W. Thewalt. Room-temperature quantum bit storage exceeding 39 minutes using ionized donors in silicon-28. *Science*, 342(6160):830–833, 2013.

[37] Christian Schaffner, Barbara Terhal, and Stephanie Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Info. Comput.*, 9(11):963–996, November 2009.

[38] Claude Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[39] Serge Vaudenay. *A Classical Introduction to Cryptography: Applications for Communications Security.* Springer, 2006.

[40] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, May 2010.

[41] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, June 2008.

[42] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.