Secure bit commitment from no-signalling (relativistic) constraints

Jędrzej Kaniewski, Marco Tomamichel, Esther Hänggi, and Stephanie Wehner

Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

We investigate two-party cryptographic protocols that are secure under assumptions motivated by physics, namely relativistic assumptions (no-signalling) and quantum mechanics. In particular, we discuss split models, i.e. models in which certain parties are not allowed to communicate during certain phases of the protocol, for the purpose of bit commitment. We find the minimal splits that are necessary to evade the Mayers-Lo-Chau no-go argument and present protocols that achieve security in these split models. Furthermore, we introduce the notion of local versus global commands, a subtle issue that arises when the split committer is required to delegate agents to perform the open phase separately, without communication. We argue that classical protocols are insecure in the global command model, even when the committer is split. On the other hand, we provide a rigorous security proof in the global command model for Kent's quantum protocol [Ken11a]. The proof employs two fundamental principles of modern physics, the no-signalling property of relativity and the uncertainty principle of quantum mechanics.

I. INTRODUCTION

The goal of two-party cryptography is to enable two parties, Alice and Bob, to solve a task in cooperation even if they do not trust each other. An example of such a task is the cryptographic primitive known as bit commitment. A bit commitment protocol traditionally consists of two phases: In the commit phase, Bob *commits* a bit to Alice[1], who receives some form of confirmation that a commitment has been made. In the open phase, Bob reveals the bit to Alice. Security means that Bob should not be able to reveal anything but the committed bit, but nevertheless Alice cannot gain any information about the bit before the open phase. While many two-party cryptographic primitives have been defined, oblivious transfer and bit commitment are undoubtedly among the most important ones because they form essential building blocks for more complex problems [Kil88].

Ideally, we would like to have protocols for such primitives that guarantee security without relying on any subjective (e.g. that a safe is difficult to open) or computational (e.g. that factoring a product of two large primes is difficult) assumptions. Unfortunately, however, it turned out that this is impossible, even if we allow quantum communication between Alice and Bob [May97, LC97, DKSW07]. Much work has thus been invested into determining what kind of assumptions allow us to obtain security. Of particular interest to this work are thereby assumptions of a physical nature, leading to information-theoretic security. Classical examples of such assumptions are, for example, access to some very special forms of shared randomness supplied in advance [Riv99], access to a noisy communication channel [2] [Cré97, WNI03] or a limited amount of memory [Mau90]. Similarly, it has been shown that security is possible if the attacker's quantum memory is bounded [DFSS08, DFR+07, Sch10] or more generally noisy [WST08, KWW09, BFW11].

Another assumption is that of *non-communication.* More precisely, one imagines that each party is split up into multiple agents which cannot communicate with each other for at least some parts of the protocol. Intuitively, the use of non-communicating agents can evade the

[1] Usually it is Alice who commits a bit to Bob. We decided to swap Alice and Bob as it allows us to simplify the notation in the proof of our main result. In the whole paper it is Bob who commits a bit to Alice.

[2] To be more specific what is needed is a channel with a guaranteed level of noise. It is important that the noise is truly random and cannot be influenced by either party.

standard no-go argument because while all agents in total have enough information to cheat, no single agent can achieve it on its own.

On the one hand, such non-communicating models have received considerable attention in classical cryptography, where such agents are often referred to as servers [KW04] or provers [Sim07]. For example, Ben-Or et al. [BGKW88] considered a simple protocol for bit commitment that is secure classically as long as the committer (Bob) is split up into two agents, Bob and Brian, which cannot communicate at any points during the protocol. This has been extended to a similar protocol that is secure even in the quantum setting [Sim07]. Similarly, many classical protocols for other tasks have been proposed under the assumption of non-communication, such as distributed oblivious transfer [NP00], i.e. symmetric private information retrieval [GIKM98, Mal00, KW04], or simple private information retrieval [Gas04]. In all such protocols it was assumed that the agents of one party can never communicate during any point in the protocol, or thereafter.

On the other hand, physicists have consider so-called relativistic assumptions for cryptography [Ken99, Ken05, Col09, Ken11b, Ken11a]. In essence, this takes the form of non-communicating models where the fact that a party's agents cannot communicate is justified by their physical separation and the theory of relativity. The key difference to classical non-communicating models is that in relativistic models the separation is generally only imposed during very specific periods of the protocol, whereas classical models generally assume a separation, i.e. non-communication, for all times. For example, relativistic protocols may only demand a split into several non-communicating agents after the commit phase of a bit commitment protocol is over [Ken11b, Ken11a]. Another assumption based on relativity is the notion of guaranteed message delivery times or the assumption of an accelerated observer [BHP09].

Here, we will consider the security of bit commitment protocols under the assumption that one (or both) parties Alice and Bob, can be split into non-communicating agents. Motivated by the relativistic protocols of [Ken11b, Ken11a], we thereby do *not* demand that the parties are split into non-communicating agents for all time, but merely during certain points in the protocol. For a bit commitment protocol, these points are naturally defined as: the commit phase, the wait phase, the open phase, and the verification phases. We thereby introduce the explicit notion of the wait and verification phases, which are usually only implicitly defined, in order to precisely divide the overall interaction between Alice and Bob into time frames. Our first contribution is

- A classification of non-communicating models into subclasses which are characterised by the phases in which either Alice (or Bob) is split into non-communicating agents. We find that we can reduce our considerations to two minimal models, namely the one in which Alice is split during the commit and wait phases (α-split) and the one in which Bob is split during the wait and open phases (β-split) (Fig. 1). Either of these two models allows to evade the no-go theorem because the operations required for cheating are forbidden by the split.

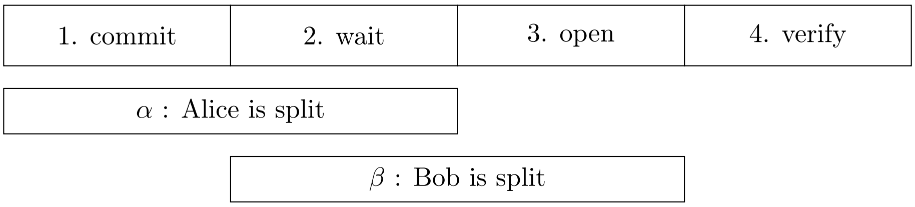
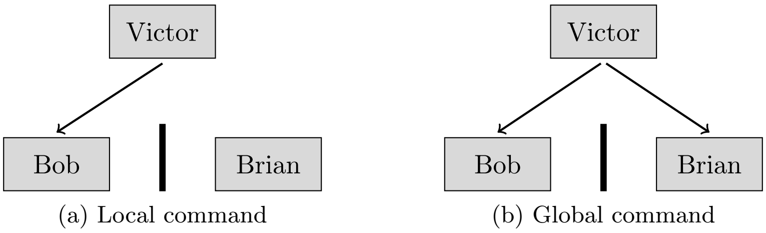


FIG. 1: The two types of separations that are necessary for security - α and β.

Next to the question during which phases the parties are actually split into non-communicating agents, there is another subtlety to address. If cheating Bob is split into two agents, Bob and

Brian, during the open phase of the commitment, who decides which bit should be opened? In standard bit commitment protocols this question does not arise, as there is only one cheating party. Bob will simply announce to Alice that he wishes to unveil a particular bit, and try to provide a matching proof. However, in a model of several distinct agents, Bob and Brian could conceivably base the decision about which bit to unveil on some external input. For example, depending on the latest stock market news they both decide to open a 0 or a 1, even though they themselves cannot communicate. Intuitively, we would like a bit commitment scheme to be secure in the latter setting, analogous to the case of a single party which can of course also base its decision on external events. To capture this subtlety, we imagine that there is an external commander, Victor, who dictates which bit should be unveiled. We thereby speak of *local* command if Victor only issues a command to one of the two agents, Bob. We speak of *global* command if Victor issues a matching command to both Bob and Brian (Fig. 2). Note that a related concept has recently been introduced in [Ken12] under the name of the *oracle input model*. In a model without separated agents, the local and global command models are equivalent but we will see that they differ in a relativistic setting. More precisely, our second contribution is to

- Introduce the distinction between local and global command, and apply it to models based on the β-split. We show that there is a simple classical protocol that is secure under the local command. However, we proceed to show that there exists *no* classical protocol that is secure under global command in the class of β-split models.



(a) Local command (b) Global command

FIG. 2: If Bob is required to perform two separate openings it becomes important whether the command from Victor indicating which bit he is supposed to unveil is transmitted to just one or both agents.

The latter naturally leads to the question, whether there is a *quantum* protocol that is secure even when Victor issues a global command. A candidate protocol was proposed by Kent [Ken11a] in which Bob and Brian are separated during the wait and open phases. This protocol has the very appealing feature that it can be implemented by the honest parties using only single qubit measurements in BB84 [BB84] bases, without the use of any quantum memory. Yet, no rigorous security proof was provided in [Ken11a], neither under local nor global command. We show that the *flying agents model*, proposed in [Ken11b, Ken11a], belongs to the class of non-communicating models (flying agents model requires both Alice and Bob to be split during the wait and open phases). Our final contribution is to

- Provide a formal security proof for the protocol proposed in [Ken11a] in the global command model.

As our proof applies to the less restrictive β-split model it also applies to Kent's flying agents model. Our proof thereby requires two ingredients: First, we make use of the fact that the two agents cannot communicate. Second, we employ an uncertainty relation in terms of min- and max-entropies [TR11]. This relation was previously used to prove the security of quantum key distribution, and our result illustrates its power to prove security of other cryptographic primitives.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BFW11] M. Berta, O. Fawzi, and S. Wehner. Quantum to classical randomness extractors, 2011. http://arxiv.org/abs/1111.2026.

[BGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, STOC '88, pages 113–131, New York, NY, USA, 1988. ACM.

[BHP09] Kamil Brádler, Patrick Hayden, and Prakash Panangaden. Private information via the Unruh effect. *Journal of High Energy Physics*, 2009(08):074, 2009.

[Col09] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation, 2009.

[Cré97] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In *Advances in Cryptology – Proceedings of EUROCRYPT '97*, 1997.

[DFR$^+$07] Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *CRYPTO*, pages 360–378, 2007.

[DFSS08] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.*, 37(6):1865–1890, 2008.

[DKSW07] G. D'Ariano, D. Kretschmann, D. Schlingemann, and R.F. Werner. Quantum bit commitment revisited: the possible and the impossible. *Physical Review A*, 76:032328, 2007. arXiv:quant-ph/0605224v2.

[Gas04] William I. Gasarch. A survey on private information retrieval. *Bulletin of the EATCS*, 82:72–107, 2004.

[GIKM98] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. In *STOC'98*, pages 151–160, 1998.

[Ken99] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[Ken05] Adrian Kent. Secure classical bit commitment using fixed capacity communication channels. *Journal of Cryptology*, 18:313–335, 2005.

[Ken11a] Adrian Kent. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Signal Processing*, pages 3–6, 2011. Available at http://arxiv.org/abs/1108.2879.

[Ken11b] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New J. Phys.*, 13:113015, 2011.

[Ken12] Adrian Kent. Quantum tasks in minkowski space. 2012.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of 20th ACM STOC*, pages 20–31, 1988.

[KW04] I. Kerenidis and R. de Wolf. Quantum symmetrically-private information retrieval. *Information Processing Letters*, 90(3):109–114, 2004. quant-ph/0307076.

[KWW09] R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 2009. arXiv:0906.1030v3.

[LC97] H-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410, 1997.

[Mal00] Tal Malkin. *A Study of secure database access and general two-party computation.* PhD thesis, Massachusetts Institute for Technology, 2000.

[Mau90] Ueli Maurer. A provably-secure strongly-randomized cipher. In *EUROCRYPT'90: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, pages 361–373, 1990.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997.

[NP00] M. Naor and B. Pinkas. Distributed oblivious transfer. In *Proceedings of ASIACRYPT*, pages 205–219, 2000.

[Riv99] Ronald L. Rivest. Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. 8 November 1999.

[Sch10] Christian Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *PHYS.REV.A*, 82:032308, 2010.

[Sim07] Jean-Raymond Simard. Classical and quantum strategies for bit commitment schemes in. 2007.

[TR11] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, Mar 2011. Available at http://arxiv.org/abs/1009.2015.

[WNI03] A. Winter, A. Nascimento, and H. Imai. Commitment capacity of discrete memoryless channels. cs/0304014, 2003.

[WST08] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100:220502, 2008. arXiv:0711.2895v3.