Composable Security in Relativistic Quantum Cryptography

V. Vilasini,[1] Christopher Portmann,[2] and Lídia del Rio[1]
[1]*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*
[2]*Department of Computer Science, ETH Zürich, 8092 Zürich, Switzerland*

(Dated: July 2017)

It has been shown using quantum information theory that secure Oblivious Transfer (OT) can be constructed from a Bit Commitment Resource (BC) [1]. Since OT is complete for multi-party computation (MPC), (i.e. any multi-party function can be securely evaluated given access to OT resources) in the quantum case, BC is complete for MPC. Further, secure Coin Flipping (CF) between two mutually distrusting parties can also be constructed from BC. Blum's protocol [7] for example, constructs an unfair and biased CF resource given a BC resource [8]. These results indicate that BC is an important cryptographic primitive. However, Mayers ([2], [3]) and Lo and Chau ([4], [5]) independently showed that no secure quantum Bit Commitment protocol can be constructed without any assumptions (for example regarding the operations that the parties can perform on their systems) because the sender can almost always cheat successfully using entangled Bell states and cleverly chosen measurements/unitaries.

One turns to relativistic protocols in the hope of avoiding such attacks by imposing relativistic causal constraints. An example is Kent's 2012 quantum relativistic protocol [6] which is immune to the Mayers-Lo-Chau attack since the sender splits into two space-like separated agents who can no longer perform suitable unitaries on their joint systems as long as they remain space-like separated. Like other relativistic BC protocols, this protocol implements a timed commitment which is secure only within a time window that depends on the time taken by light to travel between remote agents. However, it only satisfies a non-composable, weakly-binding security definition [9] and can be shown not be composable with arbitrary protocols i.e. it cannot be securely run as a subroutine in arbitrary protocols. As a consequence, this protocol cannot be used in the constructions of OT or CF mentioned before. A discussion of why relativistic protocols fail to construct OT is presented in the Appendix of [10].

The negative results mentioned above are obtained by finding ad hoc examples of protocols where composition fails. However, without an overall coherent framework for modelling composability in relativistic cryptography, it is impossible to obtain positive results. Here we introduce a framework for modelling composable cryptographic security in the presence of classical, quantum and no-signalling adversaries, and apply it to prove new positive and negative results in relativistic quantum cryptography. We do this by modelling the abstract information processing systems of the Abstract Cryptography framework [11] as causal boxes [12] (information processing systems that satisfy a causality condition and are closed under composition).

We show that relativistic bit commitment without any assumptions is also impossible. This is a non-trivial result since the impossibility result for quantum bit commitment does not directly imply the impossibility for bit commitment in the relativistic case. We prove impossibility of both unfair and biased relativistic CFs. The proof is general and applies to both classical and quantum relativistic protocols. This implies the required impossibility result for (relativistic) BC since CF can be constructed from BC and impossibility for the weaker resource (CF) implies impossibility for the stronger resource (BC).

If the parties have access to a resource such as a secure channel with delay, tasks such as CF and BC become possible. We show that an unbiased, relativistic CF resource can be constructed from a secure channel with delay (CD) resource where dishonest players can reduce the channel's delay to an arbitrary, non-zero value. Relativistic BC protocols being time restricted, closely resemble a channel with a fixed delay where adversaries cannot reduce the delay of the channel. Compared to Blum's non-relativistic construction ([7], [8]) that constructs a biased CF resource from a BC resource, here we use a weaker resource (CD) to construct a stronger resource (unbiased relativistic CF).

Our framework can also model situations where agents exchange a superposition of different numbers of messages in a superposition of orders in time [12] and provides an operational framework for studying indefinite causal structures.

[1] D. Unruh. *Universally Composable Quantum Multi-party Computation.* Advances in Cryptology, EUROCRYPT 2010. EUROCRYPT 2010. Editor: H. Gilbert. Lecture Notes in Computer Science, Vol. 6110. Springer, Berlin, Heidelberg (2010).

[2] D. Mayers. *Unconditionally secure quantum bit commitment is impossible.* Physical Review Letters, Vol. 78, Pages 3414-3417 (1997).

[3] D. Mayers. *Unconditionally secure quantum bit commitment is impossible.* Proceedings of the Fourth Workshop on Physics and Computation (New England Complex System Inst., Boston), Page 226 (1996).

[4] H. K. Lo , H. Chau. *Is quantum bit commitment really possible?* Physical Review Letters, Vol. 78, Pages 3410-3413 (1997).

[5] H. K. Lo and H. Chau. *Why quantum bit commitment and ideal quantum coin tossing are impossible.* Proceedings of the Fourth Workshop on Physics and Computation (New England Complex System Inst., Boston), Page 76 (1996).

[6] A. Kent. *Unconditionally secure bit commitment by transmitting measurement outcomes.* Physical Review Letters, Vol. 109, Pages 130501 (2012).

[7] M. Blum. *Coin Flipping by telephone a protocol for solving impossible problems.* SIGACT News, Winter-Spring 1983, Vol. 15, No. 1, Pages 23-27, ACM, New York, USA (1983).

[8] G. Demay, U. Maurer. *Unfair coin tossing.* Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, Pages 1556-1560 (2013).

[9] J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. *Secure bit commitment from relativistic constraints.* IEEE Transactions on Information Theory, Vol. 59, No. 7, Pages 4687-4699 (2013).

[10] J. Kaniewski. *Relativistic quantum cryptography.* PhD Thesis, Centre for Quantum Technologies, National University of Singapore. arXiv:1512.00602 [quant-ph] (2015).

[11] U. Maurer, R. Renner. *Abstract Cryptography.* The Second Symposium on Innovations in Computer Science, ICS 2011, Editors: B. Chazelle, Pages 1-21. Tsinghua University Press (2011).

[12] C. Portmann, C. Matt, U. Maurer, R. Renner, B. Tackmann. *Causal Boxes: Quantum Information-Processing Systems Closed Under Composition.* IEEE Transactions on Information Theory, Vol. 63, No. 5, Pages 3277-3305 (2017).