Universiteit
Leiden
The Netherlands

Two-Prover Bit-Commitments: Classical, Quantum and Non-Signaling

Fillinger, M.J.

Citation

Fillinger, M. J. (2019, March 19). *Two-Prover Bit-Commitments: Classical, Quantum and Non-Signaling*. Retrieved from https://hdl.handle.net/1887/70036

Version:	Not Applicable (or Unknown)
License:	Leiden University Non-exclusive license
Downloaded from:	https://hdl.handle.net/1887/70036

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/70036 holds various files of this Leiden University dissertation.

Author: Fillinger, M.J.
Title: Two-Prover Bit-Commitments: Classical, Quantum and Non-Signaling
Issue Date: 2019-03-19

Stellingen

behorende bij het proefschrift *Two-Prover Bit-Commitments: Classical, Quantum and Non-Signaling* van Max Fillinger

1. The two-prover *bit*-commitment scheme $\mathcal{CHSH}^q$, introduced by Crépeau, Salvail, Simard and Tapp can also be considered as a *string* commitment scheme by replacing the bit with an element of the field $\mathbb{F}_q$. However, the precise security property then becomes subtle and depends on some detail of how exactly one defines the scheme.

2. A pair of two-prover commitment schemes that satisfy some mild requirements can be composed into a new scheme. The binding parameter of the composed scheme is the sum of the binding parameters of the two original schemes. Furthermore, the composed scheme remains binding even if there is some limited communication between the dishonest provers, which makes this *composition theorem* suitable for constructing and analyzing relativistic two-prover commitment schemes.

3. Based on the original analysis, the lab implementation of the two-prover relativistic commitment scheme by Lunghi, Kaniewski, Bussières, Houlmann, Tomamichel, Wehner and Zbinden, was believed to remain binding for only 2 ms. Analyzing the scheme using the composition theorem shows that it remains binding for 10^{56} years – in other words, the limiting factor is not security, but the amount of memory in the devices executing the scheme.

4. There are many ways not to communicate. To truly base the security of a multi-prover commitment scheme on the sole assumption that the provers cannot communicate, one must consider so-called *general non-signaling* provers. In this setting, there exist hiding and binding n-prover commitment schemes if and only if $n \geq 3$.

5. In contrast to eavesdropping, forgery of a signature always leaves a trace: the forged signature itself. A forged digital signature allows for forensic analysis that might reveal how it was produced.

6. To spread within local networks, the Flame malware used a forged digital signature which was created by means of a collision attack on the hash function MD5. Forensic analysis revealed that the differential paths of the collision had not been used in any published collision attack. This analysis further made it possible to reconstruct a likely candidate for the families of differential paths they were drawn from, and to calculate the expected cost of the attack: approximately $2^{49.3}$ MD5 compressions.

7. In homomorphic encryption schemes, the main efficiency cost comes from having to *bootstrap* ciphertexts before continuing to apply homomorphic operations. There is a homomorphic encryption scheme that supports an evaluate-and-bootstrap procedure that can homomorphically evaluate any gate with $O(\log n)$ input bits and bootstrap the output in total time $\tilde{O}(n^2)$. Furthermore, this evaluate-and-bootstrap procedure can be applied to threshold gates with $O(n)$ input bits.

8. Suppose that two local networks are logically separated from the internet but connected to each other via a VPN. Even if the VPN had perfect encryption and authentication, a man-in-the-middle on the internet and a compromised host in one of the networks could exchange messages by means of the above infrastructure. A rate of 13 megabit per second from the local network to the man-in-the-middle can be achieved under ideal circumstances if the rate of the VPN connection is 1 gigabit per second. In the other direction, a rate of 6 megabit per second can be achieved.

9. If the two provers in $\mathcal{CHSH}^q$ are one light year apart, the scheme is binding if no more than one year passes between the time that the first prover received the first message and the opening. There is strong evidence that if the two provers are more than 14.4 billion light years apart, the scheme remains binding forever.