



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

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

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 19 maart 2019
klokke 10:00 uur

door

Maximilian Johannes Fillinger
geboren te Wuppertal, Duitsland,
in 1988

Promotor:

Prof. dr. Serge Fehr (CWI, Amsterdam & Universiteit Leiden)

Samenstelling van de promotiecommissie:

Dr. Stacey Jeffery (CWI, Amsterdam)

Prof. dr. Adrian Kent (University of Cambridge)

Prof. dr. Bart de Smit (Universiteit Leiden)

Prof. dr. Aad van der Vaart (Universiteit Leiden)

Prof. dr. Stefan Wolf (Università della Svizzera italiana, Lugano)

This work was supported by the *NWO Free Competition* grant 617.001.203
and carried out at CWI, Amsterdam.



Universiteit Leiden



Nederlandse Organisatie
voor Wetenschappelijk Onderzoek

Contents

1	Introduction	1
1.1	Background	1
1.2	Two-Prover Commitment Schemes	6
1.3	Relativistic Cryptography	9
1.4	Contributions of this Thesis	12
2	Preliminaries	19
2.1	Probabilities	19
2.2	Two-Prover Commitment Schemes	23
3	The Hiding and Binding Properties	27
3.1	Introduction	27
3.2	Defining The Binding Property	28
4	The Composition Theorem	41
4.1	Composition of Commitment Schemes	41
4.2	The Composition Theorems	46
4.3	Variations	50
4.4	Tightness	53
5	Towards Quantum Safety	59
5.1	Introduction	59
5.2	Quantum Information Theory	60
5.3	Protocols	65
5.4	Binding Properties	66
5.5	The Composition Theorem	70
6	Bit-commitment with Non-signaling Adversaries	73
6.1	Introduction	73
6.2	Bipartite Systems and Two-Prover Commitments	74
6.3	Impossibility of Two-Prover Commitments	80
6.4	Possibility of Three-Prover Commitments	89