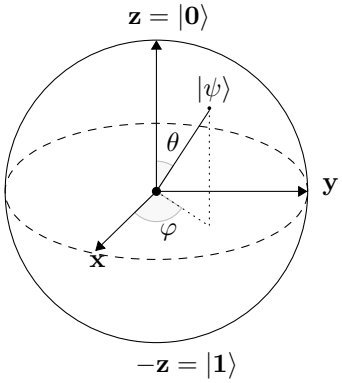
# On the Impossibility of Unconditionally Secure Quantum Bit Commitments




## Problem description

In 1996 Mayers [1] proved that unconditionally secure quantum bit commitments are impossible. The proof is split into two stages: First, he shows that any protocol comprising classical information can be translated into a protocol using only quantum information. Then he shows that a scheme that is unconditionally hiding is subject to an attack that compromises the unconditionally binding property. The proof employs the idea, that the density matrices of the two states encoding either $|0\rangle$ or $|1\rangle$ must be indistinguishable. If the density matrices are close (enough), the respective quantum states can be decomposed allowing to transform one state into the other. Hence a quantum bit commitment can not be (unconditionally) secure.

The aim of the thesis is to reconstruct the attack presented by Mayers [1], including the explicit construction transforming the encoded states. Possibly, the thesis may include an example implementation of an easy protocol and the corresponding attack using the quantum simulation framework *Q#*.

## Keywords

quantum, cryptanalysis, unconditional security

## Remarks

Prior knowledge of quantum computing and commitments is recommended.

## Point of contact


| | | |
|---|---|---|
| Level: | Bachelor | |
| Supervisor: | Prof. Dr. Jörn Müller-Quade | |
| Daily supervisor: | Marcel Tiepelt | marcel.tiepelt@kit.edu |


# References


[1] Dominic Mayers. "Unconditionally Secure Quantum Bit Commitment is Impossible." In: *Physical Review Letters* 78.17 (Apr. 1997), pp. 3414–3417. ISSN: 1079-7114. DOI: 10.1103/physrevlett.78.3414. URL: http://dx.doi.org/10.1103/PhysRevLett.78.3414.