Non-static Quantum Bit Commitment

Jeong Woon Choi, Dowon Hong, Ku-Young Chang, Dong Pyo Chi, Soojoon Lee

(Submitted on 9 Jan 2009 (v1), last revised 15 Sep 2009 (this version, v4))

Quantum bit commitment has been known to be impossible by the independent proofs of Mayers, and Lo and Chau, under the assumption that the whole quantum states right before the unveiling phase are static to users. We here provide an unconditionally secure non-static quantum bit commitment protocol with a trusted third party, which is not directly involved in any communications between users and can be limited not to get any information of commitment without being detected by users. We also prove that our quantum bit commitment protocol is not secure without the help of the trusted third party. The proof is basically different from the Mayers-Lo-Chau's no-go theorem, because we do not assume the staticity of the finally shared quantum states between users.

Comments:	5 pages
Subjects:	**Quantum Physics (quant-ph)**
Cite as:	**arXiv:0901.1178v4 [quant-ph]**

Submission history

From: Jeong Woon Choi [view email]

[v1] Fri, 9 Jan 2009 06:58:54 GMT (10kb)

[v2] Fri, 10 Apr 2009 08:50:41 GMT (12kb)

[v3] Mon, 24 Aug 2009 23:56:23 GMT (11kb)

[v4] Tue, 15 Sep 2009 05:02:56 GMT (11kb)

Which authors of this paper are endorsers?

Link back to: arXiv, form interface, contact.

Download:

- PDF
- PostScript
- Other formats

Current browse context:

quant-ph

< prev | next >

new | recent | 0901

References & Citations

- SLAC-SPIRES HEP (refers to | cited by)
- CiteBase

Bookmark(what is this?)

CiteULike logo

Connotea logo

BibSonomy logo

Mendeley logo

Facebook logo

del.icio.us logo

Digg logo Reddit logo