

# Efficient reconciliation protocol for discrete-variable quantum key distribution

David Elkouss, Anthony Leverrier, Romain Alléaume, Joseph Boutros

(Submitted on 14 Jan 2009)

Reconciliation is an essential part of any secret-key agreement protocol and hence of a Quantum Key Distribution (QKD) protocol, where two legitimate parties are given correlated data and want to agree on a common string in the presence of an adversary, while revealing a minimum amount of information.

In this paper, we show that for discrete-variable QKD protocols, this problem can be advantageously solved with Low Density Parity Check (LDPC) codes optimized for the BSC. In particular, we demonstrate that our method leads to a significant improvement of the achievable secret key rate, with respect to earlier interactive reconciliation methods used in QKD.

Subjects: **Information Theory (cs.IT)**; Quantum Physics (quant-ph)

Cite as: [arXiv:0901.2140v1](#) [cs.IT]

## Submission history

From: David Elkouss Coronas [[view email](#)]

[v1] Wed, 14 Jan 2009 23:07:59 GMT (101kb,S)

*[Which authors of this paper are endorsers?](#)*

## Download:

- [PDF](#)
- [PostScript](#)
- [Other formats](#)

Current browse context:

cs.IT

[< prev](#) | [next >](#)

[new](#) | [recent](#) | [0901](#)

Change to browse by:

[cs](#)

[math](#)

[quant-ph](#)

## References & Citations

- [CiteBase](#)

## DBLP - CS Bibliography

[listing](#) | [bibtex](#)

[David Elkouss](#)

[Anthony Leverrier](#)

[Romain Alleaume](#)

[Joseph Boutros](#)

## Bookmark<sup>(what is this?)</sup>

[CiteULike logo](#)

[Connotea logo](#)

[BibSonomy logo](#)

[Mendeley logo](#)

[Facebook logo](#)

[del.icio.us logo](#)

[Digg logo](#)

[Reddit logo](#)