

Accepted Manuscript

New multi-stage secret sharing in the standard model

Samaneh Mashhadi

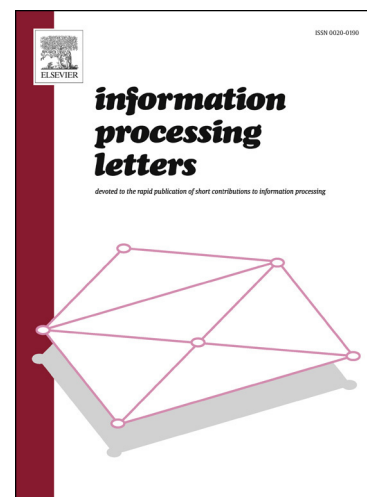
PII: S0020-0190(17)30124-2
DOI: <http://dx.doi.org/10.1016/j.ipl.2017.07.002>
Reference: IPL 5558

To appear in: *Information Processing Letters*

Received date: 7 September 2016
Revised date: 11 June 2017
Accepted date: 2 July 2017

Please cite this article in press as: S. Mashhadi, New multi-stage secret sharing in the standard model, *Inf. Process. Lett.* (2017), <http://dx.doi.org/10.1016/j.ipl.2017.07.002>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Highlights

- A multi-stage secret sharing scheme, with computational provable security.
- The security proof is in the standard model.
- New methods for the construction and the recovery phases.
- The scheme has few public values and short secret shares.
- We can design various multi-stage secret sharing schemes through a similar algorithm.

Download English Version:

<https://daneshyari.com/en/article/4950868>

Download Persian Version:

<https://daneshyari.com/article/4950868>

[Daneshyari.com](https://daneshyari.com)