The copyright to this article is transferred to the International Association for Cryptologic Research effective if and when the article is accepted for publication. The copyright transfer covers the exclusive right to reproduce and distribute the article, including reprints, translations, photographic reproductions, microform, electronic form (offline, online) or any other reproductions of similar nature.

An author may self-archive an author-created version of his/her article on his/her own website and his/her institution's repository, including his/her final version; however he/she may not use the publisher's PDF version which is posted on www.springerlink.com. Furthermore, the author may only post his/her version provided acknowledgement is given to the original source of publication and a link is inserted to the published article on Springer's website. The link must be accompanied by the following text: “The original publication is available at www.springerlink.com”.

Please use the appropriate DOI for the article (go to the Linking Options in the article, then to OpenURL and use the link with the DOI). Articles disseminated via www.springerlink.com are indexed, abstracted, and referenced by many abstracting and information services, bibliographic networks, subscription agencies, library networks, and consortia.

The author warrants that this contribution is original and that he/she has full power to make this grant. The author signs for and accepts responsibility for releasing this material on behalf of any and all co-authors.

After submission of this agreement signed by the corresponding author, changes of authorship or in the order of the authors listed will not be accepted by Springer.

Title of article:
Author(s):
Author’s signature:
Date:

Please mail form to:
Ueli Maurer
Department of Computer Science
ETH Zürich
CH-8092 Zürich
Switzerland