Robust and Efficient Sharing of RSA Functions

Rosario Gennaro and Tal Rabin

IBM T.J. Watson Research Center,
PO Box 704, Yorktown Heights, NY 10598, U.S.A.
{rosario,talr}@watson.ibm.com

Stanislav Jarecki

Laboratory of Computer Science, Massachusetts Institute of Technology,
545 Technology Square, Cambridge, MA 02139, U.S.A.
stasio@theory.lcs.mit.edu

Hugo Krawczyk

Department of Electrical Engineering, Technion,
Haifa 32000, Israel
hugo@ee.technion.ac.il

and

IBM T.J. Watson Research Center,
PO Box 704, Yorktown Heights, NY 10598, U.S.A.

Erratum: The online contents page of the original article (DOI: 10.1007/s001459910011) was inadvertently published with only the first author appearing. The correct version appears above. The publisher regrets and apologizes for the error.