

# Accepted Manuscript

Title: PriviPK: certificate-less and secure email communication

Author: Mashael AlSabah, Alin Tomescu, Ilia Lebedev, Dimitrios Serpanos, Srimi Devadas

PII: S0167-4048(17)30083-4

DOI: <http://dx.doi.org/doi: 10.1016/j.cose.2017.04.008>

Reference: COSE 1136

To appear in: *Computers & Security*

Received date: 13-11-2016

Revised date: 15-3-2017

Accepted date: 9-4-2017

Please cite this article as: Mashael AlSabah, Alin Tomescu, Ilia Lebedev, Dimitrios Serpanos, Srimi Devadas, PriviPK: certificate-less and secure email communication, *Computers & Security* (2017), <http://dx.doi.org/doi: 10.1016/j.cose.2017.04.008>.

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.



# PriviPK: Certificate-less and Secure Email Communication

Authors names:

Mashaël AlSabah

Affiliation: Qatar Computing Research Institute (QCRI) and Qatar University (QU) College of Engineering  
P.O. Box 2713 Doha-Qatar

Email: [malsabah@qu.edu.qa](mailto:malsabah@qu.edu.qa)

Alin Tomescu

Affiliation: Massachusetts Institute of Technology (MIT)

32 Vassar St., 32-G890

Cambridge, MA 02139

U.S.A.

Email: [alinush@csail.mit.edu](mailto:alinush@csail.mit.edu)

Ilia Lebedev

Affiliation: Massachusetts Institute of Technology (MIT)

32 Vassar St. Office 32-G890

Cambridge, MA 02139

U.S.A.

Email: [ilebedev@mit.edu](mailto:ilebedev@mit.edu)

Dimitrios Serpanos

Industrial Systems Institute/RC ATHENA and Dept. of ECE, University of Patras, GR-26504 Patras, Greece

PSP Building, Stadiou St.

GR-26504 Platani Patras

Greece

email: [serpanos@isi.gr](mailto:serpanos@isi.gr)

Srini Devadas

Affiliation: Massachusetts Institute of Technology (MIT) MIT Room 32G-844

32 Vassar Street

Cambridge, MA 02139

U.S.A.

[devadas@mit.edu](mailto:devadas@mit.edu)

Mashaël Al-Sabah is an Assistant Professor at the Computer Science and Engineering Department at Qatar University, and a Scientist at Qatar Computing Research Institute (QCRI). Her research interests include the general area of privacy enhancing technologies with a particular interest in anonymous and secure communication, cryptocurrency, traffic analysis and side-channel attacks.

Download English Version:

<https://daneshyari.com/en/article/4955405>

Download Persian Version:

<https://daneshyari.com/article/4955405>

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