



Call for papers

WAHC'14

2nd Workshop on Applied Homomorphic Cryptography and Encrypted Computing

Associated with Financial Cryptography & Data Security 2014

*Rockley, Christ Church, Barbados, West Indies
March 7, 2014*

Keynote

Zvika Brakerski, Computer Science Department, Stanford University

Homomorphic Cryptography is one of the hottest topics in mathematics and computer science since Gentry presented the first construction of a fully homomorphic encryption scheme in 2009. Recently, a number of extensions to the original approach, as well as new paradigms have been proposed, creating a diverse basis for further theoretical research. On the other hand, we need research on practical applications of homomorphic encryption which is still less advanced. The cloud hype and different recent disclosures clearly show that there is a strong demand for secure delegation of computation. The technologies and techniques discussed in this workshop are a key to extend the range of applications that can be securely outsourced.

Topics include (but are not limited to)

- Implementation issues of homomorphic encryption schemes
- Practical performance evaluation of homomorphic schemes
- Software architectures for encrypted applications
- Platform and system integration for encrypted applications
- Algorithmic primitives for encrypted applications

Submission

All accepted papers will be published in an LNCS volume (as part of the main FC '14 proceedings or collected in a subsidiary workshop proceedings). Submissions are limited to 12 pages including references and appendices. Authors are invited to submit anonymous versions of their papers for initial review via EasyChair.

- Encrypted search schemes
- Encrypted e-payment solutions
- Encrypted financial transactions
- Encrypted applications in bio-informatics
- Hybrid (partly encrypted) applications

Schedule

Submission Deadline: Jan 15, 2014
Notification: Jan 31, 2014
Camera Ready Due: Feb 15, 2014
Workshop: March 7, 2014

Organising Committee

Michael Brenner and Matthew Smith, Distributed Computing & Security Group, Leibniz Universitaet Hannover, Germany

Program Committee

Jose M. Alcaraz Calero, U Glasgow, UK
Dario Fiore, MPI-SWS, DE
Seny Kamara, Microsoft Res., US
Vladimir Kolesnikov, Bell Labs, US
David Naccache, ENS, FR
Maire O'Neill, QUB, UK
Elizabeth O'Sullivan, QUB, UK
Pascal Paillier, CryptoExperts, FR
Henning Perl, U Hannover, DE

Kurt Rohloff, BBN Tech, US
Christoph Sorge, U Paderborn, DE
Osman Ugus, HAW Hamburg, DE
Marten van Dijk, U Connecticut, US
Yevgeniy Vahlis, U Toronto, CA
Fre Vercauteren, KU Leuven, BE
Adrian Waller, Thales Group, UK
Xun Yi, Victoria U, AU

<https://www.dcsec.uni-hannover.de/wahc14.html>



Leibniz
Universität
Hannover

