Call for papers

WAHC'13

Workshop on Applied Homomorphic Cryptography

Associated with Financial Crypto and Data Security 2013

Bankoku Shinryokan, Busena Terrace Beach Resort, Okinawa, Japan
April 1st 2013

Keynotes
Vinod Vaikuntanathan, University of Toronto
Zvika Brakerski, Stanford University

Homomorphic Cryptography has become one of the hottest topics in mathematics and computer science since Gentry presented the first fully homomorphic scheme in 2009. This has also enhanced the interest in secret function evaluation, private information retrieval or searchable encryption in general. Many new cryptographic schemes have been proposed, creating a diverse mathematical basis for further theoretical research. Research on practical applications of homomorphic encryption, secret function evaluation, private information retrieval or searchable encryption is still less advanced due to the poor performance resulting on the complexity assumptions made in current encryption schemes. The goal of the WAHC is to bring together professionals, researchers and practitioners in the area of computer security and applied cryptography with an interest in practical applications of homomorphic encryption, secure function evaluation, private information retrieval or searchable encryption to present, discuss, and share the latest findings in the field, and to exchange ideas that address real-world problems with practical solutions using homomorphic cryptography.

Topics include (but are not limited to)
- implementation issues of homomorphic encryption schemes
- practical performance evaluation of homomorphic schemes
- software architectures for encrypted applications
- platforms and system integration for encrypted applications
- algorithmic primitives for encrypted applications
- encrypted search schemes
- encrypted applications in bio-informatics
- encrypted e-payment solutions
- encrypted financial transactions
- hybrid (partly encrypted) applications

Submission
All accepted papers will be published in an LNCS volume (as part of the main FC '13 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.

Schedule
Submission deadline (ext): 31. Dec. 2012
Acceptance notification: 1. Feb. 2013
CR deadline: 8. Feb. 2013
Workshop: 1. April 2013

http://www.dcsec.uni-hannover.de/4548.html

Leibniz Universität Hannover

DC Sec