Call for papers

WAHC'15

3rd Workshop on Encrypted Computing and Applied Homomorphic Cryptography

Associated with Financial Crypto & Data Security 2015

Isla Verde, Puerto Rico, January 30th, 2015

The cloud hype and recent disclosures show there is demand for secure and practical computing technologies. The workshop addresses the challenge to safely outsource data processing onto remote computing resources by protecting programs and data even during processing. This allows users to confidently outsource computation over confidential information independently from the trustworthiness or the security level of the remote delegate. The technologies and techniques discussed in this workshop are key to extend the range of applications that can be securely and practically outsourced. The goal of the workshop is to bring together researchers, practitioners, government and industry to present, discuss and share the latest progress in the field relevant to real-world problems with practial approaches and solutions.

Topics include (but are not limited to)

- Implementation of homomorphic encryption schemes
- Practical performance evaluations of homomorphic encryption schemes
- Practical aspects of functional encryption
- Software architectures for encrypted applications
- Platform and system integration for encrypted applications
- Algorithmic primitives for encrypted applications
- Encrypted search schemes, e-payment solutions, financial transactions
- Encrypted applications in bio-informatics
- Hybrid (partly encrypted) applications
- Hardware implementations of encrypted computing
- Secure information sharing

Intended audience

Professionals, researchers and practitioners in the area of computer security and applied cryptography with an interest in practical applications of homomorphic encryption, encrypted computing, functional encryption and secure function evaluation, private information retrieval and searchable encryption.

Schedule

- Submission Deadline: Oct. 16, 2014
- Acceptance Notice: Nov. 16, 2014
- Camera Ready Due: Dec. 31, 2014
- Workshop: Jan. 30, 2015

Submission

Workshop proceedings will be published in an LNCS volume. Submissions are limited to 12 pages including references and appendices.

Program Committee

- **Chair:** Michael Brenner, Leibniz Universität Hannover, Germany
- **Co-Chair:** Kurt Rohloff, NJIT, USA
- Dan Bogdanov, Cybernetica, Estonia
- Kevin Butler, University of Florida, USA
- David Cousins, BBN, USA
- Dario Fiore, IMDEA Software Institute, Madrid, Spain
- Shai Halevi, IBM, USA
- Vladimir Kolesnikov, Bell Labs, USA
- Tancrède Lepoint, CryptoExperts, France
- David Naccache, Ecole Normale Superieure, Paris, France
- Michael Naehrig, Microsoft, USA
- Maire O'Neill, Queen's University Belfast, UK
- Pascal Paillier, CryptoExperts, France
- Benny Pinkas, Bar Ilan University, Israel
- Christoph Sorge, Universitaet Saarland, Germany
- Osman Ugus, Exceet Secure Solutions, Germany
- Yevgeniy Vahlis, University of Toronto, Canada
- Marten van Dijk, University of Connecticut, USA
- Fre Vercauteren, Katholieke Universiteit Leuven, Belgium
- Adrian Waller, Thales, UK