

[Home](#)

[Description >](#)  
[Call for Papers >](#)

[Program >](#)

[Venue >](#)  
[Travel >](#)  
[About Zurich >](#)

[Registration >](#)

[Contact >](#)

# Workshop on Cryptography and Security in Clouds (March 15-16, 2011, Zurich)

## Program

The workshop will take place in downtown Zurich at the [IBM Forum Switzerland](#).  
The [abstracts of all talks](#) are available.

### Tuesday, March 15, 2011

08:30 **Registration**

#### Session 1

Chair: Christian Cachin

09:00 **Welcome**

*The Organizers*

09:10-09:50

**Virtual Security: Data Leakage in Third-Party Clouds and VM Reset Vulnerabilities (Invited Talk)**

*Thomas Ristenpart (University of Wisconsin, Madison, USA)*

09:50-10:30

**A Small Latte or a PetaCycle? You Decide. The Economics of Cloud Computing and What This Means for Security (Invited Talk)**

*Radu Sion (Stony Brook University, USA)*

10:30-11:00

**Coffee Break**

#### Session 2

Chair: Giuseppe Persiano

11:00-11:40

**The Cloud was Tippy and Ate my Files! (Invited Talk)**

*Giuseppe Ateniese (Johns Hopkins University, USA)*

11:40-12:20

**Writing on Wind and Water: Storage Security in the Cloud (Invited Talk)**

*Ari Juels (RSA, The Security Division of EMC, USA)*

12:30-14:00

**Lunch**

#### Session 3

Chair: Ahmad Sadeghi

14:00-14:40

**Using TPMs to Tame Uncertainty in the Cloud (Invited Talk)**

*Rodrigo Rodrigues (Max Planck Institute for Software Systems, Germany)*

14:40-15:05

**Towards Multi-Layer Autonomic Isolation of Cloud Computing and Networking Resources (PDF)**

*Aurélien Wailly, Marc Lacoste, Hervé Debar (Orange Labs and Télécom Sud Paris, France)*

15:05-15:30

**Security Considerations for Virtual Platform Provisioning (PDF)**

*Mudassar Aslam, Christian Gehrman (Swedish Institute of Computer Science)*

15:30-16:00

**Coffee Break**

#### Session 4

Chair: Matthias Schunter

16:00-16:40

**Mobile Trusted Virtual Domains (Invited Talk)**

*Ahmad Sadeghi (TU Darmstadt, Germany)*

16:40-17:05

**Technical Challenges of Forensic Investigations in Cloud Computing Environments (PDF)**

*Dominik Birk (Ruhr-Universität Bochum, Germany)*

17:05-17:30

**Self-Managed Services Conceptual Model in Trustworthy Clouds' Infrastructure (PDF)**

*Imad M. Abbadi (Oxford University Computing Laboratory, UK)*

#### Social Event

19:00

**Dinner at Restaurant Turbinenhalle**

*Directions to be posted*

### Wednesday, March 16, 2011

#### Session 5

Chair: Sören Bleikertz

09:00-09:45

**Predicate Encryption for Private and Searchable Remote Storage (Invited Talk)**

*Giuseppe Persiano (Università di Salerno, Italy)*

09:45-10:30

**Side Channels in Cloud Services: The Case of Deduplication in Cloud Storage (Invited Talk)**

*Benny Pinkas (Bar Ilan University, Israel)*

10:30-11:00

**Coffee Break**

**Session 6****Chair: Matthias Schunter**

- 11:00-11:25 **Byzantine Fault Tolerance for the Cloud** (PDF)  
*Hans P. Reiser (University of Lisboa, Portugal and University of Passau, Germany)*
- 11:25-11:50 **Integrity and Consistency for Untrusted Services** (PDF)  
*Christian Cachin (IBM Research - Zurich, Switzerland)*
- 11:50-12:15 **Verifiable Computation with Two or More Clouds** (PDF)  
*Ran Canetti, Ben Riva, Guy Rothblum (Tel Aviv University, Israel and Princeton University, USA)*

12:15-13:45

**Lunch****Session 7****Chair: Giuseppe Persiano**

- 13:45-14:10 **Twin Clouds: An Architecture for Secure Cloud Computing** (PDF)  
*Sven Bugiel, Stefan Nürnberg, Ahmad Sadeghi, Thomas Schneider (TU Darmstadt and Ruhr-Universität Bochum, Germany)*
- 14:10-14:35 **Secure Outsourced Computation in a Multi-Tenant Cloud** (PDF)  
*Seny Kamara, Mariana Raykova (Microsoft Research and Columbia University, USA)*
- 14:35-15:00 **Amortized Sublinear Secure Multi Party Computation** (PDF)  
*Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Tal Malkin, Mariana Raykova, Yevgeniy Vahlis (Columbia University, University of Maryland, and Bell Labs)*

15:00-15:30

**Coffee Break****Session 8****Chair: Christian Cachin**

- 15:30-15:55 **Computation on Randomized Data** (PDF)  
*Florian Kerschbaum and Kiayias Aggelos (SAP Research Karlsruhe, Germany and University of Athens, Greece)*
- 15:55-16:20 **Private and Perennial Distributed Computation** (PDF)  
*Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov (Ben-Gurion University, Israel, AT&T Labs Research, USA, and Bell Labs, USA)*
- 16:20-16:50 **Discussion: Cryptographic Secure Computation for Cloud Computing?**  
*Moderation: Matthias Schunter (IBM Research - Zurich, Switzerland)*
- 16:50-17:00 **Closing**  
*The Organizers*

Organization

