**Cryptography summer school - Call for participation**

 Bucharest, Romania (21st of July 2014 – 24th of July 2014)

The University of Bristol in collaboration with the Romanian Academy of Science and the University of Bucharest, and with the support of the FP7 EU project “PRACTICE” organizes a summer school on foundations of cryptography.

**Aims, audience, and prerequisites.** The school aims to introduce the participants to the principles of modern cryptography as applied to the most basic primitives. The target audience are top undergraduate and graduate students, early career researchers, as well as security professionals with an interest in cryptography. While no specific prior knowledge on cryptography is required, the participants are expected to be familiar with basic algebra and probability theory. The accepted participants may be required to study in advance some background materials

**Topics and format.** The school cover foundations for hash functions, symmetric and asymmetric encryption, message authentication codes, and digital signatures.  Some more advanced topics will cover cryptography based on lattices and bilinear pairings.

Each topic will have allocated a couple of lectures and a problem class.

**Lecturers**.

* Dario Catalano (University of Catania, Italy)
* Vadim Lyubachevsky (Ecole Normale Superieure, France)
* Marc Fischlin (Darmstadt University, Germany)
* Gregory Neven (IBM Research - Zurich, Switzerland)
* Tom Ristenpart (University of Wisconsin, U.S.)
* Tom Shrimpton (Portland University, U.S.)

**Location.** The school will be held in Bucharest at a location to be determined soon.

**Applications.** Interested participants are invited to submit their application by following the instructions on the online registration page that can be found at:

<http://www.cs.bris.ac.uk/cryptosummerschool>

Applications are accepted until 10th of May 2014, but places are limited so early applications are strongly encouraged. A limited number of scholarships that cover participation and accommodation fees are also available. In addition, the University of Bucharest will provide some low-cost student accommodation. For information, please email [cryptosummerschool@gmail.com](mailto:cryptosummerschool@gmail.com)