

Call for Papers SantaCrypt 2012

29 – 30 November, 2012, Prague, Czech Rep.

<http://mkb.buslab.org>

Intro

Santa's Crypto Get-Together (SantaCrypt) started in 2001 as the first annual Czech and Slovak workshop aiming to facilitate closer cooperation of professionals working in the field of applied cryptography and related areas of security. This get-together of experts is organised in order to foster exchange of information and ideas on past, ongoing, and also future projects. We recognise the need of experts meeting their colleagues without the hassle of taking care of their (potential) customers, bosses and other distracting forces. ;-) The workshop is run in English in the first day and then Czech and Slovak the second day.

There will be the following invited lectures:

- David Naccache (ENS, France) & Zdeněk Říha (FI MU, CZ): *Statistical Speedups for Biometric Identification*.
- Karsten Nohl (Germany): *To Be Confirmed*.
- Andreas Uhl (University of Salzburg, Austria): *Watermarking in Biometrics*.
- Vlastimil Klíma (KNZ, CZ): *SHA-3 And Lightweight Cryptography*.
- Michal Šrámka (STU Bratislava, SK): *Achieving Privacy of Shared Information: Crypto & Beyond*.
- Klaus Schmech (Book author, Germany): *Cracking Enigma Messages from WW2*.

Detailed information, including registration guidelines, will be available in due course on workshop web pages: <http://mkb.buslab.org>.

Instructions for Authors

The program committee will accept submissions targeting cryptanalysis, cryptography, security applications of cryptography and other related areas. Proposals should be of 5-15 pages and formatted for anonymous evaluation. Word and LaTeX templates for submissions are also available from the workshop web: <http://mkb.buslab.org>. Submissions can be written in Czech, Slovak, or English.

Submissions should be mailed to [matyas AT fi.muni.cz](mailto:matyas@fi.muni.cz), and clearly marked with Subject "SantaCrypt 2012". The final deadline for the submissions is *1st October 2012*. Submissions will be evaluated by the program committee and authors will be informed about the evaluation results by *29th October*. Camera-ready versions for the workshop proceedings have to be delivered by *12th November*.

Important Dates

Submission deadline: 1st October, 2012
Acceptance/rejection notification: 29th October, 2012
Camera-ready format: 12th November, 2012
Workshop: 29th – 30th November, 2012



Program Committee

Dan Cvrček, Smart Architects, UK
Otokar Grošek, STU, Bratislava, SK
Jan Krhovják, Cepia Technologies, CZ
Vašek Matyáš, FI MU, Brno, CZ – Chair

Zdeněk Říha, FI MU, Brno, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavel Vondruška, Telefónica O2 & UK, CZ