

Call for Papers SantaCrypt 2007

6 – 7 December, 2007, Prague, Czech Rep.
<http://www.buslab.cz/mkb>

Intro

Santa's Crypto Get-Together (SantaCrypt) started in December 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. ;-)

There will be five invited lectures:

- Willi Meier (Fachhochschule Nordwestschweiz): Design and analysis of eSTREAM candidates.
- Claudia Diaz (KU Leuven): Observable Steganographic File Systems.
- Vlastimil Klíma (Prague, CZ) about the recent advances in hash function research.
- Zdeněk Říha (Brno, CZ and Ispra, Italy) about crypto mechanisms in e-passports.
- Pavel Vondruška (Telefónica O2, Prague, CZ) about historical aspects of cryptology.

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

Instructions for Authors

The program committee will accept submissions targeting cryptanalysis, applied cryptography, security applications of cryptography and other related areas. Proposals should be of 5-15 pages and formatted for anonymous evaluation (no names of authors or apparent references). Word and LaTeX templates for submissions are also available from the workshop web: <http://www.buslab.cz/mkb>. Submissions can be written in Czech, Slovak, or English.

Submissions should be mailed to matyas AT fi.muni.cz. The final deadline for the submissions is 2nd October 2007. Submissions will be evaluated by program committee and authors will be informed about the evaluation results by 23rd October. Camera-ready versions for the workshop proceedings have to be delivered by 20th November, together with short (50-100 words) biographies of authors.

Important Dates

Submission deadline:	2 nd October, 2007
Acceptance/rejection notification:	23 rd October, 2007
Camera-ready format:	20 th November, 2007
Workshop:	6 th – 7 th December, 2007

Program Committee

Petr Hanáček, FIT VUT in Brno, Czech Rep.
Vašek Matyáš, FI MU, Brno, Czech Rep. – Chair
Tomáš Rosa, eBanka, Praha, Czech Rep.
Luděk Smolík, FI MU, Brno, Czech Rep.
Martin Stanek, FMFI UK, Bratislava, Slovakia
Jiří Tůma, MFF UK, Praha, Czech Rep.
Jozef Vyskoč, VaF, Bratislava, Slovakia