The 9th Central European Conference on Cryptography
Třebíč 23.-26.6.2009

THIRD & FINAL ANNOUNCEMENT

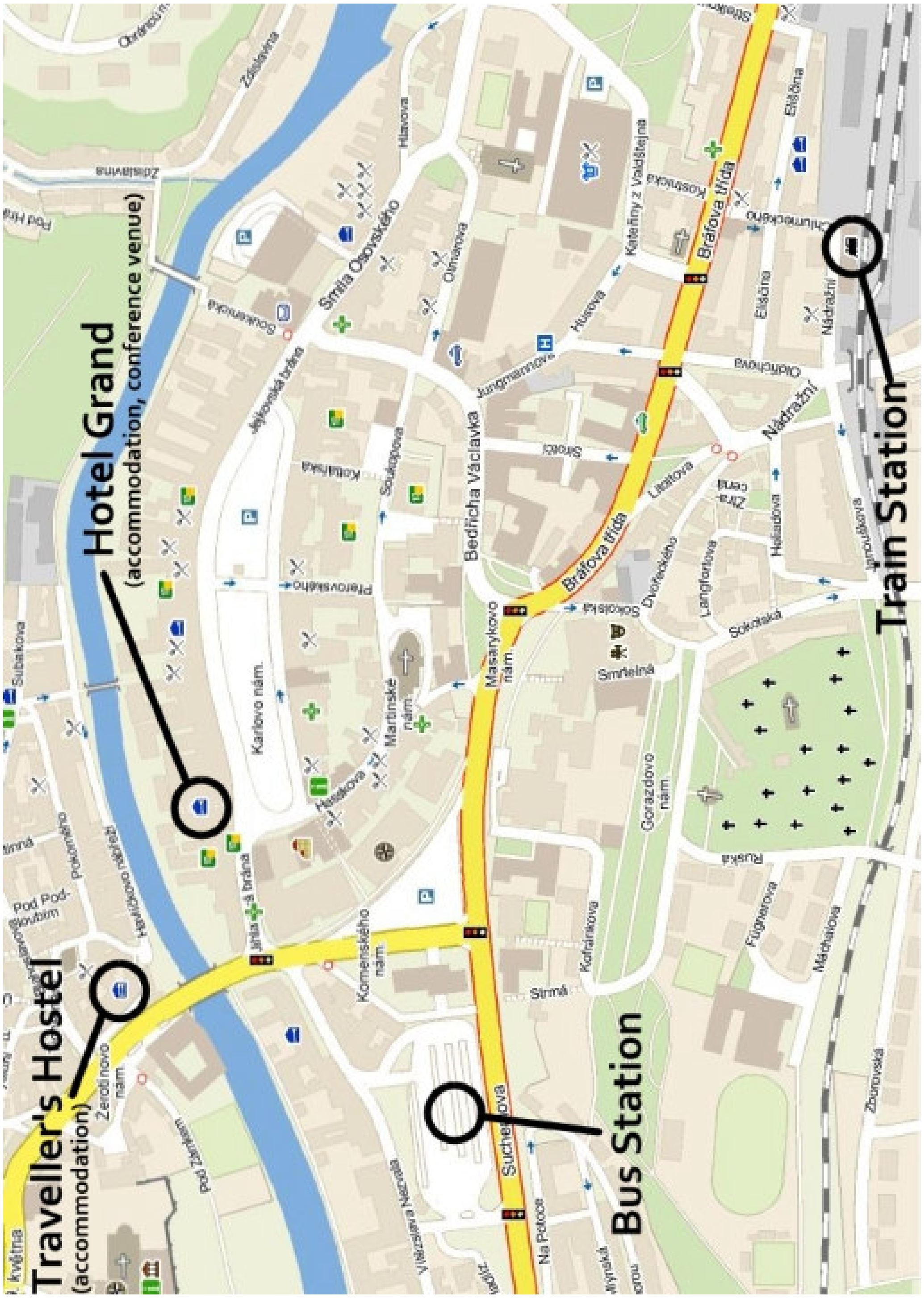
Dear Colleague,

We would like to invite you to participate on the **9th Central European Conference on Cryptography – CECC09 – Třebíč'09.** The conference is devoted to all aspects of the theory and applications of cryptography. It will take place in Třebíč (Czech Republic) from June 23-26, 2009. Třebíč, a marvelous city with a rich history reflected through many UNESCO protected monuments and surrounded by a beautiful landscape of the Czech-Moravian Highlands.

The Conference is organized by **Brno University of Technology** with the cooperation of Institute of Computer Science of the Academy of Sciences of the Czech Republic and is under the auspices of Prof. **Miroslav Doupovec**, Dean of the Faculty of Mechanical Engineering, Brno University of Technology and Mr. **Ivo Uher**, Major of City Třebíč.

The conference venue is the Congress Hall of the **Hotel Grand, Třebíč.**

City Map



Hotel Grand
(accommodation, conference venue)
Traveller's Hostel
(accommodation)
Bus Station
Train Station
Bráfova třída
Bedřicha Václavka
Karlovo nám.
Martinské nám.
Masarykovo nám.
Komenského nám.
Gorazdovo nám.
Žerotínovo nám.
Jungmannova
Nádražní
Sokolská
Smrtelná
Suchého
Strmá
Ruská
Fügnerova
Máchalova
Zborovská
Oldřichova
Eliščina
Husova
Smila Osovského
Soukenická
Havlíčkovo nábřeží
Vítězslava Nezvala
Na Potoce

Invited Speakers

The Program Committee is pleased to announce that the following speakers have accepted the invitation to deliver a plenary lecture:

Pierrick Gaudry (CNRS - LORIA, Nancy, France): *Searching a Secure Genus 2 Curve with Small Parameters over a Prime Field*

Tor Helleseth (The Selmer Center, Department of Informatics, University of Bergen, Norway): *Attacks on the Filter Generator and Nonlinear Combiner Generator*

Michael J. Jacobson, Jr. (Department of Computer Science, University of Calgary, Canada): *Cryptographic Aspects of Real Hyperelliptic Curves*

Alexander Kholosha (The Selmer Center, Department of Informatics, University of Bergen, Norway): *m-sequences with Good Cross Correlation for Communications and Cryptography*

Renate Scheidler (Department of Mathematics and Statistics, University of Calgary, Canada): *Efficient Divisor Reduction on Hyperelliptic Curves*

Igor Semaev (The Selmer Center, Department of Informatics, University of Bergen, Norway): *Multiple Side Equations over Finite Fields*

Rainer Steinwandt (Center for Cryptology and Information Security (CCIS) at Florida Atlantic University, USA): *Violating Key Separation: On Using One Secret Key for Two Purposes*

Recommended travel

If you intend to come by plane, we recommend to come via Vienna. We **shall organize a complimentary Conference shuttle transport from Vienna Airport to Třebíč** at June, 22 (Monday). Please contact us **as soon as possible** if you are interested in using this service.

Accommodation

The accommodation will be reserved in **Hotel Grand in Třebíč**, the venue of all conference activities, where a block of rooms is reserved for conference participants at a reduced rate (single room cca 53 EUR per night). The low budget alternative is the Traveller's hostel which is located in the near-by Jewish Quarter (from 10 EUR per bed in more bedded rooms). One of these two possibilities you can indicate in the registration form and we arrange your accommodation.

Registration, fees, deadlines

Please **register** on the conference web pages

http://conf.fme.vutbr.cz/cecc09

or contact us directly with your questions about the conference by e-mail cecc09@fme.vutbr.cz

The conference fee is **170 EUR** (or 4800 Czech Crowns) **if you send the money on our account before the standard registration deadline May, 20th.**

Late registration

is possible until **June, 20th.** Then the conference fee is **200 EUR** (or 5600 Czech Crowns).

Conference Talks

The participants of the conference are invited to contribute to the program of the conference by original research papers on all aspects of cryptography . The expected length of a contributed talks is twenty five minutes, though we will also try to accommodate talks of other length if required.

In the affirmative case please fill in the title and the abstract of your talk in the prepared on-line form on the conference web site.

Proceedings

The proceedings of the conference will be published as a special issue of the journal **Tatra Mountains Mathematical Publications**.

Social Program

We prepare interesting social program: a guided sight-seeing walking tour of Třebíč´s sites on the UNESCO World Heritage list formed by the Jewish Quarter, the old Jewish cemetery and the Basilica of St Procopius in Třebíč, witnesses of the co-existence of Jewish and Christian cultures from the Middle Ages to our days; an organized coach excursion to Dukovany Nuclear Power Plant with a short stop on the shore of lovely Dalešice Dam – this trip will end by a visit of the near-by picturesque Dalešice Brewery where the beer is brewed in accordance with old brewery rules and visit the in-house Brewery restaurant with typical Czech cuisine.

Post-conference facultative full day trip (June, 27 – Saturday) is also planned (UNESCO Town Telč, etc.). The trip will take place only if a sufficient number of participants join.

See You in Třebíč.

Štefan Porubský
For Program Committee

Miroslav Kureš
For Organizing Committee