About Cepia

• Small research company
• Started operation 3\textsuperscript{rd} January 2009
• Located in Brno (Platinium at Veveri)
  – Secure offices for 12 people over 2 floors + meeting rooms and reception
  – Own ICT with high level of security for own research and production
  – Very comfortable working environment for staff
What we do?

• Main focus on developing crypto analytical systems for governmental customers
  – Strong focus within research activities
  – Maintaining high academic standards for our staff

• Building a generic processing platform for cryptanalysis
  – State-of-the-art of used components/technology
  – Prototype FPGA processing unit
Current and future projects

• Time-memory Trade-off (TMTO) attacks
  – A5/1, A5/2, A5/3 & Kasumi, GEA1/2, GMR1/2, etc.
• High Performance Computing (HPC)
  – Building a generic platform, HW/SW co-design
  – Cryptanalysis, financial analysis
• HW assisted password crackers
• Proximity systems security
  – DESfire, Keeloq, etc.
Why work for Cepia?

- Research in cryptology, information security and signal/protocol processing
- Allowing employees to publish results
- Ensuring employees have time to keep up to date in their fields of expertise
- Very high education level among colleagues
- Competitive salaries
Who are we looking for?

• Master or doctoral graduates in the fields of:
  – Number theory, algebra, statistics and probability
  – Cryptography and communication/IT security
  – VHDL, GPU and DSP algorithms design and programming

• Ability to think out-side ‘the box’ & to consume new ideas quickly

• Work in international teams
Typical roles

• Research:
  – Feasibility studies
  – Construction of models
  – Design of innovative algorithms
  – Large scale testing

• Implementation:
  – C/C++ programming
  – Perl/scripting in general
  – VHDL/GPU/DSP programming
  – HW/SW co-design

Pushing hardware to the maximum
Topics of theses for Autumn 2012

- Forensic analysis of HDDs/SSDs and common file-systems
  - Creating of a several analytical utilities for OS Linux (in C/C++)
- GPU accelerated encryption/decryption of satellite communication
  - Crating of fast GPU-based implementations of cryptographic algorithms GMR-1 and GMR-2
  - Attacking GMR by using GPU acceleration
Competitions

• Best Bachelor/Master thesis in IT security and cryptology
  – In cooperation with: TNS
  – Deadline for applications: 31.5.2012
  – Awards: Up to 30K CZK for all winners

• Competition for talented students at FI
  – In cooperation with: TNS, Ysoft, Lexical Computing
  – Awards: Paid working positions in several laboratories at FI MU
Thank you for your attention