About Cepia

• Small research company
• Started operation 3rd January 2009
• Located in Brno
• Mother company in Geneva
• Solid investors
• Dedicated to building local and national partnerships
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
  – Dedicated to building bleeding edge systems

• Building a generic processing platform for cryptanalysis

• Developing data/signal acquisition systems to mate with our crypto analytical systems
Main focus

• Use 90 % of our time in find out what is possible to do, and the remaining 10 % of the time to figure out how to do it
  – Possible due to strong partnerships nationally and internationally
  – Solid experience in cutting-edge implementation of large scale systems
  – Customers pay for solutions that work, not fancy wrapping
Current and future projects

• Time-memory Trade-off (TMTO) attacks
  – A5/1, A5/2, A5/3 & Kasumi, GEA1, GEA2, etc.
• High Performance Computing (HPC)
  – Building a generic platform, HW/SW co-design
  – Cryptanalysis, radio-telemetry, financial analysis
• HW assisted password crackers
• Proximity systems security
  – Desfire, Keeloq, etc.
Why work for Cepia?

• Bleeding edge research into 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
Thank you for your attention