Cryptography on Transputer Systems

Felix Wegener
Chair for Embedded Security
Horst Görtz Institute for IT-Security / Ruhr-Universität Bochum

AI-Project No. 7
Transputer

• What is it?
  – Many-core system
  – Real parallelism
  – One thread / core

• Why does Industry care?
  – Low latency
  – Low power consumption

Taken from: http://www.transputer.net/fbooks/tarch/figure/600/fig03.png
Crypto on Transputers

- Secret key on one core
  - Power measurements can reveal it

- Share key over multiple cores
  - More secure
  - Computations based on key?
    - Adapt existing algorithms

Taken from: http://www.transputer.net/fbooks/tarch/figure/600/fig03.png
Your task

- Programm XMOS\textsuperscript{\textregistered}-transputer devices

- Understand Pseudocode in Cryptographic Papers

- Turn it into executable code
  - Language: xC (xCore extensions for C)

- Perform device-specific optimizations
Requirements / Benefits

• Who are you?
  – 2 – 3 Students
  – Bachelor’s or Master’s level

• What do you have to know?
  – Some level of C / C++ knowledge

• What are you going to learn?
  – xC (extension of C for XMOS)
  – Some crypto algorithms

• Follow-up perks?
  – SHK/WHB Jobs are available
  – Internships may be available
Organization

- Start: First Week of April
- End: Mid July

- Bi-weekly meetings

- Goal: Implement Secret Sharing

- Extended Goal: Implement Fault Detection
Contact

M. Sc. Felix Wegener
Chair for Embedded Security
Horst Görtz Institute for IT-Security / Ruhr-Universität Bochum
ID 2 / 625
felix.wegener@rub.de