HPC for Security, Privacy, Cryptography, and Trust

II Encontro do CTC - Comitê Técnico-Científico da RENASIC

Fábio Borges

Laboratório Nacional de Computação Científica (LNCC)
Coordenação de Sistemas e Redes (CSR)

Table of Contents

Outline

Crypto Server

Hardware

TECHNISCHE UNIVERSITÄT DARMSTADT

- Processor Intel(R) Xeon(R) CPU E5-2630
- 32GB Memory per host
- 1 host for login
- 2 hosts with 2 Intel Xeon Phi and Coprocessor 5110P
- 3 hosts with 2 NVIDIA Tesla K20m

Crypto Server

Software

- Main host: crypto.lncc.br
- Operating System: CentOS 6.4
- OpenCL-1.2
- CUDA Toolkit 7.0
- Intel Cluster Studio 2013
- Openmpi 1.5

Crypto Server

Measurable Results

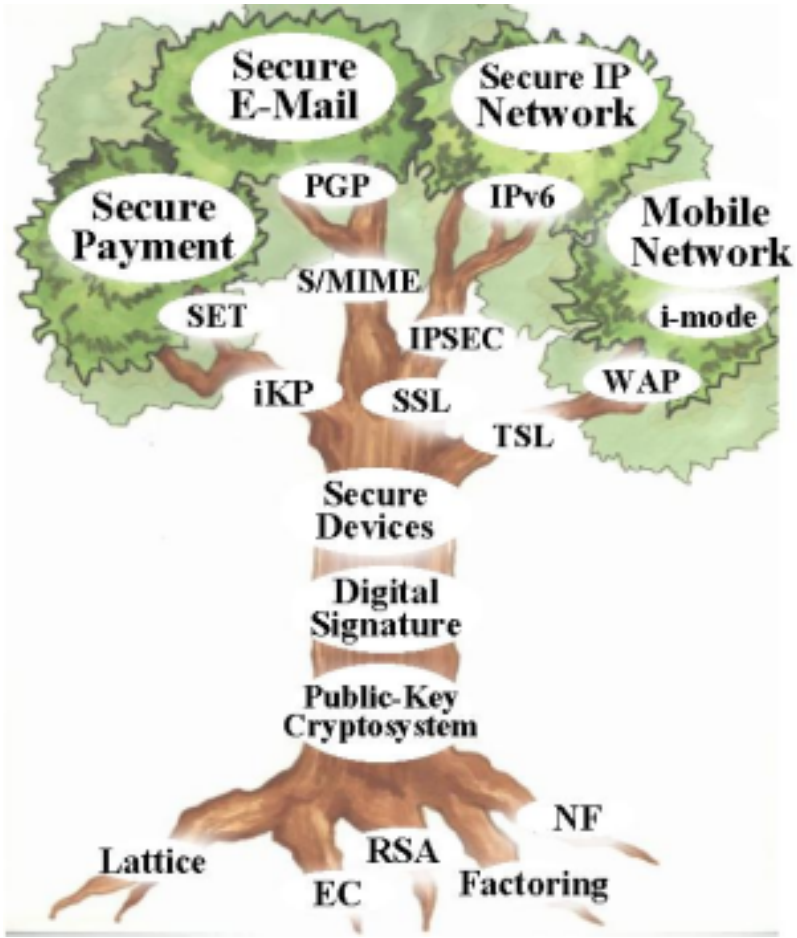
- a conference paper accepted in a journal
  - P. C. S. Lara ; A.B. Leão ; R. Portugal
  - Simulation of Quantum Walks using HPC.
- a journal paper under review
  - F. Borges; P. C. S. Lara ; R. Portugal
  - Modular Multi-exponentiation
- a master dissertation
  - Aaron Leão
- a software developed: Hiperwalk
  - http://qubit.lncc.br/qwalk/

Table of Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Security Tree

from bottom to top



Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms
- Gröbner bases

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms
- Gröbner bases
- SAT (Boolean Satisfiability Problem)

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms
- Gröbner bases
- SAT (Boolean Satisfiability Problem)
- Gaussian elimination

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms
- Gröbner bases
- SAT (Boolean Satisfiability Problem)
- Gaussian elimination
- Collision-search techniques

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms
- Gröbner bases
- SAT (Boolean Satisfiability Problem)
- Gaussian elimination
- Collision-search techniques
- Large-scale lattice reduction

Solving Problems

Reaching Thresholds

TECHNISCHE UNIVERSITÄT DARMSTADT

- Factoring
- Discrete logarithms
- Gröbner bases
- SAT (Boolean Satisfiability Problem)
- Gaussian elimination
- Collision-search techniques
- Large-scale lattice reduction
- Generalized birthday algorithms

Areas

Big Areas

- Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy
    - Homomorphic Encryption

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy
    - Homomorphic Encryption
    - DC-Nets

Alert

Applications? Differences?

Areas

Big Areas

- Security
  - Physical Security (e.g., doors)
  - Information Security
    - Malware, IDS, ...
    - Network Security
    - Host Security
  - Cryptography
    - Symmetric
    - Asymmetric
  - Privacy
    - Homomorphic Encryption
    - DC-Nets
    - ADC-Nets

Alert

Applications? Differences?

- Security

Alert

Applications? Differences?

- Security
  - Steganography

Alert

Applications? Differences?

- Security
  - Steganography
    - Old Techniques

Alert

Applications? Differences?

- Security
  - Steganography
    - Old Techniques
    - Multimedia

Alert

Applications? Differences?

Areas

Small Areas

- Security
  - Steganography
    - Old Techniques
    - Multimedia
  - Watermark

Alert

Applications? Differences?

Areas

Small Areas

- Security
  - Steganography
    - Old Techniques
    - Multimedia
  - Watermark
    - Money

Alert

Applications? Differences?

Areas

Small Areas

- Security
  - Steganography
    - Old Techniques
    - Multimedia
  - Watermark
    - Money
    - Multimedia

Alert

Applications? Differences?

Areas

Small Areas

- Security
  - Steganography
    - Old Techniques
    - Multimedia
  - Watermark
    - Money
    - Multimedia
  - Trust

Alert

Applications? Differences?

Areas

Small Areas

- Security
  - Steganography
    - Old Techniques
    - Multimedia
  - Watermark
    - Money
    - Multimedia
  - Trust
    - Reputation Systems

Alert

Applications? Differences?

Areas

Small Areas

- Security
  - Steganography
    - Old Techniques
    - Multimedia
  - Watermark
    - Money
    - Multimedia
  - Trust
    - Reputation Systems
    - Trust Models

Alert

Applications? Differences?

Table of Contents

Conclusions

- Beyond the state of the art

Conclusions

- Beyond the state of the art
- More hardware! (Always)

Conclusions

- Beyond the state of the art
- More hardware! (Always)
- More hard-workers! (Good students)

Conclusions

- Beyond the state of the art
- More hardware! (Always)
- More hard-workers! (Good students)
- I just arrived in a bad moment (Infrastructure)

Thank You!

All comments and suggestions are welcomed.

Contact: borges@lncc.de