Research at LCA-UNICAMP

Ricardo Dahab
Applied Cryptography Lab (LCA)
Unicamp

Crypto at LCA-UNICAMP

Fast elliptic curve arithmetic

- formula optimizations at finite field level as well as elliptic arithmetic.
- different field element base representations.
- hardware customization

Crypto at LCA-UNICAMP

Cooperation with code-optimization group

- Márcio Juliato, Guido Araujo, Julio López and Ricardo Dahab. *A Custom Instruction Approach for Hardware and Software Implementations of Finite Field Arithmetic over GF(2^163) using Gaussian Normal Bases.* Journal of VLSI Signal Processing Systems, 47(1), 2007.

Speed up of crypto functions through replacement of software by custom instructions implemented in hardware.

Crypto at LCA-UNICAMP

Fast bilinear pairing computation

- taking advantage of particular field sizes
- formula improvement

Applications to sensor networks

Crypto at LCA-UNICAMP

Proving crypto protocols correct

- finding attacks in fair exchange protocols using strand spaces.
- provable security of signature protocols by reduction to known hard problems

NonCrypto at LCA-UNICAMP

But security related:

- Watermarking vector maps with bitmaps. Ongoing work aims at public (non-dependent on the original map) verification.
- Security of the Brazilian Federal Revenue Service fraud detecting software systems running in potentially hostile environments.
- Introduction of secure programming practices in the development of above system.

Other projects at LCA

- A complete software and hardware solution for digital certificate management for the academic community in Brazil.
- Sponsored by RNP (Rede Nacional de Pesquisa)
- Products: certificate management system, HSM (software and hardware), prototype applications.
- With UFSC and UFMG

Just started

- A crypto library incorporating side-channel attacks prevention techniques as well as energy-aware requirements.
- Fast implementation of post-quantum crypto methods.

Thank you