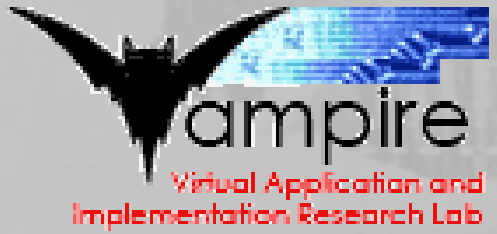
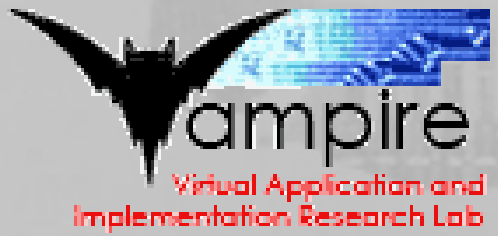


ECRYPT

Special-Purpose Hardware for Attacking Cryptographic Systems (SHARCS '09)

www.sharcs.org

Lausanne, Switzerland
September, 09.& 10.



SHARCS'09

www.sharcs.org

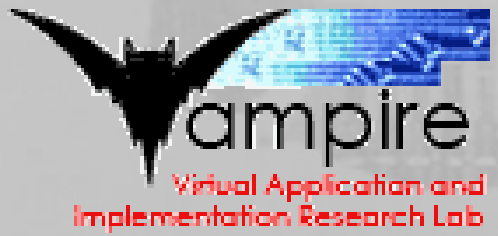
ECRYPT

Topics

- index calculus algorithms
- elliptic curve based schemes
- lattice based schemes
- hidden field equation based schemes
- specific block and stream ciphers
- algebraic cryptanalysis and SAT solvers
- hash functions, particularly SHA-1 and SHA-2

PC members

- Daniel J. Bernstein
- Roger Golliver
- Tim Güneysu
- Marcelo E. Kaihara
- Tanja Lange (co-chair)
- Arjen Lenstra (co-chair)
- Christof Paar
- Jean-Jacques Quisquater
- Eran Tromer
- Michael J. Wiener

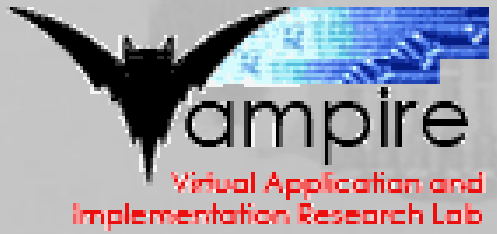


SHARCS'09

www.sharcs.org

Implementation oriented topics:

- analog and optical devices for cryptanalysis
- novel VLSI technologies for cryptanalysis
- reconfigurable computing for cryptanalysis
- clusters of standard computers for cryptanalysis
- clusters of GPUs or Playstation-3s for cryptanalysis
- routing protocols and other low-level tools
- models and evaluation techniques for special-purpose computing
- lower bounds for physical implementations of cryptanalytic algorithms



SHARCS'09

www.sharcs.org

- Deadlines
  - May 09, submission of abstract
  - May 16, submission of paper
  - July 06, notification of acceptance or rejection
  - August 19, revised version of accepted papers
  - September 09 & 10, SHARCS workshop