Vampire
Virtual Application and
Implementation Research Lab

ECRYPT

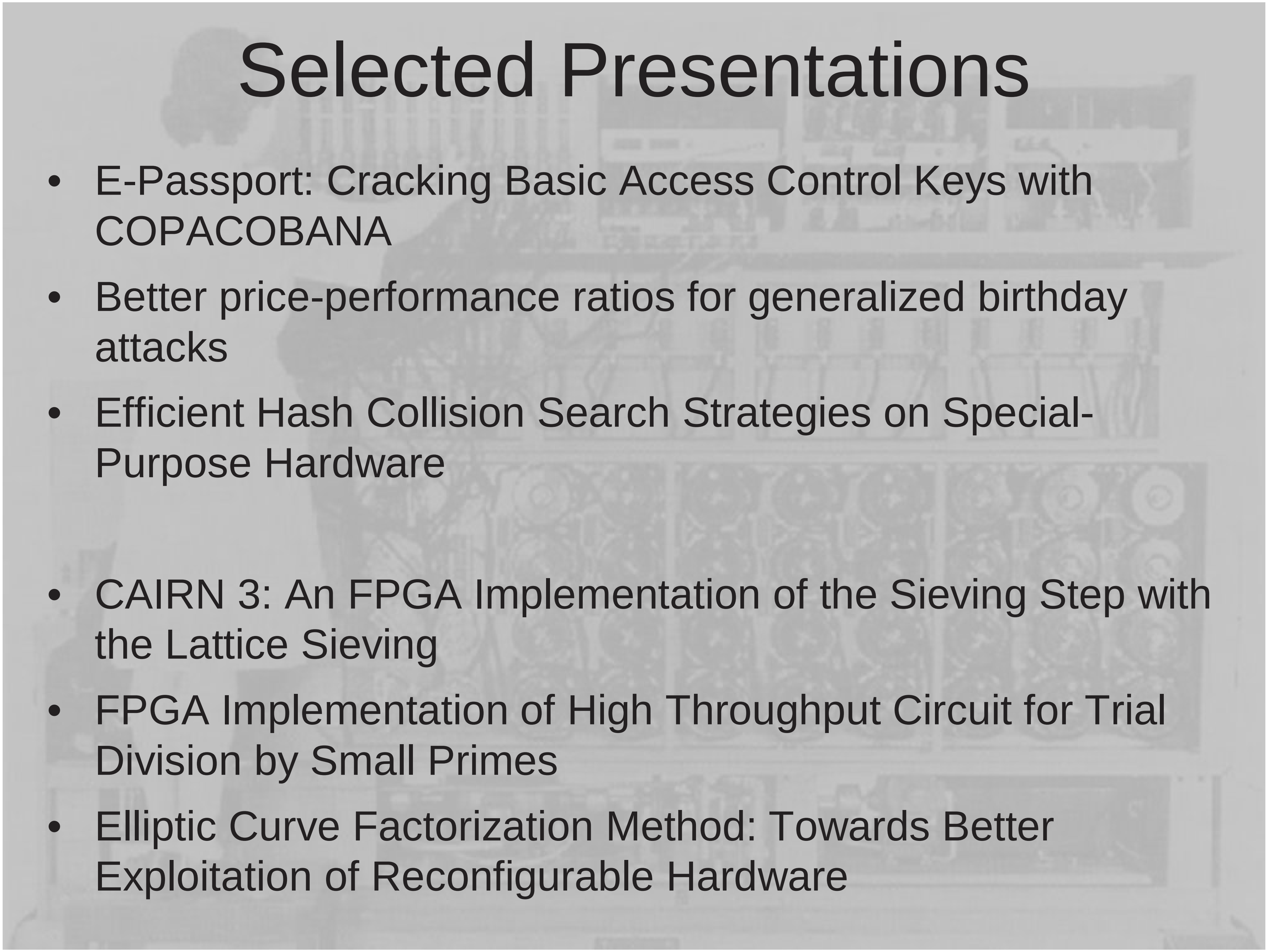
SHARCS 07
Special Purpose Hardware for Attacking Cryptographic Systems
www.sharcs.org

September 9 -10, 2007 in Vienna
(in conjunction with CHES)

SHARCS 2007

- 3rd SHARCS Workshop
  - SHARCS 05: Paris
  - SHARCS 06: Cologne
- Invited Speakers
  - Neil Costigan
  - James Hughes
  - Christian Rechberger
- Program Committee
  - Daniel J. Bernstein
  - James Hughes
  - Tanja Lange
  - Arjen Lenstra
  - Christof Paar
  - Rainer Steinwandt
  - Eran Tromer
- Organized by ecrypt – European Network of Excellence in Cryptograpy

Selected Presentations



- E-Passport: Cracking Basic Access Control Keys with COPACOBANA
- Better price-performance ratios for generalized birthday attacks
- Efficient Hash Collision Search Strategies on Special-Purpose Hardware

- CAIRN 3: An FPGA Implementation of the Sieving Step with the Lattice Sieving
- FPGA Implementation of High Throughput Circuit for Trial Division by Small Primes
- Elliptic Curve Factorization Method: Towards Better Exploitation of Reconfigurable Hardware