vampire
Virtual Application and Implementation Research Lab

ECRYPT

Special Purpose Hardware for Attacking Cryptographic Systems SHARCS '07

Vienna
September 9-10, 2007

hgi
Horst-Görtz Institut für IT Sicherheit

TU/e

ECRYPT

Network of Excellence in Cryptology
IST-2002-507932

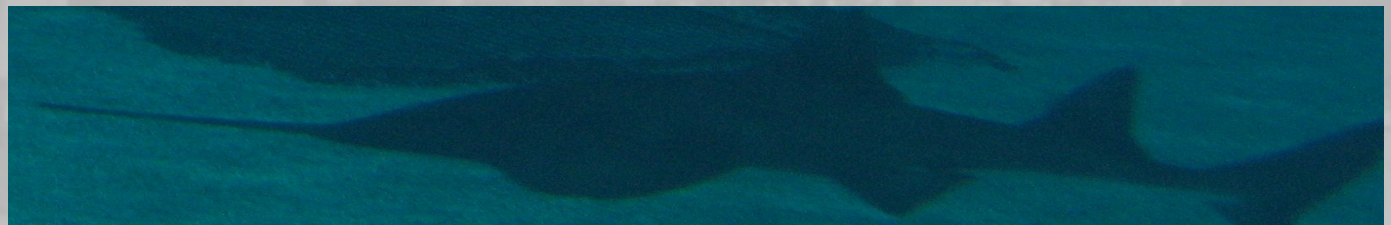
- European Network of Excellence in Cryptology
- EU FP6-IST programme
- February 2004 - July 2008
- Academia: 23 & Industry: 9
- 14 countries

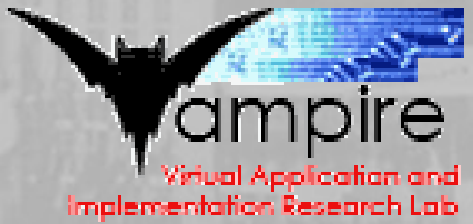
ECRYPT

- STVL Symmetric Crypto
- AZTEC Asymmetric Crypto
- VAMPIRE Implementat.
- PROVILAB Protocols
- WAVILA Watermarking

Vampire
Virtual Application and Implementation Research Lab

- VAM 1 **Software**
- VAM 2 **Hardware**
- VAM 3 **Sidechannel**





Vampire public page

- http://www.rub.de/itsc/tanja/vampire

ECRYPT public page

- http://www.ecrypt.eu.org

Contains

- AES lounge
- Side-channel analysis lounge

Brief History of SHARCS

SHARC 2005

Paris, Februar 2005

SHARC 2006

Cologne, April 2006

SHARCS 2007

Programm Committee

- Daniel J. Bernstein
- James Hughes
- Tanja Lange
- Arjen Lenstra
- Christof Paar
- Rainer Steinwandt
- Eran Tromer

SHARCS 2007

Special thanks to

- Dan Bernstein (proceedings)
- Irmgard Kühn (registration and everything else)

Progam Sunday

13:45 James Hughes: *Highly Threaded SPARC Architectures (invited talk)*

Session I: Factoring

14:45 FPGA Implementation of High Throughput Circuit for Trial Division by Small Primes

15:15 coffee break

15:45 *Elliptic Curve Factorization Method: Towards Better Exploitation of Reconfigurable Hardware*

16:15 *CAIRN 3: An FPGA Implementation of the Sieving Step with the Lattice Sieving*

16:50 new results / rump session

19:00 Dinner in the Marriott

Progam Monday

9:30 Christian Rechberger
Dedicated Collision Search

10:30 coffee break

11:00 Efficient Hash Collision Search Strategies on Special-Purpose Hardware

11:30 *Better price-performance ratios for generalized birthday attacks*

12:00 *E-Passport: Cracking Basic Access Control Keys with COPACOBANA*

12:30 lunch

14:00 Neil Costigan
The Cell processor as a cryptographic engine

15:00 Concluding Remarks (CHES Registration: 18:00)