The SHA-3 Zoo

Christian Rechberger

http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

ECRYPT II basic facts

- European Network of Excellence in Cryptology
- 4 years, started 1 August 08

- Successor of ECRYPT (2004-2008)

ECRYPT II partners

- 2 from industry: France Telecom, IBM Research
- 9 from academia: KU Leuven, ENS (Paris), EPFL (Lausanne), RU Bochum, RHUL (London), TU Eindhoven, TU Graz, Univ. of Bristol, Univ. of Salerno
- 8 countries

- 26 associate members:
  - 8 companies
  - 18 academic
- 10 additional countries

Virtual labs of ECRYPT

- Joint research organised into 3 Virtual Labs
  - SymLab Symmetric Techniques
  - MAYA Asymmetric Techniques and Protocols
  - VAMPIRE Secure and efficient implementations

Ways of working

- Workshops/Schools
- Exchange visits (internal and external)
- Joint drafting of deliverables (in meetings or via email or via web interface)
- Research retreats/brainstorming sessions (intensive 2 day meetings on a particular topic)
- Organize open competitions

The SHA-3 Zoo

Aim is to report and report on cryptanalysis results

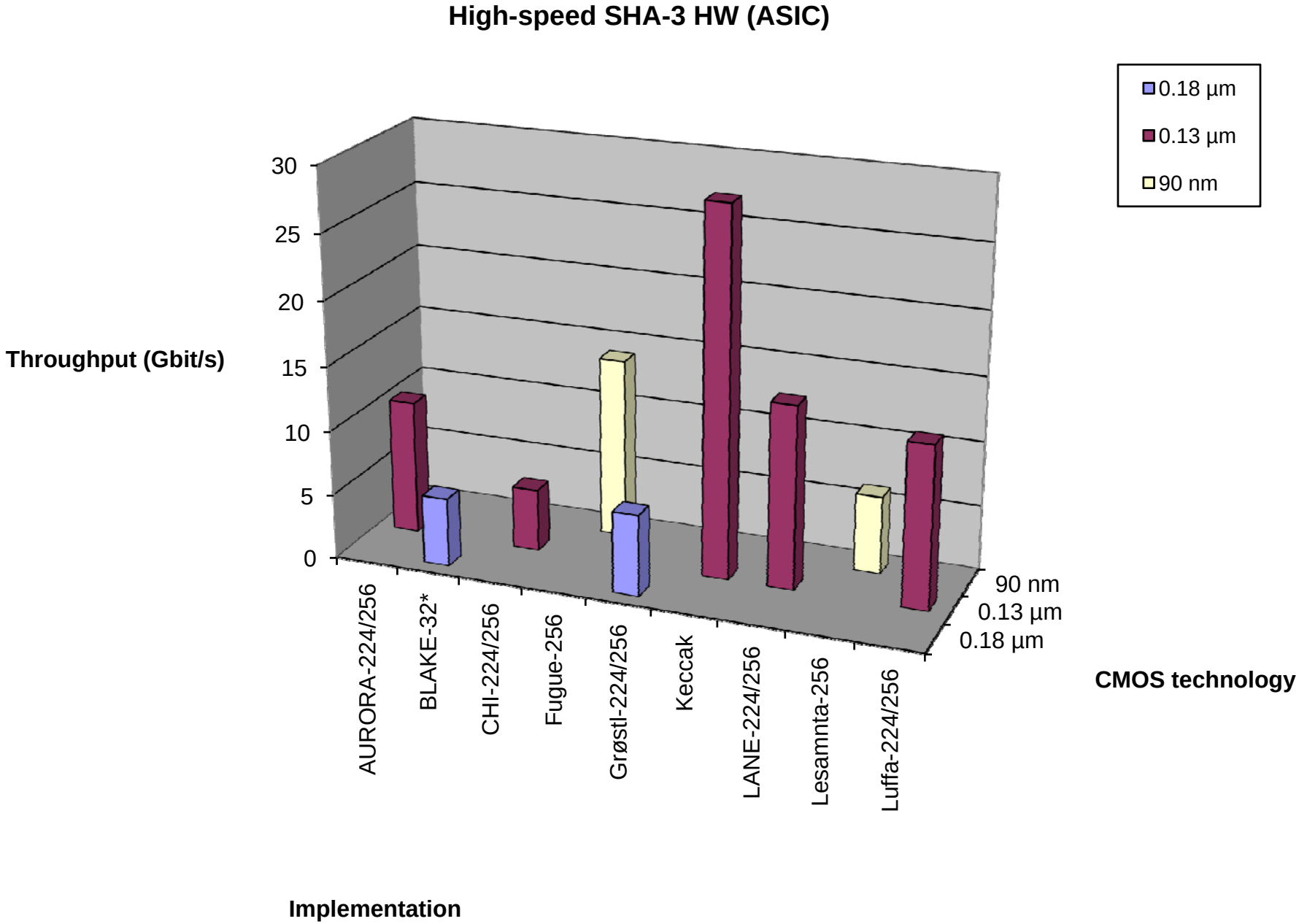
- Categories

- Overview

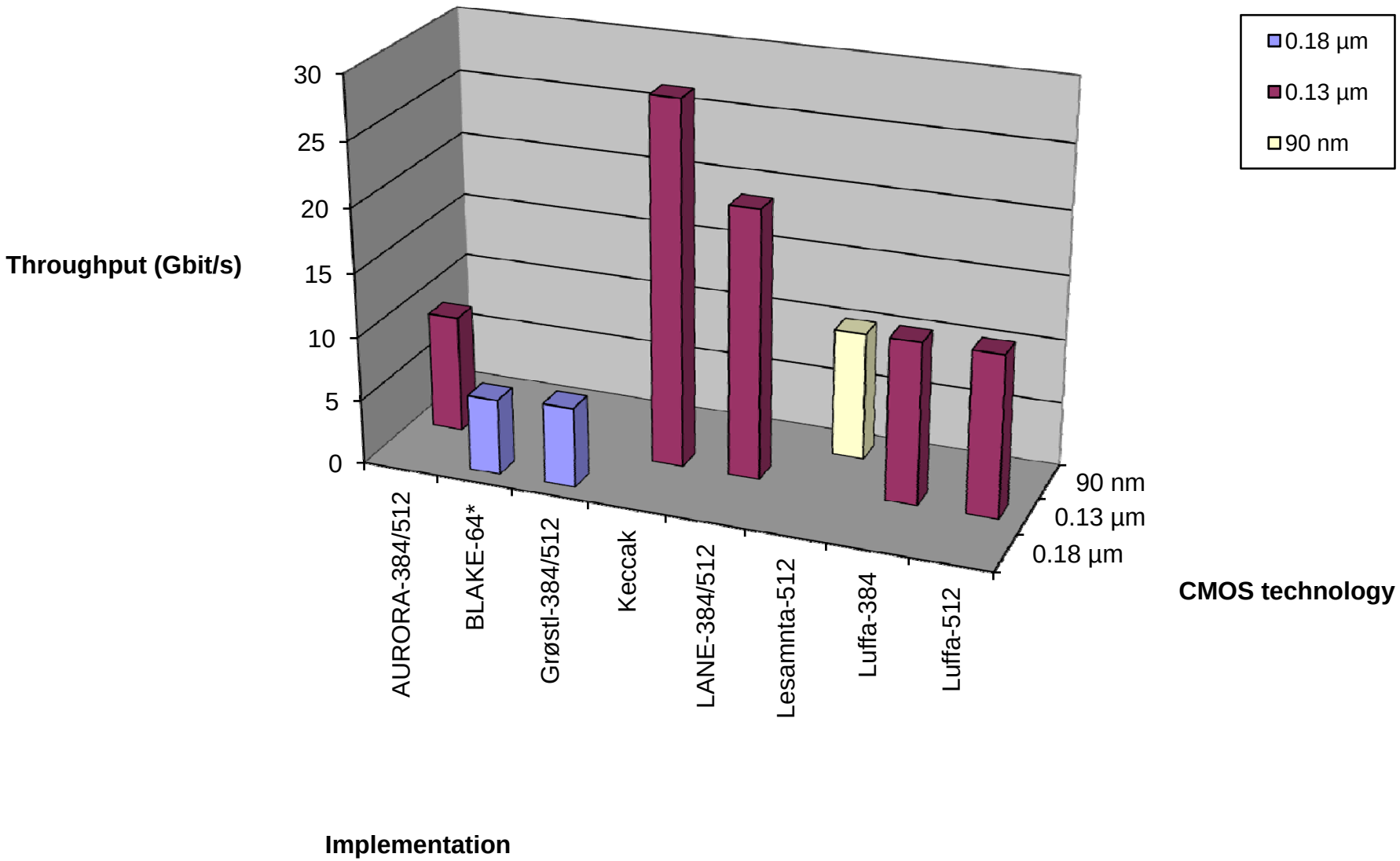
Hardware results

- Very preliminary data, only actual implementations

- http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware_Implementations


High-speed SHA-3 HW (ASIC)
0.18 µm
0.13 µm
90 nm
Throughput (Gbit/s)
30
25
20
15
10
5
0
AURORA-224/256
BLAKE-32*
CHI-224/256
Fugue-256
Grøstl-224/256
Keccak
LANE-224/256
Lesamnta-256
Luffa-224/256
Implementation
90 nm
0.13 µm
0.18 µm
CMOS technology

High-speed SHA-3 HW (ASIC)



Acknowledgements

- Thanks to the many active co-editors of the Zoo:
  - Jean-Phillipe Aumasson (FHNW & EPFL)
  - Florian Mendel (IAIK, TU-Graz)
  - Martin Schläffer (IAIK, TU-Graz)
  - Stefan Tillich (IAIK, TU-Graz)
  - Søren S. Thomsen (MAT, DTU)