Masterproef industriële ingenieurswetenschappen 2015-2016

Evaluation of CAESAR candidates on FPGA

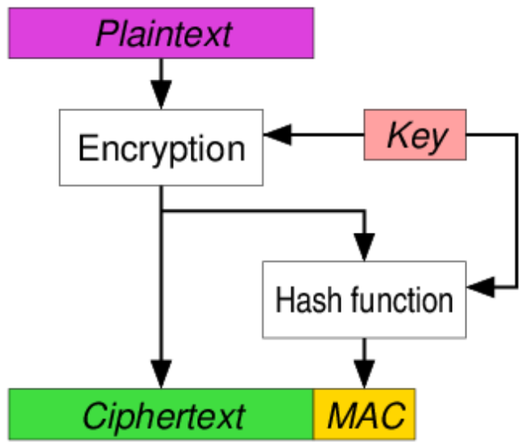
Jasper Gorissen

Master IW elektronica-ICT

Introduction

- Cryptography ➔ study of techniques to secure communication
  - Common goals in Cryptography
    - Confidentiality ➔ using key to cipher data
    - Authentication➔ using MAC
  - Both goals simultaneously ➔ Authenticated Encryption (AE)
- Goal of this Thesis ➔ Evaluating Trivia-ck, Ketje and MORUS on hardware area and speed
  - Part of CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness)

  ➔ Determine range of applications

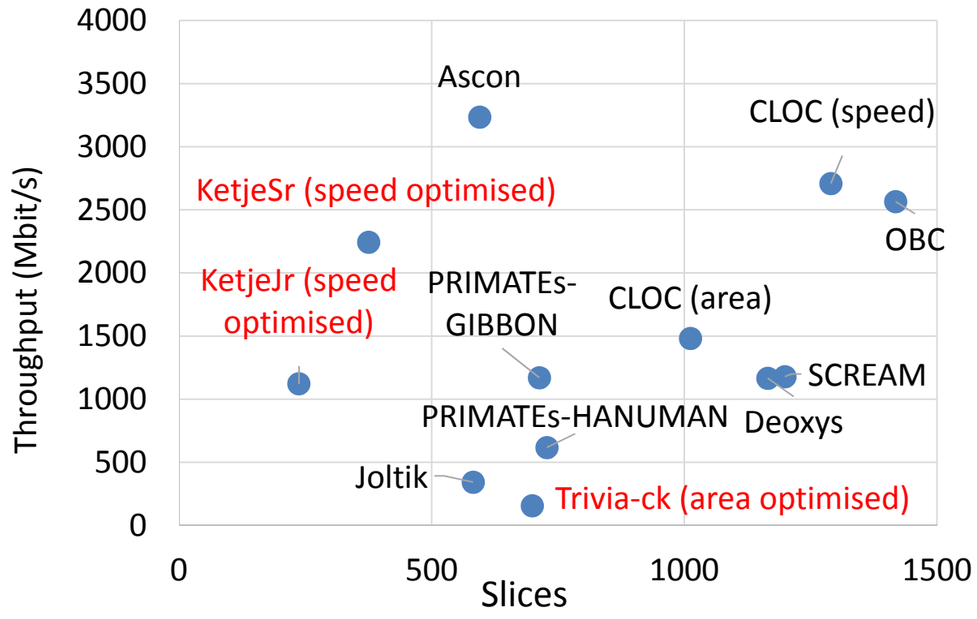


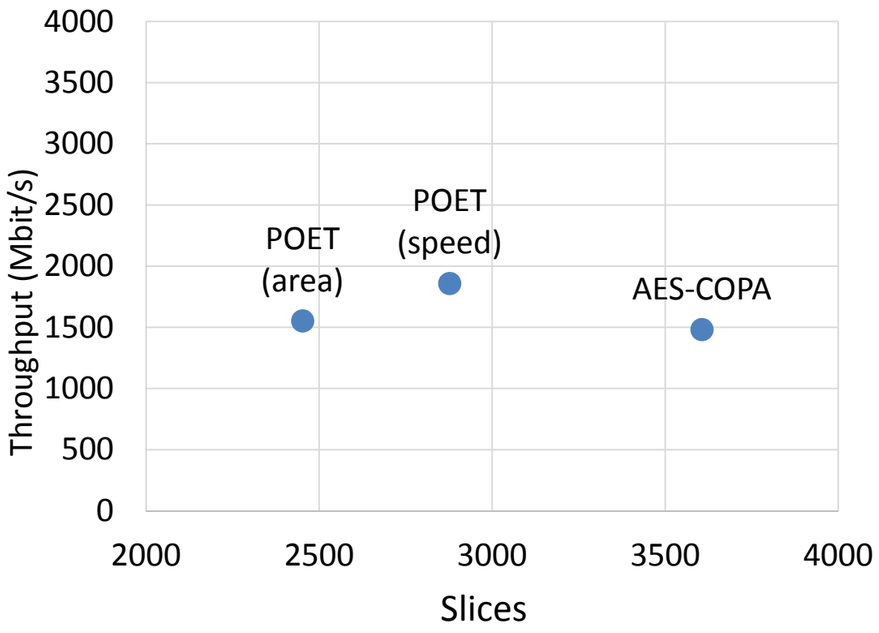
Algorithms and methods

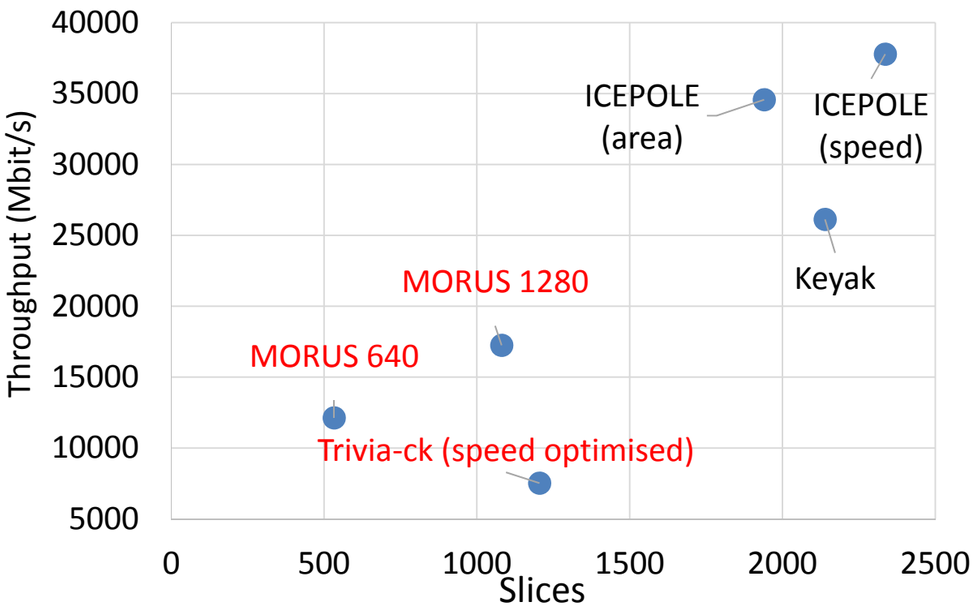
- Hardware code ➔ VHDL
- Using hardware API AEAD
- 2 optimisation strategies
  - Minimal Area
  - Maximal Speed
- FPGA results using ATHENa
- ASIC results using Design compiler

Cipher	**Trivia-ck**	**Ketje**	**MORUS**
Based on (type)	Trivium (Stream cipher)	KECCAK-f (Sponge function)	LRX (Stream cipher)
IV (bits)	128	80/128	128
Key (bits)	128	96/128	128/256
State (bits)	385	200/400	640/1280

Performance







Conclusion

- Ketje ➔ Smallest Area usage
- MORUS ➔ Excellent throughput/area ratio
- Trivia-ck ➔ High area usage/ loss of speed in multiplier

Promotoren / Copromotoren: Externe promotoren: Dr. Begül Bilgin, Dhr. Bohan Yang, Dhr. Danilo Šijačić

Interne promotor: Prof. dr. Ir. Nele Mentens

ESAT

KU LEUVEN | universiteit hasselt