State Key Lab of ASIC and System, Fudan University

A Low-Cost Cryptographic Processor for Security Embedded System

Speaker: Ronghua Lu

Xiaoyang Zeng, Jun Han, Qing Li, Lang Mai, Jia Zhao

Outline

- ***Background***
- Hardware Architecture
- Implementation Results
- Conclusions

Background

- Cryptographic algorithms are widely used in security embedded systems.

- Several algorithms are need to be implemented together in a single system.

- Cost & flexibility are as crucial as performance in these systems.

Background (Cont'd)

- Two most popular solutions for these systems:

  1) **Software**-based solutions

  Flexibility (√) Speed & Throughput (X)

  2) **SoC**-based solutions

  Flexibility (X) Speed & Throughput (√) cost (X)

- Cryptographic processors:

  1) Software-like flexibility

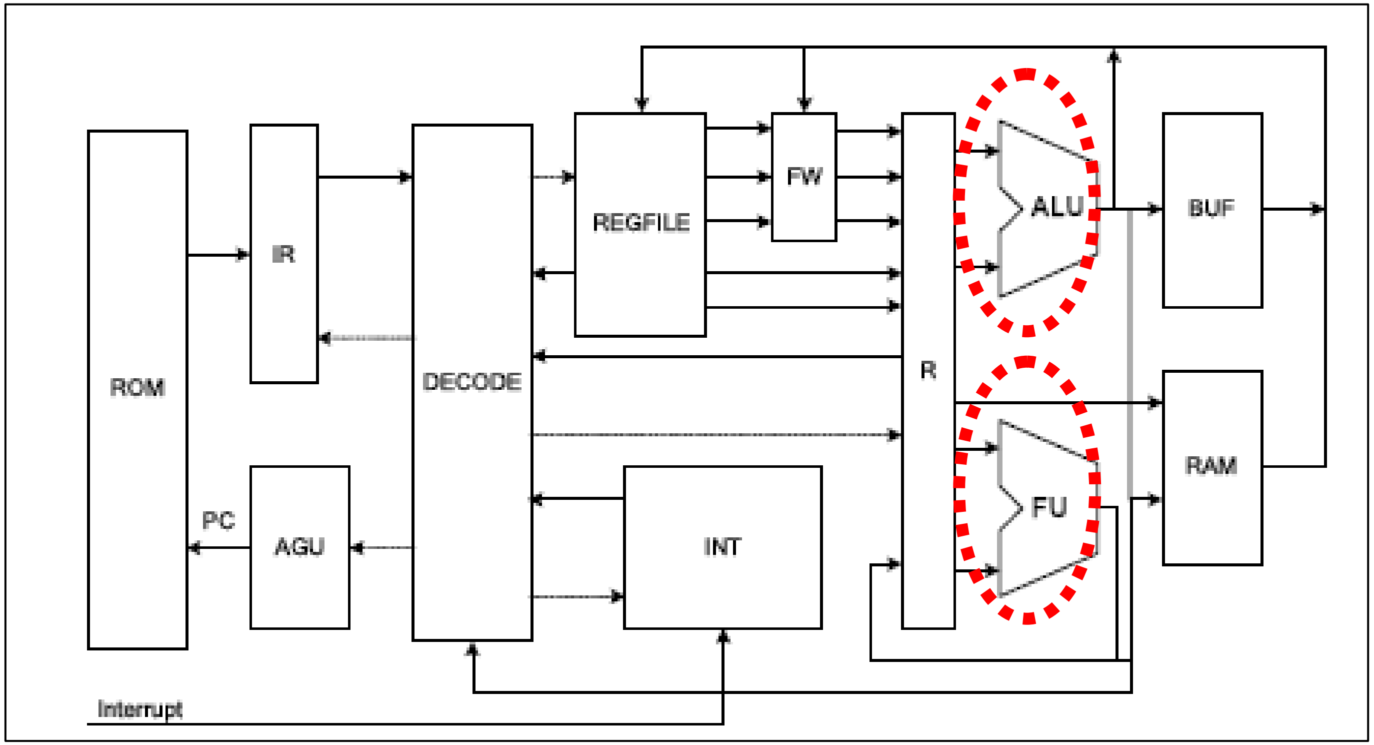
  2) Hardware-like performance

  3) Low cost

Outline

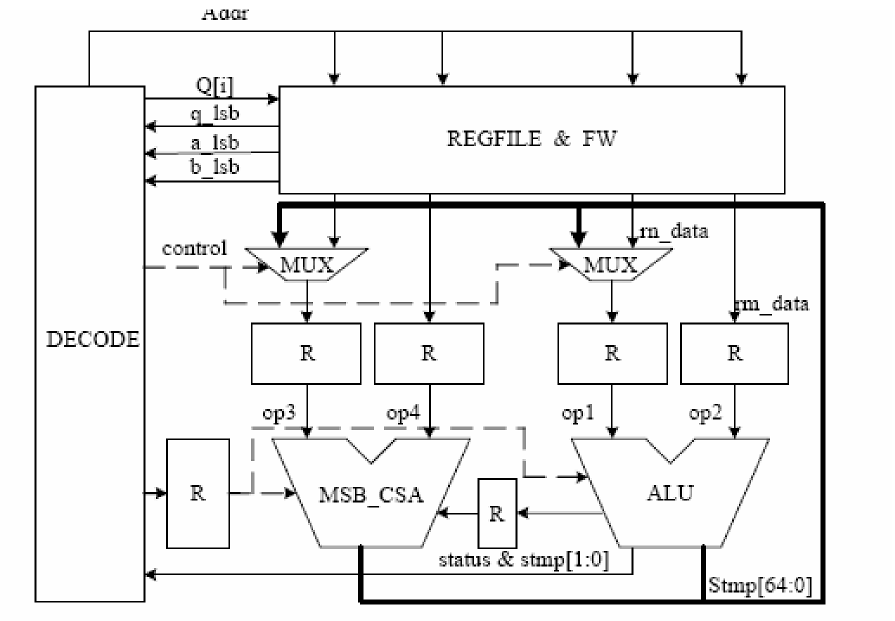
- Background
- ***Hardware Architecture***
- Implementation Results
- Conclusions

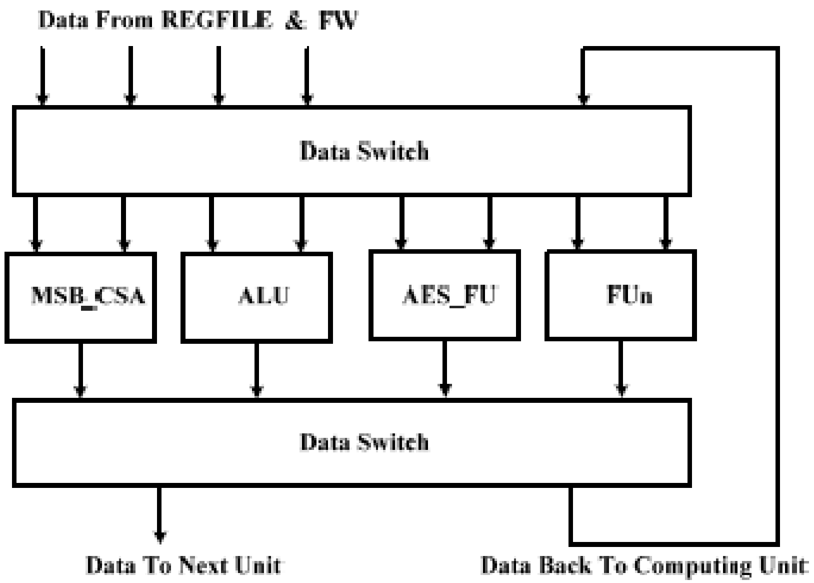
Architecture of Cryptographic Processor
(32-bit RISC Processor)



- The processor has a common 5-stage pipeline structure
- Special function units (FU) are added to speed up the execution.

Main Data Path of the Processor





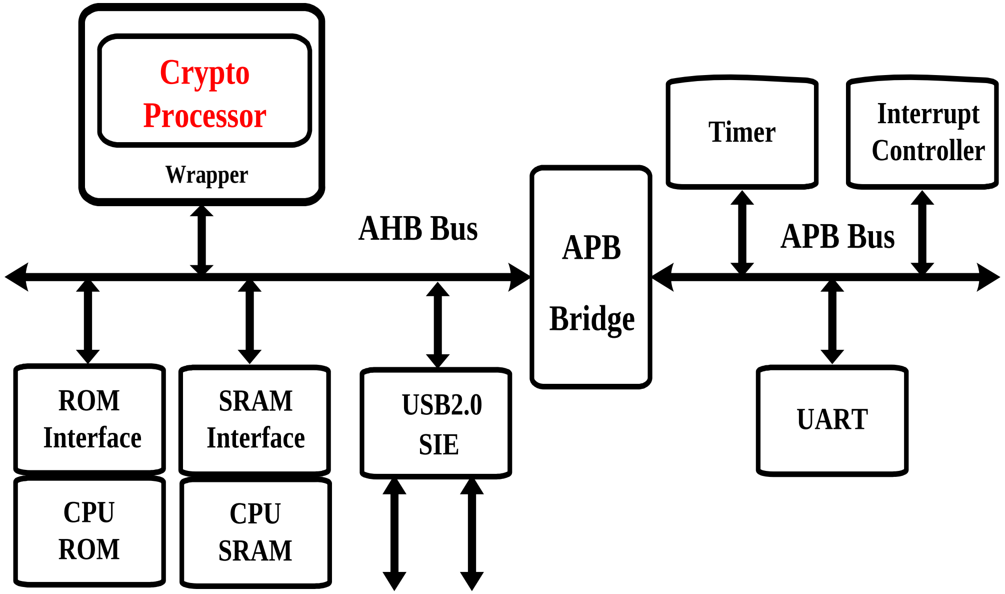
- Special purpose registers are added to help the software calculate the parameters.
- Data path is slightly modified to fit the data flow of those algorithms.
- Breaking down the algorithms & using minimum hardware to execute most complicated parts of the algorithm.

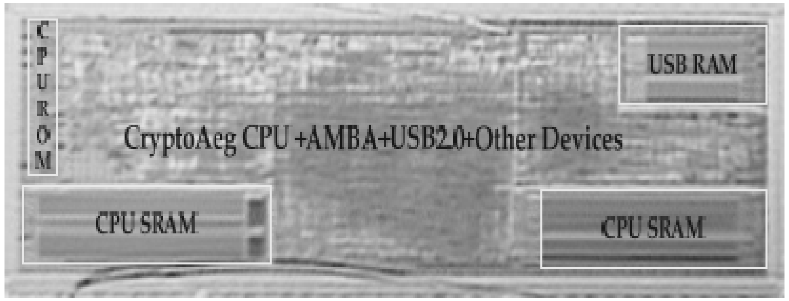
Outline

- Background
- Hardware Architecture
- ***Implementation Results***
- Conclusions

Implementation Results

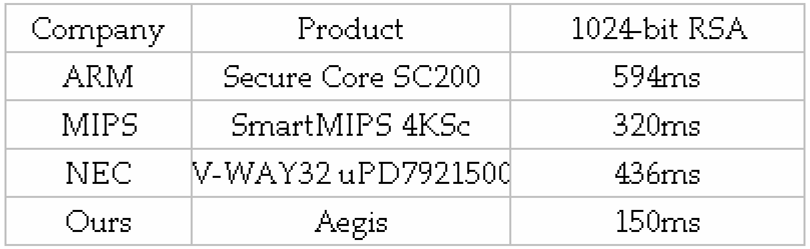
Technology (um)	0.18
Frequency (MHz)	200
Area (k-gates)	32





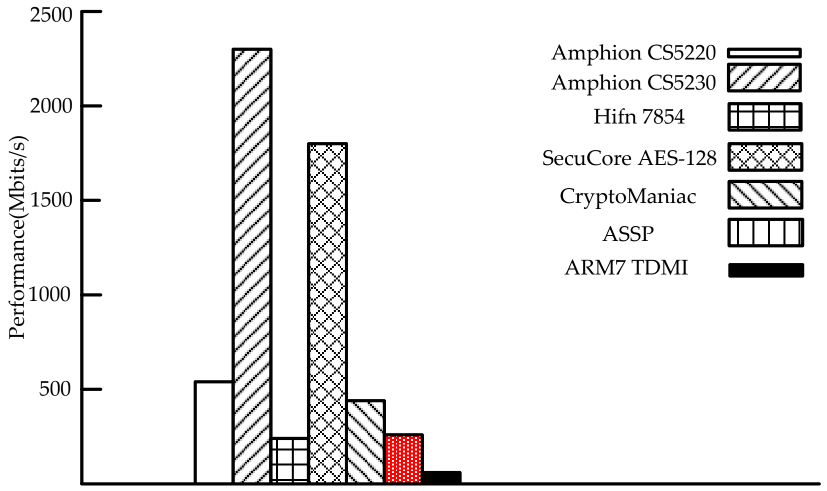
Comparison Results

RSA Performance

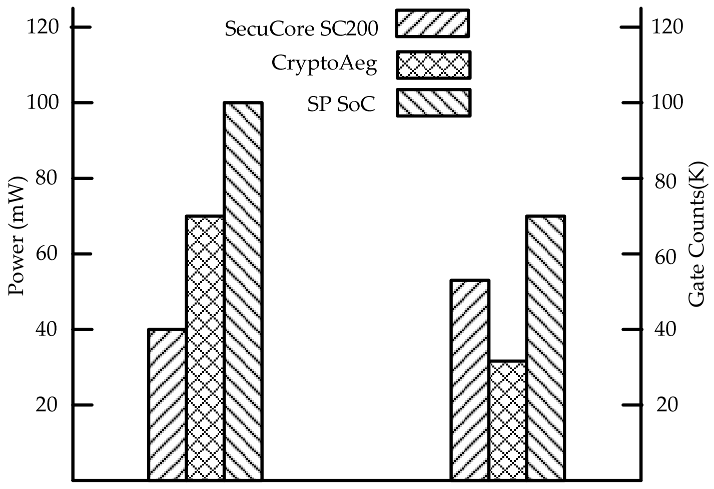


Company	Product	1024-bit RSA
ARM	Secure Core SC200	594ms
MIPS	SmartMIPS 4KSc	320ms
NEC	V-WAY32 uPD7921500	436ms
Ours	Aegis	150ms

AES Performance



Power & Cost



Conclusions

- A low-cost cryptographic processor is proposed.
- The architecture of the processor is RISC-like.
- A SoC testing platform is proposed.
- This low-cost design is very suitable for applications in security embedded systems.

Thank You!

leonrhlu@gmail.com