Supporting Cryptography on Embedded Processors: Coprocessor vs. Instruction Set Extensions

Stefan Tillich, Johann Großschädl

13th Fast Software Encryption workshop
(FSE 2006)
Rump session

Institute for Applied Information Processing and Communications (IAIK) — VLSI Group

Faculty of Computer Science
Graz University of Technology

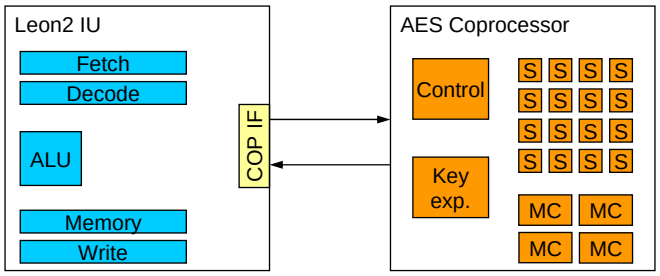
VLSI

VLSI

Cryptography on Embedded Processors

- If software implementation too slow, traditionally cryptographic coprocessors are added
- Instruction Set Extensions (ISE) for cryptography (i.e. addition of custom instructions to general-purpose processor) are an alternative approach
- ISE require less hardware and increase implementation flexibility
- ISE can also be faster than coprocessor solutions
- Case study:
  - SPARC V8-compatible Leon2 embedded processor
  - Implementation of AES with cryptographic coprocessor VS. integration of instruction set extensions

Leon2 + AES Coprocessor [1]



- Coprocessor can process one 128-bit block in 11 cycles.
- AES-128 encryption in different modes of operation supported.

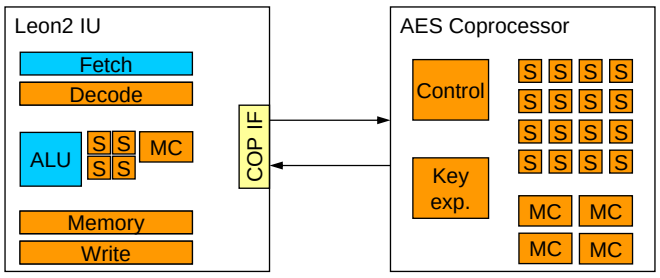
HW overhead	~ 100 %
AES-128 encryption	704 cycles*

* Including time for reading input from memory and writing output to memory.

[1] A. Hodjat and I. Verbauwhede. Interfacing a High Speed Crypto Accelerator to an Embedded CPU. In *Proceedings of the 38th Asilomar Conference on Signals, Systems, and Computers*, pp. 488–492, November 2004.

VLSI

Leon2 + Instruction Set Extensions for AES



- Extensions usable for all AES key sizes (128, 192, 256) and all modes of operation
- Support for on-the-fly key expansion

HW overhead	< 10 %
AES-128 encryption	196 cycles*

* Optimized assembly.

For comparison:

AMD Athlon 64 3500+ (64 bit, 3-way super-scalar): 175 cycles / block [2]

[2] M. Matsui. How Far Can We Go on the x64 Processors? In *Pre-Proceedings of the 16th Fast Software Encryption workshop*, pp. 488–492, March 2006.