Comparison of Hardware and Software Implementations of Selected Lightweight Block Ciphers

William Diehl, Farnoud Farahmand, Panasayya Yalla, Jens-Peter Kaps and Kris Gaj

ECE Department, George Mason University, Fairfax, Virginia, USA,

http://cryptography.gmu.edu

Introduction

- Lightweight block ciphers important for security in the Internet of Things (IoT)
- CAESAR, the Competition for Authenticated Encryption: Security, Applicability, and Robustness, evaluates lightweight authenticated ciphers; includes lightweight block ciphers as cryptographic primitives
- NIST Lightweight Cryptographic Project (Standardization and Evaluation)
- Candidate ciphers evaluated in Hardware (FPGA, ASIC) and Software (CPU, microcontroller), including resourced-challenged platforms (e.g., 8-bit CPU)
- Comparison of purely hardware approach (Register Transfer Level design on FPGA) versus software approach, on small devices, in terms of resources, throughput, power, and energy, is a relevant design consideration for IoT security deployment
- Comparison of hardware to software typically difficult (FPGA or ASIC versus CPU or microcontroller), but made possible by software running on custom-designed soft core processor, compared to custom hardware ciphers on same FPGA (e.g., Kintex-7)

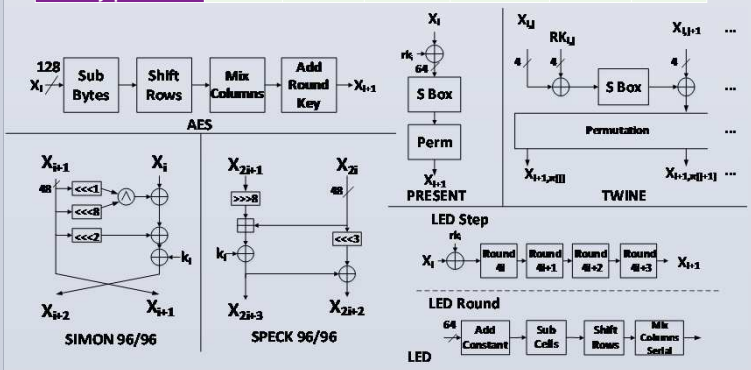
Previous Work

- Implementation and Comparison of Lightweight Ciphers in Hardware
  - HIGHT, PRESENT and AES [Yalla & Kaps, 2009]
  - AES, NOKEON, HIGHT, ICEBERG, KATAN, and PRESENT in ASIC [Kerckhof et al., 2012]
  - AES-128, PRINCE-128, PICCOLO-80, LED-128, PRESENT-80, SIMON 64/96, and TWINE-80 [Banik et al., 2015]
- Benchmarking of Lightweight Ciphers in Software
  - BLOC – C-implementation of ciphers for Wireless Sensor Networks in 16-bit TI MSP-430 microcontroller [Cazorla et al., 2013]
  - FELICS – ASM and C implementations of wide range of lightweight ciphers in multiple platforms, including ATmega128 8-bit microcontroller [Dinu et al., 2015]

Block Ciphers Studied in this Research

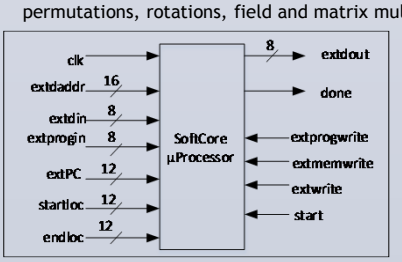
- AES-128, SIMON 96/96, SPECK 96/96, PRESENT-80, LED-80, TWINE 80
- Primitives for several CAESAR Round 3 authenticated ciphers, including AES-JAMBU, SIMON-JAMBU, CLOC-AES, CLOC-TWINE, SILC-AES, SILC-PRESENT, and SILC-LED

	AES	SIMON	SPECK	PRESENT	LED	TWINE
Block Size	128	96	96	64	64	64
Key size	128	96	96	80	80	80
Rounds	10	52	28	31	48	36
I/O Bus width	8	16	32	16	16	16
Key Bus width	8	16	32	16	16	16
Datapath Width	8	96	96	64	16	64
Cycles per Block	308	52	28	32	244	36
Latency per block	324	64	34	36	250	44



Custom-designed 8-bit Soft Core Processor

- 8-bit RISC, 30 native instructions, Harvard Architecture
- Up to 4K Program RAM, 64K Data RAM, 1K Table ROM
- 4 User-defined 1-cycle 8-bit transformations (i.e., S-Box, round constants, etc.)
- 8 User-defined 2-cycle instruction set extensions (i.e., extended word permutations, rotations, field and matrix multiplications, etc.)

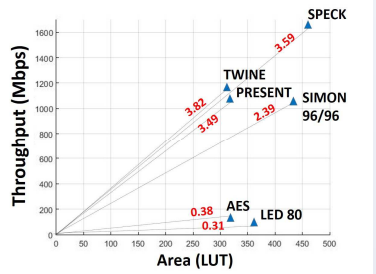


Soft core processor external interface

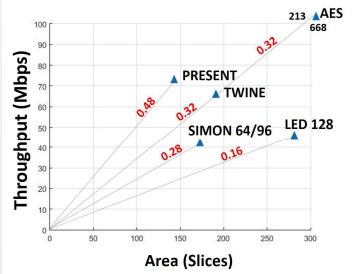
- Custom assembler and simulator (written in Python)
- Creates VHDL table-formatted object code
- Simulated and Implemented in Xilinx Vivado 2015.1
- Soft Cores "tailored" to cipher, i.e., only RAM, ROM, instruction set necessary for cipher are instantiated

Results of Custom Hardware Implementations

- RTL design using VHDL, area target of **300 - 450 LUTs**, implemented on Kintex-7 FPGA, optimized for Throughput-to-Area (TPA) ratio with "Minerva" custom tool
- Results (ranked by TPA ratio): **TWINE, SPECK, PRESENT, SIMON, AES, LED**
- Compare to TPA ratios in [Banik et al., 2015]: PRESENT, TWINE, AES, SIMON, LED



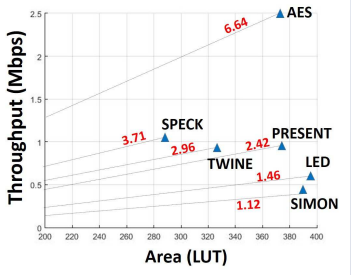
TPA ratios of HW Implementations in this research



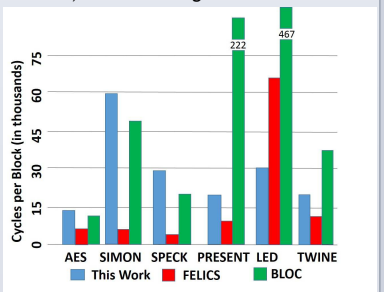
TPA ratios of ciphers in [Banik et al, 2015]

Results of Tailored Soft Core Implementations

- Assembly language on tailored soft cores, implemented in Kintex-7 FPGA, optimized for Throughput-to-Area (TPA) ratio with "Minerva" custom tool
- PRESENT and LED include instruction set extensions, including 64-bit permutation and 61-bit rotation (PRESENT), and GF(2^4) matrix multiplication (LED)
- Results (ranked by TPA ratio): **AES, TWINE, SPECK, PRESENT, LED, SIMON**; (ranked by Cycles per Block): **AES, TWINE, PRESENT, SPECK, LED, SIMON**
- Comparison in terms of Cycles per Block to pure microcontroller results in FELICS (8-bit AVR ATmega128) and BLOC (16-bit TI MSP-430) benchmarking studies



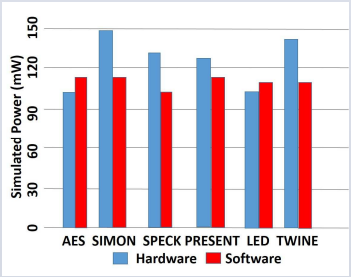
TPA ratios of SW Implementations in Tailored Soft Cores in Kintex-7 FPGA



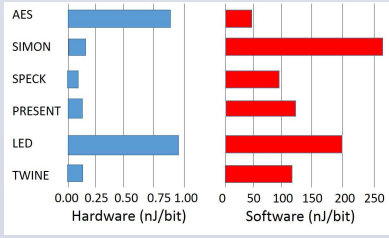
Comparison of SW Cycles per Block between this work, and FELICS and BLOC studies

Comparison of Power and Energy of HW and SW versions

- Power measurements based on Vivado Power Reports at optimal TPA ratio



Comparison of Power of HW and SW ciphers



Comparison of energy of HW (left) and software (right) versions of ciphers

Conclusions

- TWINE, SPECK, PRESENT best in HW considering TPA ratio with area 300-450 LUTs; LW block ciphers (except for LED) have better TPA than AES with this area target
- AES,TWINE, and PRESENT best in SW considering cycles per block
- AES performs nearly best among SW in this work, FELICS and BLOC, especially considering 128-bit key security of AES, 96-bit in SIMON/SPECK, and 80-bit in others
- LED disadvantaged in hardware and software in most implementations
- Optimal tailored soft cores can use less power than dedicated custom hardware
- However, dedicated hardware orders of magnitude more energy efficient

Acknowledgements

This poster is based upon work supported by the NSF under Grant No. 1314540.