Comparison of Hardware and Software Implementations of Selected Lightweight Block Ciphers

William Diehl, Farnoud Farahmand, Panasayya Yalla, Jens-Peter Kaps and Kris Gaj
Department of Electrical and Computer Engineering, George Mason University, Fairfax, U.S.A.
e-mail: {wdiehl, ffarahma, pyalla, jkaps, kgaj}@gmu.edu

***Abstract*— Lightweight block ciphers are an important topic of research in the context of the Internet of Things (IoT). Current cryptographic contests and standardization efforts seek to benchmark lightweight ciphers in both hardware and software. Although there have been several benchmarking studies of both hardware and software implementations of lightweight ciphers, direct comparison of hardware and software implementations is difficult due to differences in metrics, measures of effectiveness, and implementation platforms. In this research, we facilitate this comparison by use of a custom lightweight reconfigurable processor. We implement six ciphers, AES, SIMON, SPECK, PRESENT, LED and TWINE, in hardware using register transfer level (RTL) design, and in software using the custom reconfigurable processor. Both hardware and software implementations are instantiated in identical Xilinx Kintex-7 FPGAs, which enables direct comparison of throughput, area, throughput-to-area (TP/A) ratio, power, and energy. Results show that TWINE and AES have the highest TP/A ratios for hardware and software implementations, respectively, assuming an area target of 300 – 450 LUTs. In terms of direct comparison, software implementations on tailored reconfigurable processers generally use less power – especially where reconfigurable instruction set extensions are permitted. However, custom hardware implementations have higher throughput and energy-efficiency than software implementations on the same platform.**

***Index Terms*— Cipher, cryptography, encryption, field programmable gate array, reconfigurable, microcontroller**

I. Introduction

In the context of the "Internet of Things" (IoT), there is growing emphasis on providing cryptographic solutions that are possibly less-robust, but less power and resource-intensive than traditional standards, such as AES and Triple-DES (3DES). Many such solutions can be realized using lightweight cryptographic algorithms.

Current cryptographic contests and standards development projects are targeting improvements in lightweight cryptography. Examples include the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR), and he National Institute of Standards and Technology's (NIST) Lightweight Cryptography Project [1, 2]. In particular, the CAESAR committee specified use cases by which ciphers would be evaluated in latter rounds, including lightweight applications (resource constrained environments). The desired characteristics for authenticated ciphers conforming to this use case include performance and energy efficiency in resource-constrained hardware and software, including 8-bit CPUs [3].

In this work, we support the above efforts by implementing six secret-key block ciphers using two methods – custom hardware implementations using Register Transfer Level (RTL) design, and software using a custom lightweight reconfigurable 8-bit soft core microprocessor. Five of the ciphers chosen are lightweight ciphers: SIMON 96/96, SPECK 96/96, PRESENT-80, LED-80, and TWINE-80 [4 – 7]. The sixth cipher is AES-128 which is included for purposes of comparison [8]. Five of these ciphers are used as cryptographic primitives for authenticated ciphers being evaluated in the CAESAR third round competition, including CLOC-AES, CLOC-TWINE, AES-JAMBU, SIMON-JAMBU, SILC-AES, SILC-PRESENT, and SILC-LED [9, 10].

Custom hardware implementations are compared in terms of throughput, area, and throughput-to-area (TP/A) ratio. Software implementations in a custom reconfigurable processor are compared in two forms: 1) "Software" metrics, including cycles, memory, and cycles-per-byte, and 2) "Hardware" metrics, including throughput, area, and TP/A ratio.

The above strategy enables three types of comparisons to be performed in this research: 1) Comparison of custom hardware implementations of ciphers against each other and against previously reported implementations; 2) Comparison of software implementations against each other and against previously reported implementations; and 3) Direct comparison of hardware and software in terms of some metrics, including throughput, area, TP/A ratio, power, and energy-per-bit.

II. Background and Previous Work

A. Benchmarking of Lightweight Ciphers in Hardware

There have been several comparison studies of hardware implementations of multiple lightweight ciphers. These include comparisons of HIGHT and PRESENT, implementation of AES, NOKEON, HIGHT, ICEBERG, KATAN, and PRESENT in an ASIC design flow, and a study of AES-128, PRINCE-128, PICCOLO-80, LED-128, PRESENT-80, SIMON 64/96, and

TWINE-80 using varying degrees of round unrolling [11 – 13]. Additional relevant studies are found in [14 – 16].

B. Benchmarking of Lightweight Ciphers on Microcontrollers

We compare results of our software implementations against selected results of two previous studies: BLOC and FELICS [17, 18]. The BLOC project is an extensive effort to benchmark 17 lightweight block ciphers using the 16-bit Texas Instruments (TI) MSP430 microcontroller. In the Fair Evaluation of Lightweight Cryptographic Systems (FELICS) project, 20 ciphers are evaluated in several different scenarios, and benchmarked on three microcontrollers: the 8-bit AVR ATmega128, the 16-bit TI MSP430, and the 32-bit ARM Cortex M3.

C. Our Contribution

We focus on the subset of ciphers most relevant to the CAESAR competition, i.e., the ciphers which are the cryptographic primitives for the authenticated ciphers under evaluation for "lightweight applications" use case. As such, we are careful to choose the block size and key strength of these ciphers as specified in [9] and [10].

Our custom hardware implementations of these ciphers have a target of balanced throughput-to-area (TP/A) ratio, assuming an area target of 300 – 450 FPGA look-up tables (LUTs). The target of balanced TP/A ratio emphasizes suitability for applications that have both speed and size constraints.

With regard to software implementations, we concentrate on the criteria specifically emphasized for evaluation in the CAESAR competition lightweight applications use case, namely resource-constrained 8-bit microprocessors, power and energy/bit. Although [18] contains implementation results for a number of ciphers on the 8-bit AVR ATmega128, it is beneficial to evaluate these ciphers on a diverse set of multiple 8-bit processors, including our very lightweight reconfigurable processor.

Finally, we go further than previous hardware or software studies of these lightweight ciphers by implementing identical versions of these ciphers in both custom hardware and in software (on a custom reconfigurable processor), using an identical FPGA, in order to make relevant comparisons.

III. Methodology

A. Custom hardware implementations

Any required round keys are computed "on-the-fly," and only the encryption case is implemented. In order to ensure fairness and conformity in evaluation of multiple ciphers, we use an AXI-stream-compatible uniform lightweight block cipher interface, motivated by the adoption of the CAESAR Committee of a standardized interface and protocol – the CAESAR Hardware Applications Programming Interface (API) for authenticated ciphers [19]. Table I summarizes the custom hardware implementations of the block cipher versions in this research.

B. Software Implementations

Designs are implemented in a custom reconfigurable 8-bit soft core microprocessor, which consists of only 30 native instructions, draws 8-bit program words from program RAM, and uses an 8-bit data bus to address a separate data RAM in a Harvard Architecture.

TABLE I
Features of investigated cipher variants and their Custom hardware implementations

	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/ Block	308	52	28	32	244	36
Latency per block	324	64	34	36	250	44

The custom reconfigurable processor can be tailored to the cipher by instantiating only the minimum amount of memory required, and by removing functionality not required for the tailored application. These "tailored" processors provide a more accurate representation of area (e.g., slices, LUTs), throughput-to-area (TP/A) ratio, power, and energy-per-bit resulting from the structure of each cipher. The source files for the custom reconfigurable processor, supporting assembler, simulator, and reference manuals, are available at [20].

C. Optimization of FPGA Results

Achieving optimum throughput-to-area (TP/A) ratios in Xilinx Vivado is not trivial, as synthesis and implementation strategies attempt innovative placement and routing in order to meet a user-defined clock constraint. Maximum frequency is often estimated by iteratively varying the clock period until an acceptable worst negative slack (WNS) target (e.g., 0.1 ns) is achieved. However, this binary search procedure is time-consuming, and there is no guarantee that the user will achieve optimal throughput, area, or throughput-to-area ratio.

This research uses an optimization tool called Minerva to maximize TP/A ratios [21]. Minerva was used for all custom hardware and tailored soft core processor builds in this research, and achieved an average of 15% improvement in TP/A ratios.

IV. Results

A. Custom hardware implementations

The results for the custom hardware implementations of the subject ciphers for the Kintex-7 FPGA are shown in Table II. The results show that TWINE has the highest throughput-to-area (TP/A) ratio, followed by SPECK, PRESENT, SIMON, AES, and LED.

B. Software Results

The software benchmarking results for the six ciphers using our custom reconfigurable processor, in terms of memory (separated into program RAM, data RAM, and table ROM), cycles per block, and cycles-per-byte, are shown in Table III. AES has the lowest cycle-per-byte count, followed by SPECK, TWINE, PRESENT, LED, and SIMON.

TABLE II
CUSTOM HARDWARE RESULTS ON KINTEX-7 FPGA

	Freq (MHz)	Area (LUTs)	Throughput (Mbps)	TP/A (Mbps/LUT)
AES-128	287	318	119	0.38
SIMON 96/96	564	435	1041	2.39
SPECK 96/96	473	452	1622	3.59
PRESENT-80	542	311	1084	3.49
LED-80	423	358	111	0.31
TWINE-80	658	306	1170	3.82

TABLE III
SOFTWARE BENCHMARKING RESULTS

	Program Bytes	Data Bytes	Table Bytes	Cycles/ Block	Cycles/ Byte
AES	396	56	256	14,360	898
SIMON	274	43	0	58,234	4853
SPECK	245	32	0	29,046	2421
PRESENT	156	48	0	20,030	2504
LED	313	54	80	30,015	3752
TWINE	253	64	80	19,892	2487

In Table IV, the software implementations using respective tailored processors are compared in terms of hardware metrics, including frequency (MHz), area (LUTs), throughput (Mbps), and throughput-to-area (TP/A) ratio (Mbps/LUT). This allows comparison of tailored processors based on their required use of memory and instruction sets, which affect total area and frequency. Here "throughput" is computed as $(Block\ Size/Cycles\ per\ Block) \times Freq(MHz)$, where block size is shown in Table I and Cycles per Block is shown as Cycles/Block in Table III for corresponding software implementations.

AES has the highest TP/A, followed by SPECK, TWINE, PRESENT, LED, and SIMON.

V. ANALYSIS

A. Comparison of custom hardware with previous results

Comparison with previous hardware implementations of these lightweight ciphers is difficult, since available results are based on varying devices and optimization strategies (e.g., balanced throughput-to-area, low-area, etc.) Additionally, there is no previous study that implements all of the versions (i.e., block and key size) of these ciphers. A comparison of results is presented in Table V.

B. Comparison of software with previous results

Table VI shows a simplified comparison with results from the FELICS and BLOC benchmarking efforts. A direct comparison of results is not possible, since there are significant differences in assumptions among the three studies.

TABLE IV
RESULTS FOR SOFTWARE IMPLEMENTATIONS ON TAILORED RECONFIGURABLE PROCESSORS ON KINTEX-7

	Freq (MHz)	Area (LUTs)	Throughput (Mbps)	TP/A (Mbps/LUT)
AES-128	280	377	2.501	0.00664
SIMON 96/96	265	390	0.437	0.00112
SPECK 96/96	325	290	1.075	0.00371
PRESENT-80	285	377	0.911	0.00242
LED-80	264	386	0.563	0.00146
TWINE-80	297	323	0.956	0.00296

TABLE V
COMPARISON OF CUSTOM HARDWARE RESULTS WITH PREVIOUS RESULTS

Cipher	Ref	Dev	TP (Mbps)	Area (Slices)	TP/A	Rank
AES-128	TW	K7	119	95	1.23	5
AES-128	[13]	S6	213	668	0.32	(3)
SIMON 96/96	TW	K7	1041	149	6.99	4
SIMON 64/96	[13]	S6	43	154	0.28	(4)
SPECK 96/96	TW	K7	1622	142	11.42	1
SPECK 64/128	[22]	S3	416	153	2.72	
PRESENT-80	TW	K7	1084	103	10.52	3
PRESENT-80	[13]	S6	71	148	0.48	(1)
LED-80	TW	K7	111	115	0.97	6
LED-128	[13]	S6	46	283	0.16	(5)
TWINE-80	TW	K7	1170	103	11.36	2
TWINE-80	[13]	S6	64	198	0.32	(2)

Note: "TW" in "Ref" column refers to this work. "K7" is Kintex-7, "S6" is Spartan-6, "S3" is Spartan-3; Area listed in "slices" vice "LUTs" since majority of references list area only in slices. Rankings in parenthesis are from [13].

However, the common significant observation among the three studies is that AES ranks highly in terms of cycles per block when compared to the lightweight ciphers. Additionally, SPECK and TWINE perform well regardless of platform.

C. Comparison of hardware to software implementations

Comparison of hardware and software implementations of the same algorithm are rarely attempted, since the metrics and measures of effectiveness are typically diverse. Since we have implemented identical versions of these ciphers on identical hardware, we are able to compare certain metrics, such as throughput, area, TP/A ratio, power, and energy-per-bit, as shown in Table VII. Here, power is taken directly from the Vivado-generated power report using total on-chip power. Energy per bit is calculated as $(Power(mW = \frac{mJ}{s}) \times Cycles/Block)/(Freq\ (MHz) \times Block\ Size\ (bits))$.

One observation is that the software implementations use on average 10% less power than their corresponding hardware implementations, which could be valuable for low-power devices, for which instantaneous current must be kept low, such as RFID or remotely-controlled vehicles.

Additionally, the throughput of the custom hardware implementations is three orders of magnitude higher than the software implementations on tailored soft core processors. This leads to a greatly reduced energy requirement for the hardware implementations compared to software, despite their higher instantaneous power. Thus custom hardware implementations

TABLE VI
COMPARISON OF CYCLES PER BLOCK AMONG THREE BENCHMARKING EFFORTS

	This Work	#cycl/ #cycl (AES)	FELICS	#cycl/ #cycl (AES)	BLOC	#cycl/ #cycl (AES)
AES	14,328	1.0	4,363	1.0	11,850	1.0
SIMON	58,210	4.1	4,208	1.0	50,328	4.2
SPECK	29,022	2.0	2,238	0.5	21,812	1.8
PRESENT	20,014	1.4	10,017	2.3	222,066	18.7
LED	29,999	2.1	67,414	15.6	467,558	39.4
TWINE	19,876	1.4	13,685	3.1	36,290	3.1

Note: Results from this research use assembly language (ASM). FELICS data excerpted from [18], Scenario 0 AVR detailed results. Implementations are ASM except LED and TWINE (ASM results not available). SIMON and SPECK results are for the 64/96 version (96/96 results not available). BLOC data excerpted from [17]. All results are for C implementations MSP430. The LED version is LED64. In each case the ratio of the #cycles to the #cycles (AES) is shown next to its respective set of results.

TABLE VII
COMPARISON OF HARDWARE AND SOFTWARE RESULTS IN TERMS OF THROUGHPUT, AREA, TP/A RATIO, POWER, AND ENERGY-PER-BIT

	Impl	TP (Mbps)	Area (LUT)	TP/A (Mbps)	Power (mW)	Energy/bit (nJ/bit)
AES	HW	119	318	0.375	109	0.914
	SW	2.501	377	0.00664	115	46.0
SIMON	HW	1041	435	2.394	148	0.142
	SW	0.437	390	0.00112	115	263.1
SPECK	HW	1622	452	3.588	129	0.080
	SW	1.075	290	0.00371	102	94.9
PRESENT	HW	1084	311	3.486	124	0.114
	SW	0.911	377	0.00242	114	125.1
LED	HW	111	358	0.310	108	0.973
	SW	0.563	386	0.00146	113	200.6
TWINE	HW	1170	306	3.823	145	0.124
	SW	0.956	323	0.00296	112	117.1

have a clear advantage in cases where both throughput and resources are important, and where long-term energy consumption is constrained.

In terms of TP/A ratio, SPECK, TWINE, and PRESENT rank high in both hardware and software. AES ranks well in software, but is less suitable for hardware. SIMON, in contrast, performs well in hardware but not software. LED ranks low in terms of TP/A ratio in both hardware and software.

VI. CONCLUSION

The six ciphers, including five lightweight cryptographic algorithms (SIMON, SPECK, PRESENT, LED, and TWINE) as well as AES, are implemented using both custom hardware design and software design using a custom reconfigurable 8-bit microprocessor. The ciphers are verified, benchmarked, and instantiated on the Xilinx Kintex-7 FPGA.

In the custom hardware implementations, TWINE has the highest throughput-to-area (TP/A) ratio, followed by SPECK, PRESENT, SIMON, AES, and LED, assuming an area target of 300 – 450 LUTs. The relative rankings of these ciphers, in terms of TP/A ratio, is similar to rankings of hardware implementations in [13], even though the two studies had different optimization targets.

In the software implementations, AES has the lowest cycle per byte ratio, followed by SPECK, TWINE, PRESENT, LED, and SIMON. The order of rankings is similar to other reported results on 8- and 16-bit microcontrollers.

A direct comparison of hardware and software implementations on an identical FPGA shows that while the software implementations usually consume less power than their corresponding hardware implementations, the much higher throughput of the hardware implementations dominates over power usage. Therefore, the average energy-per-bit of these custom hardware implementations is less than the average of software by a factor of more than 300.

In a direct comparison of hardware and software in terms of throughput-to-area (TP/A) ratio, SPECK, TWINE, and PRESENT rank well in both hardware and software. AES ranks high in software but low in hardware, while SIMON ranks high in hardware but low in software. LED ranks low in both hardware and software when TP/A ratio is the primary metric.

REFERENCES

[1] "CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness." Internet: http://competitions.cr.yp.to/caesar.html, Jun. 16, 2014 [Jun. 25, 2017].

[2] K. McKay, L. Bassham, M. Turan, N. Mouha, NISTIR 8114, Report on Lightweight Cryptography, National Institute of Standards and Technology (NIST), Mar. 2017, Internet: http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf [Jun. 25, 2017].

[3] D. Bernstein, "Cryptographic Competitions," Google Groups, https://groups.google.com/forum/#!forum/crypto-competitions [Jun. 25, 2017].

[4] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith and L. Wingers, "The SIMON and SPECK lightweight block ciphers," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1-6.

[5] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, C. Vikkelsoe, P. Paillier, I. Verbauwhede, "PRESENT: An Ultra-Lightweight Block Cipher" Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, Sep. 10-13, 2007, Springer Berlin, pp. 450-466.

[6] J. Guo, T. Peyrin, A. Poschmann, M. Robshaw, "The LED Block Cipher," 2011, https://eprint.iacr.org/2012/600.pdf [Jun. 25, 2017].

[7] T. Suzaki, K. Minematsu, S. Morioka, E. Kobayashi, "TWINE: A Lightweight Block Cipher for Multiple Platforms" In: R. Knudsen, H. Wu (eds.) SAC 2012. LNCS, vol. 7707, Springer (2012), pp. 339-354.

[8] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), Nov. 26, 2001.

[9] H. Wu, T. Huang, "The JAMBU Lightweight Authenticated Encryption Mode v2.1," Sep. 2016, https://competitions.cr.yp.to/round3/jambuv21.pdf, [Jun. 25, 2017].

[10] T. Iwata, K. Minematsu, J. Guo, S. Morioka, and E. Kobayashi, "CLOC and SILC v3," Sep. 2016, https://competitions.cr.yp.to/round3/clocsilcv3.pdf, [Jun. 25, 2017].

[11] P. Yalla and J. P. Kaps, "Lightweight Cryptography for FPGAs," 2009 International Conference on Reconfigurable Computing and FPGAs, Quintana Roo, Mexico, 2009, pp. 225-230.

[12] S. Kerckhof, F. Durvaux, C. Hocquet, D. Bol, F. Standaert, E. Prouff, and P. Schaumont, "Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint", Cryptographic Hardware and Embedded Systems -- CHES 2012: 14th International Workshop, Leuven, Belgium, Sep. 9-12, 2012. Proceedings, 2012, Springer Berlin, pp. 390-407.

[13] S. Banik, A. Bogdanov and F. Regazzoni, "Exploring the energy consumption of lightweight blockciphers in FPGA," 2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig), Mexico City, 2015, pp. 1-6.

[14] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations", IEEE Design & Test of Computers, vol.24, no. 6, 2007, pp. 522-533.

[15] B. Mohd, T. Hayajneh, A. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues", Journal of Network and Computer Applications, vol. 58, 2015, pp. 73-93.

[16] C. Marchand, L. Bossuet, and K. Gaj, "Area-oriented Comparison of Lightweight Block Ciphers Implemented in Hardware for the Activation Mechanism in the Anti-counterfeiting Schemes," International Journal of Circuit Theory and Applications, vol. 45, no. 2, Feb. 2017, pp. 274-291.

[17] M. Cazorla, K. Marquet, and M. Minier. "Survey and benchmark of lightweight block ciphers for wireless sensor networks," In Pierangela Samarati, editor, SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29-31 July, 2013, SciTePress, 2013, pp. 543-548.

[18] D. Dinu, A. Biryukov, J. Großschädl, D. Khovratovich, Y. Le Corre, L. Perrin, "Fair Evaluation of Lightweight Cryptographic Systems (FELICS),"Lightweight Cryptographic Workshop, 2015, Internet: http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session7-dinu-paper.pdf [Jun. 25, 2017].

[19] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, P. Yalla, J.P. Kaps, K. Gaj, "CAESAR Hardware API," Cryptology ePrint Archive, Report 2016/626, Internet: http://eprint.iacr.org/2016/626.pdf [Jun. 25, 2017].

[20] W. Diehl, "Reconfigurable Lightweight Soft Core Processor," https://cryptography.gmu.edu/athena/

[21] F. Farahmand, "Tools and Experimental Setup for Efficient Hardware Benchmarking of Candidates in Cryptographic Contests," MS Thesis, ECE Department, George Mason University, Fairfax, U.S.A., Nov. 2016.

[22] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, "Simon and Speck: Block Ciphers for the Internet of Things," NIST Lightweight Cryptography Workshop, 20-21 July 2015, Internet: http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session1-shors-paper.pdf [Jun. 25, 2017].