Face-off between the CAESAR Lightweight Finalists: ACORN vs. Ascon

William Diehl*, Farnoud Farahmand†, Abubakr Abdulgadir†, Jens-Peter Kaps†, Kris Gaj†
* Virginia Tech, Bradley Department of Electrical and Computer Engineering, Blacksburg, VA., U.S.A.
wdiehl@vt.edu
† George Mason University, Department of Electrical and Computer Engineering, Fairfax, VA., U.S.A.
{ffarahma, aabdulga, jkaps, kgaj}@gmu.edu

***Abstract*—Authenticated ciphers potentially provide resource savings and security improvements over the joint use of secret-key ciphers and message authentication codes. The CAESAR competition aims to choose the most suitable authenticated ciphers for several categories of applications, including a lightweight use case, for which the primary criteria are performance in resource-constrained devices, and ease of protection against side channel attacks (SCA). Recently, two of the candidates from this category, ACORN and Ascon, were selected as CAESAR contest finalists. In this research, we compare two SCA-resistant FPGA implementations of ACORN and Ascon, where one set of implementations has area consumption nearly equivalent to the defacto standard AES-GCM, and the other set has throughput (TP) close to that of AES-GCM. The results show that protected implementations of ACORN and Ascon, with area consumption less than but close to AES-GCM, have 23.3 and 2.5 times, respectively, the TP of AES-GCM. Likewise, implementations of ACORN and Ascon with TP greater than but close to AES-GCM, consume 18% and 74% of the area, respectively, of AES-GCM.**

***Index Terms*—Side-channel, DPA, CAESAR, authenticated cipher, countermeasure, FPGA, TVLA, t-test, FOBOS**

I. Introduction

Authenticated ciphers offer the promise of better efficiency and higher security for modern cryptographic applications, particularly for resource-constrained devices in the Internet of Things (IoT). Specifically, authenticated ciphers combine the cryptographic services of confidentiality, integrity, and authentication into one algorithmic construct, which is often less-resource intensive than separately-implemented encryption, e.g., block or stream ciphers, and message authentication mechanisms, such as keyed-hash functions.

Current and projected cryptographic competitions and standardization processes are evaluating authenticated ciphers based on several criteria. For example, the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR), announced final round candidates in March 2018, where ACORN and Ascon were chosen as the contenders in the lightweight category. Additionally, the U.S. National Institute of Standards and Technology (NIST) announced the start of a three-year lightweight cryptography (LWC) standardization process, which will evaluate authenticated ciphers for their performance in resource-constrained environments. Candidate submissions should additionally lend themselves to countermeasures against side-channel attacks [1].

This paper is partially based upon work supported by the National Science Foundation under Grant No. 1718434, the Semiconductor Research Corporation under Grant No. 2017-TS-2772, and Air Force Research Laboratory/DARPA under Grant no. FA8650-18-1-7819.

While cryptographic algorithms are generally secure against brute-force attacks that recover sensitive information, physical implementations of cryptography are vulnerable to attacks which analyze leaking information, called side-channel attacks (SCA). One powerful side-channel attack is Differential Power Analysis (DPA), where the adversary is able to measure minute changes in power output of the device resulting from the manipulation of one or more inputs, hypothesize the contents of a secret key fragment, and conduct several electronic measurements to statistically derive the correct secret key [2]. Cryptographic implementations deployed as part of lightweight devices in the IoT, often located in remote locations with little physical protection, are especially vulnerable to these types of attacks. Therefore, the fielding of authenticated ciphers with efficient and robust side-channel resistance is paramount.

In this research, we contribute to the CAESAR final round and NIST LWC standardization process by comparing side-channel resistant FPGA implementations of ACORN and Ascon. We define two optimization targets for our side-channel resistant algorithms as follows: 1) Candidate implementations with approximately the same area as AES-GCM ("area-equivalent"), and 2) Implementations with approximately the same throughput as AES-GCM ("TP-equivalent").

We also establish the following controls for our comparison: 1) All protected (i.e., side-channel resistant) implementations use the same type and order of countermeasures for DPA protection: 3-share threshold implementations (TI) [3], resistant against 1st order DPA; 2) All implementations are compliant with the CAESAR Hardware Applications Programming Interface for Authenticated Ciphers (HW API) [4]; 3) All implementations are realized using the Development Package for CAESAR HW Implementations [5]; and 4) Countermeasures for all protected implementations are verified with Test Vector Leakage Assessment (TVLA) methodology [6], using the Flexible Open-source workBench fOr Side-channel analysis (FOBOS) in the same target device: the Spartan-6 FPGA on the Digilent Nexys-3 board [7].

II. Background and Previous Work

Authenticated ciphers implement authenticated encryption with associated data (AEAD), which is introduced in [8]. The authenticated ciphers in this research, ACORN (v3), Ascon (v1.2), and AES-GCM, are defined in [9]–[11], respectively, and discussed in [12].

There has been previous work to characterize the cost of countermeasures against power analysis side channel attacks for some individual authenticated ciphers, but very few attempts to compare two or more authenticated ciphers in terms of countermeasure costs. For example, the cost of countermeasures is analyzed for Ascon in [13], while AES-GCM has been analyzed for side channel vulnerabilities and cost of countermeasure protection in [14], [15].

A comparative study of costs of protecting 10 CAESAR Round 3 candidates was conducted in [12]. The authors' analysis showed that costs of protecting ACORN-8 and a version of Ascon-128 with a 64-bit datapath include area growth by factors of 5.0 and 3.1, respectively. However, protected implementations in this study used an earlier CAESAR HW Development Package not optimized for lightweight applications, and included the costs of an embedded PRNG, which likely skew results. Our study improves upon [12] by 1) Performing a two-dimensional comparison of subject ciphers in terms of area- and throughput-equivalency to a known standard, AES-GCM; 2) Using a newer HW Development Package optimized for lightweight applications [5]; and 3) Removing the artificial costs of including a PRNG in the reported area of protected implementations.

III. Methodology

A. Threshold Implementations

In order to establish a baseline for "side channel resistant" implementations, we apply one type of countermeasure to all protected implementations. We choose threshold implementations (TI), which have wide acceptance as a provably-secure DPA countermeasure, and are documented at [3].

In TI, sensitive data is separated into shares, on which computations are performed independently. TI must satisfy three properties: 1) Non-completeness: Each share must lack at least one piece of sensitive data, 2) Correctness: The final recombination of the result must be correct, and 3) Uniformity: An output distribution should match the input distribution.

As a constant in all of our protected implementations, we use a hybrid 2-share / 3-share approach, where all of the linear transformations in each cipher are protected using two shares, expand to three shares for non-linear transformations, and are compressed back to two shares following each non-linear operation.

B. Leakage Detection and Verification of Countermeasures

After deploying our countermeasures against DPA, we seek to verify that countermeasures actually improve resistance against DPA. we leverage the TVLA methodology [6], [16]. Using the Welch's t-test, this leakage detection methodology rapidly determines whether or not we can distinguish between two populations, e.g., Q_0 and Q_1. In our case, we leverage a "fixed versus random" non-specific t-test, where we randomly interleave either a fixed test vector, or randomly-generated test vectors possessing the same length and protocol. Using means and variances of our fixed and random populations, we compute a figure of merit t. If $|t| > 4.5$, we reason that we can distinguish between the two populations, and that our design is "leaking information."

To apply the t-test, detect leakage, and verify effectiveness of implemented DPA countermeasures, we leverage the Flexible Open-source workBench fOr Side-channel analysis, or "FOBOS" [7], using methodologies described in [12].

In this research, any required randomness for protected implementations is provided from low-grade pseudo-randomness, consisting of a variable number of concatenated 16-bit LFSRs. Any resource costs of the PRNG are not included in cipher benchmarking, but are included as part of power and energy calculations. PRNGs are initiated using a random seed, generated in software, prior to the start of every trace.

IV. Construction of Protected Implementations

A. ACORN

In order to select design targets for protected ACORN that are either area-equivalent or TP-equivalent to AES-GCM, we estimate final results based on [12]. In this case, the authors report an area of 2732 LUTs in the Spartan-6 FPGA for a protected version of ACORN-8. However, the implementations in [12] included large PRNGs, whereas we do not include PRNG cost. Since the area of protected AES-GCM in [12] is relatively large (4828 LUTs), we choose ACORN-32 as our AES-GCM area-equivalent target. As a TP target, we note that the TP of ACORN-8 reported in [12] is 570.6 Mbps. Dividing 570.6 Mbps by 8 results in 71.4 Mbps, which is close to the AES-GCM TP of 68.8 Mbps reported in [12]. Therefore, we aim for ACORN-1 as our TP-equivalent case.

We build on the TI-protection scheme described in [12]. We choose to execute the state update in two clock cycles instead of one, in order to distribute the non-linearity across two clock cycles. For our ACORN-32, we instantiate ten 32-bit hybrid 2-/ 3- share TI-protected `and` modules, each of which consumes 64 random reshare, and 32 random refresh bits, to maintain the TI uniformity during each call. When distributed over two clock cycles, this results in an average of 480 random bits per clock cycle. In ACORN-1, there are ten 1-bit TI-protected `and` modules, which consume a total of only 20 random reshare, and 10 random refresh bits per state update. In a two-cycle architecture, only 15 random bits are required per clock cycle.

B. Ascon

Ascon implementations with full-width datapaths, i.e., 64-bit block size in the case of Ascon-128, and basic-iterative architectures (i.e., one clock cycle per round), are not ideal for protection against DPA. As discussed in [13], it is imperative to analyze the parts of the algorithm that are susceptible to glitches and separate calculations into smaller independent hardware modules. In order to minimize resources required

for a 3-share TI-protected `and` module, reduce required randomness, and reduce vulnerability due to long logic paths vulnerable to glitching, we implement a hybrid 2- / 3- share TI-protected Ascon permutation, which can execute one round in five clock cycles, assuming a 64-bit permutation datapath. We use the bitslice S-Box discussed in [10], and instantiate only one hybrid 2- / 3- share TI-protected `and` module.

The largest Ascon we can make using this strategy is the 64-bit/5-cycle version, called Ascon-large. Given the reported area in [12] of 6364 LUTs using a similar architecture, which includes a costly PRNG, we assume Ascon-large as our AES-GCM area-equivalent target. In Ascon-large, the internal datapath of the permutation is 64 bits, and one 64-bit, multiplexed TI-protected `and` operation takes place in every clock cycle. Ascon-large requires 192 random bits per clock cycle – 128 bits for resharing (from two to three shares), and 64 bits to satisfy the TI uniformity property.

The TP of protected Ascon reported in [12] is 134.6 Mbps. Dividing 134.6 Mbps by 2 results in 67.3 Mbps, which is close to the TP of AES-GCM in the same study. Therefore, we choose to divide the Ascon permutation once, and assume that a 32-bit permutation datapath will achieve an AES-GCM TP-equivalent target. We call this Ascon-small. In Ascon-small, the permutation takes 12 clock cycles per round, and the internal datapath is 32 bits. Ascon-small requires 96 random bits per clock cycle, including 64 for resharing and 32 for refresh masking.

C. AES-GCM

The AES cryptographic primitive is documented in [17]. We use the AES design discussed in [12], which uses the Tower Fields method to more efficiently compute subfields of GF(2^8). The resulting protected design has a 5-stage pipeline, where a 128-bit block encryption executes in 205 clock cycles. This construction requires 16 bits of fresh randomness for resharing from two to three shares, and 24 fresh remasking bits, for a total of 40 random bits per clock cycle. We also employ a 3-share TI-protected multiplier, which executes a two-operand multiplication in 128 clock cycles.

V. Results

A. Measurement of Leakage Resistance using TVLA

T-tests are conducted on both unprotected and protected cipher implementations; Results are shown in Figure 1. The t-tests, using 2,000 FOBOS-generated traces, generally show that unprotected implementations leak information, although unprotected ACORN-1 comes close to passing. After applying countermeasures as described above, the results in Figure 1 show passing t-tests at 2,000 traces for all implementations.

B. Benchmarking of Unprotected and Protected Implementations

Implementation results for ciphers designed with register transfer level (RTL) in VHDL are reported using Xilinx 14.7 ISE for the Spartan-6 (xc6slx16 csg324-3) FPGA, and are shown in Table I.

TABLE I: Unprotected and Protected Cipher Implementations in Spartan-6 FPGA

Algorithm	Area [LUT]	Area Ratio vs GCM	Freq [MHz]	TP [Mbps]	TP Ratio vs GCM	TP/A [Mbps/ LUT]	TP/A Ratio vs GCM
Unprotected							
ACORN-1	446	0.22	141.9	70.9	0.93	0.159	3.33
ACORN-32	1,396	0.69	147.7	2,363.7	24.31	1.693	35.50
ASCON-small	1,640	0.80	146.1	114.0	1.17	0.070	1.46
ASCON-large	1,725	0.85	148.4	237.4	2.44	0.138	2.89
AES-GCM	2,039	1.00	157.3	97.2	1.00	0.048	1.00
Protected							
ACORN-1	784	**0.18**	156.6	78.3	**1.02**	0.100	5.77
ACORN-32	4,072	**0.92**	111.5	1,784.0	**23.30**	0.438	25.31
ASCON-small	3,278	**0.74**	117.0	91.4	**1.19**	0.028	0.87
ASCON-large	3,673	**0.83**	119.8	191.7	**2.50**	0.052	3.01
AES-GCM	4,429	1.00	124.0	76.7	1.00	0.017	1.00

1) Case 1: Implementations area-equivalent to AES-GCM: The protected implementation of ACORN-32 consumes 4072 LUTs, which is close to (92%) the area of our protected AES-GCM, with 4429 LUTs. However, the TP of ACORN-32 is 1,784 Mbps, which is 23.3 times that of AES-GCM at 76.7 Mbps. The protected implementation of Ascon-large (with a 64-bit permutation datapath) consumes 3673 LUTs, which is 83% of the area of AES-GCM, and has a TP of 191.1 Mbps, which is 2.5 times that of AES-GCM.

2) Case 2: Implementations TP-equivalent to AES-GCM: The protected implementation of ACORN-1 has a TP of 78.3 Mbps, which is slightly greater than that of AES-GCM, but has an area of 784 LUTs, which is only 18% that of AES-GCM. In the case of Ascon, Ascon-small (with a 32-bit permutation datapath), has a TP of 91.4 Mbps, which is 1.2 times the TP of AES-GCM, and has an area of 3278 LUTs, which is 74% that of AES-GCM.

C. Measurement of Power and Energy

Power is measured using an extension of FOBOS, by measuring amplified voltage across a 1 Ohm shunt resistor, during device operation with multiple test vectors, at 10 MHz on the Spartan-6 FPGA. Measured power results are shown in Table II.

The two AES-GCM area-equivalent implementations of ACORN-32 and Ascon-large both draw more power than AES-GCM, despite the fact that they are physically smaller. Conversely, ACORN-1 and Ascon-small both use less power than AES-GCM. In fact, the protected version of ACORN-1 uses only 13% more power than its unprotected counterpart.

We compute energy per bit (E/bit) (nJ/bit) as $Power(mJ/s)/TP_{10MHz}(Mbps)$. By this metric, all protected implementations are more energy efficient that AES-GCM, particularly ACORN-32, with only 6% of the energy usage per bit of AES-GCM.

VI. Conclusions

In this research, we compared side-channel resistant FPGA implementations of the CAESAR lightweight-finalists ACORN and Ascon, using two optimization targets. First, we compared versions of ACORN and Ascon that are roughly

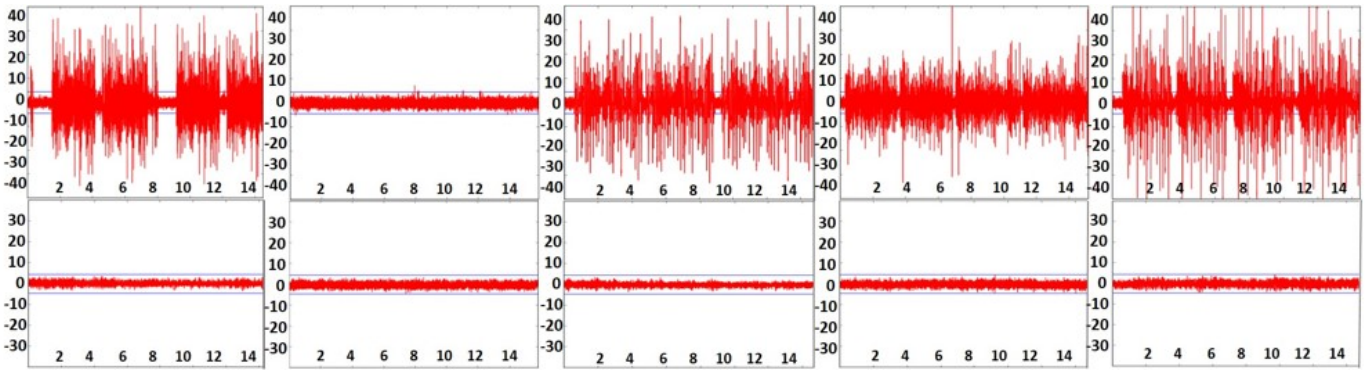

Fig. 1: Results of t-tests for (left to right) AES-GCM, ACORN-1, ACORN-32, Ascon-small, and Ascon-large. T-tests for unprotected implementations are on top, and protected implementations on bottom. Sample numbers (in thousands) are shown on x-axis; t-values are shown on y-axis. Leakage where $t > |4.5|$ denotes a t-test failure.

TABLE II: Power and Energy of Cipher Implementations at 10MHz in Spartan-6 FPGA

Algorithm	Power [mW]	Power Ratio vs GCM	Power Growth Ratio vs Unpro	E/bit [nJ/bit]	E/bit Ratio vs GCM	E/bit Growth Ratio vs Unpro
Unprotected						
ACORN-1	7.6	0.78	-	1.520	0.97	-
ACORN-32	11.7	1.21	-	0.073	0.05	-
ASCON-small	9.2	0.95	-	0.575	0.37	-
ASCON-large	10.6	1.09	-	0.663	0.42	-
AES-GCM	9.7	1.00	-	1.569	1.00	-
Protected						
ACORN-1	8.6	0.46	1.132	1.720	0.57	1.13
ACORN-32	27.4	1.47	2.342	0.171	0.06	2.34
ASCON-small	15.9	0.85	1.73	2.037	0.67	1.84
ASCON-large	22.8	1.22	2.15	1.425	0.47	2.15
AES-GCM	18.7	1.00	1.93	3.024	1.00	1.93

"area-equivalent" to AES-GCM, and noted gains in throughput (TP). Next, we compared versions of ACORN and Ascon that were close to "TP-equivalent" to AES-GCM, and noted reductions in area (LUTs). We observed that AES-GCM area-equivalent implementations of the CAESAR finalists, protected against 1st order DPA with resistance affirmed using Test Vector Leakage Methodology (TVLA), have significantly higher TP, namely 23.3 and 2.5 times for ACORN-32 and Ascon-large, respectively. Additionally, we observed that AES-GCM TP-equivalent protected versions of ACORN-1 and Ascon-small have 18% and 74%, respectively, the area of AES-GCM.

We declare ACORN as the "winner of the face-off" – it is clear that ACORN, particularly ACORN-1, is the most efficient side-channel resistant CAESAR lightweight finalist, in terms of low area, power, and external randomness, which are most relevant for lightweight applications in IoT devices. If insertion of countermeasures is required, 1st order DPA protection additions create an area overhead of only 76%, even with the inclusion of a robust I/O capability.

REFERENCES

[1] National Institute of Standards and Technology. (2018, Aug) Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. [Online]. Available: https://csrc.nist.gov/projects/lightweight-cryptography

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*, 1999, pp. 388–397.

[3] S. Nikova, C. Rechberger, and V. Rijmen, "Threshold Implementations Against Side-Channel Attacks and Glitches," in *Information and Communications Security*, 2006, pp. 529–545.

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

[5] CERG. (2017, Dec) Development Package for Hardware Implementations Compliant with the CAESAR Hardware API, v2.0. https://cryptography.gmu.edu/athena/index.php?id=CAESAR.

[6] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, "A Testing Methodology for Side Channel Resistance Validation," NIST Non-invasive Attack Testing Workshop, 2011.

[7] CERG. (2016, Oct) Flexible Open-source workBench fOr Side-channel analysis (FOBOS). [Online]. Available: https://cryptography.gmu.edu/fobos/

[8] P. Rogaway, "Authenticated-encryption with associated-data," in *In Proc. 9th CCS*, 2002, pp. 98–107.

[9] H. Wu. (2016, Sep) ACORN: A Lightweight Authenticated Cipher. Accessed Sep. 26, 2018. [Online]. Available: https://competitions.cr.yp.to/round3/acornv3.pdf

[10] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer. (2016, Sep) Ascon v1.2. Accessed Sep. 26, 2018. [Online]. Available: https://competitions.cr.yp.to/round3/asconv12.pdf

[11] National Institute of Standards and Technology. (2007, Nov) Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP800-38D. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[12] W. Diehl, A. Abdulgadir, F. Farahmand, J.-P. Kaps, and K. Gaj, "Comparison of Cost of Protection against Differential Power Analysis of Selected Authenticated Ciphers," *Cryptography*, vol. 2, no. 3, 2018.

[13] H. Groß and S. Mangard, "Reconciling $d+1$ Masking in Hardware and Software," *IACR Cryptology ePrint Archive*, vol. 2017, p. 103, 2017.

[14] S. Belaïd, P.-A. Fouque, and B. Gérard, "Side-Channel Analysis of Multiplications in GF(2^{128})," in *Advances in Cryptology – ASIACRYPT 2014*, 2014, pp. 306–325.

[15] J. Vliegen, O. Reparaz, and N. Mentens, "Maximizing the throughput of threshold-protected AES-GCM implementations on FPGA," in *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, July 2017, pp. 140–145.

[16] T. Schneider and A. Moradi, "Leakage Assessment Methodology," *Journal of Cryptographic Engineering*, vol. 6, no. 2, pp. 85–89, Jun 2016.

[17] National Institute of Standards and Technology. (2000, Oct) Report on the Development of the Advanced Encryption Standard (AES). [Online]. Available: http://csrc.nist.gov/archive/aes/round2/r2report.pdf