FPGA Benchmarking of Round 2 Candidates in the NIST Lightweight Cryptography Standardization Process: Methodology, Metrics, Tools, and Results

Kamyar Mohajerani, Richard Haeussler, Rishub Nagpal,
Farnoud Farahmand, Abubakr Abdulgadir, Jens-Peter Kaps and Kris Gaj

Cryptographic Engineering Research Group,
George Mason University
Fairfax, VA, U.S.A.

Abstract. Over 20 Round 2 candidates in the NIST Lightweight Cryptography (LWC) process have been implemented in hardware by groups from all over the world. In Fall 2020, all implementations compliant with the LWC Hardware API, proposed in 2019, have been submitted for FPGA benchmarking to George Mason University's LWC benchmarking team, who co-authored this report. The received submissions were first verified for correct functionality and compliance with the hardware API's specification. Then, the execution times in clock cycles, have been determined using behavioral simulation, for several selected input sizes. An overhead of modifying vs. reusing a key between two consecutive inputs was quantified. The compatibility of all implementations with FPGA toolsets from three major vendors, Xilinx, Intel, and Lattice Semiconductor was verified. Optimized values of the maximum clock frequency and resource utilization metrics, such as the number of look-up tables (LUTs) and flip-flops (FFs), were obtained by running optimization tools, such as Minerva, ATHENa, and Xeda. The raw post-place and route results were then converted into values of the corresponding throughputs for long, medium-size, and short inputs. The results were presented in the form of easy to interpret graphs and tables, demonstrating the relative performance of all investigated algorithms. For a few submissions, the results of the initial design-space exploration were illustrated as well. An effort was made to make the entire process as transparent as possible and results easily reproducible by other groups.

Keywords: Lightweight Cryptography · authenticated ciphers · hash functions · hardware · FPGA · benchmarking

1 Introduction

A comprehensive framework for fair and efficient benchmarking of hardware implementations of lightweight cryptography was proposed in [1]. This framework was based on the idea of the Lightweight Cryptography Hardware API [2], which was published in October 2019, and remained stable since then.

The corresponding LWC Development Package has been built as a major revision of the CAESAR Development Package [3], [4] by an extended team including representatives of the Technical University of Munich (TUM), Virginia Tech, and George Mason University. The first version of this package was published on October 14, 2019. Since then, this package was updated several times, including the most recent revision in September 2020.

The advantages of the LWC Development Package over the CAESAR Development Package in terms of the smaller area overhead was demonstrated in [5]. The new package also supports additional combinations of external-internal databus widths, namely {external: 32 - internal: 16} and {external: 32 - internal: 8}. The first implementations of candidates in the Lightweight Cryptography Standardization process, compliant with the LWC Hardware API and using the new development package, were reported by members of the Virginia Tech Signatures Analysis Lab in [6].

Before the start of Round 2 of the NIST Lightweight Cryptography Standardization Process in September 2019, multiple submission teams developed hardware implementations non-compliant with the proposed LWC API [7]. These implementations used very divergent assumptions, interfaces, and optimization goals. Only 7 out 32 teams (ACE, DryGASCON, ForkAE, Romulus, SKINNY, Subterranean 2.0, and WAGE) made their HDL code public, either as a part of the corresponding Round 2 submission package or the candidate website. Preliminary results reported in the algorithm specifications were based on the use of about a dozen different FPGA families (Artix-7, Cyclone IV, Cyclone V, iCE40, Spartan-3, Spartan-6, Stratix IV, Stratix V, Virtex-6, Virtex-7, and Zynq-7000) and about the same number of standard-cell ASIC libraries (28 nm FDSOI, 45 nm NanGate FreePDK, 130 nm IBM, 10 nm Intel FinFET, 65 nm and 90 nm STMicroelectronics, 65 nm TSMC, 90 nm, 130 nm, and 180 nm UMC). Only results obtained using the same FPGA family or the same ASIC library can be fairly compared with one another. As a result, before the start of this benchmarking effort, at most 6 FPGA implementations and 4 ASIC implementations could be possibly compared with one another. However, even such limited comparison would be highly unfair because of the use of different interfaces, assumptions, and optimization targets.

2 Previous Work

The first major cryptographic competition that included a coordinated hardware benchmarking effort based on a well-defined API was CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness), conducted in the period 2013-2019 [8].

The first version of the proposed hardware API for CAESAR was reported in [9]. This version was later substantially revised, endorsed by the CAESAR Committee in May 2016, and published as a Cryptology ePrint Archive in June 2016 [10]. A relatively minor addendum was proposed in the same month, and endorsed by the CAESAR Committee in November 2016 [11].

The commonly accepted CAESAR Hardware API provided the foundation for the GMU Development Package, released in May and June 2016 [3], [12]. This package included in particular: a) VHDL code of a generic PreProcessor, PostProcessor, and CMD FIFO, common for all Round 2 and Round 3 CAESAR Candidates (except Keyak), as well as AES-GCM, b) Universal testbench common for all API-compliant designs (aead_tb), c) Python app used to automatically generate test vectors (aeadtvgen), and d) Reference implementations of several dummy authenticated ciphers.

This package was accompanied by the Implementer's Guide to Hardware Implementations Compliant with the CAESAR Hardware API, v1.0, published at the same time [13]. A few relatively minor weaknesses of this version of the package, discovered when performing experimental testing using general-purpose prototyping boards, were reported in [14], [15].

In December 2017, a substantially revised version of the Development Package (v.2.0) and the corresponding Implementer's Guide were published by the GMU Benchmarking Team [3], [4]. The main revisions included a) Support for the development of lightweight implementations of authenticated ciphers, b) Improved support for the development of high-speed implementations of authenticated ciphers, and c) Improved support for experimental testing using FPGA boards, in applications with intermittent availability of input sources

and output destinations.

It should be stressed that at no point was the use of the Development Package required for compliance with the CAESAR Hardware API. To the contrary, [13] clearly stated that the implementations of authenticated ciphers compliant with the CAESAR Hardware API could also be developed without using any resources belonging to the package [3], [12] by just following the specification [10] directly.

In spite of being non-mandatory and the lack of official endorsement by the CAESAR Committee, the CAESAR Development Package played a significant role in increasing the number of implementations developed during Round 2 of the CAESAR contest. Out of 43 implementations reported before the end of Round 2, 32 were fully compliant, and one partially compliant with the CAESAR Hardware API. All fully compliant code used the GMU Development Package. The fully and partially compliant implementations covered 28 out of 29 Round 2 candidates (all except Tiaoxin) [3]. In Round 3, the submission of the hardware description language code (VHDL or Verilog) was made obligatory by the CAESAR Committee. As a result, the total number of designs reached 27 for 15 Round 3 candidates. Out of these 27 designs, 23 were fully compliant and 1 partially compliant with the CAESAR Hardware API [3]. Overall, publishing the CAESAR Hardware API, as well as its endorsement by the organizers of the contest, had a major influence on the fairness and the comprehensive nature of the hardware benchmarking during the CAESAR competition.

Several optimized lightweight implementations compliant with the CAESAR API, and based on v.2.0 of the Development Package, were reported in [16]. In [17]–[20], several other implementations were enhanced with countermeasures against Differential Power Analysis. In order to facilitate this enhancement, an additional Random Data Input (RDI) port was added to the CAESAR Hardware API.

Major differences between the proposed Lightweight Cryptography Hardware API and the CAESAR Hardware API, defined in [10], [11], are as follows: In terms of the Minimum Compliance Criteria: a) One additional configuration, encryption/decryption/hashing, has been added on top of the previously supported configuration: encryption/decryption. b) On top of the maximum sizes of AD/plaintext/ciphertext already supported in the CAESAR Hardware API, two additional maximum sizes, $2^{16} - 1$ and $2^{50} - 1$, have been added.

3 Methodology

3.1 LWC Hardware API

Hardware designers participating in the hardware benchmarking of Round 2 LWC candidates are expected to follow Hardware API for Lightweight Cryptography defined in detail in [2]. The major parts of this API include the minimum compliance criteria, interface, and communication protocol supported by the LWC core. The proposed API is intended to meet the requirements of all candidates submitted to the NIST Lightweight Cryptography standardization process, as well as all CAESAR candidates and current authenticated cipher and hash function standards. The main reasons for defining a common API for all hardware implementations of candidates submitted to the NIST Lightweight Cryptography standardization project [7] are: a) Fairness of benchmarking, b) Compatibility among implementations of the same algorithm by different designers, and c) Ease of creating the supporting development package, aimed at simplifying and speeding up the design process.

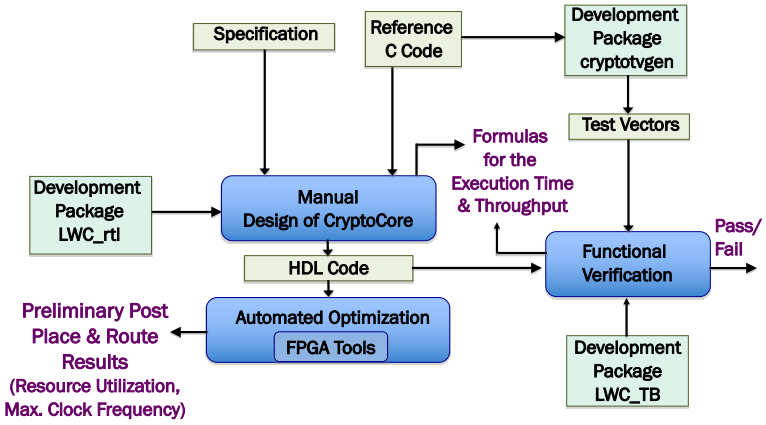

Figure 1: The API-Compliant Code Development using the Development Package

3.2 LWC Hardware Development Package

To make the benchmarking framework more efficient in terms of the hardware development time, the designers are provided with the following resources, compliant with the use of the proposed LWC Hardware API:
a) VHDL code supporting the API protocol, common to all Lightweight Cryptography standardization process candidates, as well as all CAESAR candidates and AES-GCM (LWC_rtl)
b) Universal testbench, common for all API-compliant designs (LWC_TB)
c) Python app used to automatically generate test vectors (cryptotvgen)
d) Reference implementations of a dummy authenticated cipher and a dummy hash function (dummy_lwc)
e) Implementer's Guide, describing all steps of the development and benchmarking process, including verification, experimental testing, and generation of results [21].

It should be stressed that the *implementations of authenticated ciphers (with an optional hash functionality), compliant with the LWC Hardware API, can also be developed without using any of the aforementioned resources, by just following the specification of the LWC Hardware API directly.*

In case the Development Package is used, the major phases of the API-compliant code development process are summarized in Fig. 1. The manual design process is based on the specification and the reference C code of a given algorithm. The HDL code specific for a given algorithm is combined with the code shared among all algorithms, provided in the folder LWC_rtl of the Development Package. Comprehensive test vectors are generated automatically by cryptotvgen based on the reference C code. These vectors are used together with the universal testbench, LWC_TB, to verify the HDL code using simulation. The same testbench can also be used for timing measurements in clock cycles. These measurements can be utilized to confirm or revise formulas for the Execution Time and Throughput derived during the timing analysis phase of the Manual Design. The complete HDL code can be used by design teams to obtain the preliminary post-place & route results, such as resource utilization and maximum clock frequency.

3.3 FPGA Platforms and Tools

For the purpose of this benchmarking study, the GMU group selected three benchmarking platforms representing FPGA families of three major vendors: Xilinx, Intel, and Lattice Semiconductor. The primary criteria for the selection of FPGA devices were as follows:

1. representing widely used low-cost, low-power FPGA families
2. capable of holding SCA-protected designs (possibly using up to four times more resources than unprotected designs)
3. supported by free versions of state-of-the-art industry tools.

These criteria led to the selection of the following FPGA devices:

1. From Xilinx
   Artix-7 : xc7a12tcsg325-3, including 8,000 LUTs, 16,000 FFs, 40 18Kbit BRAMs, 40 DSPs, and 150 I/Os.
2. From Intel
   Cyclone 10 LP : 10CL016-YF484C6, including 15,408 LEs, 15,408 FFs, 56 M9K blocks, 56 multipliers (MULs), and 162 I/Os, and
3. From Lattice Semiconductor
   ECP5 : LFE5U-25F-6BG381C, including 24,000 LUTs, 24,000 FFs, 56 18Kbit blocks, 28 MULs, and 197 I/Os.

The corresponding FPGA tools capable of processing HDL code targeting these (and many other FPGA devices) were:

1. From Xilinx: Xilinx Vivado 2020.1 (lin64)
2. From Intel: Intel Quartus Prime Lite Edition Design Software, ver. 20.1
3. From Lattice Semiconductor: Lattice Diamond Software v3.11 SP2.

3.4 Optimization Target

FPGA implementations of lightweight authenticated ciphers can be developed using various optimization targets. Examples include:

1. maximum throughput assuming a certain limit on resource utilization,
2. minimum resource utilization assuming a certain minimum throughput, and
3. minimum power consumption assuming a certain minimum throughput.

Generally, the more resources the implementation is allowed to use and more power to consume, the faster it can run. An additional constraint may be the need for a circuit to operate at a specific fixed clock frequency, unrelated to the critical path of the circuit (e.g., 100 kHz).

The problem with approaches 2. and 3. is that the minimum required throughput depends strongly on an application. Multiple minimum throughputs may have to be supported by implementations of a future lightweight cryptography standard. Approach 1. is more manageable, especially after the choice of a specific FPGA platform. Our underlying assumption is that the implementation of an LWC algorithm *protected against side-channel attacks* should take no more than all look-up tables (LUTs) of the selected Xilinx FPGA device, Artix-7 : xc7a12tcsg325-3. Taking into account that protected implementations take typically up to 3-4 times more LUTs than unprotected implementations, our unprotected design should take no more than one fourth of the total number of LUTs, i.e., 2000 LUTs. At the same time, we assume that the benchmarked implementations are not permitted to use any family-specific embedded resources, such as Block RAMs, DSP units, or embedded multipliers. Any storage should be implemented using either flip-flops or distributed memory, which, in case of Xilinx FPGAs, is built out of LUTs. The number of Artix-7

flip-flops is limited to 4000, as in this FPGA family each LUT is accompanied by two flip-flops. The designs are also prohibited from using any family-specific primitives or megafunctions.

This proposed optimization target has been clearly communicated to all LWC submission teams, through the document titled Suggested FPGA Design Goals, posted on the LWC hardware benchmarking project website [21], as well as announcements on the lwc-forum, and private communication.

At the same time, it was never our intention to strictly enforce it. Instead, the designers have been encouraged to develop several alternative architectures, such as:

1. Basic-iterative architecture
   (a) Executing one round per clock cycle in block-cipher-based submissions
   (b) Generating one output bit per clock cycle in stream-cipher-based submissions.
2. Architectures most natural for a given authenticated cipher, such as those based on
   (a) Folding in block-cipher-based submissions
   (b) Generating 2^d bits per clock cycle in stream-cipher-based submissions.
3. Maximum throughput, assuming
   - 1000 or less LUTs
   - 2000 or less FFs
   - No BRAMs and no DSP units

   of Xilinx Artix-7 FPGAs.
   Other limits, such as 1500 LUTs, 500 LUTs, etc. are welcome too.

3.5 Deliverables

The format of deliverables was described in detail in the document titled LWC HDL Code: Suggested List of Deliverables, posted on the LWC hardware benchmarking project website [21]. Two very important parts of each submission were files: `assumptions.txt` and `variants.txt`.

The former document can be used to describe any non-standard assumptions (including any deviations from the LWC Hardware API), usage and the modifications in the LWC Development Package, an expected order of segments (such as Npub, AD, plaintext) at the input to the LWC unit, etc.

The latter file, `variants.txt`, is used to define various variants of the hardware design. Different variants may correspond to

- different algorithms of the same family described in a single submission to the NIST LWC standardization process
- different parameter sets, such as sizes of keys, nonces, tags, etc.
- support for AEAD vs. AEAD+Hash
- different hardware architectures, e.g., basic iterative, folded, unrolled, pipelined, etc.
- different parameters of the external interface, such as widths of the input and output buses.

Each variant is expected to be fully characterized in terms of its design goals, corresponding reference software implementation, non-default values of generics and constants, block sizes (for AD, plaintext, ciphertext, and hash message), and detailed formulas for the execution times of all major operations (authenticated encryption, authenticated decryption, and hashing), expressed in clock cycles.

3.6 Functional Verification

All submitted implementations were first investigated in terms of compliance with the LWC Hardware API and the completeness of their deliverables, requested for benchmarking. In particular, the compliance with the two-pass interface ([2], Fig. 2) and the use of an external FIFO was expected from two-pass implementations.

Then, a comprehensive set of new test vectors, unknown in advance to hardware designers, was generated separately for each variant of each algorithm. These tests included multiple special cases, such as empty AD, empty plaintext, various widths of an incomplete last block, etc. If these test vectors passed, the implementation was judged functionally correct and compliant with the LWC Hardware API. If these test vectors failed, the source of failure was investigated in close collaboration with hardware designers. The designers were allowed to submit revised versions of their code. In some cases, an error was on the side of the benchmarking team. For example, an incorrect version of the reference implementation was used, or an incorrect order of segments (such as Npub, AD, plaintext, ciphertext, tag) at the PDI input to the LWC core was assumed. In other cases, the previously-submitted HDL code had to be modified by the designers.

If the code did not pass all tests until the final deadline, it was still included in our study. However, our description of the corresponding hardware design, included in Section 4, clearly indicates that such a problem occurred.

Our original testbench was extended with additional features and a post-processing program to clearly document all test-vector failures. Log files generated by this program were passed back to hardware designers.

3.7 Timing Measurements

The testbench LWC_TB, being a part of the LWC Development package, has been extended to include support for measurements of the execution times for authenticated encryption, authenticated decryption, and hashing. In the current version of this testbench, these measurements rely on the proper implementation of an optional output of the LWC core called do_last. In the cases when the hardware teams did not implement this output, requests were made to support this relatively straightforward extension.

Then, the testbench was used to measure the execution times for:

1. Input sizes used in the definitions of benchmarking metrics, such as 16 bytes, 64 bytes, 1536 bytes, N input blocks, $N + d$ input blocks, with $N = 4$ and $d = 1$ or 2, and three major input types: AD only, Plaintext (PT)/Ciphertext (CT) only, equal-size AD and Plaintext/Ciphertext (AD+PT/AD+CT).

2. All possible AD and plaintext lengths (in bytes) between 0 and 2 full input blocks, in increments of one byte.

The measurement results were compared with expected execution times, based on formulas provided by the design teams. The ideal match was very rare. However, in most cases, the difference between the execution times for $N + d$ and N blocks, required for the calculation of throughput for large inputs, was correct. Simultaneously, the actual execution times differed from expected execution times by a constant for all investigated input sizes. This kind of differences were considered minor.

In other cases, the differences between the actual and expected execution times were dependent on the input type (e.g., AD only, PT only, or AD+PT). Still, in others, they were depended on the input lengths. In most cases, such mismatches were reported back to hardware designers.

In no case, values of the final benchmarking metrics, such as throughputs for particular input sizes were calculated based on estimated values. In all cases, only the execution

times obtained experimentally, using the timing measurements, were used to calculate values of the corresponding throughputs.

In most cases, the task of deriving the detailed execution-time formulas was left as the future work for design teams.

3.8 Synthesis, Implementation, and Optimization of Tool Options

As a next step, each variant of each code was prepared in a separate folder for synthesis and implementation. This preparation was based primarily on the file `source_list.txt`, containing the list of all synthesizeable files in the bottom-up order, i.e., packages and low-level units first, and the top-level unit last. Additionally, the description of each variant in the file `variants.txt` was crucial as well.

In a limited number of cases, the synthesis did not work with any of the three FPGA toolsets we used. As a result, the resubmission of the code was required. In some other cases, the problems concerned a single FPGA toolset. If any of such problems occurred, the designers were provided with the corresponding synthesis reports and requested to investigate the source of synthesis errors and warnings.

The determination of the maximum clock frequency and the corresponding resource utilization was performed using tools specific for each FPGA vendor. For Artix-7 FPGAs, Minerva: An Automated Hardware Optimization Tool described in [22], was used. An average time required to find the optimum requested clock frequency and the best optimization strategy was about 3.5 hours per algorithm variant. Still, in some cases, hardware design teams were able to generate better results by themselves. The source of such discrepancies is still under investigation, but possible reasons include different versions of Vivado, use vs. no use of the out-of-context mode, limited time that could be devoted to each Minerva run (affecting tool options), etc.

For Intel FPGAs, ATHENa – Automated Tool for Hardware EvaluatioN [23], was used. This tool supports all recent Intel FPGA families as well as older Xilinx FPGA families before Series 7. Within this tool, we used the following settings: APPLICATION=GMU_optimization_1, and the OPTIMIZATION_TARGET=Balanced.

A new tool, Xeda[24], which stands for cross (X) electronic design automation, was developed. Xeda provides a layer of abstraction over simulation and synthesis tools and removes the difficulty associated with testing a design across multiple FPGA vendors. Additionally, Xeda allows user-made plugins which can extend functionality to new tools or allow for post-processing of synthesis and simulation results.

For Lattice Semiconductor FPGAs, Xeda and a plugin developed to find the maximum clock frequency were used. Only single optimization strategy (i.e., the collection of flow settings), targeting optimal timing, was considered. We used Synplify Pro as the default synthesis engine for Lattice Diamond as it resulted in better timing/utilization results across the majority of submissions. Additionally, it is the only Lattice Diamond synthesis engine with support for SystemVerilog. Some variants were unable to pass synthesis using Synplify Pro. For these cases, the Lattice Synthesis Engine (LSE) was used instead.

3.9 Performance Metrics

The following performance metrics have been evaluated as a part of Phases 1 and 2 of the Round 2 LWC Benchmarking Project:
Metrics obtained from tool reports after placing and routing:

1. Resource utilization
   Number of LUTs for Artix-7 and ECP5 FPGAs, LEs for Cyclone 10 LP FPGAs, and flip-flops for all FPGAs, assuming no use of embedded memories (such as BRAMs), DSP units, and embedded multipliers.

2. Maximum clock frequency in MHz.
   This metric by itself is not used for ranking of algorithms, but it affects other metrics defined below.

Metrics calculated based on universal formulas, with variables replaced by values obtained from tool reports and timing measurements:

1. Throughput in Mbits/s
   for the following sizes of inputs
   (a) Long [with Throughput = d·Block_size/(Time(N+d blocks)−Time(N blocks))]
   (b) 1536 bytes
   (c) 64 bytes
   (d) 16 bytes.

   All throughputs are calculated separately for
   - AD, plaintext (PT), AD+PT (sender's side)
   - AD, ciphertext (CT), AD+CT (receiver's side), and
   - hash message.

   We assume no difference in the execution time depending on the result of verification on the receiver's side.

2. Speed in clock cycles per byte
   This metric is suitable only for the case of a constant clock frequency determined by an application or implementation environment, independently of the maximum clock frequency supported by the LWC unit. Examples include RFIDs operating with the frequencies such as 60 kHz or 13.56 MHz. This metric is similar to the metric used in software benchmarking, but its use should be limited to the above mentioned special cases only. Otherwise, values of this metric may hide very significant differences in the maximum clock frequency, which in hardware is a strong function of an algorithm and hardware architecture.

4 Hardware Designs

An overview of hardware designs submitted for benchmarking is given in Table 1. A total of 27 designs were received. These designs covered 22 out of 32 Round 2 candidates. Candidates implemented independently by two different groups included Ascon, COMET, Gimli, TinyJAMBU, and Xoodyak.

Several hardware design groups contributed more than one design. In particular,

- George Mason University Cryptographic Engineering Research Group (CERG), USA, implemented 6 candidates: Elephant, PHOTON-Beetle, Pyjamask, Saturnin, TinyJAMBU, and Xoodyak;
- Virginia Tech Signatures Analysis Lab, USA, contributed implementations of 5 candidates: Ascon, COMET, GIFT-COFB, SCHWAEMM & ESCH, and Spoc;
- CINVESTAV-IPN, Mexico, contributed implementations of 4 candidates: COMET, ESTATE, LOCUS-AEAD/LOTUS-AEAD, and Oribatida;
- Institute of Applied Information Processing and Communications, TU Graz, Austria, implemented 2 candidates: Ascon and ISAP.

Table 1: Overview of hardware designs submitted for FPGA benchmarking

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
1a	Ascon	Institute of Applied Information Processing and Communications, TU Graz, Austria	Robert Primas https://rprimas.github.io rprimas@gmail.com	Stefan Mangard https://www.iaik.tugraz.at/person/stefan-mangard stefan.mangard@iaik.tugraz.at	Yes, Unmodified	VHDL	2
1b	Ascon	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
2a	COMET	CINVESTAV, Mexico	Jose A. Bernal jose.bernal@cinvestav.mx, Cuauhtemoc Mancillas-Lopez cuauhtemoc.mancillas@cinvestav.mx	Francisco Rodriguez-Henriquez franccisco.cinvestav.mx Cuauhtemoc Macillas_Lopez cuauhtemoc.mancillas@cinvestav.mx	Yes, Unmodified	VHDL	2
2b	COMET	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
3	DryGASCON	Independent (previously CERG GMU)	Ekawat Homsirikamol ekawat@gmail.com		Yes, Unmodified	Verilog (CryptoCore)	1
4	Elephant	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	2
5	ESTATE	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas Lopez cuauhtemoc.mancillas@cinvestav.mx http://www.cs.cinvestav.mx/Investigadores/Cmancillas		Yes, Modified	VHDL	4
6	GIFT-COFB	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	1
7a	Gimli	Gimli Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	7

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
7b	Gimli	Chair of Security in Information Technology, Technical University of Munich, Germany	Patrick Karl patrick.karl@tum.de	Michael Tempelmeier michael.tempelmeier@ tum.de	Yes, Unmodified	VHDL	3
8	ISAP	Institute of Applied Information Processing and Communications, TU Graz, Austria	Robert Primas https://rprimas.github.io rprimas@gmail.com	Stefan Mangard https://www.iaik.tugraz.at/ person/stefan-mangard stefan.mangard@ iaik.tugraz.at	Yes, Modified	VHDL	2
9	KNOT	KNOT Team, Tsinghua University, China	Bohan Yang bohanyang@tsinghua.edu.cn, Zhengdong Li lizd@tsinghua.edu.cn	Wentao Zhang zhangwentao@iie.ac.cn, Leibo Liu liulb@ tsinghua.edu.cn	Yes, Unmodified	Verilog (CryptoCore)	4
10	LOCUS-AEAD & LOTUS-AEAD	CINVESTAV-IPN, Mexico	Brisbane Ovilla Martinez brisbane@cinvestav.mx		Yes, Unmodified	VHDL	2
11	Oribatida	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas López cuauhtemoc.mancillas@ cinvestav.mx, Alberto F. Martínez Herrera alberto.herrera.tec@gmail.com		Yes, Unmodified	VHDL	2
12	PHOTON-Beetle	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Vivian Ledynh vledynh@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	1
13	Pyjamask	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/ team/rishub.php rnagpal2@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	2

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
14	Romulus	Romulus-Team, Symmetric Key and Lightweight Cryptography Lab (SyLLab), Nanyang Technological University, Singapore	Mustafa Khairallah http://www.mustafa-khairallah.com mustafam001@e.ntu.edu.sg	Thomas Peyrin https://thomaspeyrin.github.io/web/ thomas.peyrin@ntu.edu.sg	No	Verilog (LWC)	5
15	Saturnin	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/team/rishub.php rnagpal2@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	2
16	SCHWAEMM & ESCH	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Flora Coleman googly2@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
17	SpoC	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	William Diehl wdiehl@vt.edu		Yes, Modified	Verilog (CryptoCore)	1
18	Spook-v2	Spook Team	Davide Bellizia davide.bellizia@uclouvain.be, Gaetan Cassiers gaetan.cassiers@uclouvain.be, Charles Momin charles.momin@uclouvain.be	François-Xavier Standaert fstandae@uclouvain.be	No	Verilog (LWC)	1
19	Subterranean 2.0	Subterranean 2.0 Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	1
20a	TinyJAMBU	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Sammy Lin https://cryptography.gmu.edu/team/slin5.php slin5@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	3

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
20b	TinyJAMBU	TinyJAMBU Team	Tao Huang huangtaochn@gmail.com	Hongjun Wu https://www3.ntu.edu.sg/home/wuhj wuhongjun@gmail.com	Yes, Unmodified	VHDL	3
21	WAGE	WAGE Team	Nusa Zidaric nzidaric@uwaterloo.ca	Mark Aagaard https://ece.uwaterloo.ca/ ∼maagaard maagaard@uwaterloo.ca	Yes, Modified	VHDL	1
22a	Xoodyak	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/ team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	2
22b	Xoodyak	Xoodyak Team + Silvia	Silvia Mella silvia.mella@st.com		Yes, Unmodified	VHDL	12
						Total	**72**

The following submissions were provided by co-authors of algorithms submitted to the NIST LWC standardization process: ESTATE, Gimli, ISAP, KNOT, LOCUS-AEAD/LOTUS-AEAD, Oribatida, Romulus, Spook, Subterranean 2.0, TinyJAMBU, WAGE, and Xoodyak.

The implementation of DryGASCON was developed by an independent researcher, Ekawat Homsirikamol, in close collaboration with the author of the algorithm. The implementation of Gimli was contributed by members of the Chair of Security in Information Technology at the Technical University of Munich, Germany.

Most groups used VHDL. Four design teams used exclusively Verilog for the implementation of the entire LWC unit. As a result, these implementations did not take advantage of the LWC Development Package, available only in VHDL. Algorithms implemented this way included Gimli, Romulus, Spook-v2, and Subterranean 2.0. Three implementations modeled only the part unique to a given algorithm, its CryptoCore, in Verilog. These designs included DryGASCON, KNOT, and SpoC. Altogether, 15 hardware design submissions used VHDL pre-processing and post-processing units, provided as a part of the LWC Development Package without any modifications, 8 with modifications, and 4 did not use them at all.

Eight submissions contained a single variant. In the remaining, the number of variants varied between 2 and 12, with an average of 2.7 per hardware design submission. Most of the variants of the same algorithm share a significant portion of the HDL source code and differ only in values of generics or constants. In some cases, a separate source code was provided for each variant.

The total number of implemented variants reached 72. In Table 2, we summarize basic features of each variant, and assign each variant a unique name used in the rest of the paper. For algorithms implemented by a single group, this name consists of the name of the algorithm followed by "-<variant_number>". For algorithms implemented by two groups we add "_<Group_Name_Abbreviation>" after the algorithm name. The abbreviations used are: CI for CINVESTAV-IPN, GMU for George Mason University, Graz for TU Graz, Austria, GT for Gimli Team, VT for Virginia Tech, TJT for TinyJAMBU Team, and XT for Xoodyak Team + Silvia. For Spook, exceptionally, the name of the variant is Spook-v2-v1. In this name, v2 indicates the version 2 of Spook proposed in [25]. This version is known to have higher security margins at the cost of relatively small performance overheads [25]. For each variant, we also list the name of the corresponding reference software implementation. Most of these implementations can be found in the most recent version of SUPERCOP [26]. Some were submitted as a part of the hardware package (KNOT and WAGE) or were provided through candidate's website (Subterranean 2.0).

The maximum length of inputs that can be processed by the implementations is often unlimited by the hardware design itself. In such cases, the designers either stated the maximum length required by the NIST Submission Requirements and Evaluation Criteria [7], $2^{50}-1$, declared the maximum length as "unlimited", or left the respective field of `variants.txt` blank. The following designs have the maximum length specified explicitly as $2^{16}-1$: two-pass implementations (ESTATE, ISAP, and Saturnin), implementations performing precomputations dependent on the maximum input size (Pyjamask), and COMET_CI (v1 and v2).

The following designs do not support key reuse between consecutive inputs: Gimli_GT (v1-v7), Subterranean-v1, TinyJAMBU_GMU (v1-v3), and Xoodyak_XT (v1-v12). For algorithms that support key reuse, we list in the separate column the number of additional clock cycles required to load a new key. This number has been determined experimentally through our own measurements and often differed from the value provided as a part of the submission package. The highest overhead for loading a new key was observed in the case of Pyjamask-v1 (433 cycles), Xoodyak_GMU-v2 (266 cycles), and Pyjamask-v2 (245 cycles). The smallest overhead of 3 clock cycles was measured for Ascon_Graz

(v1 and v2) and Gimli_TUM (v1-v3). The second smallest, in the amount of 4 clock cycles, for DryGASCON-v1, ISAP-v2, LOCUS-v1, LOTUS-v1, TinyJAMBU_TJT-v2, and TinyJAMBU_TJT-v3.

Table 2: Unique names and features of the hardware design variants, including the maximum input length and support for key reuse.

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
1a	Ascon_Graz-v1	Ascon-128+ Ascon-Hash, Folded architecture	ascon128v12, asconhashv12	Y	3	unlimited
	Ascon_Graz-v2	Ascon-128a+ Ascon-Hash, Folded architecture	ascon128av12, asconhashv12	Y	3	unlimited
1b	Ascon_VT-v1	Ascon-128, Basic iterative architecture	ascon128v12	Y	8	N/A
	Ascon_VT-v2	Ascon-128+ Ascon-Hash Basic iterative architecture	ascon128v12, asconhashv12	Y	8	N/A
2a	COMET_CI-v1	Folded architecture	comet128aesv1	Y	8	$2^{16}-1$
	COMET_CI-v2	Folded architecture	comet128aesv1	Y	23	$2^{16}-1$
2b	COMET_VT-v1	Basic iterative architecture	comet128aesv1	Y	7	N/A
	COMET_VT-v2	Basic iterative architecture	comet128chamv1	Y	8	N/A
3	DryGASCON-v1	Basic iterative architecture, support for hashing	drygascon128k32(aead) drygascon128(hash)	Y	4	N/A
4	Elephant-v1	Basic iterative architecture	elephant160v1	Y	84	unlimited
	Elephant-v2	x5 Unrolled	elephant160v1	Y	20	unlimited
5	ESTATE-v1	Two-pass AES-based, 32-bit datapath	estatetweaes128v1	Y	8	$2^{16}-1$
	ESTATE-v2	Two-pass AES-based, 8-bit datapath	estatetweaes128v1	Y	23	$2^{16}-1$
	ESTATE-v3	Two-pass Gift-based, 32-bit datapath	estatetwegift128v1	Y	8	$2^{16}-1$
	ESTATE-v4	Two-pass, Gift-based, 8-bit datapath	estatetwegift128v1	Y	16	$2^{16}-1$
6	GIFT-COFB-v1	Basic iterative architecture	giftcofb128v1	Y	8	N/A
7a	Gimli_GT-v1	1 combinational round	gimli24v1	N		N/A
	Gimli_GT-v2	2 combinational rounds	gimli24v1	N		N/A
	Gimli_GT-v3	3 combinational rounds	gimli24v1	N		N/A
	Gimli_GT-v4	4 combinational rounds	gimli24v1	N		N/A

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	Gimli_GT-v5	6 combinational rounds	gimli24v1	N		N/A
	Gimli_GT-v6	8 combinational rounds	gimli24v1	N		N/A
	Gimli_GT-v7	12 combinational rounds	gimli24v1	N		N/A
7b	Gimli_TUM-v1	Customized FSM based on 3x32-bit register, RAM-based state-memory, 32-bit datapath	gimli24v1	Y	3	N/A
	Gimli_TUM-v2	Customized FSM based on 3x32-bit register, RAM-based state-memory, 16-bit datapath	gimli24v1	Y	3	N/A
	Gimli_TUM-v3	Customized FSM based on 3x32-bit register, RAM-based state-memory, 8-bit datapath	gimli24v1	Y	3	N/A
8	ISAP-v1	Two-pass implementation, Folded architecture	isapk128av20	Y	9	$2^{16}-1$
	ISAP-v2	Two-pass implementation, Folded architecture	isapa128av20	Y	4	$2^{16}-1$
9	KNOT-v1	KNOT-AEAD (128, 256, 64), Basic iterative architecture	submitted with HW package	Y	7	unlimited
	KNOT-v2	KNOT-AEAD (128, 384, 192), Basic iterative architecture	submitted with HW package	Y	7	unlimited
	KNOT-v3	KNOT-AEAD (192, 384, 96), Basic iterative architecture	submitted with HW package	Y	9	unlimited
	KNOT-v4	KNOT-AEAD (256, 512, 128), Basic iterative architecture	submitted with HW package	Y	11	unlimited
10	LOCUS-v1	LOCUS, 32-bit datapath	twegift-64locusaeadv1	Y	4	unlimited
	LOTUS-v1	LOTUS, 32-bit datapath	twegift-64lotusaeadv1	Y	4	unlimited
11	Oribatida-v1	Oribatida256 256-bit datapath	oribatida256v12	Y	8	unlimited
	Oribatida-v2	Oribatida192 192-bit datapath	oribatida192v12	Y	8	unlimited

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
12	PHOTON-Beetle-v1	AEAD+Hash	photonbeetle-aead128rate128v1, photonbeetle-hash256rate32v1	Y	6	$2^{50}-1$
13	Pyjamask-v1	Pyjamask128d16, folded architecture	pyjamask 128aeadv1	Y	433	$2^{16}-1$
	Pyjamask-v2	Pipeline implementation of MixRows	pyjamask 128aeadv1	Y	245	$2^{16}-1$
14	Romulus-v1	Round based architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v2	Two-Round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v3	Four-round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v4	Eight-round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v5	Low-area architecture	romulusn1v12	Y	22	$2^{50}-1$
13	Saturnin-v1	Folded architecture	saturninctrcascadev2 saturninhashv2	Y	20	$2^{16}-1$
	Saturnin-v2	Unrolled SuperRound	saturninctrcascadev2 saturninhashv2	Y	20	$2^{16}-1$
15	SCHWAEMM-v1	Schwaemm-256128, AEAD only, Basic iterative architecture	schwaemm-256128v1	Y	8	N/A
	SCHWAEMM-v2	Schwaemm-256128 and Esch256 AEAD+HASH	schwaemm-256128v1, esch256v1	Y	8	N/A
16	SpoC-v1	spoc64, Basic iterative architecture	spoc64 sliscplight 192v1	Y	7	N/A
17	Spook-v2-v1	Folded architecture resource sharing Clyde128 Shadow512	spook 128su512v2	Y	7	unlimited
18	Subterranean-v1	32-bit bus	Candidate website	N		$2^{50}-1$
19a	TinyJAMBU_GMU-v1	32-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU_GMU-v2	16-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU_GMU-v3	Bit-serial NLFSR	tinyjambu128	N		$2^{50}-1$
19b	TinyJAMBU_TJT-v1	8-step state update	tinyjambu128	Y	15	$2^{50}-1$
	TinyJAMBU_TJT-v2	32-step state update	tinyjambu128	Y	4	$2^{50}-1$

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	TinyJAMBU_TJT-v3	128-step state update	tinyjambu128	Y	4	$2^{50}-1$
20	WAGE-v1	Baseline	submitted with HW package	Y	7	N/A
21a	Xoodyak_GMU-v1	384-bit datapath AEAD+Hash	xoodyakv1	Y	18	unlimited
	Xoodyak_GMU-v2	128-bit datapath AEAD+Hash	xoodyakv1	Y	266	unlimited
21b	Xoodyak_XT-v1	Basic iterative architecture, AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v2	x2 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v3	x3 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v4	x4 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v5	x6 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v6	x12 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v7	Basic iterative architecture, AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v8	x2 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v9	x3 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v10	x4 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v11	x6 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v12	x12 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$

In Table 3, we summarize basic properties of each design variant. The following properties are specific to an algorithm and its parameter set: AD block size, Plaintext (PT)-Ciphertext (CT) block size, Hash block size. All these block sizes are expressed in bits. The numbers of clock cycles per block are influenced by the combination of the algorithm, parameter set, and hardware architecture. In authenticated ciphers based on block ciphers or permutations, basic iterative architecture is defined as an architecture executing one round of the underlying block cipher/permutation per clock cycle. In authenticated ciphers based on stream ciphers, basic iterative architecture is defined as an architecture calculating one basic block (typically one bit) of the output per clock cycle. The number of clock cycles decreases in unrolled architectures and increases in folded architecture. The resource utilization in LUTs changes in the opposite direction.

Three interesting properties of each variant include the ratios of

- processing AD vs. plaintext
- decrypting ciphertext vs. encrypting plaintext
- processing equal-size AD+plaintext vs. pure plaintext.

Additionally, for candidates that support hashing, we are interested in the ratio of hashing vs. processing plaintext.

Table 3: Summary of basic properties of all benchmarked design variants. All throughput data are for long inputs.

No.	Variant Name	AD Block Size [bits]	Cycles per AD Block	PT-CT Block Size [bits]	Cycles per PT-CT Block	Hash Msg. Block Size [bits]	Cycles per Hash Msg Block	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
1a	Ascon_Graz-v1	64	8	64	8	64	14	1.00	1.00	1.00	0.57
	Ascon_Graz-v2	128	12	128	12	64	14	1.00	1.00	1.00	0.43
1b	Ascon_VT-v1	64	10	64	10			1.00	1.00	1.00	
	Ascon_VT-v2	64	10	64	9	64	15	0.90	1.00	0.95	0.60
2a	COMET_CI-v1	128	60	128	70			1.17	1.00	1.08	
	COMET_CI-v2	128	264	128	297			1.13	1.00	1.06	
2b	COMET_VT-v1	128	16	128	20			1.25	1.00	1.11	
	COMET_VT-v2	128	85	128	89			1.05	1.00	1.02	
3	DryGASCON-v1	128	21	128	21	128	21	1.00	1.00	1.00	1.00
4	Elephant-v1	160	88	160	171			1.94	1.00	1.32	
	Elephant-v2	160	24	160	43			1.79	1.00	1.28	
5	ESTATE-v1	128	44	128	88			2.00	1.00	1.33	
	ESTATE-v2	128	226	128	452			2.00	1.00	1.33	
	ESTATE-v3	128	204	128	408			2.00	1.00	1.33	
	ESTATE-v4	128	696	128	1,392			2.00	1.00	1.33	
6	GIFT-COFB-v1	128	49	128	47			0.96	1.00	0.98	
7a	Gimli_GT-v1	128	24	128	24	128	24	1.00	1.00	1.00	1.00
	Gimli_GT-v2	128	12	128	12	128	12	1.00	1.00	1.00	1.00
	Gimli_GT-v3	128	8	128	8	128	8	1.00	1.00	1.00	1.00
	Gimli_GT-v4	128	6	128	6	128	6	1.00	1.00	1.00	1.00
	Gimli_GT-v5	128	4	128	4	128	4	1.00	1.00	1.00	1.00
	Gimli_GT-v6	128	4	128	4	128	4	1.00	1.00	1.00	1.00
	Gimli_GT-v7	128	4	128	4	128	4	1.00	1.00	1.00	1.00
7b	Gimli_TUM-v1	128	786	128	789	128	786	1.00	1.00	1.00	1.00
	Gimli_TUM-v2	128	1,474	128	1,481	128	1,474	1.00	1.00	1.00	1.00
	Gimli_TUM-v3	128	2,850	128	2,865	128	2,850	1.01	1.00	1.00	1.01
8	ISAP-v1	144	25	144	42			1.68	1.00	1.25	
	ISAP-v2	64	14	64	22			1.57	1.00	1.22	
9	KNOT-v1	64	28	64	28			1.00	1.00	1.00	
	KNOT-v2	192	28	192	28			1.00	1.00	1.00	
	KNOT-v3	96	40	96	40			1.00	1.00	1.00	
	KNOT-v4	128	52	128	52			1.00	1.00	1.00	
10	LOCUS-v1	64	57	64	114			2.00	0.95	1.33	
	LOTUS-v1	64	57	64	114			2.00	1.00	1.33	
11	Oribatida-v1	128	69	128	137			1.99	1.00	1.33	
	Oribatida-v2	96	53	96	105			1.98	1.00	1.33	
12	PHOTON-Beetle-v1	128	28	128	33	32	25	1.18	1.00	1.08	0.33
13	Pyjamask-v1	128	258	128	262			1.02	0.96	1.01	
	Pyjamask-v2	128	98	128	102			1.04	1.00	1.02	
14	Romulus-v1	128	32	128	60			1.88	1.00	1.30	
	Romulus-v2	128	18	128	32			1.78	1.00	1.28	
	Romulus-v3	128	11	128	18			1.64	1.00	1.24	
	Romulus-v4	128	7.5	128	11			1.47	1.00	1.19	

Table 3 continued from previous page

No.	Variant Name	AD Block Size [bits]	Cycles per AD Block	PT-CT Block Size [bits]	Cycles per PT-CT Block	Hash Msg. Block Size [bits]	Cycles per Hash Msg Block	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
	Romulus-v5	128	660	128	1304			1.98	1.00	1.33	
15	Saturnin-v1	256	197	256	394	256	197	2.00	1.00	1.33	2.00
	Saturnin-v2	256	27	256	54	256	27	2.00	1.00	1.33	2.00
16	SCHWAEMM-v2	256	38	256	47	128	34	1.24	1.00	1.11	0.69
	SCHWAEMM-v1	256	38	256	47			1.24	1.00	1.11	
17	SpoC-v1	64	109	64	111			1.02	1.00	1.01	
18	Spook-v2-v1	256	48	256	48			1.00	1.00	1.00	
19	Subterranean-v1	8	0.25	8	0.25	8	2	1.00	1.00	1.00	0.13
20a	TinyJAMBU_GMU-v1	32	14	32	34			2.43	1.00	1.42	
	TinyJAMBU_GMU-v2	32	26	32	66			2.54	1.00	1.43	
	TinyJAMBU_GMU-v3	32	386	32	1,026			2.66	1.00	1.45	
20b	TinyJAMBU_TJT-v1	32	49	32	129			2.63	1.00	1.42	
	TinyJAMBU_TJT-v2	32	13	32	33			2.54	1.00	1.43	
	TinyJAMBU_TJT-v3	32	3	32	8			2.67	1.00	1.45	
21	WAGE-v1	64	114	64	114			1.00	1.00	1.00	
22a	Xoodyak_GMU-v1	352	24	192	19	128	17	1.45	1.00	1.25	0.75
	Xoodyak_GMU-v2	352	266	192	261	128	259	1.80	1.00	1.40	0.67
22b	Xoodyak_XT-v1	352	26	192	21			1.48	1.00	1.27	
	Xoodyak_XT-v2	352	20	192	15			1.38	1.00	1.21	
	Xoodyak_XT-v3	352	18	192	13			1.32	1.00	1.19	
	Xoodyak_XT-v4	352	17	192	12			1.29	1.00	1.17	
	Xoodyak_XT-v5	352	16	192	11			1.26	1.00	1.15	
	Xoodyak_XT-v6	352	15	192	10			1.22	1.00	1.13	
	Xoodyak_XT-v7	352	26	192	21	128	19	1.48	1.00	1.27	0.74
	Xoodyak_XT-v8	352	20	192	15	128	13	1.38	1.00	1.21	0.77
	Xoodyak_XT-v9	352	18	192	13	128	11	1.32	1.00	1.19	0.79
	Xoodyak_XT-v10	352	17	192	12	128	10	1.29	1.00	1.17	0.80
	Xoodyak_XT-v11	352	16	192	11	128	9	1.26	1.00	1.15	0.81
	Xoodyak_XT-v12	352	15	192	10	128	8	1.22	1.00	1.13	0.83

For almost all candidates, decryption can be performed with exactly the same speed as encryption. As a result, in the Results section, we focus only on the timing metrics related to encryption. The following candidates process AD significantly faster than plaintext: TinyJAMBU, ESTATE, LOCUS & LOTUS, Oribatida, and Romulus. The ratio of the hashing throughput to the plaintext processing throughput is 2.00 for Saturnin, 1.00 for DryGASCON and Gimli, and the smallest for PHOTON-Beetle and Subterranean 2.0.

4.1 Unique Features

Most of the designs assume the following standard order of segments provided at the Public Data Input (PDI) ports during encryption: Public Message Number (Npub), Associated Data (AD), Plaintext (PT). For decryption, the corresponding order is: Public Message Number (Npub), Associated Data (AD), Ciphertext (PT), and Tag. For ESTATE, the order for decryption is changed to Npub, AD, Tag, Ciphertext. For ISAP, the order for encryption is: Npub, Plaintext, AD; the order for decryption is: Npub, AD, Ciphertext, Tag. For Romulus, the order for encryption is: AD, Npub, Plaintext; the order for decryption is: AD, Npub, Ciphertext, Tag.

Subterranean 2.0 is the only design that uses an unconventional maximum segment size of 2^{15}, instead of the recommended $2^{16} - 1$. This feature does not considerably affect the x, as segments of the size between $2^{15} + 1$ and $2^{16} - 1$ can be easily divided into two segments supported by the submitted design using a simple preprocessor.

5 Results and Their Analysis

5.1 Results of Functional Verification and Timing Measurements

All variants of 26 out of 27 hardware designs passed all GMU known-answer tests (KATs) and produced reliable timing measurements. The only exception was the submission for COMET_VT-v1, which did not pass all tests, but still produced consistent timing measurements.

5.2 Results of Synthesis and Implementation

Initial versions of several designs were shown to be not fully synthesizable by at least one of the three FPGA toolsets used in this study. However, the underlying problems were located and addressed by the hardware designers within the benchmarking period.

The details of resource utilization and maximum clock frequency after placing and routing are provided for all evaluated designs in the Appendix, in Tables 22, 23, and 24.

In Table 23, the ratios between the numbers of Cyclone 10 LP LEs vs. Artix-7 LUTs are provided. The average ratio is 1.83. However, the actual ratios vary in a relatively wide range, between 1.19 for Gimli_GT-v7 and 4.76 for Xoodyak_GMU-v2. Additionally, the following designs have significantly larger area in LEs for Cyclone 10 LP FPGAs as compared to the area in LUTs for Artix-7: Xoodyak_GMU-v2, Pyjamask-v1, Pyjamask-v2, COMET_VT-v1, and COMET_VT-v2. The average ratios of the numbers of FFs and clock frequencies, in Cyclone 10 LP vs. Artix-7, are 1.67 and 1.62, respectively.

In Table 24, the ratios between the numbers of LUTs, flip-flops (FFs), and maximum clock frequencies in ECP5 vs. Artix-7 are summarized. The average ratio is 1.91 for LUTs, 1.13 for FFs, and 2.69 for frequencies. However, the actual ratios vary in a relatively wide range. For example, the ratio of LUTs varies between 1.22 for TinyJAMBU_GMU-v1 and 4.21 for Ascon_Graz-v2. In particular, the following designs have significantly larger area in LUTs for ECP5 as compared to Artix-7: Ascon_Graz-v2, Ascon_Graz-v1, Romulus-v1, and ISAP-v2.

5.3 Throughputs for Long Inputs

5.3.1 Results for Xilinx Artix-7

The two-dimensional graphs Throughput vs. Number of Used LUTs are shown in Figs. 2, 3, and 4. The throughputs concern the cases of Plaintext (PT) only, Associated Data (AD) only, and equal-size AD+PT, respectively. All three mentioned above graphs concern results for the Xilinx Artix-7 FPGA xc7a12tcsg325-3. The results apply to long inputs. We use the logarithmic scale on both axes. Dashed lines represent the same throughput over area ratio. In the legends of these figures, the algorithms are listed in the order of decreasing throughput. While the order of the symbols remains the same, the mapping of symbol to algorithm changes.

In these graphs, each candidate is represented by only one variant, selected according to the following rules. If a candidate has one or more variants with the area below 2500 LUTs, the fastest variant meeting this criterion is selected. If a candidate does not have a variant with the area below 2500 LUTs, a variant with the smallest area is selected.

The threshold of 2500 LUTs (25% more than the intended target of 2000 LUTs) was selected because many designers tried to aggressively use close to 2000 LUTs to achieve the highest possible speed. As a result many of them ended up with designs taking between 2000 and 2500 LUTs. Additionally, the exact number of LUTs may depend on the exact options of tools, providing different trade-offs between the area and speed. Thus, relaxing the upper limit of 2000 LUTs seems to be fully warranted, at least at this stage of the analysis, when the full space exploration remain still incomplete for the majority of candidates.

The clear winner for all three aforementioned input types is Subterranean 2.0. Its implementation is approximately two times faster than its closest competitor. Additionally, it is the second smallest in terms of the number of LUTs.

For PT Only, the next group includes two algorithms, Xoodyak and Ascon, with the throughputs between 2 and 3 Gbits/s. Out of these two, the implementation of Ascon is smaller by approximately 300 LUTs. The third group includes four algorithms with the throughputs between 1 and 2 Gbits/s: Gimli, KNOT, DryGASCON, and Spook-v2. Their areas are in the range between 1500 and 2500 LUTs. The implementation of KNOT is the smallest, followed by Gimli, DryGASCON, and Spook-v2. The next algorithm in the ranking is TinyJAMBU, which reaches the speed very close to 1 Gbit/s and at the same time has by far the smallest area, around 600 LUTs.

The design of SCHWAEMM-v1 is by far the largest, above 3000 LUTs, yet still only average (rank 12) in terms of Throughput. More effort is required to demonstrate the competitiveness of this algorithm with the first 8 candidates mentioned above. Five more algorithms have throughputs exceeding 500 Mbits/s: Romulus, Saturnin, GIFT-COFB, PHOTON-Beetle, and Elephant. Out of them GIFT-COFB is by far the smallest, with the area slightly above 1000 LUTs.

The designs for ISAP, COMET, Pyjamask, and LOCUS seem to be all aiming at the proposed optimization target of 2000 LUTs, but fail to achieve performance comparable to the mentioned above algorithms.

The designs for Spoc, WAGE, and GIFT-COFB are all in the vicinity of 1000 LUTs, and clearly were not optimized for the maximum throughput assuming the resource utilization of 2000 LUTs or less. To the lower extent, the designs for ESTATE and Oribatida, both slightly below 1500 LUTs, are also too small to be fairly compared with others. As a result, it would be too premature to assign any negative evaluation to these candidates.

For AD only, the following changes in the rankings are the most significant. The second fastest, Xoodyak is significantly faster than Ascon, with the throughput exceeding 3 Gbit/s. TinyJAMBU joins and outperforms Ascon in the group of algorithms with throughputs in the range of 2-3 Gbit/s. The new algorithms with throughputs in the range between 1 and 2 Gbit/s include: Saturnin, Romulus, and Elephant.

Only 8 out of 22 investigated candidates support hashing. The two-dimensional graph, Throughput vs. Area for hashing long messages on Artix-7 FPGA is shown in Fig. 5.

The two fastest designs are Gimli_GT-v2 and Xoodyak_XT-v7, with throughputs approaching 2 Gbits/s and areas very close to 2000 LUTs. Very close behind are Saturnin and DryGASCON, with the throughputs between 1.4 and 1.6 Gbits/s. They are followed by Ascon_Graz-v2 at about 1000 Mbit/s and Subterranean-v1 at around 750 Mbits/s. SCHWAEMM-v2 (ESCH) reaches slightly less than 500 Mbit/s, and PHOTON-Beetle around 225 Mbits/s.

The corresponding detailed numerical results can be found in Tables 4, 5, 6, 7.

These tables include the subsets of all designs selected as follows. For hardware submissions that have two designs below the threshold of 2500 LUTs, the fastest two of them are included in the table. For hardware submissions that have one design below the threshold and all remaining designs above the threshold, only the design falling below the threshold is listed. For hardware submissions that have only designs exceeding the

area threshold, only the smallest of these designs is included. Only one variant per LWC candidate is ranked. If the ranked variant has area exceeding the threshold, its rank is marked with *, and the area is given in the bold font.

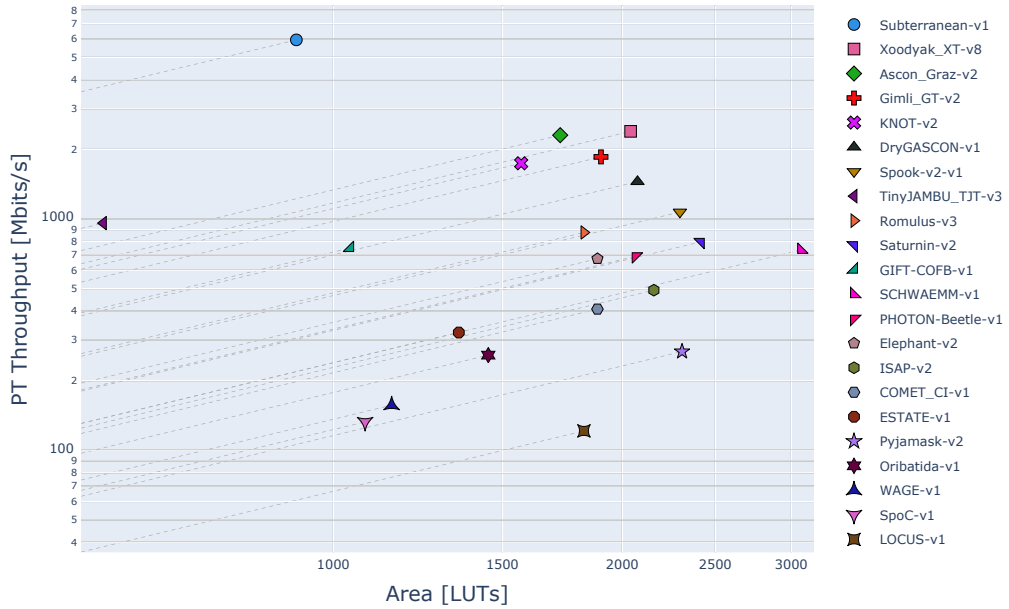

Figure 2: Artix-7 Encryption PT Throughput for Long Messages vs LUTs

5.3.2 Results for Intel Cyclone 10 LP and Lattice Semiconductor ECP5

The equivalent graphs for Intel Cyclone 10 LP are shown in Figs. 6, 7, 8, and 9. The corresponding tables are listed as Tables 8, 9, 10, and 11.

The area threshold used for the selection of the best designs has been set to 5000 LEs. This value was selected based on the fact that the average ratio of the number of Cyclone 10 LP LEs to the number of Artix-7 LUTs, calculated over all available designs, was close to 2.0.

The conclusions from these tables and graphs are very close to the conclusions based on the results for the Artix-7 FPGA. Pyjamask-v2 is the only candidate with no variant fitting within 5000 LEs. In case of Artix-7 FPGAs, the only candidate exceeding the corresponding area threshold was SCHWAEMM.

For PT only, Subterranean is still more than twice as fast as other candidates. Ascon, Gimli, Xoodyak, and KNOT are the only algorithms with the speeds between 1 and 2 Gbit/s. Out of them, Gimli has by far the largest area, approaching 5000 LEs. For AD only, the fastest 5 algorithms are joined by TinyJAMBU, which jumps to the position no. 3 in terms of speed, despite the tiny area, only slightly above 1000 LEs. Romulus and Saturnin are very close behind, with throughputs approaching 1 Gbit/s. For hashing, compared to Artix-7, Saturnin and Xoodyak swap places on positions 2 and 3. The differences in areas between the 5 leading candidates become bigger.

The two-dimesional graphs for Lattice Semiconductor ECP5 are shown in Figs. 10, 11, 12, and 13. The corresponding tables are listed as Tables 12, 13, 14, and 15.

The area threshold used for the selection of the best designs has been set to 5000 LUTs. This value was selected based on the fact that the average ratio of the number of ECP5 LUTs to the number of Artix-7 LUTs, calculated over all available designs, was close to 2.0.

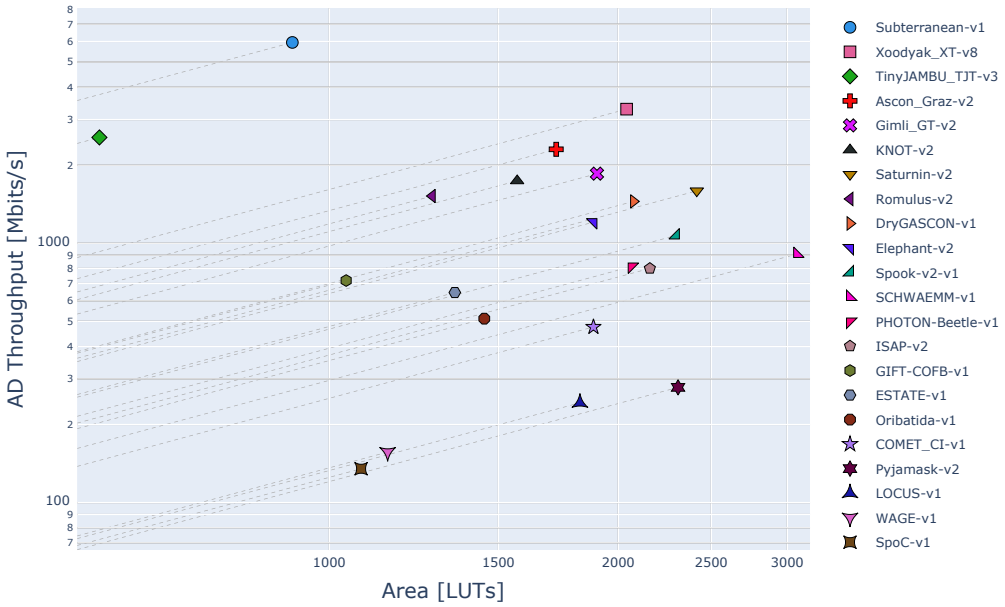

Figure 3: Artix-7 Encryption AD Throughput for Long Messages vs LUTs

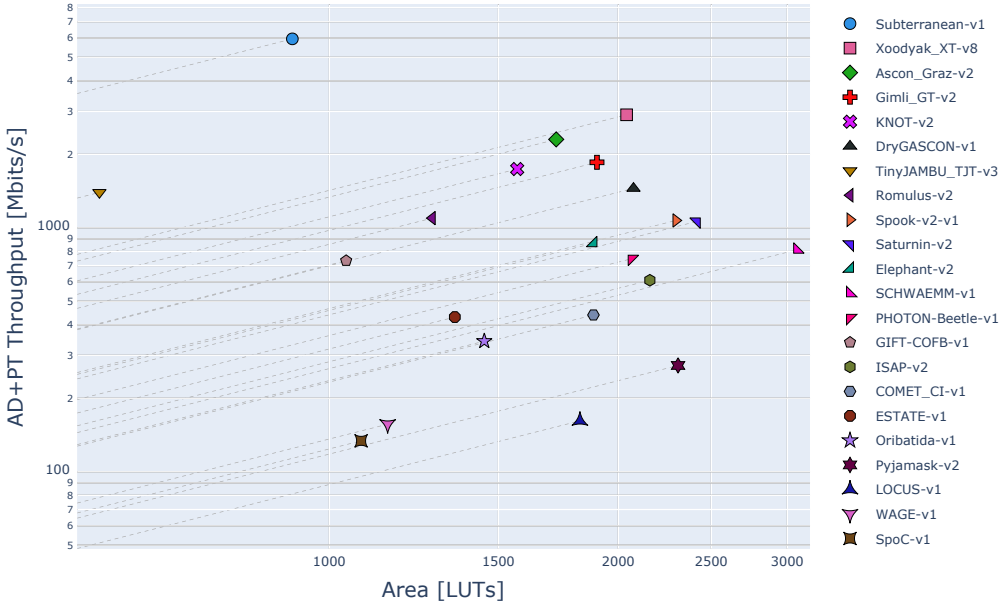

Figure 4: Artix-7 Encryption AD+PT Throughput for Long Messages vs LUTs

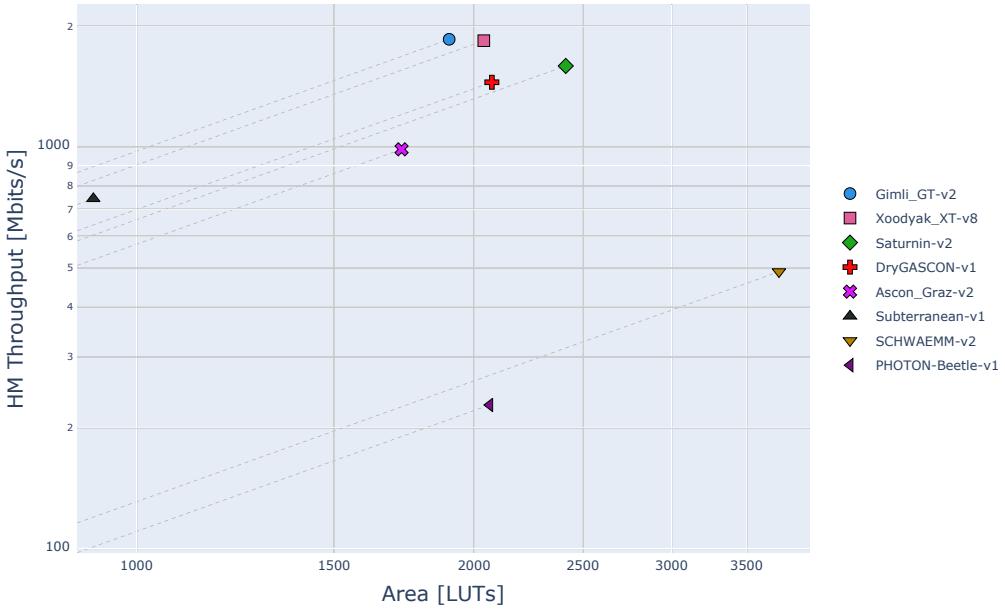

Figure 5: Artix-7 Hashing Throughput for Long Messages vs LUTs

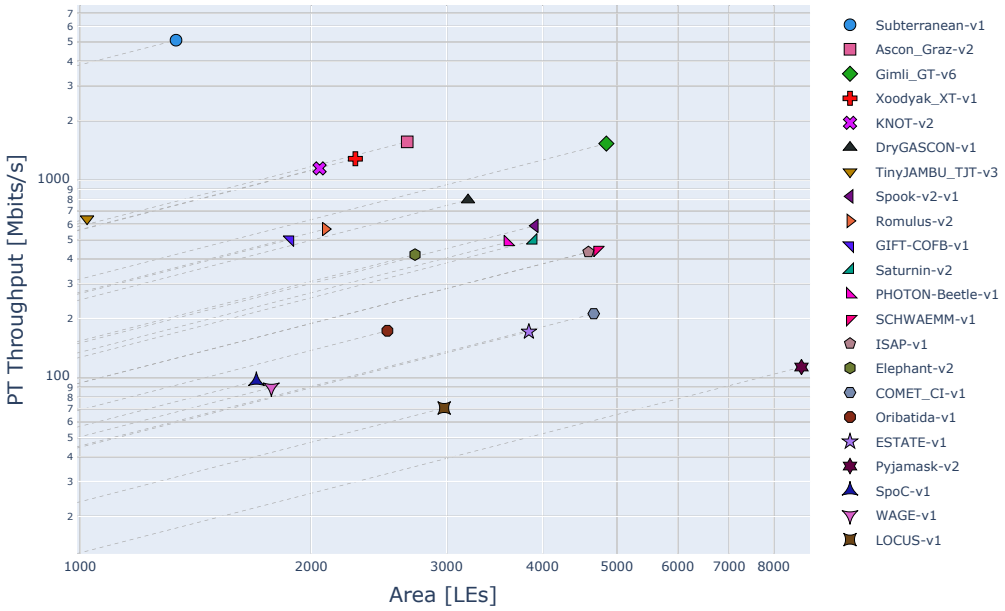

Figure 6: Cyclone-10-LP Encryption PT Throughput for Long Messages vs LEs

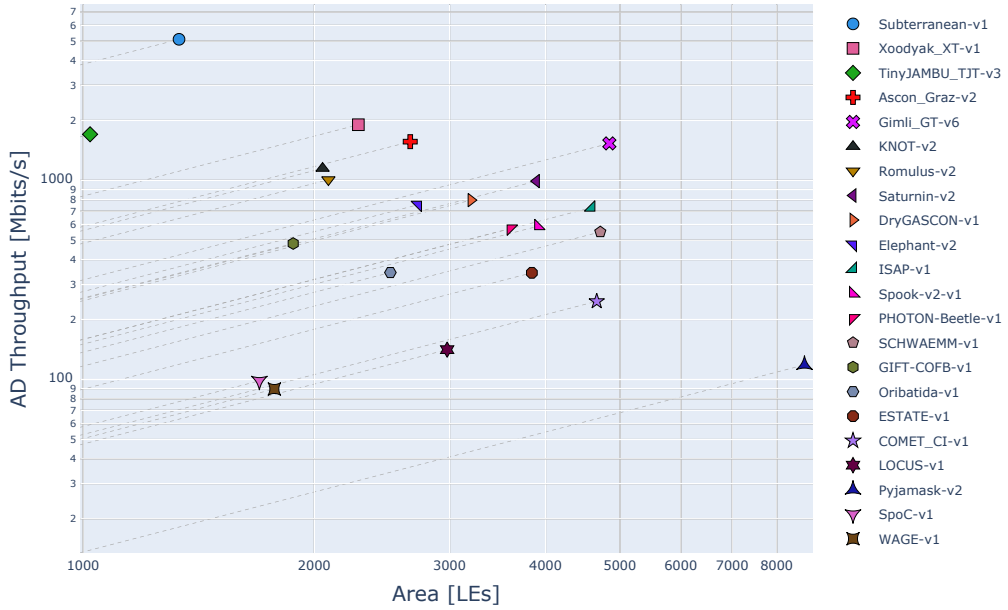

Figure 7: Cyclone-10-LP Encryption AD Throughput for Long Messages vs LEs

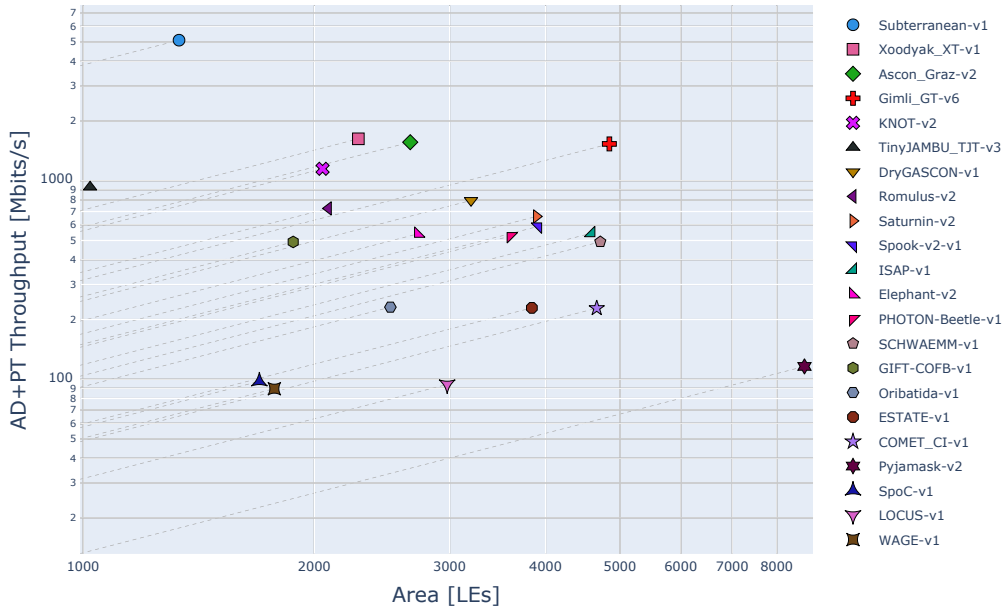

Figure 8: Cyclone-10-LP Encryption AD+PT Throughput for Long Messages vs LEs

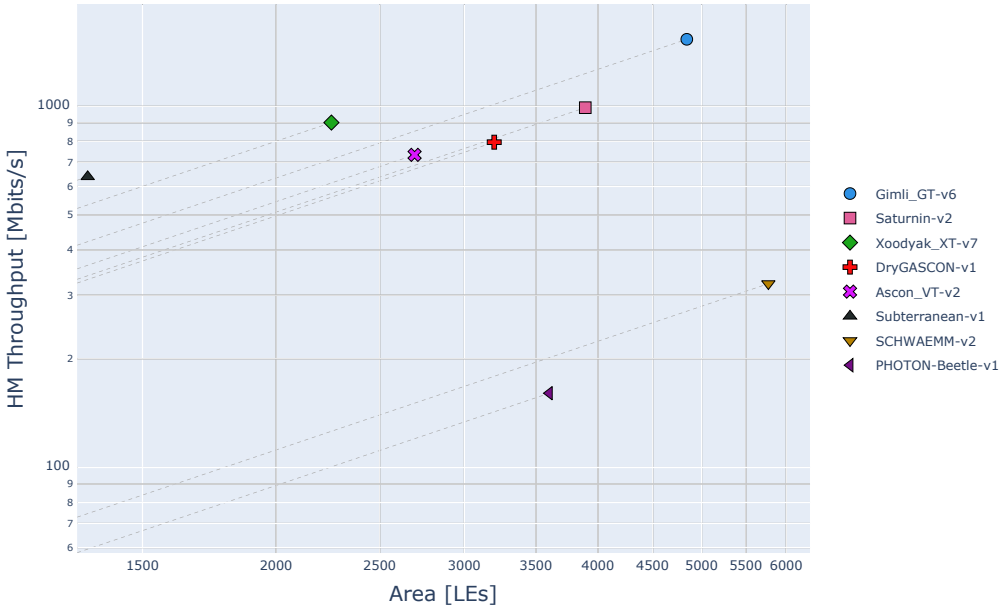

Figure 9: Cyclone-10-LP Hashing Throughput for Long Messages vs LEs

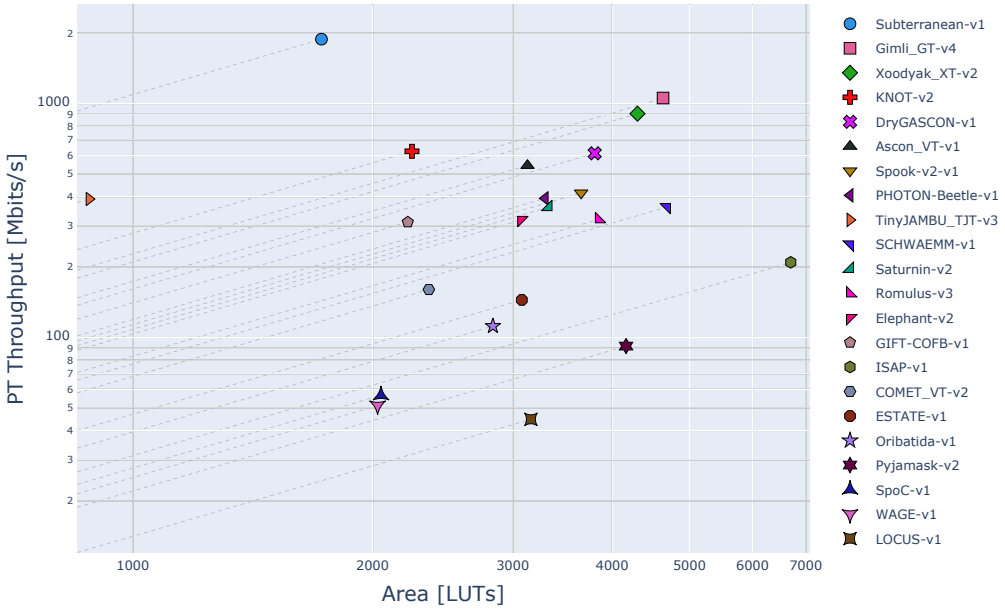

Figure 10: ECP5 Encryption PT Throughput for Long Messages vs LUTs

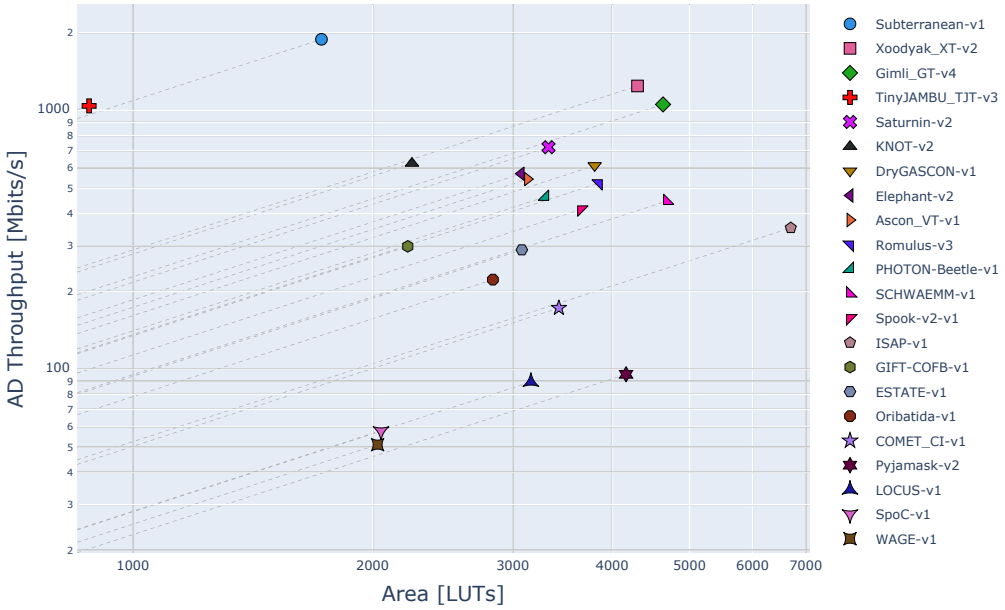

Figure 11: ECP5 Encryption AD Throughput for Long Messages vs LUTs

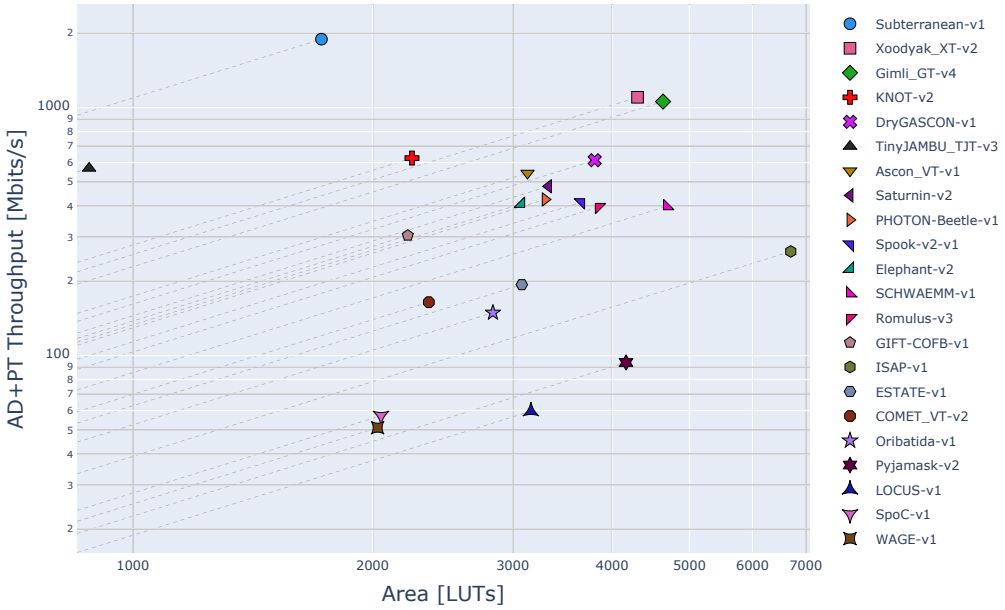

Figure 12: ECP5 Encryption AD+PT Throughput for Long Messages vs LUTs

Table 4: Xilinx Artix-7 Encryption PT Throughput for Long Messages

Variant	**Throughput PT [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	5,952.0	1	915	186	0.25
Xoodyak_XT-v8	2,393.6	2	2,040	187	15
Xoodyak_XT-v2	2,342.4		2,071	183	15
Ascon_Graz-v2	2,304.0	3	1,723	216	12
Gimli_GT-v2	1,856.0	4	1,900	174	12
KNOT-v2	1,741.7	5	1,569	254	28
Xoodyak_GMU-v1	1,717.9		1,808	170	19
Ascon_Graz-v1	1,672.0		1,551	209	8
Ascon_VT-v2	1,557.3		1,928	219	9
Ascon_VT-v1	1,491.2		1,913	233	10
DryGASCON-v1	1,450.7	6	2,074	238	21
Spook-v2-v1	1,072.0	7	2,296	201	48
TinyJAMBU_TJT-v3	960.0	8	576	240	8
Gimli_GT-v1	944.0		1,683	177	24
Romulus-v3	874.7	9	1,824	123	18
Romulus-v2	856.0		1,280	214	32
Saturnin-v2	796.4	10	2,414	168	54
GIFT-COFB-v1	748.9	11	1,041	275	47
SCHWAEMM-v1	735.3	12*	**3,071**	135	47
PHOTON-Beetle-v1	690.4	13	2,065	178	33
Elephant-v2	673.5	14	1,884	181	43
KNOT-v3	633.6		1,367	264	40
ISAP-v2	492.3	15	2,157	200	26
COMET_CI-v1	407.8	16	1,884	223	70
COMET_VT-v2	336.5		1,703	234	89
ESTATE-v1	322.9	17	1,351	222	88
TinyJAMBU_TJT-v2	305.5		461	315	33
Pyjamask-v2	267.3	18	2,308	213	102
Oribatida-v1	257.9	19	1,450	276	137
Oribatida-v2	252.3		1,450	276	105
TinyJAMBU_GMU-v1	250.4		591	266	34
Elephant-v1	214.3		1,291	229	171
WAGE-v1	156.6	20	1,150	279	114
SpoC-v1	132.6	21	1,079	230	111
TinyJAMBU_GMU-v2	129.9		564	268	66
Saturnin-v1	124.8		2,020	192	394
Xoodyak_GMU-v2	123.6		1,234	168	261
LOCUS-v1	121.3	22	1,824	216	114
Pyjamask-v1	111.9		1,979	229	262
COMET_CI-v2	95.7		1,096	222	297
LOTUS-v1	81.4		1,652	145	114
ESTATE-v3	81.3		1,130	259	408
Gimli_TUM-v1	39.1		933	241	789
Gimli_TUM-v2	21.1		905	244	1,481

Table 5: Xilinx Artix-7 Encryption AD Throughput for Long Messages

Variant	Throughput AD [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean-v1	5,952.0	1	915	186	0.25
Xoodyak_XT-v8	3,291.2	2	2,040	187	20
Xoodyak_XT-v2	3,220.8		2,071	183	20
TinyJAMBU_TJT-v3	2,560.0	3	576	240	3
Xoodyak_GMU-v1	2,493.3		1,808	170	24
Ascon_Graz-v2	2,304.0	4	1,723	216	12
Gimli_GT-v2	1,856.0	5	1,900	174	12
KNOT-v2	1,741.7	6	1,569	254	28
Ascon_Graz-v1	1,672.0		1,551	209	8
Saturnin-v2	1,592.9	7	2,414	168	27
Romulus-v2	1,521.8	8	1,280	214	18
Ascon_VT-v1	1,491.2		1,913	233	10
DryGASCON-v1	1,450.7	9	2,074	238	21
Romulus-v3	1,431.3		1,824	123	11
Ascon_VT-v2	1,401.6		1,928	219	10
Elephant-v2	1,206.7	10	1,884	181	24
Spook-v2-v1	1,072.0	11	2,296	201	48
Gimli_GT-v1	944.0		1,683	177	24
SCHWAEMM-v1	909.5	12*	**3,071**	135	38
PHOTON-Beetle-v1	813.7	13	2,065	178	28
ISAP-v2	800.0	14	2,157	200	16
TinyJAMBU_TJT-v2	775.4		461	315	13
GIFT-COFB-v1	718.4	15	1,041	275	49
ESTATE-v1	645.8	16	1,351	222	44
KNOT-v3	633.6		1,367	264	40
TinyJAMBU_GMU-v1	608.0		591	266	14
Oribatida-v1	512.0	17	1,450	276	69
Oribatida-v2	499.9		1,450	276	53
COMET_CI-v1	475.7	18	1,884	223	60
Elephant-v1	416.4		1,291	229	88
COMET_VT-v2	352.4		1,703	234	85
TinyJAMBU_GMU-v2	329.8		564	268	26
Pyjamask-v2	278.2	19	2,308	213	98
Saturnin-v1	249.5		2,020	192	197
LOCUS-v1	242.5	20	1,824	216	57
Xoodyak_GMU-v2	222.3		1,234	168	266
LOTUS-v1	162.8		1,652	145	57
ESTATE-v3	162.5		1,130	259	204
WAGE-v1	156.6	21	1,150	279	114
SpoC-v1	135.0	22	1,079	230	109
Pyjamask-v1	113.6		1,979	229	258
COMET_CI-v2	107.6		1,096	222	264
Gimli_TUM-v1	39.2		933	241	786
Gimli_TUM-v2	21.2		905	244	1,474

Table 6: Xilinx Artix-7 Encryption AD+PT Throughput for Long Messages

Variant	**Throughput AD+PT [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	5,952.0	1	915	186	0.5
Xoodyak_XT-v8	2,906.5	2	2,040	187	35
Xoodyak_XT-v2	2,844.3		2,071	183	35
Ascon_Graz-v2	2,304.0	3	1,723	216	24
Xoodyak_GMU-v1	2,150.7		1,808	170	43
Gimli_GT-v2	1,856.0	4	1,900	174	24
KNOT-v2	1,741.7	5	1,569	254	56
Ascon_Graz-v1	1,672.0		1,551	209	16
Ascon_VT-v1	1,491.2		1,913	233	20
Ascon_VT-v2	1,475.4		1,928	219	19
DryGASCON-v1	1,450.7	6	2,074	238	42
TinyJAMBU_TJT-v3	1,396.4	7	576	240	11
Romulus-v2	1,095.7	8	1,280	214	50
Romulus-v3	1,085.8		1,824	123	29
Spook-v2-v1	1,072.0	9	2,296	201	96
Saturnin-v2	1,061.9	10	2,414	168	81
Gimli_GT-v1	944.0		1,683	177	48
Elephant-v2	864.5	11	1,884	181	67
SCHWAEMM-v1	813.2	12*	**3,071**	135	85
PHOTON-Beetle-v1	747.0	13	2,065	178	61
GIFT-COFB-v1	733.3	14	1,041	275	96
KNOT-v3	633.6		1,367	264	80
ISAP-v2	609.5	15	2,157	200	42
COMET_CI-v1	439.1	16	1,884	223	130
TinyJAMBU_TJT-v2	438.3		461	315	46
ESTATE-v1	430.5	17	1,351	222	132
TinyJAMBU_GMU-v1	354.7		591	266	48
COMET_VT-v2	344.3		1,703	234	174
Oribatida-v1	343.0	18	1,450	276	206
Oribatida-v2	335.4		1,450	276	158
Elephant-v1	282.9		1,291	229	259
Pyjamask-v2	272.6	19	2,308	213	200
TinyJAMBU_GMU-v2	186.4		564	268	92
Xoodyak_GMU-v2	173.4		1,234	168	527
Saturnin-v1	166.3		2,020	192	591
LOCUS-v1	161.7	20	1,824	216	171
WAGE-v1	156.6	21	1,150	279	228
SpoC-v1	133.8	22	1,079	230	220
Pyjamask-v1	112.7		1,979	229	520
LOTUS-v1	108.5		1,652	145	171
ESTATE-v3	108.3		1,130	259	612
COMET_CI-v2	101.3		1,096	222	561
Gimli_TUM-v1	39.2		933	241	1,575
Gimli_TUM-v2	21.1		905	244	2,955

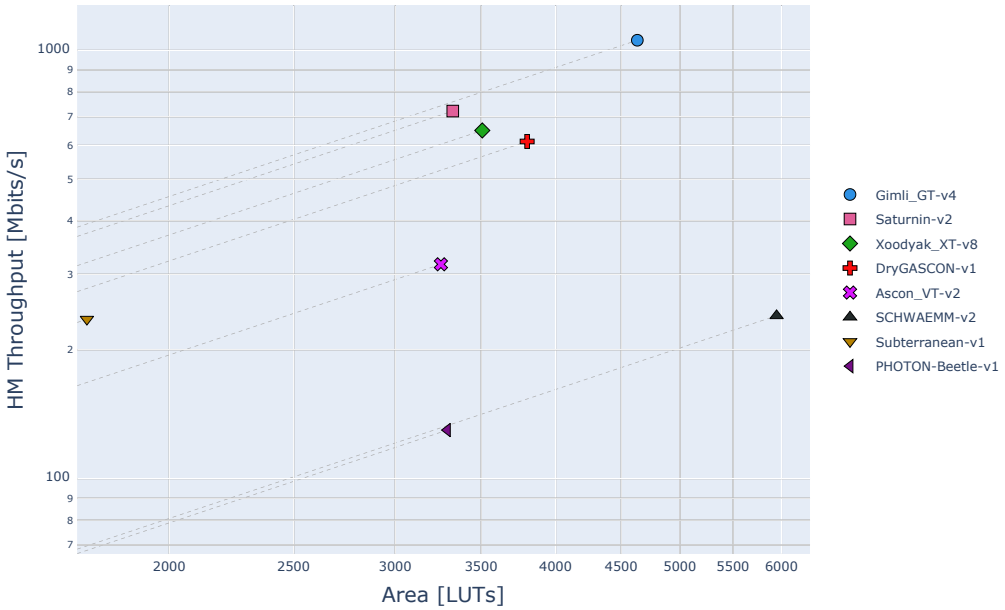

Figure 13: ECP5 Hashing Throughput for Long Messages vs LUTs

Table 7: Xilinx Artix-7 Hash Throughput for Long Messages

Variant	**Throughput HM [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Gimli_GT-v2	1,856.0	1	1,900	174	12
Xoodyak_XT-v8	1,841.2	2	2,040	187	13
Saturnin-v2	1,592.9	3	2,414	168	27
Xoodyak_XT-v7	1,536.0		1,405	228	19
DryGASCON-v1	1,450.7	4	2,074	238	21
Ascon_Graz-v2	987.4	5	1,723	216	14
Gimli_GT-v1	944.0		1,683	177	24
Ascon_VT-v2	934.4		1,928	219	15
Subterranean-v1	744.0	6	915	186	2
Xoodyak_GMU-v1	640.0		1,808	170	34
SCHWAEMM-v2	489.4	7*	**3,740**	130	34
Saturnin-v1	249.5		2,020	192	197
PHOTON-Beetle-v1	227.8	8	2,065	178	25
Xoodyak_GMU-v2	41.5		1,234	168	518
Gimli_TUM-v1	39.2		933	241	786
Gimli_TUM-v2	21.2		905	244	1,474

Table 8: Intel Cyclone 10 LP Encryption PT Throughput for Long Messages

Variant	**Throughput PT [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	5,108.5	1	1,333	159.6	0.25
Ascon_Graz-v2	1,564.3	2	2,666	146.7	12
Gimli_GT-v6	1,533.1	3	4,843	47.9	4
Gimli_GT-v3	1,391.8		3,652	87.0	8
Xoodyak_XT-v1	1,285.0	4	2,282	140.6	21
Xoodyak_XT-v7	1,223.6		2,253	133.8	21
Ascon_VT-v2	1,223.1		2,695	172.0	9
Ascon_Graz-v1	1,222.3		2,484	152.8	8
KNOT-v2	1,148.6	5	2,050	167.5	28
Ascon_VT-v1	1,130.4		2,432	176.6	10
Xoodyak_GMU-v1	1,079.1		3,135	106.8	19
DryGASCON-v1	795.6	6	3,199	130.5	21
TinyJAMBU_TJT-v3	638.8	7	1,021	159.7	8
Spook-v2-v1	588.7	8	3,912	110.4	48
Romulus-v2	566.8	9	2,086	141.7	32
Romulus-v3	563.9		2,407	79.3	18
GIFT-COFB-v1	502.2	10	1,877	184.4	47
Saturnin-v2	495.7	11	3,892	104.6	54
PHOTON-Beetle-v1	486.6	12	3,602	125.4	33
SCHWAEMM-v1	445.3	13	4,713	81.8	47
ISAP-v1	434.1	14	4,589	126.6	42
KNOT-v4	421.8		2,412	171.3	52
Elephant-v2	421.0	15	2,729	113.2	43
ISAP-v2	335.7		3,852	136.4	26
COMET_CI-v1	211.7	16	4,663	115.8	70
TinyJAMBU_TJT-v2	190.3		777	196.2	33
TinyJAMBU_GMU-v1	185.2		856	196.8	34
Oribatida-v1	173.5	17	2,512	185.7	137
ESTATE-v1	171.6	18	3,839	118.0	88
Oribatida-v2	159.5		2,221	174.5	105
Elephant-v1	152.6		2,056	163.1	171
Pyjamask-v2	113.7	19*	**8,692**	90.6	102
SpoC-v1	96.7	20	1,696	167.7	111
TinyJAMBU_GMU-v2	95.1		841	196.2	66
Saturnin-v1	94.2		3,802	145.0	394
WAGE-v1	89.6	21	1,774	159.6	114
LOCUS-v1	70.6	22	2,978	125.8	114
LOTUS-v1	58.1		2,642	103.5	114
COMET_CI-v2	57.3		2,629	132.9	297
ESTATE-v3	56.5		2,279	180.2	408

Table 9: Intel Cyclone 10 LP Encryption AD Throughput for Long Messages

Variant	**Throughput AD [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	5,108.5	1	1,333	159.6	0.25
Xoodyak_XT-v1	1,902.8	2	2,282	140.6	26
Xoodyak_XT-v7	1,811.9		2,253	133.8	26
TinyJAMBU_TJT-v3	1,703.4	3	1,021	159.7	3
Xoodyak_GMU-v1	1,566.3		3,135	106.8	24
Ascon_Graz-v2	1,564.3	4	2,666	146.7	12
Gimli_GT-v6	1,533.1	5	4,843	47.9	4
Gimli_GT-v3	1,391.8		3,652	87.0	8
Ascon_Graz-v1	1,222.3		2,484	152.8	8
KNOT-v2	1,148.6	6	2,050	167.5	28
Ascon_VT-v1	1,130.4		2,432	176.6	10
Ascon_VT-v2	1,100.8		2,695	172.0	10
Romulus-v2	1,007.6	7	2,086	141.7	18
Saturnin-v2	991.4	8	3,892	104.6	27
Romulus-v3	922.8		2,407	79.3	11
DryGASCON-v1	795.6	9	3,199	130.5	21
Elephant-v2	754.3	10	2,729	113.2	24
ISAP-v1	729.2	11	4,589	126.6	25
Spook-v2-v1	588.7	12	3,912	110.4	48
PHOTON-Beetle-v1	573.4	13	3,602	125.4	28
SCHWAEMM-v1	550.7	14	4,713	81.8	38
ISAP-v2	545.6		3,852	136.4	16
TinyJAMBU_TJT-v2	483.0		777	196.2	13
GIFT-COFB-v1	481.7	15	1,877	184.4	49
TinyJAMBU_GMU-v1	449.9		856	196.8	14
KNOT-v4	421.8		2,412	171.3	52
Oribatida-v1	344.4	16	2,512	185.7	69
ESTATE-v1	343.2	17	3,839	118.0	44
Oribatida-v2	316.1		2,221	174.5	53
Elephant-v1	296.5		2,056	163.1	88
COMET_CI-v1	246.9	18	4,663	115.8	60
TinyJAMBU_GMU-v2	241.4		841	196.2	26
Saturnin-v1	188.4		3,802	145.0	197
LOCUS-v1	141.2	19	2,978	125.8	57
Pyjamask-v2	118.4	20*	**8,692**	90.6	98
LOTUS-v1	116.2		2,642	103.5	57
ESTATE-v3	113.1		2,279	180.2	204
SpoC-v1	98.5	21	1,696	167.7	109
WAGE-v1	89.6	22	1,774	159.6	114
COMET_CI-v2	64.5		2,629	132.9	264

Table 10: Intel Cyclone 10 LP Encryption AD+PT Throughput for Long Messages

Variant	**Throughput AD+PT [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	5,108.5	1	1,333	159.6	0.5
Xoodyak_XT-v1	1,626.8	2	2,282	140.6	47
Ascon_Graz-v2	1,564.3	3	2,666	146.7	24
Xoodyak_XT-v7	1,549.0		2,253	133.8	47
Gimli_GT-v6	1,533.1	4	4,843	47.9	8
Gimli_GT-v3	1,391.8		3,652	87.0	16
Xoodyak_GMU-v1	1,351.0		3,135	106.8	43
Ascon_Graz-v1	1,222.3		2,484	152.8	16
Ascon_VT-v2	1,158.7		2,695	172.0	19
KNOT-v2	1,148.6	5	2,050	167.5	56
Ascon_VT-v1	1,130.4		2,432	176.6	20
TinyJAMBU_TJT-v3	929.1	6	1,021	159.7	11
DryGASCON-v1	795.6	7	3,199	130.5	42
Romulus-v2	725.5	8	2,086	141.7	50
Romulus-v3	700.0		2,407	79.3	29
Saturnin-v2	660.9	9	3,892	104.6	81
Spook-v2-v1	588.7	10	3,912	110.4	96
ISAP-v1	544.2	11	4,589	126.6	67
Elephant-v2	540.4	12	2,729	113.2	67
PHOTON-Beetle-v1	526.4	13	3,602	125.4	61
SCHWAEMM-v1	492.4	14	4,713	81.8	85
GIFT-COFB-v1	491.7	15	1,877	184.4	96
KNOT-v4	421.8		2,412	171.3	104
ISAP-v2	415.7		3,852	136.4	42
TinyJAMBU_TJT-v2	273.0		777	196.2	46
TinyJAMBU_GMU-v1	262.4		856	196.8	48
Oribatida-v1	230.7	16	2,512	185.7	206
ESTATE-v1	228.8	17	3,839	118.0	132
COMET_CI-v1	227.9	18	4,663	115.8	130
Oribatida-v2	212.0		2,221	174.5	158
Elephant-v1	201.5		2,056	163.1	259
TinyJAMBU_GMU-v2	136.5		841	196.2	92
Saturnin-v1	125.6		3,802	145.0	591
Pyjamask-v2	116.0	19*	**8,692**	90.6	200
SpoC-v1	97.6	20	1,696	167.7	220
LOCUS-v1	94.1	21	2,978	125.8	171
WAGE-v1	89.6	22	1,774	159.6	228
LOTUS-v1	77.5		2,642	103.5	171
ESTATE-v3	75.4		2,279	180.2	612
COMET_CI-v2	60.7		2,629	132.9	561

Table 11: Intel Cyclone 10 LP Hash Throughput for Long Messages

Variant	Throughput HM [Mbits/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per Block
Gimli_GT-v6	1,533.1	1	4,843	47.9	4
Gimli_GT-v3	1,391.8		3,652	87.0	8
Saturnin-v2	991.4	2	3,892	104.6	27
Xoodyak_XT-v7	901.6	3	2,253	133.8	19
Xoodyak_XT-v8	899.4		4,337	91.3	13
DryGASCON-v1	795.6	4	3,199	130.5	21
Ascon_VT-v2	733.9	5	2,695	172.0	15
Ascon_Graz-v2	670.4		2,666	146.7	14
Subterranean-v1	638.6	6	1,333	159.6	2
Xoodyak_GMU-v1	402.0		3,135	106.8	34
SCHWAEMM-v2	322.8	7*	**5,773**	85.7	34
Saturnin-v1	188.4		3,802	145.0	197
PHOTON-Beetle-v1	160.6	8	3,602	125.4	25

The conclusions from these tables and graphs are relatively close to the conclusions based on the results for the Artix-7 FPGA.

The ranking of candidates depending on the FPGA family used is summarized in Tables 16, 17, and 18, for PT only, AD only, and AD+PT, respectively. The major differences are as follows: Cyclone 10 LP seems to favor Ascon vs. Xoodyak, but only in the case of processing PT. On Cyclone 10 LP, the ranking of COMET_VT-v1 drops by 3-4 positions vs. Artix-7 and ECP5. At the same time, the ranking of TinyJAMBU-v1 increases by 1-3 positions vs. Artix-7. The ranking of PHOTON-Beetle improves by 3-5 positions and the ranking of ISAP-v1 drops by 0-4 positions between Artix-7 and ECP5. The changes in positions of other algorithms are relatively minor.

5.3.3 Initial Design Space Explorations

Initial design space explorations, involving at least four variants, were conducted for the following six candidates: Ascon, COMET, ESTATE, KNOT, Romulus, and Xoodyak. In the following two-dimensional graphs, apart from points representing variants of an investigated algorithm, we include also points corresponding to the implementations with the highest Throughput (Subterranean-v1), smallest area (TinyJAMBU-v1), and largest area (SCHWAEMM-v1).

In Figs. 14 and 15, the Artix-7 results are presented for four designs of Ascon. The comparison between Ascon_VT-v1 and Ascon_VT-v2, demonstrates that, in Ascon, adding hashing functionality comes with no penalty in terms of area or throughput. The designs from TU Graz outperform those from Virginia Tech. In terms of area, the advantage seems to come from using a folded vs. basic iterative architecture. Among the two designs from TU Graz, the main difference is a parameter set. Ascon_Graz-v2 implements Ascon-128a, with the 128-bit data block. Ascon_Graz-v1 implements Ascon-128, with the 64-bit data block. Both designs support hashing. Ascon_Graz-v2 is faster because of higher ratio of the Block_Size/Cycles_per_Block for both PT only and AD only, as shown in Table 3.

In Figs. 16 and 17, the Artix-7 results are presented for four designs of COMET. COMET_VT-v1, COMET_CI-v1, and COMET_CI-v2 are realizations of the primary parameter set: COMET-128_AES-128/128. COMET_VT-v2 is the realization of the parameter set COMET-128_CHAM-128/128. The difference in performance between the first three variants comes from using different hardware architectures. COMET_VT-v1

Table 12: Lattice ECP5 Encryption PT Throughput for Long Messages

Variant	**Throughput PT [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	1,884.8	1	1,725	58.9	0.25
Gimli_GT-v4	1,056.0	2	4,632	49.5	6
Xoodyak_XT-v2	905.0	3	4,302	70.7	15
Xoodyak_XT-v8	845.2		3,507	66.0	15
Xoodyak_GMU-v1	747.8		3,172	74.0	19
Gimli_GT-v3	710.4		4,934	44.4	8
KNOT-v2	625.0	4	2,241	91.2	28
DryGASCON-v1	612.8	5	3,801	100.5	21
Ascon_VT-v1	543.4	6	3,130	84.9	10
Ascon_VT-v2	527.6		3,256	74.2	9
Spook-v2-v1	414.9	7	3,655	77.8	48
PHOTON-Beetle-v1	393.5	8	3,294	101.4	33
TinyJAMBU_TJT-v3	390.8	9	881	97.7	8
SCHWAEMM-v1	361.3	10	4,685	66.3	47
Saturnin-v2	360.8	11	3,326	76.1	54
Romulus-v3	320.0	12	3,847	45.0	18
Elephant-v2	318.1	13	3,073	85.5	43
GIFT-COFB-v1	311.3	14	2,214	114.3	47
Romulus-v2	257.6		3,080	64.4	32
KNOT-v1	214.5		1,597	93.8	28
ISAP-v1	209.5	15*	**6,701**	61.1	42
COMET_VT-v2	160.3	16	2,353	111.5	89
COMET_CI-v1	147.9		3,427	80.9	70
ESTATE-v1	144.7	17	3,079	99.5	88
TinyJAMBU_GMU-v1	117.5		720	124.8	34
Oribatida-v1	111.8	18	2,832	119.7	137
Oribatida-v2	104.4		2,497	114.2	105
TinyJAMBU_TJT-v2	96.0		913	99.0	33
Pyjamask-v2	91.9	19	4,162	73.2	102
Elephant-v1	91.2		2,368	97.5	171
TinyJAMBU_GMU-v2	62.2		908	128.3	66
Saturnin-v1	59.1		3,156	91.0	394
SpoC-v1	56.6	20	2,049	98.2	111
Xoodyak_GMU-v2	55.0		2,316	74.8	261
WAGE-v1	51.1	21	2,029	91.1	114
Pyjamask-v1	45.3		3,897	92.7	262
LOCUS-v1	44.7	22	3,161	79.6	114
COMET_CI-v2	40.7		1,974	94.3	297
ESTATE-v3	33.3		2,026	106.3	408
LOTUS-v1	31.2		2,820	55.6	114

Table 13: Lattice ECP5 Encryption AD Throughput for Long Messages

Variant	Throughput AD [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Subterranean-v1	1,884.8	1	1,725	58.9	0.25
Xoodyak_XT-v2	1,244.3	2	4,302	70.7	20
Xoodyak_XT-v8	1,162.1		3,507	66.0	20
Xoodyak_GMU-v1	1,085.3		3,172	74.0	24
Gimli_GT-v4	1,056.0	3	4,632	49.5	6
TinyJAMBU_TJT-v3	1,042.1	4	881	97.7	3
Saturnin-v2	721.5	5	3,326	76.1	27
Gimli_GT-v3	710.4		4,934	44.4	8
KNOT-v2	625.0	6	2,241	91.2	28
DryGASCON-v1	612.8	7	3,801	100.5	21
Elephant-v2	570.0	8	3,073	85.5	24
Ascon_VT-v1	543.4	9	3,130	84.9	10
Romulus-v3	523.6	10	3,847	45.0	11
Ascon_VT-v2	474.9		3,256	74.2	10
PHOTON-Beetle-v1	463.7	11	3,294	101.4	28
Romulus-v2	458.0		3,080	64.4	18
SCHWAEMM-v1	446.9	12	4,685	66.3	38
Spook-v2-v1	414.9	13	3,655	77.8	48
ISAP-v1	351.9	14*	**6,701**	61.1	25
GIFT-COFB-v1	298.6	15	2,214	114.3	49
ESTATE-v1	289.5	16	3,079	99.5	44
TinyJAMBU_GMU-v1	285.3		720	124.8	14
TinyJAMBU_TJT-v2	243.7		913	99.0	13
Oribatida-v1	222.0	17	2,832	119.7	69
KNOT-v1	214.5		1,597	93.8	28
Oribatida-v2	206.9		2,497	114.2	53
Elephant-v1	177.3		2,368	97.5	88
COMET_CI-v1	172.6	18	3,427	80.9	60
COMET_VT-v2	167.8		2,353	111.5	85
TinyJAMBU_GMU-v2	157.9		908	128.3	26
Saturnin-v1	118.3		3,156	91.0	197
Xoodyak_GMU-v2	99.0		2,316	74.8	266
Pyjamask-v2	95.6	19	4,162	73.2	98
LOCUS-v1	89.4	20	3,161	79.6	57
ESTATE-v3	66.7		2,026	106.3	204
LOTUS-v1	62.4		2,820	55.6	57
SpoC-v1	57.7	21	2,049	98.2	109
WAGE-v1	51.1	22	2,029	91.1	114
Pyjamask-v1	46.0		3,897	92.7	258
COMET_CI-v2	45.7		1,974	94.3	264

Table 14: Lattice ECP5 Encryption AD+PT Throughput for Long Messages

Variant	**Throughput AD+PT [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per Block**
Subterranean-v1	1,884.8	1	1,725	58.9	0.5
Xoodyak_XT-v2	1,098.9	2	4,302	70.7	35
Gimli_GT-v4	1,056.0	3	4,632	49.5	12
Xoodyak_XT-v8	1,026.3		3,507	66.0	35
Xoodyak_GMU-v1	936.2		3,172	74.0	43
Gimli_GT-v3	710.4		4,934	44.4	16
KNOT-v2	625.0	4	2,241	91.2	56
DryGASCON-v1	612.8	5	3,801	100.5	42
TinyJAMBU_TJT-v3	568.4	6	881	97.7	11
Ascon_VT-v1	543.4	7	3,130	84.9	20
Ascon_VT-v2	499.9		3,256	74.2	19
Saturnin-v2	481.0	8	3,326	76.1	81
PHOTON-Beetle-v1	425.7	9	3,294	101.4	61
Spook-v2-v1	414.9	10	3,655	77.8	96
Elephant-v2	408.4	11	3,073	85.5	67
SCHWAEMM-v1	399.6	12	4,685	66.3	85
Romulus-v3	397.2	13	3,847	45.0	29
Romulus-v2	329.7		3,080	64.4	50
GIFT-COFB-v1	304.8	14	2,214	114.3	96
ISAP-v1	262.6	15*	**6,701**	61.1	67
KNOT-v1	214.5		1,597	93.8	56
ESTATE-v1	193.0	16	3,079	99.5	132
TinyJAMBU_GMU-v1	166.4		720	124.8	48
COMET_VT-v2	164.0	17	2,353	111.5	174
COMET_CI-v1	159.3		3,427	80.9	130
Oribatida-v1	148.7	18	2,832	119.7	206
Oribatida-v2	138.8		2,497	114.2	158
TinyJAMBU_TJT-v2	137.7		913	99.0	46
Elephant-v1	120.5		2,368	97.5	259
Pyjamask-v2	93.7	19	4,162	73.2	200
TinyJAMBU_GMU-v2	89.3		908	128.3	92
Saturnin-v1	78.8		3,156	91.0	591
Xoodyak_GMU-v2	77.2		2,316	74.8	527
LOCUS-v1	59.6	20	3,161	79.6	171
SpoC-v1	57.1	21	2,049	98.2	220
WAGE-v1	51.1	22	2,029	91.1	228
Pyjamask-v1	45.6		3,897	92.7	520
ESTATE-v3	44.5		2,026	106.3	612
COMET_CI-v2	43.0		1,974	94.3	561
LOTUS-v1	41.6		2,820	55.6	171

Table 15: Lattice ECP5 Hash Throughput for Long Messages

Variant	Throughput HM [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Gimli_GT-v4	1,056.0	1	4,632	49.5	6
Saturnin-v2	721.5	2	3,326	76.1	27
Gimli_GT-v3	710.4		4,934	44.4	8
Xoodyak_XT-v8	650.1	3	3,507	66.0	13
DryGASCON-v1	612.8	4	3,801	100.5	21
Xoodyak_XT-v7	450.4		3,272	66.9	19
Ascon_VT-v2	316.6	5	3,256	74.2	15
Xoodyak_GMU-v1	278.6		3,172	74.0	34
SCHWAEMM-v2	240.1	6*	**5,947**	63.8	34
Subterranean-v1	235.6	7	1,725	58.9	2
PHOTON-Beetle-v1	129.8	8	3,294	101.4	25
Saturnin-v1	118.3		3,156	91.0	197
Xoodyak_GMU-v2	18.5		2,316	74.8	518

Table 16: FPGA Rankings based on Encryption PT Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Xoodyak_XT-v8	Ascon_Graz-v2	Gimli_GT-v4
3	Ascon_Graz-v2	Gimli_GT-v6	Xoodyak_XT-v2
4	Gimli_GT-v2	Xoodyak_XT-v1	KNOT-v2
5	KNOT-v2	KNOT-v2	DryGASCON-v1
6	DryGASCON-v1	DryGASCON-v1	Ascon_VT-v1
7	Spook-v2-v1	TinyJAMBU_TJT-v3	Spook-v2-v1
8	TinyJAMBU_TJT-v3	Spook-v2-v1	PHOTON-Beetle-v1
9	Romulus-v3	Romulus-v2	TinyJAMBU_TJT-v3
10	Saturnin-v2	GIFT-COFB-v1	SCHWAEMM-v1
11	GIFT-COFB-v1	Saturnin-v2	Saturnin-v2
12	SCHWAEMM-v1	PHOTON-Beetle-v1	Romulus-v3
13	PHOTON-Beetle-v1	SCHWAEMM-v1	Elephant-v2
14	Elephant-v2	ISAP-v1	GIFT-COFB-v1
15	ISAP-v2	Elephant-v2	ISAP-v1
16	COMET_CI-v1	COMET_CI-v1	COMET_VT-v2
17	ESTATE-v1	Oribatida-v1	ESTATE-v1
18	Pyjamask-v2	ESTATE-v1	Oribatida-v1
19	Oribatida-v1	Pyjamask-v2	Pyjamask-v2
20	WAGE-v1	SpoC-v1	SpoC-v1
21	SpoC-v1	WAGE-v1	WAGE-v1
22	LOCUS-v1	LOCUS-v1	LOCUS-v1

Table 17: FPGA Rankings based on Encryption AD Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Xoodyak_XT-v8	Xoodyak_XT-v1	Xoodyak_XT-v2
3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Gimli_GT-v4
4	Ascon_Graz-v2	Ascon_Graz-v2	TinyJAMBU_TJT-v3
5	Gimli_GT-v2	Gimli_GT-v6	Saturnin-v2
6	KNOT-v2	KNOT-v2	KNOT-v2
7	Saturnin-v2	Romulus-v2	DryGASCON-v1
8	Romulus-v2	Saturnin-v2	Elephant-v2
9	DryGASCON-v1	DryGASCON-v1	Ascon_VT-v1
10	Elephant-v2	Elephant-v2	Romulus-v3
11	Spook-v2-v1	ISAP-v1	PHOTON-Beetle-v1
12	SCHWAEMM-v1	Spook-v2-v1	SCHWAEMM-v1
13	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Spook-v2-v1
14	ISAP-v2	SCHWAEMM-v1	ISAP-v1
15	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1
16	ESTATE-v1	Oribatida-v1	ESTATE-v1
17	Oribatida-v1	ESTATE-v1	Oribatida-v1
18	COMET_CI-v1	COMET_CI-v1	COMET_CI-v1
19	Pyjamask-v2	LOCUS-v1	Pyjamask-v2
20	LOCUS-v1	Pyjamask-v2	LOCUS-v1
21	WAGE-v1	SpoC-v1	SpoC-v1
22	SpoC-v1	WAGE-v1	WAGE-v1

Table 18: FPGA Rankings based on Encryption AD+PT Throughput for Long Messages

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Xoodyak_XT-v8	Xoodyak_XT-v1	Xoodyak_XT-v2
3	Ascon_Graz-v2	Ascon_Graz-v2	Gimli_GT-v4
4	Gimli_GT-v2	Gimli_GT-v6	KNOT-v2
5	KNOT-v2	KNOT-v2	DryGASCON-v1
6	DryGASCON-v1	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
7	TinyJAMBU_TJT-v3	DryGASCON-v1	Ascon_VT-v1
8	Romulus-v2	Romulus-v2	Saturnin-v2
9	Spook-v2-v1	Saturnin-v2	PHOTON-Beetle-v1
10	Saturnin-v2	Spook-v2-v1	Spook-v2-v1
11	Elephant-v2	ISAP-v1	Elephant-v2
12	SCHWAEMM-v1	Elephant-v2	SCHWAEMM-v1
13	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Romulus-v3
14	GIFT-COFB-v1	SCHWAEMM-v1	GIFT-COFB-v1
15	ISAP-v2	GIFT-COFB-v1	ISAP-v1
16	COMET_CI-v1	Oribatida-v1	ESTATE-v1
17	ESTATE-v1	ESTATE-v1	COMET_VT-v2
18	Oribatida-v1	COMET_CI-v1	Oribatida-v1
19	Pyjamask-v2	Pyjamask-v2	Pyjamask-v2
20	LOCUS-v1	SpoC-v1	LOCUS-v1
21	WAGE-v1	LOCUS-v1	SpoC-v1
22	SpoC-v1	WAGE-v1	WAGE-v1

uses the basic iterative architecture, while COMET_CI-v1 and COMET_CI-v2 use folded architectures with different folding factors. For the same basic iterative architecture, the implementation of COMET-128_AES-128/128 (COMET_VT-v1) is both faster and bigger than the implementation of COMET-128_CHAM-128/128 (COMET_VT-v2). As shown in Table 3, the number of clock cycles per block is significantly higher for COMET-128_CHAM-128/128. At the same time, implementing one round of CHAM-128/128 takes significantly less area than implementing one round of AES-128/128.

In Figs. 18 and 19, the Artix-7 results are presented for four designs of ESTATE. ESTATE-v1 and ESTATE-v2 are implementations of the parameter set ESTATE_TweAES-128, obtained by instantiating the ESTATE mode of operation with the TweAES-128 block cipher. ESTATE-v3 and ESTATE-v4 are implementations of the parameter set ESTATE_TweGIFT-128, obtained by instantiating the ESTATE mode of operation with the TweGIFT-128 block cipher. Within each pair, the former implementation uses a 32-bit datapath and the latter an 8-bit datapath. For the implementations using the same datapath width, the realizations of ESTATE_TweAES-128 (ESTATE-v1 and ESTATE-v2) are significantly faster. At the same time, both 8-bit architectures (ESTATE-v2 and ESTATE-v4) have their areas smaller than 1000 LUTs.

In Figs. 20, 21, and 22, the Artix-7 results are presented for ten designs of Gimli. Seven designs from the Gimli Team are optimized for the maximum throughput. Three designs from the Technical University of Munich (TUM) are optimized for the minimum area. Gimli_GT-v1 is a basic iterative architecture of Gimli, with one round executed per one clock cycle. The designs from Gimli_GT-v2 to Gimli_GT-v7 are unrolled architectures, with a different number of rounds executed per clock cycle. The unrolling factor is 2 for Gimli_GT-v2, 3 for Gimli_GT-v3, 4 for Gimli_GT-v4, 6 for Gimli_GT-v5, and 8 for Gimli_GT-v6, and 12 for Gimli_GT-v7. Only Gimli_GT-v1 and Gimli_GT-v2 have areas smaller than 2500 LUTs. Out of these two, Gimli_GT-v2 is almost two times faster. The number of clock cycles per block in Gimli_GT-v6 and Gimli_GT-v7 is limited by the LWC interface, capable of reading one 128-bit block in no less than 4 clock cycles. As a result, the speed of designs with 6 and 8 rounds unrolled is approximately the same. The throughput of Gimli_GT-v7, with 12 rounds unrolled, is lower because of the decrease in the maximum clock frequency. Somewhat surprisingly, Gimli_GT-v4, with 4 rounds unrolled, is both smaller and faster than Gimli_GT-v4, with 3 rounds unrolled. The designs from the Technical University of Munich (TUM) have substantially higher number of clock cycles per round (786, 1474, and 2850 vs. 24 for Gimli_GT-v1). At the same time, they all reach area below 1000 LUTs, which may be important in some applications.

In Figs. 23 and 24, the Artix-7 results are presented for four designs of KNOT. The four variants correspond to four different parameter sets, denoted as KNOT-AEAD(k, b, r), where k is the key length, b is the state size, and r is the bitrate. The bitrate determines the block size of plaintext and AD. KNOT-v1 and KNOT-v2 represent the parameter sets KNOT-AEAD(128, 256, 64) and KNOT-AEAD (128, 384, 192), respectively. Both are believed to have the same security strength, but the latter uses a higher bitrate due to its bigger state size (permutation width), hence it has a higher throughput. KNOT-v4 represents the parameter set KNOT-AEAD(256, 512, 128) which has the highest security level, and KNOT-v3 represents KNOT-AEAD(192, 384, 96), which has the intermediate security level. Higher security levels come with the penalty of a higher number of clock cycles per block: 40 for KNOT-v3=KNOT-AEAD(192, 384, 96) and 52 for KNOT-v4=KNOT-AEAD(256, 512, 128), vs. 28 for KNOT-v1=KNOT-AEAD(128, 256, 64) and KNOT-v2=KNOT-AEAD (128, 384, 192). As a result, KNOT-v2, which has the highest block size for plaintext and AD (192 bits) is by far the fastest. The remaining variants offer similar speed, but differ in terms of area, which is determined primarily by the state size (permutation width), which is equal to 128 for KNOT-v1, 384 for KNOT-v3, and 512 for KNOT-v4.

In Figs. 25 and 26, the Artix-7 results are presented for five designs of Romulus. All variants are implementations of the same primary parameter set Romulus-N1, with the plaintext and AD block sizes of 128-bits. The implemented variants differ only in hardware architecture. These hardware architectures are called by authors: the round-based architecture (Romulus-v1), two-round architecture (Romulus-v2), four-round architecture (Romulus-v3), eight-round architecture (Romulus-v4), and low-area architecture (Romulus-v4). With the increase in the number of rounds unrolled, the number of clock cycles per block decreases, but at the same time, the clock frequency decreases. For Artix-7, Romulus-v2 with the two-round architecture is optimal from the point of view of throughput. Romulus-v3 and Romulus-v4 are both bigger and slower. Romulus-v1 has a somewhat comparable speed and area smaller than 1000 LUTs. As a result, its throughput/area ratio is the second largest. Romulus-v5 is only about 70 LUTs smaller than Romulus-v1 and over 20 times slower. As shown in Tables 8, 9, 10, and 11, 12, 13, 14 for Cyclone 10 LP FPGAs, Romulus-v2 is the also fastest, but for ECP5 FPGAs, it is outperformed by Romulus-v3.

In Figs. 27 and 28, the Artix-7 results are presented for six designs of TinyJAMBU. These designs differ in the number of steps executed per clock cycle. These numbers of steps are: 128 for TinyJAMBU_TJT-v3, 32 for TinyJAMBU_TJT-v2 and TinyJAMBU_GMU-v1, 16 for TinyJAMBU_GMU-v2, 8 for TinyJAMBU_TJT-v1, and 1 for TinyJAMBU_GMU-v1. The larger number of steps per clock cycle, the higher the throughput. At the same time the area of the circuit increases only moderately. For the same number of steps per clock cycle, 32, TinyJAMBU_TJT-v2 is both slightly faster and significantly smaller than TinyJAMBU_GMU-v1.

In Figs. 29, 30, and 31 the Artix-7 results are presented for six designs of Xoodyak. Four designs were submitted by the Xoodyak Team + Silvia, with Silvia Mella as the primary designer. Two designs were submitted by GMU. Variants Xoodyak_XT-v7, Xoodyak_XT-v8, Xoodyak_GMU-v1, and Xoodyak_GMU-v2 support hashing. By comparing the throughput and area of Xoodyak_XT-v7 vs. Xoodyak_XT-v1, and Xoodyak_XT-v8 vs. Xoodyak_XT-v2, it can be seen that the support for hashing does not introduce any performance penalty in terms of either area or speed. Xoodyak_XT-v8 (a 2x unrolled architecture) is slightly faster than the basic iterative architecture, but it also takes over 600 more LUTs. One of the GMU designs, Xoodyak_GMU-v1, with the 384-bit datapath, is slightly slower than the four investigated designs from Xoodyak Team. Its area falls between areas of Xoodyak_XT-v7 and Xoodyak_XT-v8, with the same AEAD+Hash functionality. The second design from GMU is very significantly slower, and only about 170 LUTs smaller than Xoodyak_XT-v1. Thus, this design is not really competitive.

5.4 Throughputs for Short Inputs

In the Appendix, in Tables 25–51, we provide values of throughputs for medium and short input sizes, such as 1536 bytes, 64 bytes, and 16 bytes, respectively.

For 1536-byte plaintexts, the throughputs are very close to throughputs for long inputs. The average percentage is 97%, the minimum 89% (Subterranean-v1). Multiple algorithms reach 99%. For 64-byte plaintexts, this ratio varies from 25% for Subterranean-v1 to 88% for ESTATE-v3, with an average of 61%. For 16-byte plaintexts, the ratio varies from 8% for Subterranean-v1 to 65% for ESTATE-v3, with an average of 31%.

For 1536-byte ADs, the average percentage is 96%, the minimum 89% (Subterranean-v1). Multiple algorithms reach 99%. For 64-byte ADs, this ratio varies from 25% Subterranean-v1 to 79% for ESTATE-v3 and SpoC-v1, with an average of 53%. For 16-byte plaintexts, the ratio varies from 8% for Subterranean-v1 to 48% for ESTATE-v3 and SpoC-v1, with an average of 24%.

All mentioned above percentages are dependent only on the algorithm and its hardware architecture. They do not depend on a particular FPGA device.

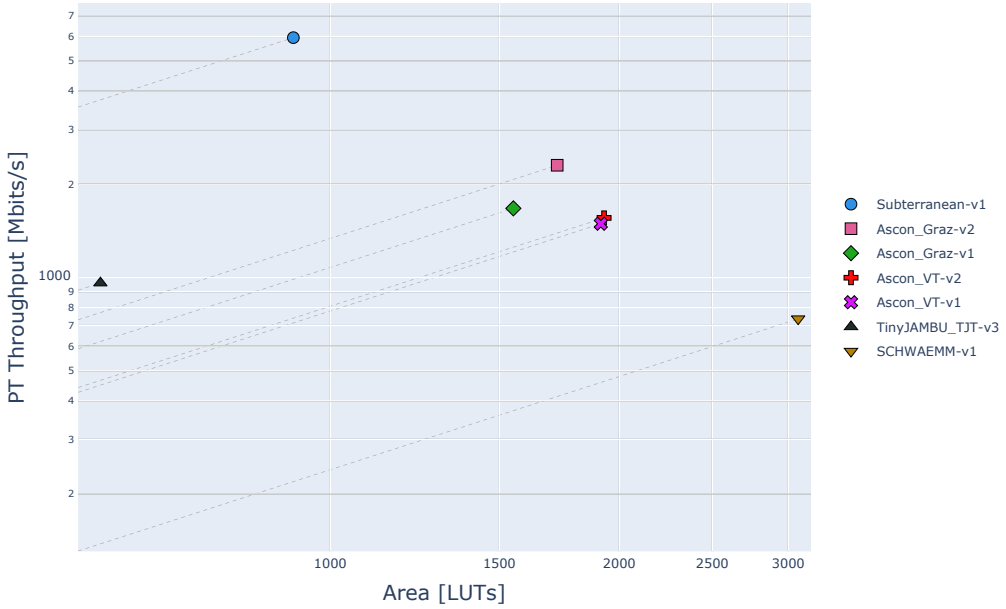

Figure 14: Artix-7 Ascon PT Throughput for Long Messages vs LUTs

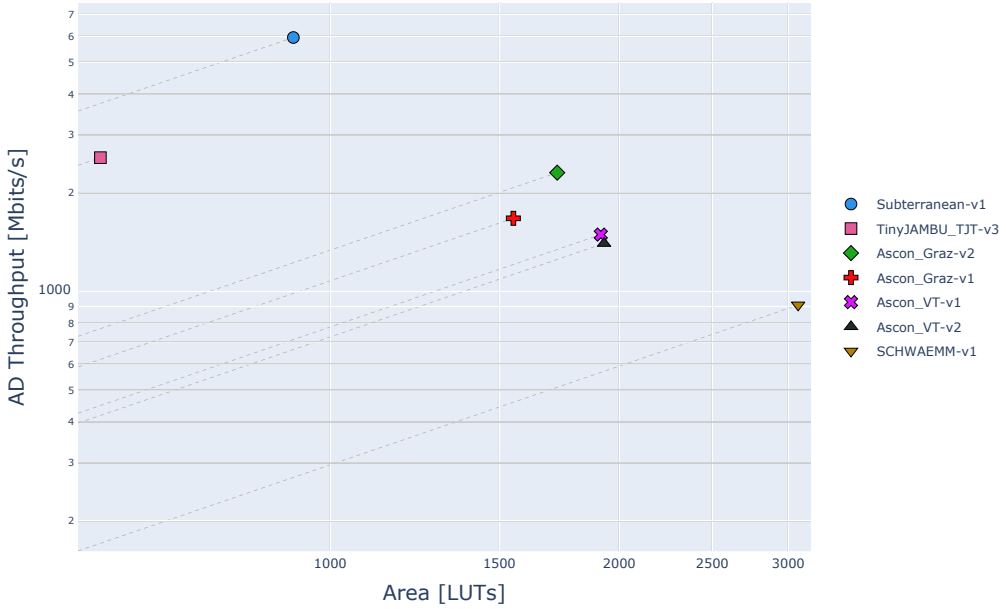

Figure 15: Artix-7 Ascon AD Throughput for Long Messages vs LUTs

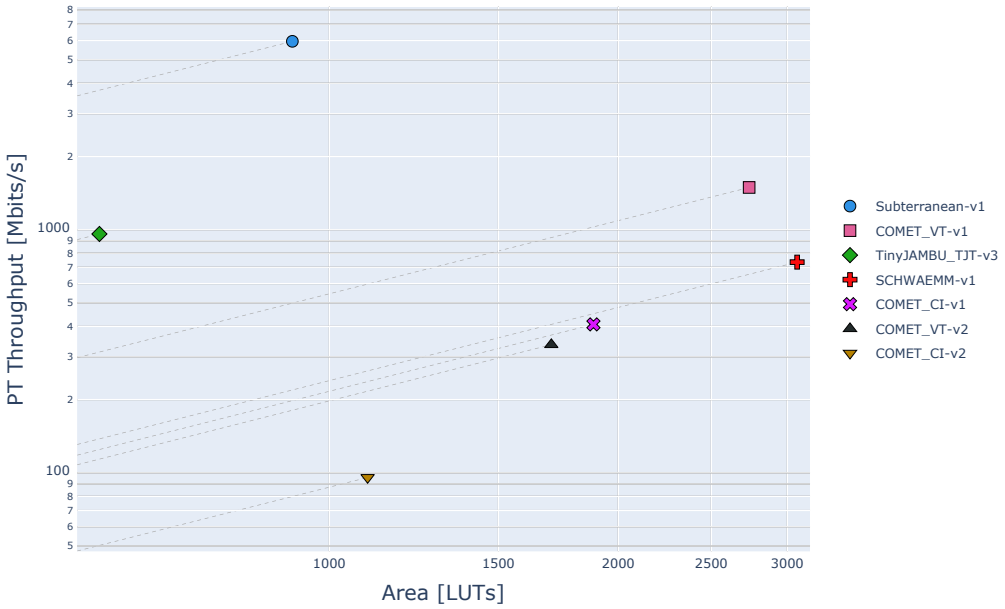

Figure 16: Artix-7 COMET PT Throughput for Long Messages vs LUTs

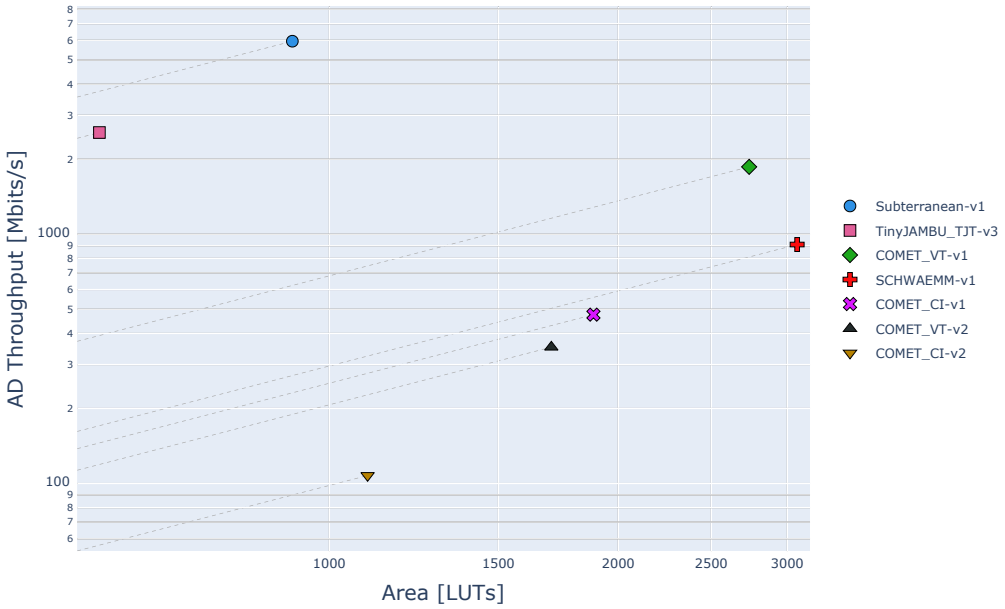

Figure 17: Artix-7 COMET AD Throughput for Long Messages vs LUTs

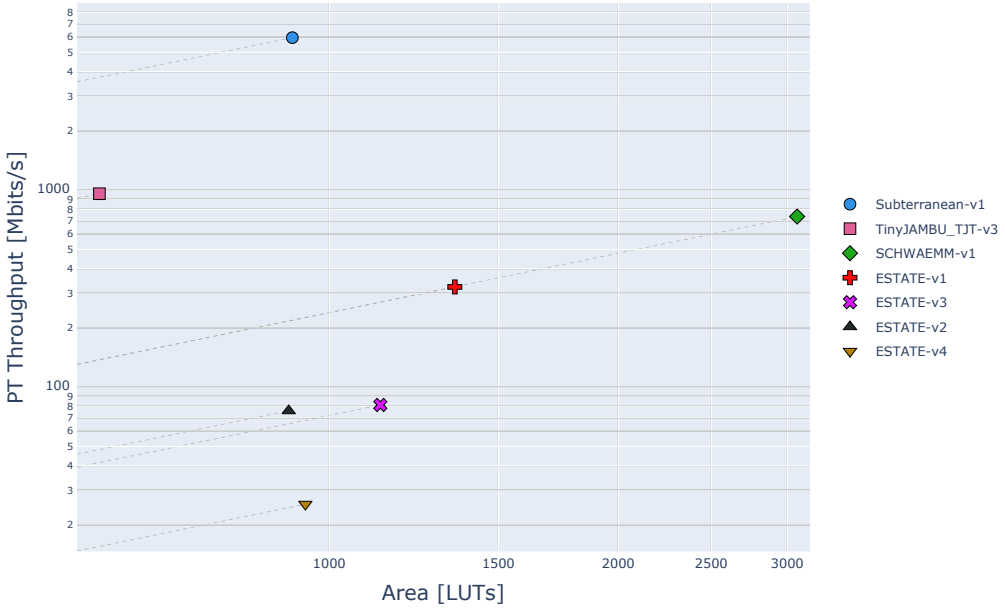

Figure 18: Artix-7 ESTATE PT Throughput for Long Messages vs LUTs

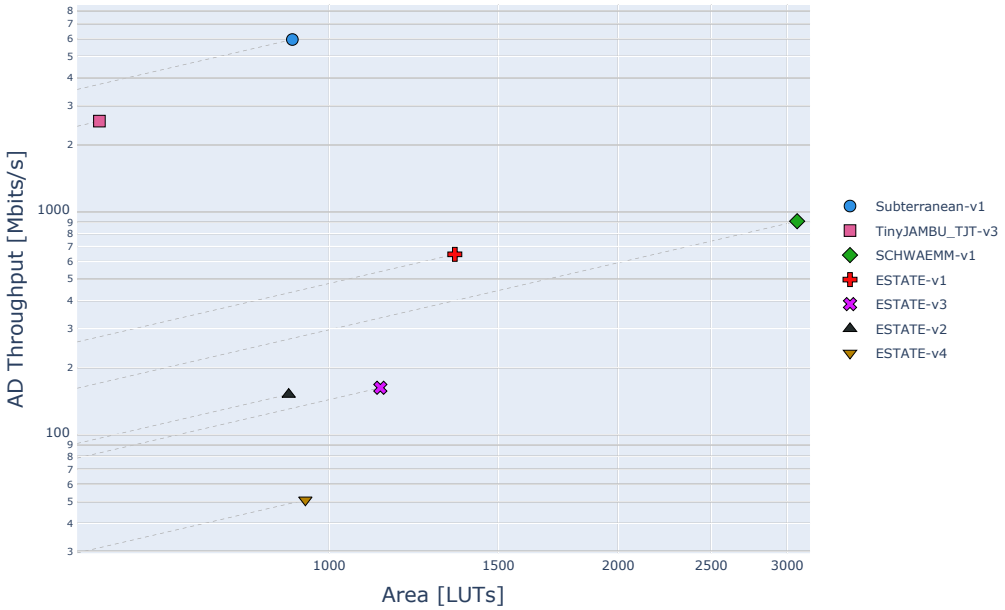

Figure 19: Artix-7 ESTATE AD Throughput for Long Messages vs LUTs

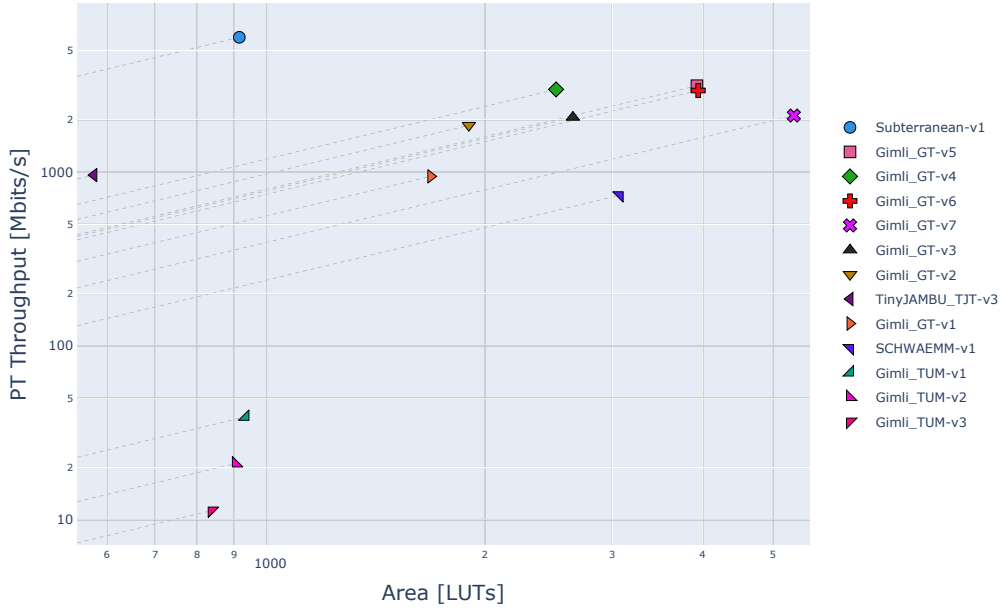

Figure 20: Artix-7 Gimli PT Throughput for Long Messages vs LUTs

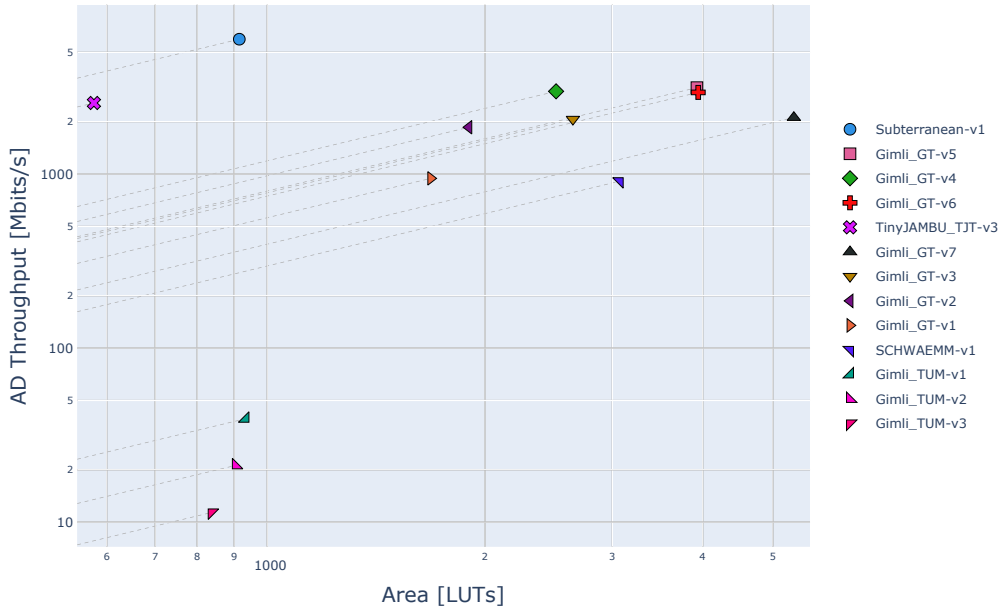

Figure 21: Artix-7 Gimli AD Throughput for Long Messages vs LUTs

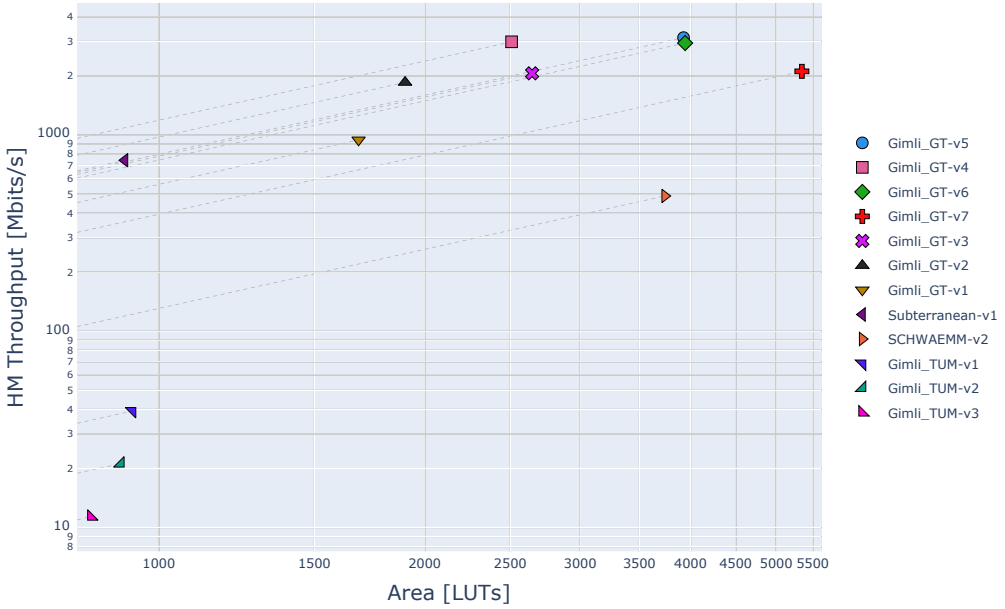

Figure 22: Artix-7 Gimli Hash Throughput for Long Messages vs LUTs

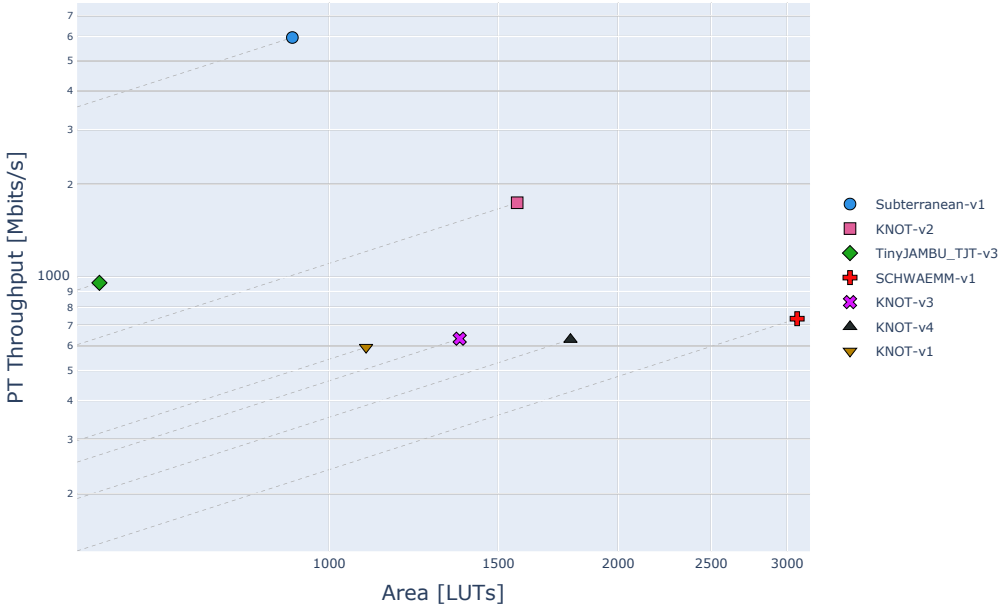

Figure 23: Artix-7 KNOT PT Throughput for Long Messages vs LUTs

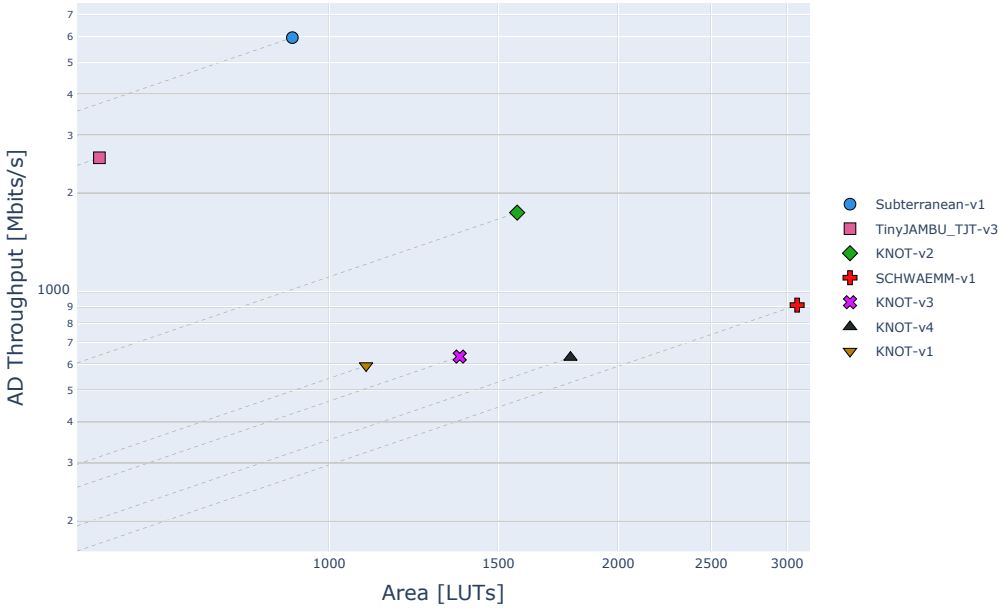

Figure 24: Artix-7 KNOT AD Throughput for Long Messages vs LUTs

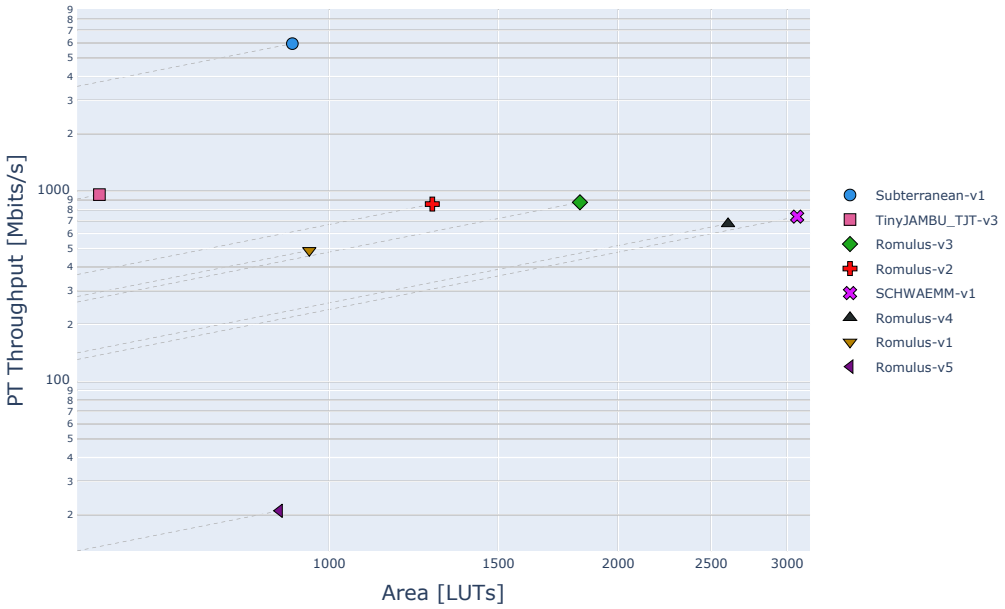

Figure 25: Artix-7 Romulus PT Throughput for Long Messages vs LUTs

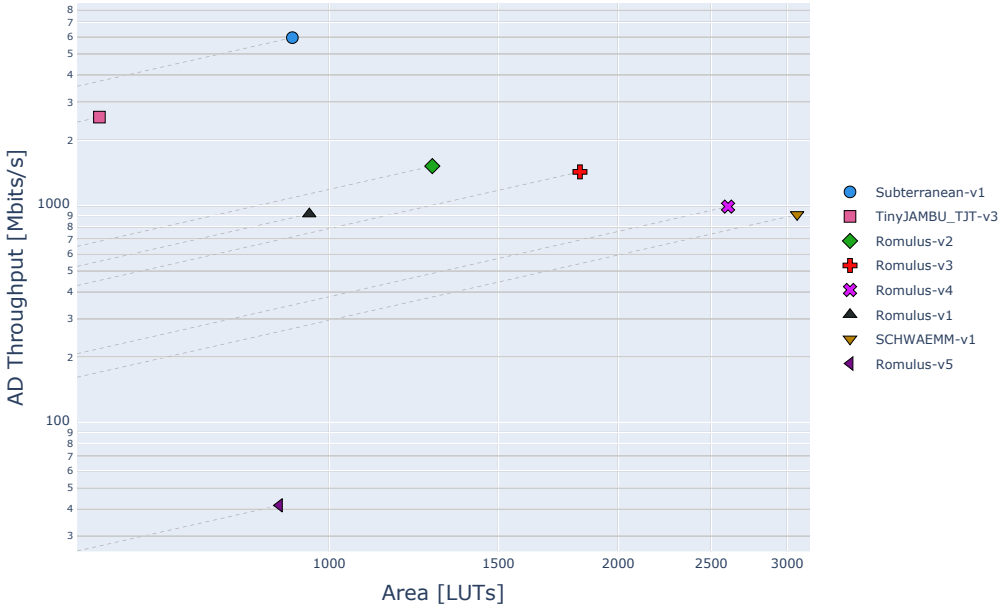

Figure 26: Artix-7 Romulus AD Throughput for Long Messages vs LUTs

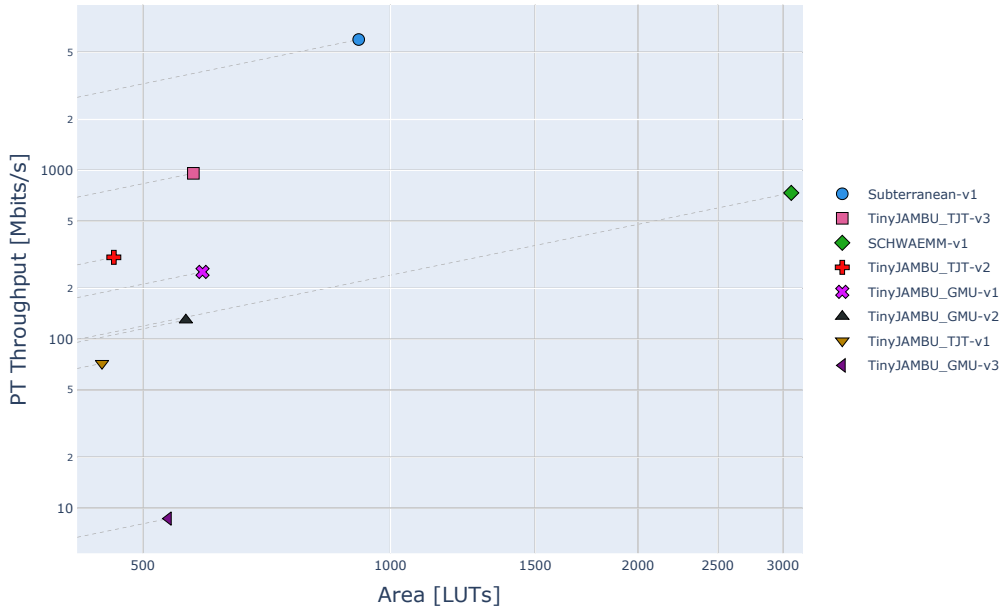

Figure 27: Artix-7 TinyJAMBU PT Throughput for Long Messages vs LUTs

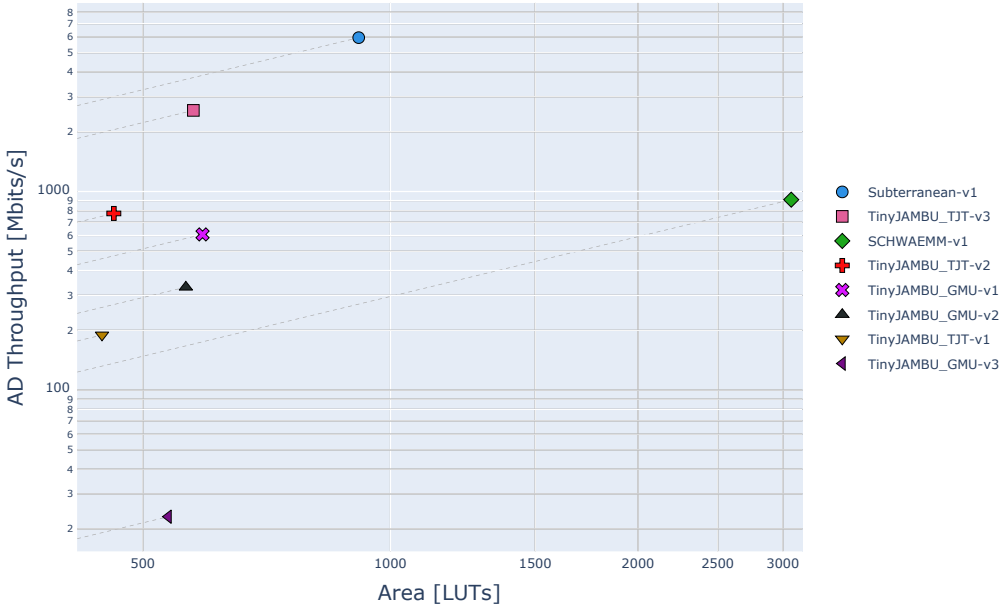

Figure 28: Artix-7 TinyJAMBU AD Throughput for Long Messages vs LUTs

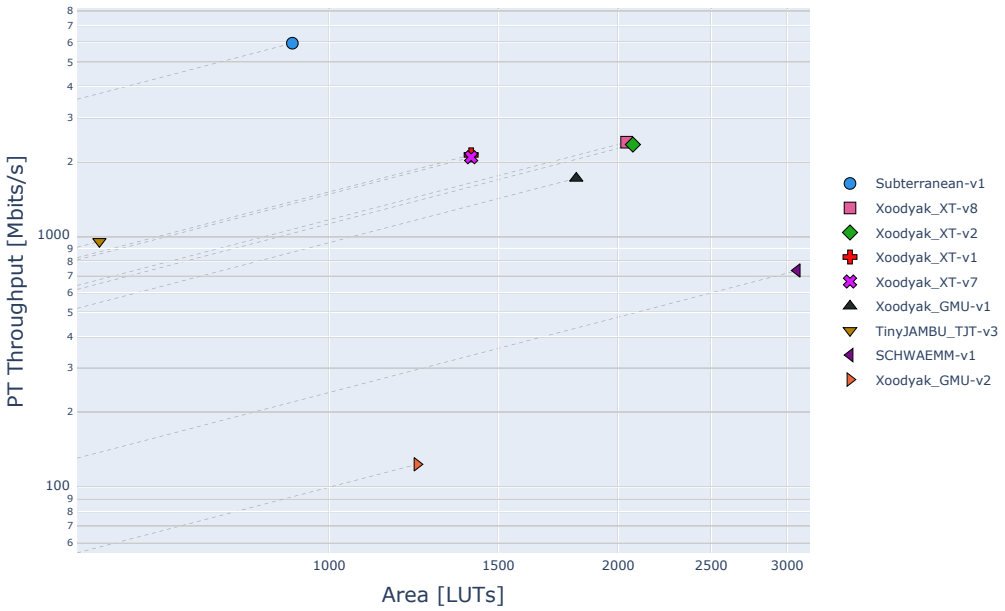

Figure 29: Artix-7 Xoodyak PT Throughput for Long Messages vs LUTs

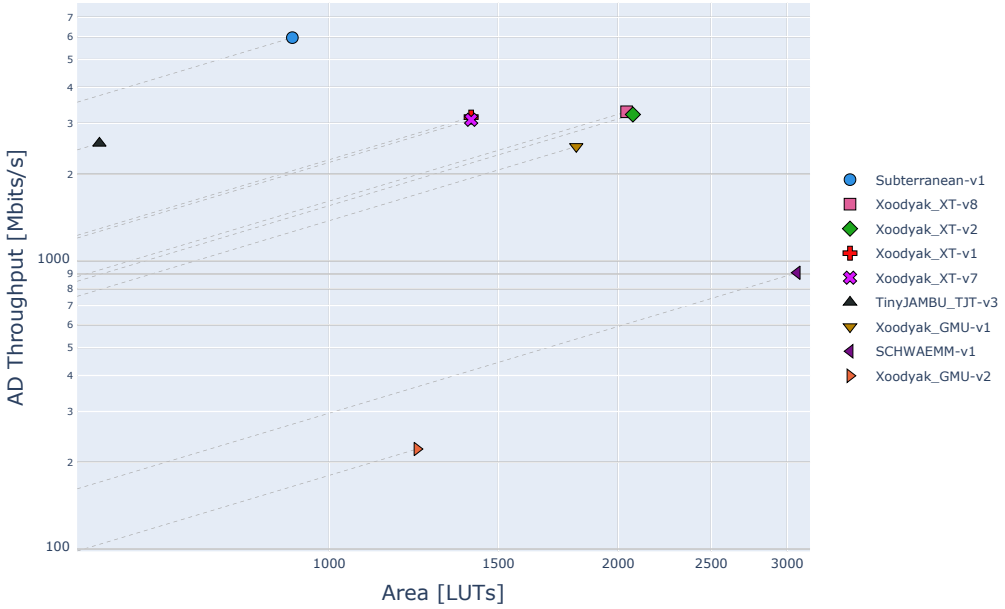

Figure 30: Artix-7 Xoodyak AD Throughput for Long Messages vs LUTs

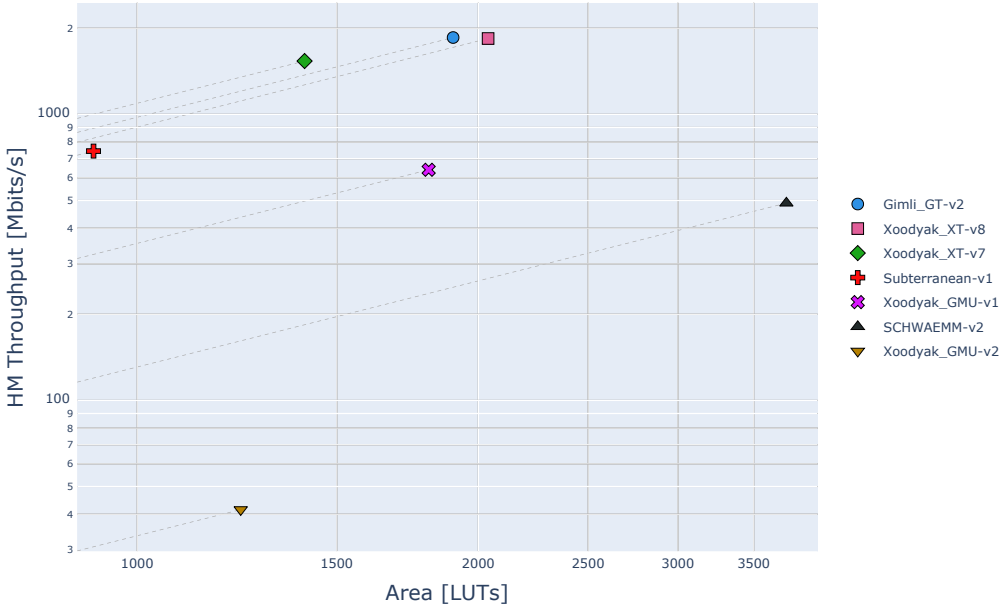

Figure 31: Artix-7 Xoodyak Hash Throughput for Long Messages vs LUTs

Table 19: Xilinx Artix-7 Encryption PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	Ascon_VT-v1
2	Xoodyak_XT-v8	Xoodyak_XT-v8	Ascon_Graz-v2	Subterranean-v1
3	Ascon_Graz-v2	Ascon_Graz-v2	Xoodyak_XT-v8	DryGASCON-v1
4	Gimli_GT-v2	Gimli_GT-v2	DryGASCON-v1	Xoodyak_XT-v8
5	KNOT-v2	KNOT-v2	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
6	DryGASCON-v1	DryGASCON-v1	KNOT-v2	Romulus-v2
7	Spook-v2-v1	Spook-v2-v1	Gimli_GT-v2	PHOTON-Beetle-v1
8	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Romulus-v2	KNOT-v2
9	Romulus-v3	Romulus-v3	Spook-v2-v1	Elephant-v2
10	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	Gimli_GT-v2
11	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1
12	SCHWAEMM-v1	SCHWAEMM-v1	Elephant-v2	ESTATE-v1
13	PHOTON-Beetle-v1	PHOTON-Beetle-v1	SCHWAEMM-v1	Spook-v2-v1
14	Elephant-v2	Elephant-v2	Saturnin-v2	COMET_CI-v1
15	ISAP-v2	ISAP-v2	COMET_CI-v1	SCHWAEMM-v1
16	COMET_CI-v1	COMET_CI-v1	ESTATE-v1	Oribatida-v1
17	ESTATE-v1	ESTATE-v1	Oribatida-v1	Saturnin-v2
18	Pyjamask-v2	Pyjamask-v2	ISAP-v2	LOCUS-v1
19	Oribatida-v1	Oribatida-v1	Pyjamask-v2	SpoC-v1
20	WAGE-v1	WAGE-v1	SpoC-v1	ISAP-v2
21	SpoC-v1	SpoC-v1	LOCUS-v1	Pyjamask-v2
22	LOCUS-v1	LOCUS-v1	WAGE-v1	WAGE-v1

Table 20: Xilinx Artix-7 Encryption AD Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	TinyJAMBU_TJT-v3
2	Xoodyak_XT-v8	Xoodyak_XT-v8	TinyJAMBU_TJT-v3	Subterranean-v1
3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Xoodyak_XT-v8	Xoodyak_XT-v8
4	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_Graz-v2	DryGASCON-v1
5	Gimli_GT-v2	Gimli_GT-v2	DryGASCON-v1	Ascon_VT-v1
6	KNOT-v2	KNOT-v2	Romulus-v2	Romulus-v2
7	Saturnin-v2	Romulus-v2	Gimli_GT-v2	GIFT-COFB-v1
8	Romulus-v2	Saturnin-v2	KNOT-v2	PHOTON-Beetle-v1
9	DryGASCON-v1	DryGASCON-v1	PHOTON-Beetle-v1	ESTATE-v1
10	Elephant-v2	Elephant-v2	Elephant-v2	Gimli_GT-v2
11	Spook-v2-v1	Spook-v2-v1	GIFT-COFB-v1	KNOT-v2
12	SCHWAEMM-v1	SCHWAEMM-v1	Spook-v2-v1	Elephant-v2
13	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ESTATE-v1	Spook-v2-v1
14	ISAP-v2	ISAP-v2	SCHWAEMM-v1	COMET_CI-v1
15	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	SCHWAEMM-v1
16	ESTATE-v1	ESTATE-v1	COMET_CI-v1	Saturnin-v2
17	Oribatida-v1	Oribatida-v1	Oribatida-v1	Oribatida-v2
18	COMET_CI-v1	COMET_CI-v1	ISAP-v2	LOCUS-v1
19	Pyjamask-v2	Pyjamask-v2	LOCUS-v1	ISAP-v2
20	LOCUS-v1	LOCUS-v1	Pyjamask-v2	SpoC-v1
21	WAGE-v1	WAGE-v1	SpoC-v1	Pyjamask-v2
22	SpoC-v1	SpoC-v1	WAGE-v1	WAGE-v1

Table 21: Xilinx Artix-7 Encryption AD+PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Xoodyak_XT-v8	Xoodyak_XT-v8	Xoodyak_XT-v8	Xoodyak_XT-v8
3	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_Graz-v2	TinyJAMBU_TJT-v3
4	Gimli_GT-v2	Gimli_GT-v2	TinyJAMBU_TJT-v3	Ascon_Graz-v2
5	KNOT-v2	KNOT-v2	DryGASCON-v1	DryGASCON-v1
6	DryGASCON-v1	DryGASCON-v1	Gimli_GT-v2	Romulus-v2
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	KNOT-v2	GIFT-COFB-v1
8	Romulus-v2	Romulus-v2	Romulus-v2	Gimli_GT-v2
9	Spook-v2-v1	Spook-v2-v1	Spook-v2-v1	KNOT-v2
10	Saturnin-v2	Saturnin-v2	GIFT-COFB-v1	PHOTON-Beetle-v1
11	Elephant-v2	Elephant-v2	Elephant-v2	Elephant-v2
12	SCHWAEMM-v1	SCHWAEMM-v1	PHOTON-Beetle-v1	ESTATE-v1
13	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Saturnin-v2	Spook-v2-v1
14	GIFT-COFB-v1	GIFT-COFB-v1	SCHWAEMM-v1	Saturnin-v2
15	ISAP-v2	ISAP-v2	ESTATE-v1	COMET_CI-v1
16	COMET_CI-v1	COMET_CI-v1	COMET_CI-v1	SCHWAEMM-v1
17	ESTATE-v1	ESTATE-v1	ISAP-v2	Oribatida-v1
18	Oribatida-v1	Oribatida-v1	Oribatida-v1	ISAP-v2
19	Pyjamask-v2	Pyjamask-v2	Pyjamask-v2	LOCUS-v1
20	LOCUS-v1	LOCUS-v1	LOCUS-v1	SpoC-v1
21	WAGE-v1	WAGE-v1	SpoC-v1	Pyjamask-v2
22	SpoC-v1	SpoC-v1	WAGE-v1	WAGE-v1

In Tables 19, 20, and 21, we summarize the relative changes in rankings for Artix-7. For the processing of PT only, the following algorithms rank higher for short messages than for long messages: Ascon, DryGASCON, TinyJAMBU, Romulus, PHOTON-Beetle, Elephant, ESTATE, COMET, Oribatida, LOCUS, and SpoC. The opposite is true for the following candidates: Xoodyak, KNOT, Gimli, Spook, SCHWAEMM, Saturnin, ISAP, Pyjamask, and WAGE. The following 4 algorithms remain among the best 6, independently of the size and type of inputs: Subterranean 2.0, Xoodyak, Ascon, and DryGASCON.

For the processing of AD only, the following algorithms rank higher for short messages than for long messages: TinyJAMBU, DryGASCON, Romulus, GIFT-COFB, PHOTON-Beetle, ESTATE, COMET, LOCUS, and SpoC. The opposite is true for the following candidates: Xoodyak, KNOT, Elephant, Gimli, Spook, SCHWAEMM, Saturnin, ISAP, and Pyjamask. The following 4 algorithms remain among the best 6, independently of the size and type of inputs: Subterranean 2.0, Xoodyak, Ascon, and DryGASCON.

In Tables 52–57, we summarize the relative changes in rankings for Cyclone 10 LP and ECP5.

6 Future Work

Before drawing final conclusions, we are planning to perform one additional phase of Round 2 benchmarking, with the submission deadline on November 9, 2020. Only after the results of this additional phase is known, final conclusions can be drawn. At the end of this effort, we hope for the close to full coverage of all 32 Round 2 candidates and the implementation of multiple variants of each candidate. This benchmarking effort should clearly demonstrate the major strengths and weaknesses of unprotected implementations of Round 2 candidates. It should also provide a strong foundation for the fair and comprehensive evaluation of the SCA-protected implementations in Round 3 of the NIST LWC standardization process.

References

[1] J.-P. Kaps, W. Diehl, M. Tempelmeier, F. Farahmand, E. Homsirikamol, and K. Gaj, "A Comprehensive Framework for Fair and Efficient Benchmarking of Hardware Implementations," Cryptology ePrint Archive 2019/1273, Nov. 2019.

[2] J.-P. Kaps, W. Diehl, M. Tempelmeier, E. Homsirikamol, and K. Gaj, "Hardware API for Lightweight Cryptography," GMU, Fairfax, VA, GMU Report, Oct. 2019.

[3] Cryptographic Engineering Research Group (CERG) at George Mason University, *Hardware Benchmarking of CAESAR Candidates*, 2019. [Online]. Available: https://cryptography.gmu.edu/athena/index.php?id=CAESAR.

[4] P. Yalla and J.-P. Kaps, "Evaluation of the CAESAR hardware API for lightweight implementations," en, in *2017 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2017*, Cancun, Mexico: IEEE, Dec. 2017, pp. 1–6.

[5] P. Karl and M. Tempelmeier, "A Detailed Report on the Overhead of Hardware APIs for Lightweight Cryptography," Cryptology ePrint Archive 2020/112, Feb. 2020.

[6] B. Rezvani, F. Coleman, S. Sachin, and W. Diehl, "Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look," en, Cryptology ePrint Archive 2019/824, Feb. 2020, p. 26.

[7] NIST, *Lightweight Cryptography: Project Overview*, 2019. [Online]. Available: https://csrc.nist.gov/projects/lightweight-cryptography.

[8] *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness - web page*, 2019. [Online]. Available: https://competitions.cr.yp.to/caesar.html.

[9] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, M. U. Sharif, and K. Gaj, "A universal hardware API for authenticated ciphers," in *2015 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2015*, Riviera Maya, Mexico, Dec. 2015.

[10] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, P. Yalla, J.-P. Kaps, and K. Gaj, "CAESAR Hardware API," Cryptology ePrint Archive 2016/626, 2016.

[11] ——, "Addendum to the CAESAR Hardware API v1.0," George Mason University, Fairfax, VA, GMU Report, Jun. 2016.

[12] E. Homsirikamol, P. Yalla, and F. Farahmand, *Development Package for Hardware Implementations Compliant with the CAESAR Hardware API*, 2016. [Online]. Available: https://cryptography.gmu.edu/athena/index.php?id=CAESAR.

[13] E. Homsirikamol, P. Yalla, F. Farahmand, W. Diehl, A. Ferozpuri, J.-P. Kaps, and K. Gaj, "Implementer's Guide to Hardware Implementations Compliant with the CAESAR Hardware API," GMU, Fairfax, VA, GMU Report, 2016.

[14] M. Tempelmeier, G. Sigl, and J.-P. Kaps, "Experimental Power and Performance Evaluation of CAESAR Hardware Finalists," in *2018 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2018*, Cancun, Mexico, Dec. 2018, pp. 1–6.

[15] M. Tempelmeier, F. De Santis, G. Sigl, and J.-P. Kaps, "The CAESAR-API in the Real World — Towards a Fair Evaluation of Hardware CAESAR Candidates," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018*, Washington, DC, Apr. 2018, pp. 73–80.

[16] F. Farahmand, W. Diehl, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Improved Lightweight Implementations of CAESAR Authenticated Ciphers," in *2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines, FCCM 2018*, Boulder, CO, Apr. 2018, pp. 29–36.

[17] 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," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018*, Washington, DC: IEEE, Apr. 2018, pp. 147–152.

[18] ——, "Comparison of Cost of Protection against Differential Power Analysis of Selected Authenticated Ciphers," en, *Cryptography*, vol. 2, no. 3, p. 26, Sep. 2018.

[19] W. Diehl, F. Farahmand, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Face-off between the CAESAR Lightweight Finalists: ACORN vs. Ascon," in *2018 International Conference on Field Programmable Technology, FPT 2018*, vol. 2, Naha, Okinawa, Japan, Dec. 2018, p. 26.

[20] ——, "Face-off between the CAESAR Lightweight Finalists: ACORN vs. Ascon," Cryptology ePrint Archive 2019/184, Mar. 2019.

[21] Cryptographic Engineering Research Group (CERG) at George Mason University, *Hardware Benchmarking of Lightweight Cryptography*, 2020. [Online]. Available: https://cryptography.gmu.edu/athena/index.php?id=LWC.

[22] F. Farahmand, A. Ferozpuri, W. Diehl, and K. Gaj, "Minerva: Automated hardware optimization tool," in *2017 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2017*, Cancun: IEEE, Dec. 2017, pp. 1–8.

[23] K. Gaj, J.-P. Kaps, V. Amirineni, M. Rogawski, E. Homsirikamol, and B. Y. Brewster, "ATHENa - Automated Tool for Hardware EvaluatioN: Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware Using FPGAs," in *2010 International Conference on Field Programmable Logic and Applications, FPL 2010*, Milan, Italy: IEEE, Aug. 2010, pp. 414–421.

[24] K. Mohajerani and R. Nagpal, *Xeda*, Sep. 22, 2020. [Online]. Available: https://github.com/kammoh/xeda (visited on 09/25/2020).

[25] D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, C. Momin, O. Pereira, T. Peters, B. Udvarhelyi, and F. Wiemer, "Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. S1, pp. 295–349, 2020.

[26] D. J. Bernstein and T. Lange, *eBACS: ECRYPT Benchmarking of Cryptographic Systems*, 2020. [Online]. Available: https://bench.cr.yp.to.

A Additional Results

Table 22: Xilinx Artix-7 Resource Usage and Maximum Frequency

Variant	LUTs	FFs	Slices	Freq. [MHz]
Ascon_Graz-v1	1,551	666	438	209
Ascon_Graz-v2	1,723	669	487	216
Ascon_VT-v1	1,913	539	518	233
Ascon_VT-v2	1,928	544	515	219
COMET_CI-v1	1,884	1,543	639	223

Table 22 continued from previous page

Variant	LUTs	FFs	Slices	Freq. [MHz]
COMET_CI-v2	1,096	1,034	372	222
COMET_VT-v1	2,737	1,044	734	233
COMET_VT-v2	1,703	736	504	234
DryGASCON-v1	2,074	1,220	596	238
Elephant-v1	1,291	910	379	229
Elephant-v2	1,884	900	541	181
ESTATE-v1	1,351	733	428	222
ESTATE-v2	907	416	269	268
ESTATE-v3	1,130	846	347	259
ESTATE-v4	944	557	292	277
GIFT-COFB-v1	1,041	604	321	275
Gimli_GT-v1	1,683	1,166	514	177
Gimli_GT-v2	1,900	1,161	556	174
Gimli_GT-v3	2,646	1,162	776	129
Gimli_GT-v4	2,508	1,160	755	140
Gimli_GT-v5	3,927	1,161	1,084	98
Gimli_GT-v6	3,943	1,159	1,099	92
Gimli_GT-v7	5,346	1,160	1,435	66
Gimli_TUM-v1	933	261	269	241
Gimli_TUM-v2	905	245	266	244
Gimli_TUM-v3	838	249	252	253
ISAP-v1	3,491	1,177	937	193
ISAP-v2	2,157	1,005	618	200
KNOT-v1	1,092	575	317	260
KNOT-v2	1,569	854	467	254
KNOT-v3	1,367	806	414	264
KNOT-v4	1,783	1,037	527	256
LOCUS-v1	1,824	1,037	613	216
LOTUS-v1	1,652	916	469	145
Oribatida-v1	1,450	1,319	466	276
Oribatida-v2	1,450	1,319	466	276
PHOTON-Beetle-v1	2,065	729	620	178
Pyjamask-v1	1,979	1,306	592	229
Pyjamask-v2	2,308	1,415	780	213
Romulus-v1	953	501	271	229
Romulus-v2	1,280	501	344	214
Romulus-v3	1,824	504	507	123
Romulus-v4	2,602	503	702	58
Romulus-v5	887	422	246	214
Saturnin-v1	2,020	1,315	610	192
Saturnin-v2	2,414	766	679	168
SCHWAEMM-v1	3,071	1,396	872	135
SCHWAEMM-v2	3,740	1,541	1,004	130
SpoC-v1	1,079	805	348	230
Spook-v2-v1	2,296	1,502	693	201
Subterranean-v1	915	584	260	186
TinyJAMBU_GMU-v1	591	428	212	266
TinyJAMBU_GMU-v2	564	430	197	268
TinyJAMBU_GMU-v3	537	433	191	278

Table 22 continued from previous page

Variant	LUTs	FFs	Slices	Freq. [MHz]
TinyJAMBU_TJT-v1	446	209	136	290
TinyJAMBU_TJT-v2	461	325	142	315
TinyJAMBU_TJT-v3	576	432	215	240
WAGE-v1	1,150	760	332	279
Xoodyak_GMU-v1	1,808	851	495	170
Xoodyak_GMU-v2	1,234	98	323	168
Xoodyak_XT-v1	1,405	480	398	233
Xoodyak_XT-v2	2,071	480	564	183
Xoodyak_XT-v7	1,405	480	391	228
Xoodyak_XT-v8	2,040	480	542	187
AVERAGE	**1,740**	**806**	**505**	**210.9**
MINIMUM	**446**	**98**	**136**	**58.0**
MAXIMUM	**5,346**	**1,543**	**1,435**	**315.0**

Table 23: Intel Cyclone 10 LP Resource Usage and Maximum Frequency

Variant	LEs	$\frac{\text{LEs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
Ascon_Graz-v1	2,484	1.60	775	1.16	152.8	1.37
Ascon_Graz-v2	2,666	1.55	775	1.16	146.7	1.47
Ascon_VT-v1	2,432	1.27	634	1.18	176.6	1.32
Ascon_VT-v2	2,695	1.40	640	1.18	172.0	1.27
COMET_CI-v1	4,663	2.48	1,885	1.22	115.8	1.93
COMET_CI-v2	2,629	2.40	1,632	1.58	132.9	1.67
COMET_VT-v1	10,035	3.67	1,153	1.10	84.1	2.77
COMET_VT-v2	5,204	3.06	826	1.12	110.6	2.12
DryGASCON-v1	3,199	1.54	1,310	1.07	130.5	1.82
Elephant-v1	2,056	1.59	1,005	1.10	163.1	1.40
Elephant-v2	2,729	1.45	998	1.11	113.2	1.60
ESTATE-v1	3,839	2.84	1,401	1.91	118.0	1.88
ESTATE-v2	1,946	2.15	1,026	2.47	174.3	1.54
ESTATE-v3	2,279	2.02	1,442	1.70	180.2	1.44
ESTATE-v4	1,572	1.67	1,098	1.97	200.1	1.38
GIFT-COFB-v1	1,877	1.80	774	1.28	184.4	1.49
Gimli_GT-v1	2,628	1.56	1,156	0.99	138.5	1.28
Gimli_GT-v2	2,678	1.41	1,155	0.99	110.4	1.58
Gimli_GT-v3	3,652	1.38	1,156	0.99	87.0	1.48
Gimli_GT-v4	5,019	2.00	1,154	0.99	88.6	1.58
Gimli_GT-v5	5,951	1.51	1,155	0.99	57.8	1.70
Gimli_GT-v6	4,843	1.23	1,153	0.99	47.9	1.92
Gimli_GT-v7	6,373	1.19	1,154	0.99	32.5	2.03
ISAP-v1	4,589	1.31	1,268	1.08	126.6	1.52
ISAP-v2	3,852	1.79	1,108	1.10	136.4	1.47

Table 23 continued from previous page

Variant	LEs	$\frac{\text{LEs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
KNOT-v1	1,485	1.36	674	1.17	177.9	1.46
KNOT-v2	2,050	1.31	955	1.12	167.5	1.52
KNOT-v3	1,962	1.44	905	1.12	170.7	1.55
KNOT-v4	2,412	1.35	1,135	1.09	171.3	1.49
LOCUS-v1	2,978	1.63	1,045	1.01	125.8	1.72
LOTUS-v1	2,642	1.60	1,010	1.10	103.5	1.40
Oribatida-v1	2,512	1.73	1,331	1.01	185.7	1.49
Oribatida-v2	2,221	1.53	1,202	0.91	174.5	1.58
PHOTON-Beetle-v1	3,602	1.74	836	1.15	125.4	1.42
Pyjamask-v1	8,599	4.34	6,236	4.78	109.7	2.09
Pyjamask-v2	8,692	3.77	6,092	4.30	90.6	2.35
Romulus-v1	1,735	1.82	500	1.00	143.2	1.60
Romulus-v2	2,086	1.63	500	1.00	141.7	1.51
Romulus-v3	2,407	1.32	500	0.99	79.3	1.55
Romulus-v4	3,409	1.31	500	0.99	40.4	1.44
Romulus-v5	1,960	2.21	507	1.20	130.2	1.64
Saturnin-v1	3,802	1.88	2,155	1.64	145.0	1.32
Saturnin-v2	3,892	1.61	1,641	2.14	104.6	1.61
SCHWAEMM-v1	4,713	1.53	1,489	1.07	81.8	1.65
SCHWAEMM-v2	5,773	1.54	1,624	1.05	85.7	1.52
SpoC-v1	1,696	1.57	820	1.02	167.7	1.37
Spook-v2-v1	3,912	1.70	1,485	0.99	110.4	1.82
Subterranean-v1	1,333	1.46	578	0.99	159.6	1.17
TinyJAMBU_GMU-v1	856	1.45	447	1.04	196.8	1.35
TinyJAMBU_GMU-v2	841	1.49	448	1.04	196.2	1.37
TinyJAMBU_GMU-v3	817	1.52	452	1.04	191.1	1.46
TinyJAMBU_TJT-v1	686	1.54	429	2.05	200.8	1.44
TinyJAMBU_TJT-v2	777	1.69	435	1.34	196.2	1.60
TinyJAMBU_TJT-v3	1,021	1.77	432	1.00	159.7	1.50
WAGE-v1	1,774	1.54	846	1.11	159.6	1.75
Xoodyak_GMU-v1	3,135	1.73	947	1.11	106.8	1.59
Xoodyak_GMU-v2	5,871	4.76	2,237	22.83	77.0	2.18
Xoodyak_XT-v1	2,282	1.62	589	1.23	140.6	1.66
Xoodyak_XT-v2	3,518	1.70	589	1.23	87.8	2.08
Xoodyak_XT-v3	5,540		589		71.3	
Xoodyak_XT-v4	5,213		589		55.2	
Xoodyak_XT-v7	2,253	1.60	602	1.25	133.8	1.70
Xoodyak_XT-v8	4,337	2.13	602	1.25	91.3	2.05
Xoodyak_XT-v9	5,611		602		70.7	
Xoodyak_XT-v10	5,263		602		55.8	
Average	**3,347**	**1.83**	**1,123**	**1.67**	**128.7**	**1.62**
Minimum	**686**	**1.19**	**429**	**0.91**	**32.5**	**1.17**
Maximum	**10,035**	**4.76**	**6,236**	**22.83**	**200.8**	**2.77**

Table 24: Lattice ECP5 Resource Usage and Maximum Frequency

Variant	LUTs	$\frac{\text{LUTs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Slices	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
Ascon_Graz-v1	6,507	4.20	692	1.04	4,307	82.7	2.53
Ascon_Graz-v2	7,246	4.21	692	1.03	4,617	83.9	2.57
Ascon_VT-v1	3,130	1.64	550	1.02	1,673	84.9	2.74
Ascon_VT-v2	3,256	1.69	556	1.02	1,678	74.2	2.95
COMET_CI-v1	3,427	1.82	1,798	1.17	2,175	80.9	2.76
COMET_CI-v2	1,974	1.80	1,607	1.55	1,662	94.3	2.35
COMET_VT-v1	6,613	2.42	1,154	1.10	3,698	111.6	2.09
COMET_VT-v2	2,353	1.38	748	1.02	1,449	111.5	2.10
DryGASCON-v1	3,801	1.83	1,223	1.00	2,223	100.5	2.37
Elephant-v1	2,368	1.83	923	1.01	1,464	97.5	2.35
Elephant-v2	3,073	1.63	916	1.02	1,823	85.5	2.12
ESTATE-v1	3,079	2.28	1,300	1.77	2,107	99.5	2.23
ESTATE-v2	1,700	1.87	995	2.39	1,232	95.5	2.81
ESTATE-v3	2,026	1.79	1,350	1.60	1,530	106.3	2.44
ESTATE-v4	1,404	1.49	1,063	1.91	1,025	92.0	3.01
GIFT-COFB-v1	2,214	2.13	689	1.14	1,248	114.3	2.41
Gimli_GT-v1	3,729	2.22	1,128	0.97	2,176	49.2	3.60
Gimli_GT-v2	3,962	2.08	1,127	0.97	2,286	49.2	3.54
Gimli_GT-v3	4,934	1.86	1,128	0.97	2,764	44.4	2.90
Gimli_GT-v4	4,632	1.85	1,126	0.97	2,616	49.5	2.83
Gimli_GT-v5	5,738	1.46	1,127	0.97	3,214	23.3	4.21
Gimli_GT-v6	6,341	1.61	1,126	0.97	3,466	31.5	2.92
Gimli_GT-v7	8,238	1.54	1,126	0.97	4,418	16.4	4.01
ISAP-v1	6,701	1.92	1,185	1.01	4,164	61.1	3.16
ISAP-v2	5,708	2.65	1,028	1.02	3,475	68.0	2.94
KNOT-v1	1,597	1.46	581	1.01	930	93.8	2.77
KNOT-v2	2,241	1.43	865	1.01	1,304	91.2	2.79
KNOT-v3	2,037	1.49	813	1.01	1,193	83.2	3.17
KNOT-v4	2,408	1.35	1,043	1.01	1,429	85.6	2.99
LOCUS-v1	3,161	1.73	1,036	1.00	2,019	79.6	2.71
LOTUS-v1	2,820	1.71	936	1.02	1,748	55.6	2.61
Oribatida-v1	2,832	1.95	1,246	0.94	1,781	119.7	2.31
Oribatida-v2	2,497	1.72	1,117	0.85	1,563	114.2	2.42
PHOTON-Beetle-v1	3,294	1.59	753	1.03	1,938	101.4	1.75
Pyjamask-v1	3,897	1.97	1,937	1.48	2,593	92.7	2.47
Pyjamask-v2	4,162	1.80	1,791	1.27	2,794	73.2	2.91
Romulus-v1	2,633	2.76	502	1.00	1,486	78.8	2.91
Romulus-v2	3,080	2.41	519	1.04	1,678	64.4	3.32
Romulus-v3	3,847	2.11	569	1.13	2,092	45.0	2.73
Romulus-v4	5,086	1.96	571	1.14	2,710	21.6	2.69
Romulus-v5	1,961	2.21	395	0.94	1,131	76.5	2.80
Saturnin-v1	3,156	1.56	2,093	1.59	2,235	91.0	2.11
Saturnin-v2	3,326	1.38	1,578	2.06	2,330	76.1	2.21
SCHWAEMM-v1	4,685	1.53	1,408	1.01	2,933	66.3	2.04

Table 24 continued from previous page

Variant	LUTs	$\frac{\text{LUTs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Slices	Freq. [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
SCHWAEMM-v2	5,947	1.59	1,546	1.00	3,839	63.8	2.04
SpoC-v1	2,049	1.90	740	0.92	1,314	98.2	2.34
Spook-v2-v1	3,655	1.59	1,494	0.99	2,254	77.8	2.58
Subterranean-v1	1,725	1.89	545	0.93	1,069	58.9	3.16
TinyJAMBU_GMU-v1	720	1.22	397	0.93	456	124.8	2.13
TinyJAMBU_GMU-v2	908	1.61	355	0.83	550	128.3	2.09
TinyJAMBU_GMU-v3	1,277	2.38	352	0.81	807	108.1	2.57
TinyJAMBU_TJT-v1	928	2.08	363	1.74	563	99.7	2.91
TinyJAMBU_TJT-v2	913	1.98	364	1.12	588	99.0	3.18
TinyJAMBU_TJT-v3	881	1.53	368	0.85	552	97.7	2.46
WAGE-v1	2,029	1.76	794	1.04	1,270	91.1	3.06
Xoodyak_GMU-v1	3,172	1.75	878	1.03	1,990	74.0	2.30
Xoodyak_GMU-v2	2,316	1.88	114	1.16	1,286	74.8	2.25
Xoodyak_XT-v1	2,657	1.89	488	1.02	1,642	81.7	2.85
Xoodyak_XT-v2	4,302	2.08	526	1.10	2,215	70.7	2.59
Xoodyak_XT-v3	5,569		526		2,854	38.3	
Xoodyak_XT-v5	9,386		526		4,775	16.6	
Xoodyak_XT-v7	3,272	2.33	657	1.37	1,744	66.9	3.41
Xoodyak_XT-v8	3,507	1.72	488	1.02	1,815	66.0	2.83
Xoodyak_XT-v9	5,614		538		2,875	36.0	
Xoodyak_XT-v10	6,899		538		3,520	26.5	
Xoodyak_XT-v11	9,447		538		4,799	16.6	
Average	**3,637**	**1.91**	**898**	**1.13**	**2,139**	**76.3**	**2.69**
Minimum	**720**	**1.22**	**114**	**0.81**	**456**	**16.4**	**1.75**
Maximum	**9,447**	**4.21**	**2,093**	**2.39**	**4,799**	**128.3**	**4.21**

Table 25: Xilinx Artix-7 Encryption PT Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbits/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean-v1	5,290.7	89%	1	915	186	432
Xoodyak_XT-v8	2,288.7	96%	2	2,040	187	1,004
Xoodyak_XT-v2	2,239.7	96%		2,071	183	1,004
Ascon_Graz-v2	2,210.0	96%	3	1,723	216	1,201
Gimli_GT-v2	1,734.1	93%	4	1,900	174	1,233
Xoodyak_GMU-v1	1,642.3	96%		1,808	170	1,272
KNOT-v2	1,626.4	93%	5	1,569	254	1,919
Ascon_Graz-v1	1,620.3	97%		1,551	209	1,585
Ascon_VT-v2	1,517.0	97%		1,928	219	1,774
Ascon_VT-v1	1,457.1	98%		1,913	233	1,965
DryGASCON-v1	1,414.9	98%	6	2,074	238	2,067
Spook-v2-v1	1,030.0	96%	7	2,296	201	2,398
TinyJAMBU_TJT-v3	946.4	99%	8	576	240	3,116
Gimli_GT-v1	898.4	95%		1,683	177	2,421
Romulus-v3	855.8	98%	9	1,824	123	1,766
Romulus-v2	841.8	98%		1,280	214	3,124
Saturnin-v2	747.2	94%	10	2,414	168	2,763
GIFT-COFB-v1	731.9	98%	11	1,041	275	4,617
SCHWAEMM-v1	708.6	96%	12*	**3,071**	135	2,341
PHOTON-Beetle-v1	680.3	99%	13	2,065	178	3,215
Elephant-v2	661.4	98%	14	1,884	181	3,363
KNOT-v3	616.2	97%		1,367	264	5,265
ISAP-v2	456.5	93%	15	2,157	200	5,384
COMET_CI-v1	400.8	98%	16	1,884	223	6,837
COMET_VT-v2	329.6	98%		1,703	234	8,725
ESTATE-v1	320.5	99%	17	1,351	222	8,512
TinyJAMBU_TJT-v2	302.3	99%		461	315	12,803
Pyjamask-v2	255.0	95%	18	2,308	213	10,263
Oribatida-v1	255.0	99%	19	1,450	276	13,301
Oribatida-v2	250.0	99%		1,450	276	13,564
TinyJAMBU_GMU-v1	247.8	99%		591	266	13,189
Elephant-v1	210.8	98%		1,291	229	13,347
WAGE-v1	151.7	97%	20	1,150	279	22,600
SpoC-v1	131.2	99%	21	1,079	230	21,545
TinyJAMBU_GMU-v2	128.7	99%		564	268	25,589
Saturnin-v1	120.4	97%		2,020	192	19,593
LOCUS-v1	120.3	99%	22	1,824	216	22,068
Xoodyak_GMU-v2	118.0	95%		1,234	168	17,495
Pyjamask-v1	107.7	96%		1,979	229	26,131
COMET_CI-v2	94.0	98%		1,096	222	29,031
ESTATE-v3	80.8	99%		1,130	259	39,392
LOTUS-v1	80.7	99%		1,652	145	22,068
Gimli_TUM-v1	37.9	97%		933	241	78,117
Gimli_TUM-v2	20.4	97%		905	244	146,617
Average		**97%**				
Minimum		**89%**				
Maximum		**99%**				

Table 26: Xilinx Artix-7 Encryption PT Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbits/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean-v1	1,488.0	25%	1	915	186	64
Ascon_Graz-v2	1,140.1	49%	2	1,723	216	97
Xoodyak_XT-v8	1,100.5	46%	3	2,040	187	87
Xoodyak_XT-v2	1,077.0	46%		2,071	183	87
Ascon_VT-v1	954.4	64%		1,913	233	125
Ascon_VT-v2	950.2	61%		1,928	219	118
Ascon_Graz-v1	947.0	57%		1,551	209	113
DryGASCON-v1	902.6	62%	4	2,074	238	135
Xoodyak_GMU-v1	784.1	46%		1,808	170	111
TinyJAMBU_TJT-v3	714.4	74%	5	576	240	172
KNOT-v2	710.6	41%	6	1,569	254	183
Gimli_GT-v2	690.6	37%	7	1,900	174	129
Romulus-v2	608.7	71%	8	1,280	214	180
Romulus-v3	572.5	65%		1,824	123	110
Spook-v2-v1	541.6	51%	9	2,296	201	190
PHOTON-Beetle-v1	509.1	74%	10	2,065	178	179
GIFT-COFB-v1	480.5	64%	11	1,041	275	293
Gimli_GT-v1	425.5	45%		1,683	177	213
Elephant-v2	413.7	61%	12	1,884	181	224
KNOT-v1	407.1	69%		1,092	260	327
SCHWAEMM-v1	386.1	53%	13*	**3,071**	135	179
Saturnin-v2	308.3	39%	14	2,414	168	279
COMET_CI-v1	287.6	71%	15	1,884	223	397
ESTATE-v1	273.2	85%	16	1,351	222	416
TinyJAMBU_TJT-v2	244.7	80%		461	315	659
COMET_VT-v2	223.1	66%		1,703	234	537
Oribatida-v1	202.7	79%	17	1,450	276	697
TinyJAMBU_GMU-v1	201.2	80%		591	266	677
Oribatida-v2	187.4	74%		1,450	276	754
ISAP-v2	171.0	35%	18	2,157	200	599
Elephant-v1	135.7	63%		1,291	229	864
Pyjamask-v2	124.1	46%	19	2,308	213	879
TinyJAMBU_GMU-v2	105.5	81%		564	268	1,301
SpoC-v1	105.0	79%	20	1,079	230	1,121
LOCUS-v1	101.3	84%	21	1,824	216	1,092
WAGE-v1	88.0	56%	22	1,150	279	1,624
ESTATE-v3	71.4	88%		1,130	259	1,856
LOTUS-v1	68.0	84%		1,652	145	1,092
Saturnin-v1	66.9	54%		2,020	192	1,469
COMET_CI-v2	66.6	70%		1,096	222	1,707
Pyjamask-v1	57.8	52%		1,979	229	2,027
Xoodyak_GMU-v2	54.7	44%		1,234	168	1,572
Gimli_TUM-v1	22.3	57%		933	241	5,529
Gimli_TUM-v2	12.1	57%		905	244	10,365
Average		**61%**				
Minimum		**25%**				
Maximum		**88%**				

Table 27: Xilinx Artix-7 Encryption PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbits/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Ascon_VT-v1	458.8	31%	1	1,913	233	65
Subterranean-v1	457.8	8%	2	915	186	52
Ascon_Graz-v2	453.2	20%		1,723	216	61
Ascon_VT-v2	438.0	28%		1,928	219	64
DryGASCON-v1	423.1	29%	3	2,074	238	72
Xoodyak_XT-v8	419.9	18%	4	2,040	187	57
Ascon_Graz-v1	411.6	25%		1,551	209	65
Xoodyak_XT-v2	410.9	18%		2,071	183	57
TinyJAMBU_TJT-v3	404.2	42%	5	576	240	76
Romulus-v2	326.1	38%	6	1,280	214	84
Xoodyak_GMU-v1	298.1	17%		1,808	170	73
PHOTON-Beetle-v1	284.8	41%	7	2,065	178	80
Romulus-v3	281.1	32%		1,824	123	56
KNOT-v2	256.0	15%	8	1,569	254	127
Elephant-v2	243.9	36%	9	1,884	181	95
Gimli_GT-v2	239.5	13%	10	1,900	174	93
GIFT-COFB-v1	231.6	31%	11	1,041	275	152
KNOT-v1	209.3	35%		1,092	260	159
ESTATE-v1	186.9	58%	12	1,351	222	152
Spook-v2-v1	181.2	17%	13	2,296	201	142
Gimli_GT-v1	160.7	17%		1,683	177	141
TinyJAMBU_TJT-v2	153.3	50%		461	315	263
COMET_CI-v1	152.6	37%	14	1,884	223	187
SCHWAEMM-v1	135.0	18%	15*	**3,071**	135	128
TinyJAMBU_GMU-v1	126.6	51%		591	266	269
Oribatida-v1	123.5	48%	16	1,450	276	286
Saturnin-v2	118.2	15%	17	2,414	168	182
COMET_VT-v2	110.9	33%		1,703	234	270
Oribatida-v2	105.8	42%		1,450	276	334
Elephant-v1	83.5	39%		1,291	229	351
LOCUS-v1	67.8	56%	18	1,824	216	408
TinyJAMBU_GMU-v2	67.4	52%		564	268	509
SpoC-v1	64.7	49%	19	1,079	230	455
ISAP-v2	57.8	12%	20	2,157	200	443
ESTATE-v3	52.5	65%		1,130	259	632
Pyjamask-v2	47.6	18%	21	2,308	213	573
LOTUS-v1	45.5	56%		1,652	145	408
WAGE-v1	38.0	24%	22	1,150	279	940
COMET_CI-v2	34.8	36%		1,096	222	816
Saturnin-v1	28.5	23%		2,020	192	862
Pyjamask-v1	23.6	21%		1,979	229	1,241
Xoodyak_GMU-v2	20.5	17%		1,234	168	1,050
Gimli_TUM-v1	9.8	25%		933	241	3,162
Gimli_TUM-v2	5.3	25%		905	244	5,922
Average		**31%**				
Minimum		**8%**				
Maximum		**65%**				

Table 28: Xilinx Artix-7 Encryption AD Throughput for 1536 Byte Messages

Variant	**Throughput 1536B [Mbits/s]**	**Thr AD 1536B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 1536B**
Subterranean-v1	5,302.9	89%	1	915	186	431
Xoodyak_XT-v8	3,096.8	94%	2	2,040	187	742
Xoodyak_XT-v2	3,030.6	94%		2,071	183	742
TinyJAMBU_TJT-v3	2,467.9	96%	3	576	240	1,195
Xoodyak_GMU-v1	2,334.0	94%		1,808	170	895
Ascon_Graz-v2	2,195.4	95%	4	1,723	216	1,209
Gimli_GT-v2	1,734.1	93%	5	1,900	174	1,233
Ascon_Graz-v1	1,614.2	97%		1,551	209	1,591
KNOT-v2	1,603.9	92%	6	1,569	254	1,946
Romulus-v2	1,451.2	95%	7	1,280	214	1,812
Ascon_VT-v1	1,451.1	97%		1,913	233	1,973
Saturnin-v2	1,422.7	89%	8	2,414	168	1,451
DryGASCON-v1	1,414.9	98%	9	2,074	238	2,067
Ascon_VT-v2	1,363.9	97%		1,928	219	1,973
Romulus-v3	1,359.2	95%		1,824	123	1,112
Elephant-v2	1,144.7	95%	10	1,884	181	1,943
Spook-v2-v1	1,030.0	96%	11	2,296	201	2,398
Gimli_GT-v1	898.4	95%		1,683	177	2,421
SCHWAEMM-v1	869.0	96%	12*	**3,071**	135	1,909
PHOTON-Beetle-v1	799.1	98%	13	2,065	178	2,737
TinyJAMBU_TJT-v2	755.7	97%		461	315	5,122
ISAP-v2	741.8	93%	14	2,157	200	3,313
GIFT-COFB-v1	709.3	99%	15	1,041	275	4,764
ESTATE-v1	636.9	99%	16	1,351	222	4,283
KNOT-v3	611.6	97%		1,367	264	5,304
TinyJAMBU_GMU-v1	593.4	98%		591	266	5,508
Oribatida-v1	495.8	97%	17	1,450	276	6,841
Oribatida-v2	487.3	97%		1,450	276	6,960
COMET_CI-v1	466.3	98%	18	1,884	223	5,877
Elephant-v1	394.8	95%		1,291	229	7,127
COMET_VT-v2	344.7	98%		1,703	234	8,341
TinyJAMBU_GMU-v2	322.0	98%		564	268	10,228
Pyjamask-v2	264.7	95%	19	2,308	213	9,887
LOCUS-v1	238.6	98%	20	1,824	216	11,124
Saturnin-v1	233.1	93%		2,020	192	10,121
Xoodyak_GMU-v2	204.4	92%		1,234	168	10,100
ESTATE-v3	160.7	99%		1,130	259	19,803
LOTUS-v1	160.2	98%		1,652	145	11,124
WAGE-v1	150.9	96%	21	1,150	279	22,713
SpoC-v1	133.6	99%	22	1,079	230	21,161
Pyjamask-v1	109.3	96%		1,979	229	25,755
COMET_CI-v2	105.5	98%		1,096	222	25,863
Gimli_TUM-v1	38.1	97%		933	241	77,829
Gimli_TUM-v2	20.5	97%		905	244	145,945
Average		**96%**				
Minimum		**89%**				
Maximum		**99%**				

Table 29: Xilinx Artix-7 Encryption AD Throughput for 64 Byte Messages

Variant	Through-put 64B [Mbits/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean-v1	1,511.6	25%	1	915	186	63
TinyJAMBU_TJT-v3	1,350.3	53%	2	576	240	91
Xoodyak_XT-v8	1,243.4	38%	3	2,040	187	77
Xoodyak_XT-v2	1,216.8	38%		2,071	183	77
Ascon_Graz-v2	1,053.3	46%	4	1,723	216	105
DryGASCON-v1	902.6	62%	5	2,074	238	135
Ascon_Graz-v1	899.2	54%		1,551	209	119
Ascon_VT-v1	897.0	60%		1,913	233	133
Xoodyak_GMU-v1	888.2	36%		1,808	170	98
Ascon_VT-v2	843.1	60%		1,928	219	133
Romulus-v2	702.4	46%	6	1,280	214	156
Gimli_GT-v2	690.6	37%	7	1,900	174	129
Romulus-v3	629.8	44%		1,824	123	100
KNOT-v2	619.3	36%	8	1,569	254	210
PHOTON-Beetle-v1	566.1	70%	9	2,065	178	161
Elephant-v2	554.9	46%	10	1,884	181	167
GIFT-COFB-v1	550.0	77%	11	1,041	275	256
Spook-v2-v1	541.6	51%	12	2,296	201	190
ESTATE-v1	483.7	75%	13	1,351	222	235
TinyJAMBU_TJT-v2	477.2	62%		461	315	338
SCHWAEMM-v1	429.3	47%	14*	**3,071**	135	161
Gimli_GT-v1	425.5	45%		1,683	177	213
Saturnin-v2	411.6	26%	15	2,414	168	209
TinyJAMBU_GMU-v1	382.6	63%		591	266	356
KNOT-v1	376.0	63%		1,092	260	354
COMET_CI-v1	319.8	67%	16	1,884	223	357
Oribatida-v1	286.6	56%	17	1,450	276	493
Oribatida-v2	286.1	57%		1,450	276	494
ISAP-v2	277.5	35%	18	2,157	200	369
COMET_VT-v2	230.0	65%		1,703	234	521
TinyJAMBU_GMU-v2	207.9	63%		564	268	660
Elephant-v1	190.6	46%		1,291	229	615
LOCUS-v1	173.9	72%	19	1,824	216	636
ESTATE-v3	128.1	79%		1,130	259	1,035
Pyjamask-v2	125.2	45%	20	2,308	213	871
LOTUS-v1	116.7	72%		1,652	145	636
SpoC-v1	106.6	79%	21	1,079	230	1,105
Saturnin-v1	92.8	37%		2,020	192	1,059
WAGE-v1	82.2	53%	22	1,150	279	1,737
COMET_CI-v2	72.2	67%		1,096	222	1,575
Xoodyak_GMU-v2	65.3	29%		1,234	168	1,317
Pyjamask-v1	58.1	51%		1,979	229	2,019
Gimli_TUM-v1	22.4	57%		933	241	5,517
Gimli_TUM-v2	12.1	57%		905	244	10,337
Average		**53%**				
Minimum		**25%**				
Maximum		**79%**				

Table 30: Xilinx Artix-7 Encryption AD Throughput for 16 Byte Messages

Variant	**Throughput 16B [Mbits/s]**	**Thr AD 16B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 16B**
TinyJAMBU_TJT-v3	558.5	22%	1	576	240	55
Subterranean-v1	466.8	8%	2	915	186	51
Xoodyak_XT-v8	427.4	13%	3	2,040	187	56
DryGASCON-v1	423.1	29%	4	2,074	238	72
Xoodyak_XT-v2	418.3	13%		2,071	183	56
Ascon_VT-v1	408.5	27%	5	1,913	233	73
Ascon_Graz-v2	400.7	17%		1,723	216	69
Ascon_VT-v2	384.0	27%		1,928	219	73
Ascon_Graz-v1	376.8	23%		1,551	209	71
Romulus-v2	326.1	21%	6	1,280	214	84
GIFT-COFB-v1	322.9	45%	7	1,041	275	109
Xoodyak_GMU-v1	298.1	12%		1,808	170	73
PHOTON-Beetle-v1	295.9	36%	8	2,065	178	77
Romulus-v3	281.1	20%		1,824	123	56
ESTATE-v1	275.9	43%	9	1,351	222	103
Gimli_GT-v2	239.5	13%	10	1,900	174	93
TinyJAMBU_TJT-v2	221.5	29%		461	315	182
KNOT-v2	211.1	12%	11	1,569	254	154
Elephant-v2	194.7	16%	12	1,884	181	119
Spook-v2-v1	181.2	17%	13	2,296	201	142
TinyJAMBU_GMU-v1	181.1	30%		591	266	188
KNOT-v1	178.9	30%		1,092	260	186
COMET_CI-v1	161.3	34%	14	1,884	223	177
Gimli_GT-v1	160.7	17%		1,683	177	141
SCHWAEMM-v1	140.5	15%	15*	**3,071**	135	123
Saturnin-v2	138.7	9%	16	2,414	168	155
Oribatida-v2	125.3	25%	17	1,450	276	282
Oribatida-v1	123.5	24%		1,450	276	286
COMET_VT-v2	112.6	32%		1,703	234	266
TinyJAMBU_GMU-v2	98.6	30%		564	268	348
LOCUS-v1	94.0	39%	18	1,824	216	294
ISAP-v2	93.8	12%	19	2,157	200	273
ESTATE-v3	78.4	48%		1,130	259	423
Elephant-v1	66.8	16%		1,291	229	439
SpoC-v1	65.3	48%	20	1,079	230	451
LOTUS-v1	63.1	39%		1,652	145	294
Pyjamask-v2	47.3	17%	21	2,308	213	577
Saturnin-v1	37.0	15%		2,020	192	665
COMET_CI-v2	36.3	34%		1,096	222	783
WAGE-v1	33.9	22%	22	1,150	279	1,053
Pyjamask-v1	23.5	21%		1,979	229	1,245
Xoodyak_GMU-v2	20.5	9%		1,234	168	1,050
Gimli_TUM-v1	9.8	25%		933	241	3,159
Gimli_TUM-v2	5.3	25%		905	244	5,915
Average		**24%**				
Minimum		**8%**				
Maximum		**48%**				

Table 31: Xilinx Artix-7 Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbits/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean-v1	2,804.4	47%	1	915	186	815
Xoodyak_XT-v8	1,357.3	47%	2	2,040	187	1,693
Xoodyak_XT-v2	1,328.2	47%		2,071	183	1,693
Ascon_Graz-v2	1,124.2	49%	3	1,723	216	2,361
Xoodyak_GMU-v1	996.2	46%		1,808	170	2,097
Gimli_GT-v2	896.5	48%	4	1,900	174	2,385
KNOT-v2	834.8	48%	5	1,569	254	3,739
Ascon_Graz-v1	822.9	49%		1,551	209	3,121
Ascon_VT-v1	735.4	49%		1,913	233	3,893
Ascon_VT-v2	726.9	49%		1,928	219	3,702
DryGASCON-v1	716.3	49%	6	2,074	238	4,083
TinyJAMBU_TJT-v3	691.1	49%	7	576	240	4,267
Romulus-v2	542.0	49%	8	1,280	214	4,852
Romulus-v3	535.6	49%		1,824	123	2,822
Spook-v2-v1	525.3	49%	9	2,296	201	4,702
Saturnin-v2	508.6	48%	10	2,414	168	4,059
Gimli_GT-v1	460.3	49%		1,683	177	4,725
Elephant-v2	426.8	49%	11	1,884	181	5,211
SCHWAEMM-v1	396.8	49%	12*	**3,071**	135	4,181
PHOTON-Beetle-v1	370.4	50%	13	2,065	178	5,905
GIFT-COFB-v1	364.3	50%	14	1,041	275	9,276
KNOT-v3	311.2	49%		1,367	264	10,425
ISAP-v2	290.6	48%	15	2,157	200	8,456
COMET_CI-v1	217.5	50%	16	1,884	223	12,597
TinyJAMBU_TJT-v2	217.5	50%		461	315	17,795
ESTATE-v1	214.2	50%	17	1,351	222	12,736
TinyJAMBU_GMU-v1	176.1	50%		591	266	18,564
COMET_VT-v2	170.3	49%		1,703	234	16,885
Oribatida-v1	169.6	49%	18	1,450	276	19,995
Oribatida-v2	166.2	50%		1,450	276	20,400
Elephant-v1	139.8	49%		1,291	229	20,123
Pyjamask-v2	133.0	49%	19	2,308	213	19,680
TinyJAMBU_GMU-v2	92.6	50%		564	268	35,572
Saturnin-v1	81.2	49%		2,020	192	29,049
LOCUS-v1	80.4	50%	20	1,824	216	33,012
Xoodyak_GMU-v2	77.8	45%		1,234	168	26,548
WAGE-v1	76.9	49%	21	1,150	279	44,601
SpoC-v1	66.5	50%	22	1,079	230	42,473
Pyjamask-v1	55.3	49%		1,979	229	50,908
LOTUS-v1	54.0	50%		1,652	145	33,012
ESTATE-v3	54.0	50%		1,130	259	58,976
COMET_CI-v2	50.2	50%		1,096	222	54,375
Gimli_TUM-v1	19.3	49%		933	241	153,573
Gimli_TUM-v2	10.4	49%		905	244	288,121
Average		**49%**				
Minimum		**45%**				
Maximum		**50%**				

Table 32: Xilinx Artix-7 Encryption AD+PT Throughput for 64 Byte Messages

Variant	**Through-put 64B [Mbits/s]**	**Thr AD+PT 64B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 64B**
Subterranean-v1	1,205.5	20%	1	915	186	79
Xoodyak_XT-v8	862.6	30%	2	2,040	187	111
Xoodyak_XT-v2	844.1	30%		2,071	183	111
Ascon_Graz-v2	722.8	31%	3	1,723	216	153
Xoodyak_GMU-v1	626.2	29%		1,808	170	139
Ascon_Graz-v1	604.6	36%		1,551	209	177
TinyJAMBU_TJT-v3	561.1	40%	4	576	240	219
Ascon_VT-v1	560.1	38%		1,913	233	213
DryGASCON-v1	556.4	38%	5	2,074	238	219
Ascon_VT-v2	544.3	37%		1,928	219	206
Gimli_GT-v2	503.3	27%	6	1,900	174	177
KNOT-v2	487.1	28%	7	1,569	254	267
Romulus-v2	434.8	40%	8	1,280	214	252
Romulus-v3	408.9	38%		1,824	123	154
Spook-v2-v1	359.8	34%	9	2,296	201	286
GIFT-COFB-v1	317.1	43%	10	1,041	275	444
Elephant-v2	313.1	36%	11	1,884	181	296
PHOTON-Beetle-v1	311.0	42%	12	2,065	178	293
Gimli_GT-v1	293.3	31%		1,683	177	309
Saturnin-v2	258.3	24%	13	2,414	168	333
SCHWAEMM-v1	255.1	31%	14*	**3,071**	135	271
KNOT-v3	231.1	36%		1,367	264	585
ESTATE-v1	192.0	45%	15	1,351	222	592
TinyJAMBU_TJT-v2	186.0	42%		461	315	867
COMET_CI-v1	179.2	41%	16	1,884	223	637
TinyJAMBU_GMU-v1	151.3	43%		591	266	900
ISAP-v2	140.7	23%	17	2,157	200	728
COMET_VT-v2	136.6	40%		1,703	234	877
Oribatida-v1	135.5	40%	18	1,450	276	1,043
Oribatida-v2	125.7	37%		1,450	276	1,124
Elephant-v1	103.9	37%		1,291	229	1,128
Pyjamask-v2	85.2	31%	19	2,308	213	1,280
TinyJAMBU_GMU-v2	80.0	43%		564	268	1,716
LOCUS-v1	71.4	44%	20	1,824	216	1,548
SpoC-v1	59.1	44%	21	1,079	230	1,993
WAGE-v1	53.9	34%	22	1,150	279	2,649
Saturnin-v1	52.8	32%		2,020	192	1,863
ESTATE-v3	49.6	46%		1,130	259	2,672
LOTUS-v1	48.0	44%		1,652	145	1,548
Xoodyak_GMU-v2	46.7	27%		1,234	168	1,842
COMET_CI-v2	41.1	41%		1,096	222	2,763
Pyjamask-v1	38.2	34%		1,979	229	3,068
Gimli_TUM-v1	14.2	36%		933	241	8,673
Gimli_TUM-v2	7.7	36%		905	244	16,261
Average		**36%**				
Minimum		**20%**				
Maximum		**46%**				

Table 33: Xilinx Artix-7 Encryption AD+PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbits/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Subterranean-v1	432.9	7%	1	915	186	55
Xoodyak_XT-v8	398.9	14%	2	2,040	187	60
Xoodyak_XT-v2	390.4	14%		2,071	183	60
TinyJAMBU_TJT-v3	353.1	25%	3	576	240	87
Ascon_Graz-v2	341.3	15%	4	1,723	216	81
Ascon_Graz-v1	330.3	20%		1,551	209	81
DryGASCON-v1	327.6	23%	5	2,074	238	93
Romulus-v2	326.1	30%	6	1,280	214	84
Ascon_VT-v1	320.7	22%		1,913	233	93
Ascon_VT-v2	304.7	21%		1,928	219	92
Xoodyak_GMU-v1	286.3	13%		1,808	170	76
Romulus-v3	281.1	26%		1,824	123	56
GIFT-COFB-v1	225.6	31%	7	1,041	275	156
Gimli_GT-v2	212.1	11%	8	1,900	174	105
KNOT-v2	209.8	12%	9	1,569	254	155
PHOTON-Beetle-v1	207.1	28%	10	2,065	178	110
Elephant-v2	194.7	23%	11	1,884	181	119
ESTATE-v1	145.0	34%	12	1,351	222	196
Gimli_GT-v1	137.3	15%		1,683	177	165
KNOT-v1	137.0	23%		1,092	260	243
Spook-v2-v1	135.4	13%	13	2,296	201	190
TinyJAMBU_TJT-v2	128.0	29%		461	315	315
Saturnin-v2	118.2	11%	14	2,414	168	182
COMET_CI-v1	115.6	26%	15	1,884	223	247
TinyJAMBU_GMU-v1	105.1	30%		591	266	324
SCHWAEMM-v1	94.9	12%	16*	**3,071**	135	182
COMET_VT-v2	84.4	25%		1,703	234	355
Oribatida-v1	83.1	24%	17	1,450	276	425
Oribatida-v2	71.8	21%		1,450	276	492
Elephant-v1	66.8	24%		1,291	229	439
TinyJAMBU_GMU-v2	56.1	30%		564	268	612
ISAP-v2	53.8	9%	18	2,157	200	476
LOCUS-v1	53.0	33%	19	1,824	216	522
SpoC-v1	43.7	33%	20	1,079	230	673
Pyjamask-v2	40.1	15%	21	2,308	213	680
ESTATE-v3	39.7	37%		1,130	259	836
LOTUS-v1	35.6	33%		1,652	145	522
Saturnin-v1	28.5	17%		2,020	192	862
WAGE-v1	27.9	18%	22	1,150	279	1,281
COMET_CI-v2	26.3	26%		1,096	222	1,080
Xoodyak_GMU-v2	20.4	12%		1,234	168	1,053
Pyjamask-v1	19.4	17%		1,979	229	1,508
Gimli_TUM-v1	7.8	20%		933	241	3,948
Gimli_TUM-v2	4.2	20%		905	244	7,396
Average		**21%**				
Minimum		**7%**				
Maximum		**37%**				

Table 34: Intel Cyclone 10 LP Encryption PT Throughput for 1536 Byte Messages

Variant	**Through-put 1536B [Mbits/s]**	**Thr PT 1536B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 1536B**
Subterranean-v1	4,540.9	89%	1	1,333	159.6	432
Ascon_Graz-v2	1,500.4	96%	2	2,666	146.7	1,201
Gimli_GT-v6	1,350.3	88%	3	4,843	47.9	436
Gimli_GT-v3	1,277.1	92%		3,652	87.0	837
Xoodyak_XT-v1	1,228.4	96%	4	2,282	140.6	1,406
Ascon_VT-v2	1,191.4	97%		2,695	172.0	1,774
Ascon_Graz-v1	1,184.5	97%		2,484	152.8	1,585
Xoodyak_XT-v7	1,169.6	96%		2,253	133.8	1,406
Ascon_VT-v1	1,104.5	98%		2,432	176.6	1,965
KNOT-v2	1,072.6	93%	5	2,050	167.5	1,919
Xoodyak_GMU-v1	1,031.6	96%		3,135	106.8	1,272
DryGASCON-v1	776.0	98%	6	3,199	130.5	2,067
TinyJAMBU_TJT-v3	629.7	99%	7	1,021	159.7	3,116
Spook-v2-v1	565.7	96%	8	3,912	110.4	2,398
Romulus-v2	557.4	98%	9	2,086	141.7	3,124
Romulus-v3	551.8	98%		2,407	79.3	1,766
GIFT-COFB-v1	490.8	98%	10	1,877	184.4	4,617
PHOTON-Beetle-v1	479.4	99%	11	3,602	125.4	3,215
Saturnin-v2	465.0	94%	12	3,892	104.6	2,763
SCHWAEMM-v1	429.1	96%	13	4,713	81.8	2,341
Elephant-v2	413.4	98%	14	2,729	113.2	3,363
KNOT-v4	406.6	96%		2,412	171.3	5,179
ISAP-v1	392.6	90%	15	4,589	126.6	3,962
ISAP-v2	311.3	93%		3,852	136.4	5,384
COMET_CI-v1	208.0	98%	16	4,663	115.8	6,837
TinyJAMBU_TJT-v2	188.3	99%		777	196.2	12,803
TinyJAMBU_GMU-v1	183.4	99%		856	196.8	13,189
Oribatida-v1	171.5	99%	17	2,512	185.7	13,301
ESTATE-v1	170.3	99%	18	3,839	118.0	8,512
Oribatida-v2	158.1	99%		2,221	174.5	13,564
Elephant-v1	150.1	98%		2,056	163.1	13,347
Pyjamask-v2	108.5	95%	19*	**8,692**	90.6	10,263
SpoC-v1	95.7	99%	20	1,696	167.7	21,545
TinyJAMBU_GMU-v2	94.2	99%		841	196.2	25,589
Saturnin-v1	90.9	97%		3,802	145.0	19,593
WAGE-v1	86.8	97%	21	1,774	159.6	22,600
LOCUS-v1	70.0	99%	22	2,978	125.8	22,068
LOTUS-v1	57.6	99%		2,642	103.5	22,068
COMET_CI-v2	56.3	98%		2,629	132.9	29,031
ESTATE-v3	56.2	99%		2,279	180.2	39,392
Average		**97%**				
Minimum		**88%**				
Maximum		**99%**				

Table 35: Intel Cyclone 10 LP Encryption PT Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbits/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Subterranean-v1	1,277.1	25%	1	1,333	159.6	64
Ascon_Graz-v2	774.1	49%	2	2,666	146.7	97
Ascon_VT-v2	746.3	61%		2,695	172.0	118
Ascon_VT-v1	723.4	64%		2,432	176.6	125
Ascon_Graz-v1	692.3	57%		2,484	152.8	113
Xoodyak_XT-v1	585.1	46%	3	2,282	140.6	123
Xoodyak_XT-v7	557.1	46%		2,253	133.8	123
DryGASCON-v1	495.0	62%	4	3,199	130.5	135
Xoodyak_GMU-v1	492.6	46%		3,135	106.8	111
TinyJAMBU_TJT-v3	475.4	74%	5	1,021	159.7	172
KNOT-v2	468.6	41%	6	2,050	167.5	183
Gimli_GT-v3	441.0	32%	7	3,652	87.0	101
Gimli_GT-v2	438.3	37%		2,678	110.4	129
Romulus-v2	403.1	71%	8	2,086	141.7	180
Romulus-v3	369.1	65%		2,407	79.3	110
PHOTON-Beetle-v1	358.8	74%	9	3,602	125.4	179
GIFT-COFB-v1	322.2	64%	10	1,877	184.4	293
Spook-v2-v1	297.5	51%	11	3,912	110.4	190
KNOT-v1	278.5	69%		1,485	177.9	327
Elephant-v2	258.6	61%	12	2,729	113.2	224
SCHWAEMM-v1	233.8	53%	13	4,713	81.8	179
Saturnin-v2	191.9	39%	14	3,892	104.6	279
TinyJAMBU_TJT-v2	152.5	80%		777	196.2	659
COMET_CI-v1	149.3	71%	15	4,663	115.8	397
TinyJAMBU_GMU-v1	148.8	80%		856	196.8	677
ESTATE-v1	145.2	85%	16	3,839	118.0	416
Oribatida-v1	136.4	79%	17	2,512	185.7	697
ISAP-v1	124.2	29%	18	4,589	126.6	522
Oribatida-v2	118.5	74%		2,221	174.5	754
ISAP-v2	116.6	35%		3,852	136.4	599
Elephant-v1	96.6	63%		2,056	163.1	864
TinyJAMBU_GMU-v2	77.2	81%		841	196.2	1,301
SpoC-v1	76.6	79%	19	1,696	167.7	1,121
LOCUS-v1	59.0	84%	20	2,978	125.8	1,092
Pyjamask-v2	52.8	46%	21*	**8,692**	90.6	879
Saturnin-v1	50.5	54%		3,802	145.0	1,469
WAGE-v1	50.3	56%	22	1,774	159.6	1,624
ESTATE-v3	49.7	88%		2,279	180.2	1,856
LOTUS-v1	48.5	84%		2,642	103.5	1,092
COMET_CI-v2	39.9	70%		2,629	132.9	1,707
Average		**61%**				
Minimum		**25%**				
Maximum		**88%**				

Table 36: Intel Cyclone 10 LP Encryption PT Throughput for 16 Byte Messages

Variant	**Throughput 16B [Mbits/s]**	**Thr PT 16B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 16B**
Subterranean-v1	393.0	8%	1	1,333	159.6	52
Ascon_VT-v1	347.8	31%	2	2,432	176.6	65
Ascon_VT-v2	344.0	28%		2,695	172.0	64
Ascon_Graz-v2	307.7	20%		2,666	146.7	61
Ascon_Graz-v1	300.9	25%		2,484	152.8	65
TinyJAMBU_TJT-v3	269.0	42%	3	1,021	159.7	76
DryGASCON-v1	232.1	29%	4	3,199	130.5	72
Xoodyak_XT-v1	222.1	17%	5	2,282	140.6	81
Romulus-v2	215.9	38%	6	2,086	141.7	84
Xoodyak_XT-v7	211.5	17%		2,253	133.8	81
PHOTON-Beetle-v1	200.7	41%	7	3,602	125.4	80
Xoodyak_GMU-v1	187.2	17%		3,135	106.8	73
Romulus-v3	181.3	32%		2,407	79.3	56
KNOT-v2	168.8	15%	8	2,050	167.5	127
GIFT-COFB-v1	155.3	31%	9	1,877	184.4	152
Elephant-v2	152.5	36%	10	2,729	113.2	95
Gimli_GT-v2	152.0	13%	11	2,678	110.4	93
Gimli_GT-v3	144.6	10%		3,652	87.0	77
KNOT-v1	143.2	35%		1,485	177.9	159
Spook-v2-v1	99.5	17%	12	3,912	110.4	142
ESTATE-v1	99.4	58%	13	3,839	118.0	152
TinyJAMBU_TJT-v2	95.5	50%		777	196.2	263
TinyJAMBU_GMU-v1	93.6	51%		856	196.8	269
Oribatida-v1	83.1	48%	14	2,512	185.7	286
SCHWAEMM-v1	81.8	18%	15	4,713	81.8	128
COMET_CI-v1	79.2	37%	16	4,663	115.8	187
Saturnin-v2	73.5	15%	17	3,892	104.6	182
Oribatida-v2	66.9	42%		2,221	174.5	334
Elephant-v1	59.5	39%		2,056	163.1	351
TinyJAMBU_GMU-v2	49.3	52%		841	196.2	509
SpoC-v1	47.2	49%	18	1,696	167.7	455
ISAP-v1	40.3	9%	19	4,589	126.6	402
LOCUS-v1	39.5	56%	20	2,978	125.8	408
ISAP-v2	39.4	12%		3,852	136.4	443
ESTATE-v3	36.5	65%		2,279	180.2	632
LOTUS-v1	32.5	56%		2,642	103.5	408
WAGE-v1	21.7	24%	21	1,774	159.6	940
Saturnin-v1	21.5	23%		3,802	145.0	862
COMET_CI-v2	20.9	36%		2,629	132.9	816
Pyjamask-v2	20.2	18%	22*	**8,692**	90.6	573
Average		**32%**				
Minimum		**8%**				
Maximum		**65%**				

Table 37: Intel Cyclone 10 LP Encryption AD Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbits/s]	Thr AD 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Subterranean-v1	4,551.4	89%	1	1,333	159.6	431
Xoodyak_XT-v1	1,780.5	94%	2	2,282	140.6	970
Xoodyak_XT-v7	1,695.4	94%		2,253	133.8	970
TinyJAMBU_TJT-v3	1,642.1	96%	3	1,021	159.7	1,195
Ascon_Graz-v2	1,490.5	95%	4	2,666	146.7	1,209
Xoodyak_GMU-v1	1,466.2	94%		3,135	106.8	895
Gimli_GT-v6	1,350.3	88%	5	4,843	47.9	436
Gimli_GT-v3	1,275.6	92%		3,652	87.0	838
Ascon_Graz-v1	1,180.1	97%		2,484	152.8	1,591
Ascon_VT-v1	1,100.0	97%		2,432	176.6	1,973
Ascon_VT-v2	1,071.2	97%		2,695	172.0	1,973
KNOT-v2	1,057.7	92%	6	2,050	167.5	1,946
Romulus-v2	960.9	95%	7	2,086	141.7	1,812
Saturnin-v2	885.5	89%	8	3,892	104.6	1,451
Romulus-v3	876.3	95%		2,407	79.3	1,112
DryGASCON-v1	776.0	98%	9	3,199	130.5	2,067
Elephant-v2	715.6	95%	10	2,729	113.2	1,943
ISAP-v1	658.1	90%	11	4,589	126.6	2,364
Spook-v2-v1	565.7	96%	12	3,912	110.4	2,398
PHOTON-Beetle-v1	563.2	98%	13	3,602	125.4	2,737
SCHWAEMM-v1	526.2	96%	14	4,713	81.8	1,909
ISAP-v2	505.9	93%		3,852	136.4	3,313
GIFT-COFB-v1	475.6	99%	15	1,877	184.4	4,764
TinyJAMBU_TJT-v2	470.8	97%		777	196.2	5,122
TinyJAMBU_GMU-v1	439.1	98%		856	196.8	5,508
KNOT-v4	402.6	95%		2,412	171.3	5,230
ESTATE-v1	338.5	99%	16	3,839	118.0	4,283
Oribatida-v1	333.5	97%	17	2,512	185.7	6,841
Oribatida-v2	308.1	97%		2,221	174.5	6,960
Elephant-v1	281.1	95%		2,056	163.1	7,127
COMET_CI-v1	242.0	98%	18	4,663	115.8	5,877
TinyJAMBU_GMU-v2	235.7	98%		841	196.2	10,228
Saturnin-v1	176.0	93%		3,802	145.0	10,121
LOCUS-v1	138.9	98%	19	2,978	125.8	11,124
LOTUS-v1	114.3	98%		2,642	103.5	11,124
Pyjamask-v2	112.7	95%	20*	**8,692**	90.6	9,887
ESTATE-v3	111.8	99%		2,279	180.2	19,803
SpoC-v1	97.4	99%	21	1,696	167.7	21,161
WAGE-v1	86.3	96%	22	1,774	159.6	22,713
COMET_CI-v2	63.2	98%		2,629	132.9	25,863
Average		**95%**				
Minimum		**88%**				
Maximum		**99%**				

Table 38: Intel Cyclone 10 LP Encryption AD Throughput for 64 Byte Messages

Variant	**Throughput 64B [Mbits/s]**	**Thr AD 64B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 64B**
Subterranean-v1	1,297.4	25%	1	1,333	159.6	63
TinyJAMBU_TJT-v3	898.5	53%	2	1,021	159.7	91
Ascon_Graz-v2	715.1	46%	3	2,666	146.7	105
Ascon_VT-v1	679.9	60%		2,432	176.6	133
Xoodyak_XT-v1	672.5	35%	4	2,282	140.6	107
Ascon_VT-v2	662.1	60%		2,695	172.0	133
Ascon_Graz-v1	657.4	54%		2,484	152.8	119
Xoodyak_XT-v7	640.4	35%		2,253	133.8	107
Xoodyak_GMU-v1	557.9	36%		3,135	106.8	98
DryGASCON-v1	495.0	62%	5	3,199	130.5	135
Romulus-v2	465.1	46%	6	2,086	141.7	156
Gimli_GT-v2	438.3	37%	7	2,678	110.4	129
Gimli_GT-v3	436.7	31%		3,652	87.0	102
KNOT-v2	408.4	36%	8	2,050	167.5	210
Romulus-v3	406.0	44%		2,407	79.3	100
PHOTON-Beetle-v1	398.9	70%	9	3,602	125.4	161
GIFT-COFB-v1	368.8	77%	10	1,877	184.4	256
Elephant-v2	346.9	46%	11	2,729	113.2	167
Spook-v2-v1	297.5	51%	12	3,912	110.4	190
TinyJAMBU_TJT-v2	297.2	62%		777	196.2	338
TinyJAMBU_GMU-v1	283.1	63%		856	196.8	356
SCHWAEMM-v1	260.0	47%	13	4,713	81.8	161
KNOT-v1	257.3	63%		1,485	177.9	354
ESTATE-v1	257.0	75%	14	3,839	118.0	235
Saturnin-v2	256.1	26%	15	3,892	104.6	209
ISAP-v1	205.1	28%	16	4,589	126.6	316
Oribatida-v1	192.8	56%	17	2,512	185.7	493
ISAP-v2	189.2	35%		3,852	136.4	369
Oribatida-v2	180.8	57%		2,221	174.5	494
COMET_CI-v1	166.0	67%	18	4,663	115.8	357
TinyJAMBU_GMU-v2	152.2	63%		841	196.2	660
Elephant-v1	135.7	46%		2,056	163.1	615
LOCUS-v1	101.2	72%	19	2,978	125.8	636
ESTATE-v3	89.1	79%		2,279	180.2	1,035
LOTUS-v1	83.3	72%		2,642	103.5	636
SpoC-v1	77.7	79%	20	1,696	167.7	1,105
Saturnin-v1	70.1	37%		3,802	145.0	1,059
Pyjamask-v2	53.3	45%	21*	**8,692**	90.6	871
WAGE-v1	47.0	53%	22	1,774	159.6	1,737
COMET_CI-v2	43.2	67%		2,629	132.9	1,575
Average		**52%**				
Minimum		**25%**				
Maximum		**79%**				

Table 39: Intel Cyclone 10 LP Encryption AD Throughput for 16 Byte Messages

Variant	Throughput 16B [Mbits/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 16B
Subterranean-v1	400.7	8%	1	1,333	159.6	51
TinyJAMBU_TJT-v3	371.6	22%	2	1,021	159.7	55
Ascon_VT-v1	309.7	27%	3	2,432	176.6	73
Ascon_VT-v2	301.6	27%		2,695	172.0	73
Ascon_Graz-v1	275.5	23%		2,484	152.8	71
Ascon_Graz-v2	272.0	17%		2,666	146.7	69
DryGASCON-v1	232.1	29%	4	3,199	130.5	72
Xoodyak_XT-v1	224.9	12%	5	2,282	140.6	80
GIFT-COFB-v1	216.5	45%	6	1,877	184.4	109
Romulus-v2	215.9	21%	7	2,086	141.7	84
Xoodyak_XT-v7	214.1	12%		2,253	133.8	80
PHOTON-Beetle-v1	208.5	36%	8	3,602	125.4	77
Xoodyak_GMU-v1	187.2	12%		3,135	106.8	73
Romulus-v3	181.3	20%		2,407	79.3	56
Gimli_GT-v2	152.0	13%	9	2,678	110.4	93
ESTATE-v1	146.6	43%	10	3,839	118.0	103
Gimli_GT-v3	142.8	10%		3,652	87.0	78
KNOT-v2	139.2	12%	11	2,050	167.5	154
TinyJAMBU_TJT-v2	138.0	29%		777	196.2	182
TinyJAMBU_GMU-v1	134.0	30%		856	196.8	188
KNOT-v1	122.4	30%		1,485	177.9	186
Elephant-v2	121.7	16%	12	2,729	113.2	119
Spook-v2-v1	99.5	17%	13	3,912	110.4	142
Saturnin-v2	86.3	9%	14	3,892	104.6	155
SCHWAEMM-v1	85.1	15%	15	4,713	81.8	123
COMET_CI-v1	83.7	34%	16	4,663	115.8	177
Oribatida-v1	83.1	24%	17	2,512	185.7	286
Oribatida-v2	79.2	25%		2,221	174.5	282
TinyJAMBU_GMU-v2	72.2	30%		841	196.2	348
ISAP-v1	66.4	9%	18	4,589	126.6	244
ISAP-v2	63.9	12%		3,852	136.4	273
LOCUS-v1	54.8	39%	19	2,978	125.8	294
ESTATE-v3	54.5	48%		2,279	180.2	423
SpoC-v1	47.6	48%	20	1,696	167.7	451
Elephant-v1	47.5	16%		2,056	163.1	439
LOTUS-v1	45.1	39%		2,642	103.5	294
Saturnin-v1	27.9	15%		3,802	145.0	665
COMET_CI-v2	21.7	34%		2,629	132.9	783
Pyjamask-v2	20.1	17%	21*	**8,692**	90.6	577
WAGE-v1	19.4	22%	22	1,774	159.6	1,053
Average		**24%**				
Minimum		**8%**				
Maximum		**48%**				

Table 40: Intel Cyclone 10 LP Encryption AD+PT Throughput for 64 Byte Messages

Variant	**Throughput 64B [Mbits/s]**	**Thr AD+PT 64B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 64B**
Subterranean-v1	1,034.6	20%	1	1,333	159.6	79
Ascon_Graz-v2	490.8	31%	2	2,666	146.7	153
Xoodyak_XT-v1	470.3	29%	3	2,282	140.6	153
Xoodyak_XT-v7	447.8	29%		2,253	133.8	153
Ascon_Graz-v1	442.0	36%		2,484	152.8	177
Ascon_VT-v2	427.5	37%		2,695	172.0	206
Ascon_VT-v1	424.6	38%		2,432	176.6	213
Xoodyak_GMU-v1	393.4	29%		3,135	106.8	139
TinyJAMBU_TJT-v3	373.3	40%	4	1,021	159.7	219
Gimli_GT-v3	332.4	24%	5	3,652	87.0	134
KNOT-v2	321.2	28%	6	2,050	167.5	267
Gimli_GT-v2	319.4	27%		2,678	110.4	177
DryGASCON-v1	305.2	38%	7	3,199	130.5	219
Romulus-v2	287.9	40%	8	2,086	141.7	252
Romulus-v3	263.6	38%		2,407	79.3	154
PHOTON-Beetle-v1	219.2	42%	9	3,602	125.4	293
GIFT-COFB-v1	212.6	43%	10	1,877	184.4	444
Spook-v2-v1	197.6	34%	11	3,912	110.4	286
Elephant-v2	195.7	36%	12	2,729	113.2	296
Saturnin-v2	160.8	24%	13	3,892	104.6	333
KNOT-v1	157.3	39%		1,485	177.9	579
SCHWAEMM-v1	154.5	31%	14	4,713	81.8	271
TinyJAMBU_TJT-v2	115.9	42%		777	196.2	867
TinyJAMBU_GMU-v1	112.0	43%		856	196.8	900
ISAP-v1	107.5	20%	15	4,589	126.6	603
ESTATE-v1	102.0	45%	16	3,839	118.0	592
ISAP-v2	95.9	23%		3,852	136.4	728
COMET_CI-v1	93.0	41%	17	4,663	115.8	637
Oribatida-v1	91.1	40%	18	2,512	185.7	1,043
Oribatida-v2	79.5	37%		2,221	174.5	1,124
Elephant-v1	74.0	37%		2,056	163.1	1,128
TinyJAMBU_GMU-v2	58.5	43%		841	196.2	1,716
SpoC-v1	43.1	44%	19	1,696	167.7	1,993
LOCUS-v1	41.6	44%	20	2,978	125.8	1,548
Saturnin-v1	39.8	32%		3,802	145.0	1,863
Pyjamask-v2	36.3	31%	21*	**8,692**	90.6	1,280
ESTATE-v3	34.5	46%		2,279	180.2	2,672
LOTUS-v1	34.2	44%		2,642	103.5	1,548
WAGE-v1	30.8	34%	22	1,774	159.6	2,649
COMET_CI-v2	24.6	41%		2,629	132.9	2,763
Average		**35%**				
Minimum		**20%**				
Maximum		**46%**				

Table 41: Intel Cyclone 10 LP Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbits/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Subterranean-v1	2,406.9	47%	1	1,333	159.6	815
Ascon_Graz-v2	763.3	49%	2	2,666	146.7	2,361
Xoodyak_XT-v1	751.2	46%	3	2,282	140.6	2,299
Gimli_GT-v6	719.7	47%	4	4,843	47.9	818
Xoodyak_XT-v7	715.3	46%		2,253	133.8	2,299
Gimli_GT-v3	665.6	48%		3,652	87.0	1,606
Xoodyak_GMU-v1	625.8	46%		3,135	106.8	2,097
Ascon_Graz-v1	601.6	49%		2,484	152.8	3,121
Ascon_VT-v2	570.9	49%		2,695	172.0	3,702
Ascon_VT-v1	557.5	49%		2,432	176.6	3,893
KNOT-v2	550.5	48%	5	2,050	167.5	3,739
TinyJAMBU_TJT-v3	459.9	49%	6	1,021	159.7	4,267
DryGASCON-v1	392.8	49%	7	3,199	130.5	4,083
Romulus-v2	358.9	49%	8	2,086	141.7	4,852
Romulus-v3	345.3	49%		2,407	79.3	2,822
Saturnin-v2	316.5	48%	9	3,892	104.6	4,059
Spook-v2-v1	288.5	49%	10	3,912	110.4	4,702
Elephant-v2	266.8	49%	11	2,729	113.2	5,211
PHOTON-Beetle-v1	261.0	50%	12	3,602	125.4	5,905
ISAP-v1	255.4	47%	13	4,589	126.6	6,091
GIFT-COFB-v1	244.3	50%	14	1,877	184.4	9,276
SCHWAEMM-v1	240.3	49%	15	4,713	81.8	4,181
KNOT-v4	206.0	49%		2,412	171.3	10,223
ISAP-v2	198.2	48%		3,852	136.4	8,456
TinyJAMBU_TJT-v2	135.5	50%		777	196.2	17,795
TinyJAMBU_GMU-v1	130.3	50%		856	196.8	18,564
Oribatida-v1	114.1	49%	16	2,512	185.7	19,995
ESTATE-v1	113.8	50%	17	3,839	118.0	12,736
COMET_CI-v1	112.9	50%	18	4,663	115.8	12,597
Oribatida-v2	105.1	50%		2,221	174.5	20,400
Elephant-v1	99.6	49%		2,056	163.1	20,123
TinyJAMBU_GMU-v2	67.8	50%		841	196.2	35,572
Saturnin-v1	61.3	49%		3,802	145.0	29,049
Pyjamask-v2	56.6	49%	19*	**8,692**	90.6	19,680
SpoC-v1	48.5	50%	20	1,696	167.7	42,473
LOCUS-v1	46.8	50%	21	2,978	125.8	33,012
WAGE-v1	44.0	49%	22	1,774	159.6	44,601
LOTUS-v1	38.5	50%		2,642	103.5	33,012
ESTATE-v3	37.5	50%		2,279	180.2	58,976
COMET_CI-v2	30.0	50%		2,629	132.9	54,375
Average		**49%**				
Minimum		**46%**				
Maximum		**50%**				

Table 42: Intel Cyclone 10 LP Encryption AD+PT Throughput for 16 Byte Messages

Variant	**Throughput 16B [Mbits/s]**	**Thr AD+PT 16B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 16B**
Subterranean-v1	371.5	7%	1	1,333	159.6	55
Ascon_VT-v1	243.1	22%	2	2,432	176.6	93
Ascon_Graz-v1	241.4	20%		2,484	152.8	81
Ascon_VT-v2	239.3	21%		2,695	172.0	92
TinyJAMBU_TJT-v3	234.9	25%	3	1,021	159.7	87
Ascon_Graz-v2	231.7	15%		2,666	146.7	81
Romulus-v2	215.9	30%	4	2,086	141.7	84
Xoodyak_XT-v1	214.2	13%	5	2,282	140.6	84
Xoodyak_XT-v7	203.9	13%		2,253	133.8	84
Romulus-v3	181.3	26%		2,407	79.3	56
Xoodyak_GMU-v1	179.9	13%		3,135	106.8	76
DryGASCON-v1	179.7	23%	6	3,199	130.5	93
GIFT-COFB-v1	151.3	31%	7	1,877	184.4	156
PHOTON-Beetle-v1	146.0	28%	8	3,602	125.4	110
KNOT-v2	138.3	12%	9	2,050	167.5	155
Gimli_GT-v2	134.6	11%	10	2,678	110.4	105
Gimli_GT-v3	129.5	9%		3,652	87.0	86
Elephant-v2	121.7	23%	11	2,729	113.2	119
KNOT-v1	93.7	23%		1,485	177.9	243
TinyJAMBU_TJT-v2	79.7	29%		777	196.2	315
TinyJAMBU_GMU-v1	77.8	30%		856	196.8	324
ESTATE-v1	77.0	34%	12	3,839	118.0	196
Spook-v2-v1	74.4	13%	13	3,912	110.4	190
Saturnin-v2	73.5	11%	14	3,892	104.6	182
COMET_CI-v1	60.0	26%	15	4,663	115.8	247
SCHWAEMM-v1	57.5	12%	16	4,713	81.8	182
Oribatida-v1	55.9	24%	17	2,512	185.7	425
Elephant-v1	47.5	24%		2,056	163.1	439
Oribatida-v2	45.4	21%		2,221	174.5	492
TinyJAMBU_GMU-v2	41.0	30%		841	196.2	612
ISAP-v1	39.4	7%	18	4,589	126.6	411
ISAP-v2	36.7	9%		3,852	136.4	476
SpoC-v1	31.9	33%	19	1,696	167.7	673
LOCUS-v1	30.8	33%	20	2,978	125.8	522
ESTATE-v3	27.6	37%		2,279	180.2	836
LOTUS-v1	25.4	33%		2,642	103.5	522
Saturnin-v1	21.5	17%		3,802	145.0	862
Pyjamask-v2	17.1	15%	21*	**8,692**	90.6	680
WAGE-v1	15.9	18%	22	1,774	159.6	1,281
COMET_CI-v2	15.8	26%		2,629	132.9	1,080
Average		**21%**				
Minimum		**7%**				
Maximum		**37%**				

Table 43: Lattice ECP5 Encryption PT Throughput for 1536 Byte Messages

Variant	Throughput 1536B [Mbits/s]	Thr PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean-v1	1,675.4	89%	1	1,725	58.9	432
Gimli_GT-v4	960.9	91%	2	4,632	49.5	633
Xoodyak_XT-v2	865.3	96%	3	4,302	70.7	1,004
Xoodyak_XT-v8	808.1	96%		3,507	66.0	1,004
Xoodyak_GMU-v1	714.9	96%		3,172	74.0	1,272
Gimli_GT-v3	651.8	92%		4,934	44.4	837
DryGASCON-v1	597.6	98%	4	3,801	100.5	2,067
KNOT-v2	583.7	93%	5	2,241	91.2	1,919
Ascon_VT-v1	530.9	98%	6	3,130	84.9	1,965
Ascon_VT-v2	514.0	97%		3,256	74.2	1,774
Spook-v2-v1	398.7	96%	7	3,655	77.8	2,398
PHOTON-Beetle-v1	387.7	99%	8	3,294	101.4	3,215
TinyJAMBU_TJT-v3	385.3	99%	9	881	97.7	3,116
SCHWAEMM-v1	348.2	96%	10	4,685	66.3	2,341
Saturnin-v2	338.4	94%	11	3,326	76.1	2,763
Romulus-v3	313.1	98%	12	3,847	45.0	1,766
Elephant-v2	312.4	98%	13	3,073	85.5	3,363
GIFT-COFB-v1	304.2	98%	14	2,214	114.3	4,617
Romulus-v2	253.3	98%		3,080	64.4	3,124
KNOT-v1	210.5	98%		1,597	93.8	5,479
ISAP-v1	189.5	90%	15*	**6,701**	61.1	3,962
COMET_VT-v2	157.0	98%	16	2,353	111.5	8,725
COMET_CI-v1	145.4	98%		3,427	80.9	6,837
ESTATE-v1	143.6	99%	17	3,079	99.5	8,512
TinyJAMBU_GMU-v1	116.3	99%		720	124.8	13,189
Oribatida-v1	110.6	99%	18	2,832	119.7	13,301
Oribatida-v2	103.5	99%		2,497	114.2	13,564
TinyJAMBU_TJT-v2	95.0	99%		913	99.0	12,803
Elephant-v1	89.8	98%		2,368	97.5	13,347
Pyjamask-v2	87.6	95%	19	4,162	73.2	10,263
TinyJAMBU_GMU-v2	61.6	99%		908	128.3	25,589
Saturnin-v1	57.1	97%		3,156	91.0	19,593
SpoC-v1	56.0	99%	20	2,049	98.2	21,545
Xoodyak_GMU-v2	52.5	95%		2,316	74.8	17,495
WAGE-v1	49.5	97%	21	2,029	91.1	22,600
LOCUS-v1	44.3	99%	22	3,161	79.6	22,068
Pyjamask-v1	43.6	96%		3,897	92.7	26,131
COMET_CI-v2	39.9	98%		1,974	94.3	29,031
ESTATE-v3	33.2	99%		2,026	106.3	39,392
LOTUS-v1	31.0	99%		2,820	55.6	22,068
Average		**97%**				
Minimum		**89%**				
Maximum		**99%**				

Table 44: Lattice ECP5 Encryption PT Throughput for 64 Byte Messages

Variant	**Through-put 64B [Mbits/s]**	**Thr PT 64B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 64B**
Subterranean-v1	471.2	25%	1	1,725	58.9	64
Xoodyak_XT-v2	416.1	46%	2	4,302	70.7	87
Xoodyak_XT-v8	388.6	46%		3,507	66.0	87
DryGASCON-v1	381.3	62%	3	3,801	100.5	135
Ascon_VT-v1	347.8	64%	4	3,130	84.9	125
Xoodyak_GMU-v1	341.3	46%		3,172	74.0	111
Ascon_VT-v2	322.0	61%		3,256	74.2	118
Gimli_GT-v4	312.9	30%	5	4,632	49.5	81
TinyJAMBU_TJT-v3	290.8	74%	6	881	97.7	172
PHOTON-Beetle-v1	290.2	74%	7	3,294	101.4	179
KNOT-v2	255.0	41%	8	2,241	91.2	183
Gimli_GT-v3	225.1	32%		4,934	44.4	101
Spook-v2-v1	209.7	51%	9	3,655	77.8	190
Romulus-v3	209.5	65%	10	3,847	45.0	110
GIFT-COFB-v1	199.7	64%	11	2,214	114.3	293
Elephant-v2	195.4	61%	12	3,073	85.5	224
SCHWAEMM-v1	189.8	53%	13	4,685	66.3	179
Romulus-v2	183.2	71%		3,080	64.4	180
KNOT-v1	146.9	69%		1,597	93.8	327
Saturnin-v2	139.7	39%	14	3,326	76.1	279
ESTATE-v1	122.5	85%	15	3,079	99.5	416
COMET_VT-v2	106.3	66%	16	2,353	111.5	537
COMET_CI-v1	104.3	71%		3,427	80.9	397
TinyJAMBU_GMU-v1	94.4	80%		720	124.8	677
Oribatida-v1	87.9	79%	17	2,832	119.7	697
Oribatida-v2	77.5	74%		2,497	114.2	754
TinyJAMBU_TJT-v2	76.9	80%		913	99.0	659
ISAP-v2	58.1	35%	18*	**5,708**	68.0	599
Elephant-v1	57.8	63%		2,368	97.5	864
TinyJAMBU_GMU-v2	50.5	81%		908	128.3	1,301
SpoC-v1	44.9	79%	19	2,049	98.2	1,121
Pyjamask-v2	42.6	46%	20	4,162	73.2	879
LOCUS-v1	37.3	84%	21	3,161	79.6	1,092
Saturnin-v1	31.7	54%		3,156	91.0	1,469
ESTATE-v3	29.3	88%		2,026	106.3	1,856
WAGE-v1	28.7	56%	22	2,029	91.1	1,624
COMET_CI-v2	28.3	70%		1,974	94.3	1,707
LOTUS-v1	26.1	84%		2,820	55.6	1,092
Xoodyak_GMU-v2	24.4	44%		2,316	74.8	1,572
Pyjamask-v1	23.4	52%		3,897	92.7	2,027
Average		**61%**				
Minimum		**25%**				
Maximum		**88%**				

Table 45: Lattice ECP5 Encryption PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbits/s]	Thr PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
DryGASCON-v1	178.7	29%	1	3,801	100.5	72
Ascon_VT-v1	167.2	31%	2	3,130	84.9	65
TinyJAMBU_TJT-v3	164.5	42%	3	881	97.7	76
PHOTON-Beetle-v1	162.3	41%	4	3,294	101.4	80
Xoodyak_XT-v2	158.8	18%	5	4,302	70.7	57
Ascon_VT-v2	148.4	28%		3,256	74.2	64
Xoodyak_XT-v8	148.3	18%		3,507	66.0	57
Subterranean-v1	145.0	8%	6	1,725	58.9	52
Xoodyak_GMU-v1	129.8	17%		3,172	74.0	73
Elephant-v2	115.2	36%	7	3,073	85.5	95
Romulus-v3	102.9	32%	8	3,847	45.0	56
Gimli_GT-v4	100.6	10%	9	4,632	49.5	63
Romulus-v2	98.1	38%		3,080	64.4	84
GIFT-COFB-v1	96.3	31%	10	2,214	114.3	152
KNOT-v2	91.9	15%	11	2,241	91.2	127
ESTATE-v1	83.8	58%	12	3,079	99.5	152
KNOT-v1	75.6	35%		1,597	93.8	159
Gimli_GT-v3	73.8	10%		4,934	44.4	77
Spook-v2-v1	70.1	17%	13	3,655	77.8	142
SCHWAEMM-v1	66.3	18%	14	4,685	66.3	128
TinyJAMBU_GMU-v1	59.4	51%		720	124.8	269
COMET_CI-v1	55.4	37%	15	3,427	80.9	187
Oribatida-v1	53.6	48%	16	2,832	119.7	286
Saturnin-v2	53.5	15%	17	3,326	76.1	182
COMET_VT-v2	52.8	33%		2,353	111.5	270
TinyJAMBU_TJT-v2	48.2	50%		913	99.0	263
Oribatida-v2	43.8	42%		2,497	114.2	334
Elephant-v1	35.6	39%		2,368	97.5	351
TinyJAMBU_GMU-v2	32.3	52%		908	128.3	509
SpoC-v1	27.6	49%	18	2,049	98.2	455
LOCUS-v1	25.0	56%	19	3,161	79.6	408
ESTATE-v3	21.5	65%		2,026	106.3	632
ISAP-v2	19.6	12%	20*	**5,708**	68.0	443
LOTUS-v1	17.4	56%		2,820	55.6	408
Pyjamask-v2	16.4	18%	21	4,162	73.2	573
COMET_CI-v2	14.8	36%		1,974	94.3	816
Saturnin-v1	13.5	23%		3,156	91.0	862
WAGE-v1	12.4	24%	22	2,029	91.1	940
Pyjamask-v1	9.6	21%		3,897	92.7	1,241
Xoodyak_GMU-v2	9.1	17%		2,316	74.8	1,050
Average		**32%**				
Minimum		**8%**				
Maximum		**65%**				

Table 46: Lattice ECP5 Encryption AD Throughput for 1536 Byte Messages

Variant	**Through-put 1536B [Mbits/s]**	**Thr AD 1536B / Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per 1536B**
Subterranean-v1	1,679.3	89%	1	1,725	58.9	431
Xoodyak_XT-v2	1,170.8	94%	2	4,302	70.7	742
Xoodyak_XT-v8	1,093.5	94%		3,507	66.0	742
Xoodyak_GMU-v1	1,016.0	94%		3,172	74.0	895
TinyJAMBU_TJT-v3	1,004.6	96%	3	881	97.7	1,195
Gimli_GT-v4	962.4	91%	4	4,632	49.5	632
Gimli_GT-v3	651.1	92%		4,934	44.4	838
Saturnin-v2	644.5	89%	5	3,326	76.1	1,451
DryGASCON-v1	597.6	98%	6	3,801	100.5	2,067
KNOT-v2	575.6	92%	7	2,241	91.2	1,946
Elephant-v2	540.7	95%	8	3,073	85.5	1,943
Ascon_VT-v1	528.8	97%	9	3,130	84.9	1,973
Romulus-v3	497.3	95%	10	3,847	45.0	1,112
Ascon_VT-v2	462.1	97%		3,256	74.2	1,973
PHOTON-Beetle-v1	455.4	98%	11	3,294	101.4	2,737
Romulus-v2	436.7	95%		3,080	64.4	1,812
SCHWAEMM-v1	427.0	96%	12	4,685	66.3	1,909
Spook-v2-v1	398.7	96%	13	3,655	77.8	2,398
ISAP-v1	317.6	90%	14*	**6,701**	61.1	2,364
GIFT-COFB-v1	294.8	99%	15	2,214	114.3	4,764
ESTATE-v1	285.5	99%	16	3,079	99.5	4,283
TinyJAMBU_GMU-v1	278.4	98%		720	124.8	5,508
TinyJAMBU_TJT-v2	237.5	97%		913	99.0	5,122
Oribatida-v1	215.0	97%	17	2,832	119.7	6,841
KNOT-v1	209.4	98%		1,597	93.8	5,506
Oribatida-v2	201.6	97%		2,497	114.2	6,960
COMET_CI-v1	169.2	98%	18	3,427	80.9	5,877
Elephant-v1	168.1	95%		2,368	97.5	7,127
COMET_VT-v2	164.2	98%		2,353	111.5	8,341
TinyJAMBU_GMU-v2	154.1	98%		908	128.3	10,228
Saturnin-v1	110.5	93%		3,156	91.0	10,121
Xoodyak_GMU-v2	91.0	92%		2,316	74.8	10,100
Pyjamask-v2	91.0	95%	19	4,162	73.2	9,887
LOCUS-v1	87.9	98%	20	3,161	79.6	11,124
ESTATE-v3	66.0	99%		2,026	106.3	19,803
LOTUS-v1	61.4	98%		2,820	55.6	11,124
SpoC-v1	57.0	99%	21	2,049	98.2	21,161
WAGE-v1	49.3	96%	22	2,029	91.1	22,713
COMET_CI-v2	44.8	98%		1,974	94.3	25,863
Pyjamask-v1	44.2	96%		3,897	92.7	25,755
Average		**96%**				
Minimum		**89%**				
Maximum		**99%**				

Table 47: Lattice ECP5 Encryption AD Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbits/s]	Thr AD 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
TinyJAMBU_TJT-v3	549.7	53%	1	881	97.7	91
Subterranean-v1	478.7	25%	2	1,725	58.9	63
Xoodyak_XT-v2	470.1	38%	3	4,302	70.7	77
Xoodyak_XT-v8	439.1	38%		3,507	66.0	77
Xoodyak_GMU-v1	386.6	36%		3,172	74.0	98
DryGASCON-v1	381.3	62%	4	3,801	100.5	135
Ascon_VT-v1	326.8	60%	5	3,130	84.9	133
PHOTON-Beetle-v1	322.6	70%	6	3,294	101.4	161
Gimli_GT-v4	316.8	30%	7	4,632	49.5	80
Ascon_VT-v2	285.6	60%		3,256	74.2	133
Elephant-v2	262.1	46%	8	3,073	85.5	167
Romulus-v3	230.4	44%	9	3,847	45.0	100
GIFT-COFB-v1	228.6	77%	10	2,214	114.3	256
Gimli_GT-v3	222.9	31%		4,934	44.4	102
KNOT-v2	222.2	36%	11	2,241	91.2	210
ESTATE-v1	216.8	75%	12	3,079	99.5	235
Romulus-v2	211.4	46%		3,080	64.4	156
SCHWAEMM-v1	211.0	47%	13	4,685	66.3	161
Spook-v2-v1	209.7	51%	14	3,655	77.8	190
Saturnin-v2	186.4	26%	15	3,326	76.1	209
TinyJAMBU_GMU-v1	179.5	63%		720	124.8	356
TinyJAMBU_TJT-v2	150.0	62%		913	99.0	338
KNOT-v1	135.7	63%		1,597	93.8	354
Oribatida-v1	124.3	56%	16	2,832	119.7	493
Oribatida-v2	118.4	57%		2,497	114.2	494
COMET_CI-v1	116.0	67%	17	3,427	80.9	357
COMET_VT-v2	109.5	65%		2,353	111.5	521
TinyJAMBU_GMU-v2	99.5	63%		908	128.3	660
ISAP-v2	94.3	35%	18*	**5,708**	68.0	369
Elephant-v1	81.2	46%		2,368	97.5	615
LOCUS-v1	64.1	72%	19	3,161	79.6	636
ESTATE-v3	52.6	79%		2,026	106.3	1,035
SpoC-v1	45.5	79%	20	2,049	98.2	1,105
LOTUS-v1	44.8	72%		2,820	55.6	636
Saturnin-v1	44.0	37%		3,156	91.0	1,059
Pyjamask-v2	43.0	45%	21	4,162	73.2	871
COMET_CI-v2	30.7	67%		1,974	94.3	1,575
Xoodyak_GMU-v2	29.1	29%		2,316	74.8	1,317
WAGE-v1	26.9	53%	22	2,029	91.1	1,737
Pyjamask-v1	23.5	51%		3,897	92.7	2,019
Average		**53%**				
Minimum		**25%**				
Maximum		**79%**				

Table 48: Lattice ECP5 Encryption AD Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbits/s]	Thr AD 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
TinyJAMBU_TJT-v3	227.4	22%	1	881	97.7	55
DryGASCON-v1	178.7	29%	2	3,801	100.5	72
PHOTON-Beetle-v1	168.6	36%	3	3,294	101.4	77
Xoodyak_XT-v2	161.6	13%	4	4,302	70.7	56
Xoodyak_XT-v8	150.9	13%		3,507	66.0	56
Ascon_VT-v1	148.9	27%	5	3,130	84.9	73
Subterranean-v1	147.8	8%	6	1,725	58.9	51
GIFT-COFB-v1	134.2	45%	7	2,214	114.3	109
Ascon_VT-v2	130.1	27%		3,256	74.2	73
Xoodyak_GMU-v1	129.8	12%		3,172	74.0	73
ESTATE-v1	123.7	43%	8	3,079	99.5	103
Romulus-v3	102.9	20%	9	3,847	45.0	56
Gimli_GT-v4	102.2	10%	10	4,632	49.5	62
Romulus-v2	98.1	21%		3,080	64.4	84
Elephant-v2	92.0	16%	11	3,073	85.5	119
TinyJAMBU_GMU-v1	85.0	30%		720	124.8	188
KNOT-v2	75.8	12%	12	2,241	91.2	154
Gimli_GT-v3	72.9	10%		4,934	44.4	78
Spook-v2-v1	70.1	17%	13	3,655	77.8	142
TinyJAMBU_TJT-v2	69.6	29%		913	99.0	182
SCHWAEMM-v1	69.0	15%	14	4,685	66.3	123
KNOT-v1	64.6	30%		1,597	93.8	186
Saturnin-v2	62.8	9%	15	3,326	76.1	155
COMET_CI-v1	58.5	34%	16	3,427	80.9	177
COMET_VT-v2	53.6	32%		2,353	111.5	266
Oribatida-v1	53.6	24%	17	2,832	119.7	286
Oribatida-v2	51.8	25%		2,497	114.2	282
TinyJAMBU_GMU-v2	47.2	30%		908	128.3	348
LOCUS-v1	34.7	39%	18	3,161	79.6	294
ESTATE-v3	32.2	48%		2,026	106.3	423
ISAP-v2	31.9	12%	19*	**5,708**	68.0	273
Elephant-v1	28.4	16%		2,368	97.5	439
SpoC-v1	27.9	48%	20	2,049	98.2	451
LOTUS-v1	24.2	39%		2,820	55.6	294
Saturnin-v1	17.5	15%		3,156	91.0	665
Pyjamask-v2	16.2	17%	21	4,162	73.2	577
COMET_CI-v2	15.4	34%		1,974	94.3	783
WAGE-v1	11.1	22%	22	2,029	91.1	1,053
Pyjamask-v1	9.5	21%		3,897	92.7	1,245
Xoodyak_GMU-v2	9.1	9%		2,316	74.8	1,050
Average		**24%**				
Minimum		**8%**				
Maximum		**48%**				

Table 49: Lattice ECP5 Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Through-put 1536B [Mbits/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Subterranean-v1	888.1	47%	1	1,725	58.9	815
Xoodyak_XT-v2	513.1	47%	2	4,302	70.7	1,693
Gimli_GT-v4	503.5	48%	3	4,632	49.5	1,208
Xoodyak_XT-v8	479.3	47%		3,507	66.0	1,693
Xoodyak_GMU-v1	433.6	46%		3,172	74.0	2,097
Gimli_GT-v3	339.7	48%		4,934	44.4	1,606
DryGASCON-v1	302.6	49%	4	3,801	100.5	4,083
KNOT-v2	299.6	48%	5	2,241	91.2	3,739
TinyJAMBU_TJT-v3	281.4	49%	6	881	97.7	4,267
Ascon_VT-v1	268.0	49%	7	3,130	84.9	3,893
Ascon_VT-v2	246.3	49%		3,256	74.2	3,702
Saturnin-v2	230.4	48%	8	3,326	76.1	4,059
PHOTON-Beetle-v1	211.1	50%	9	3,294	101.4	5,905
Spook-v2-v1	203.3	49%	10	3,655	77.8	4,702
Elephant-v2	201.6	49%	11	3,073	85.5	5,211
Romulus-v3	195.9	49%	12	3,847	45.0	2,822
SCHWAEMM-v1	195.0	49%	13	4,685	66.3	4,181
Romulus-v2	163.1	49%		3,080	64.4	4,852
GIFT-COFB-v1	151.4	50%	14	2,214	114.3	9,276
ISAP-v1	123.3	47%	15*	**6,701**	61.1	6,091
KNOT-v1	106.0	49%		1,597	93.8	10,883
ESTATE-v1	96.0	50%	16	3,079	99.5	12,736
TinyJAMBU_GMU-v1	82.6	50%		720	124.8	18,564
COMET_VT-v2	81.1	49%	17	2,353	111.5	16,885
COMET_CI-v1	78.9	50%		3,427	80.9	12,597
Oribatida-v1	73.6	49%	18	2,832	119.7	19,995
Oribatida-v2	68.8	50%		2,497	114.2	20,400
TinyJAMBU_TJT-v2	68.4	50%		913	99.0	17,795
Elephant-v1	59.5	49%		2,368	97.5	20,123
Pyjamask-v2	45.7	49%	19	4,162	73.2	19,680
TinyJAMBU_GMU-v2	44.3	50%		908	128.3	35,572
Saturnin-v1	38.5	49%		3,156	91.0	29,049
Xoodyak_GMU-v2	34.6	45%		2,316	74.8	26,548
LOCUS-v1	29.6	50%	20	3,161	79.6	33,012
SpoC-v1	28.4	50%	21	2,049	98.2	42,473
WAGE-v1	25.1	49%	22	2,029	91.1	44,601
Pyjamask-v1	22.4	49%		3,897	92.7	50,908
ESTATE-v3	22.1	50%		2,026	106.3	58,976
COMET_CI-v2	21.3	50%		1,974	94.3	54,375
LOTUS-v1	20.7	50%		2,820	55.6	33,012
Average		**49%**				
Minimum		**45%**				
Maximum		**50%**				

Table 50: Lattice ECP5 Encryption AD+PT Throughput for 64 Byte Messages

Variant	Throughput 64B [Mbits/s]	Thr AD+PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Subterranean-v1	381.7	20%	1	1,725	58.9	79
Xoodyak_XT-v2	326.1	30%	2	4,302	70.7	111
Xoodyak_XT-v8	304.6	30%		3,507	66.0	111
Xoodyak_GMU-v1	272.6	29%		3,172	74.0	139
Gimli_GT-v4	243.7	23%	3	4,632	49.5	104
DryGASCON-v1	235.0	38%	4	3,801	100.5	219
TinyJAMBU_TJT-v3	228.4	40%	5	881	97.7	219
Ascon_VT-v1	204.1	38%	6	3,130	84.9	213
Ascon_VT-v2	184.4	37%		3,256	74.2	206
PHOTON-Beetle-v1	177.3	42%	7	3,294	101.4	293
KNOT-v2	174.8	28%	8	2,241	91.2	267
Gimli_GT-v3	169.6	24%		4,934	44.4	134
Romulus-v3	149.6	38%	9	3,847	45.0	154
Elephant-v2	147.9	36%	10	3,073	85.5	296
Spook-v2-v1	139.3	34%	11	3,655	77.8	286
GIFT-COFB-v1	131.8	43%	12	2,214	114.3	444
Romulus-v2	130.8	40%		3,080	64.4	252
SCHWAEMM-v1	125.3	31%	13	4,685	66.3	271
Saturnin-v2	117.0	24%	14	3,326	76.1	333
ESTATE-v1	86.1	45%	15	3,079	99.5	592
KNOT-v1	83.0	39%		1,597	93.8	579
TinyJAMBU_GMU-v1	71.0	43%		720	124.8	900
COMET_VT-v2	65.1	40%	16	2,353	111.5	877
COMET_CI-v1	65.0	41%		3,427	80.9	637
Oribatida-v1	58.8	40%	17	2,832	119.7	1,043
TinyJAMBU_TJT-v2	58.5	42%		913	99.0	867
Oribatida-v2	52.0	37%		2,497	114.2	1,124
ISAP-v2	47.8	23%	18*	**5,708**	68.0	728
Elephant-v1	44.3	37%		2,368	97.5	1,128
TinyJAMBU_GMU-v2	38.3	43%		908	128.3	1,716
Pyjamask-v2	29.3	31%	19	4,162	73.2	1,280
LOCUS-v1	26.3	44%	20	3,161	79.6	1,548
SpoC-v1	25.2	44%	21	2,049	98.2	1,993
Saturnin-v1	25.0	32%		3,156	91.0	1,863
Xoodyak_GMU-v2	20.8	27%		2,316	74.8	1,842
ESTATE-v3	20.4	46%		2,026	106.3	2,672
LOTUS-v1	18.4	44%		2,820	55.6	1,548
WAGE-v1	17.6	34%	22	2,029	91.1	2,649
COMET_CI-v2	17.5	41%		1,974	94.3	2,763
Pyjamask-v1	15.5	34%		3,897	92.7	3,068
Average		**36%**				
Minimum		**20%**				
Maximum		**46%**				

Table 51: Lattice ECP5 Encryption AD+PT Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbits/s]	Thr AD+PT 16B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 16B
Xoodyak_XT-v2	150.8	14%	1	4,302	70.7	60
TinyJAMBU_TJT-v3	143.7	25%	2	881	97.7	87
Xoodyak_XT-v8	140.9	14%		3,507	66.0	60
DryGASCON-v1	138.4	23%	3	3,801	100.5	93
Subterranean-v1	137.1	7%	4	1,725	58.9	55
Xoodyak_GMU-v1	124.6	13%		3,172	74.0	76
PHOTON-Beetle-v1	118.0	28%	5	3,294	101.4	110
Ascon_VT-v1	116.9	22%	6	3,130	84.9	93
Ascon_VT-v2	103.2	21%		3,256	74.2	92
Romulus-v3	102.9	26%	7	3,847	45.0	56
Romulus-v2	98.1	30%		3,080	64.4	84
GIFT-COFB-v1	93.8	31%	8	2,214	114.3	156
Gimli_GT-v4	93.2	9%	9	4,632	49.5	68
Elephant-v2	92.0	23%	10	3,073	85.5	119
KNOT-v2	75.3	12%	11	2,241	91.2	155
Gimli_GT-v3	66.1	9%		4,934	44.4	86
ESTATE-v1	65.0	34%	12	3,079	99.5	196
Saturnin-v2	53.5	11%	13	3,326	76.1	182
Spook-v2-v1	52.4	13%	14	3,655	77.8	190
KNOT-v1	49.4	23%		1,597	93.8	243
TinyJAMBU_GMU-v1	49.3	30%		720	124.8	324
SCHWAEMM-v1	46.7	12%	15	4,685	66.3	182
COMET_CI-v1	41.9	26%	16	3,427	80.9	247
TinyJAMBU_TJT-v2	40.2	29%		913	99.0	315
COMET_VT-v2	40.2	25%		2,353	111.5	355
Oribatida-v1	36.0	24%	17	2,832	119.7	425
Oribatida-v2	29.7	21%		2,497	114.2	492
Elephant-v1	28.4	24%		2,368	97.5	439
TinyJAMBU_GMU-v2	26.8	30%		908	128.3	612
LOCUS-v1	19.5	33%	18	3,161	79.6	522
SpoC-v1	18.7	33%	19	2,049	98.2	673
ISAP-v2	18.3	9%	20*	**5,708**	68.0	476
ESTATE-v3	16.3	37%		2,026	106.3	836
Pyjamask-v2	13.8	15%	21	4,162	73.2	680
LOTUS-v1	13.6	33%		2,820	55.6	522
Saturnin-v1	13.5	17%		3,156	91.0	862
COMET_CI-v2	11.2	26%		1,974	94.3	1,080
WAGE-v1	9.1	18%	22	2,029	91.1	1,281
Xoodyak_GMU-v2	9.1	12%		2,316	74.8	1,053
Pyjamask-v1	7.9	17%		3,897	92.7	1,508
Average		**21%**				
Minimum		**7%**				
Maximum		**37%**				

Table 52: Intel Cyclone 10 LP Encryption PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_VT-v1
3	Gimli_GT-v6	Gimli_GT-v6	Xoodyak_XT-v1	TinyJAMBU_TJT-v3
4	Xoodyak_XT-v1	Xoodyak_XT-v1	DryGASCON-v1	DryGASCON-v1
5	KNOT-v2	KNOT-v2	TinyJAMBU_TJT-v3	Xoodyak_XT-v1
6	DryGASCON-v1	DryGASCON-v1	KNOT-v2	Romulus-v2
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Gimli_GT-v3	PHOTON-Beetle-v1
8	Spook-v2-v1	Spook-v2-v1	Romulus-v2	KNOT-v2
9	Romulus-v2	Romulus-v2	PHOTON-Beetle-v1	GIFT-COFB-v1
10	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1	Elephant-v2
11	Saturnin-v2	PHOTON-Beetle-v1	Spook-v2-v1	Gimli_GT-v2
12	PHOTON-Beetle-v1	Saturnin-v2	Elephant-v2	Spook-v2-v1
13	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	ESTATE-v1
14	ISAP-v1	Elephant-v2	Saturnin-v2	Oribatida-v1
15	Elephant-v2	ISAP-v1	COMET_CI-v1	SCHWAEMM-v1
16	COMET_CI-v1	COMET_CI-v1	ESTATE-v1	COMET_CI-v1
17	Oribatida-v1	Oribatida-v1	Oribatida-v1	Saturnin-v2
18	ESTATE-v1	ESTATE-v1	ISAP-v1	SpoC-v1
19	Pyjamask-v2	Pyjamask-v2	SpoC-v1	ISAP-v1
20	SpoC-v1	SpoC-v1	LOCUS-v1	LOCUS-v1
21	WAGE-v1	WAGE-v1	Pyjamask-v2	WAGE-v1
22	LOCUS-v1	LOCUS-v1	WAGE-v1	Pyjamask-v2

Table 53: Intel Cyclone 10 LP Encryption AD Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Xoodyak_XT-v1	Xoodyak_XT-v1	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Ascon_Graz-v2	Ascon_VT-v1
4	Ascon_Graz-v2	Ascon_Graz-v2	Xoodyak_XT-v1	DryGASCON-v1
5	Gimli_GT-v6	Gimli_GT-v6	DryGASCON-v1	Xoodyak_XT-v1
6	KNOT-v2	KNOT-v2	Romulus-v2	GIFT-COFB-v1
7	Romulus-v2	Romulus-v2	Gimli_GT-v2	Romulus-v2
8	Saturnin-v2	Saturnin-v2	KNOT-v2	PHOTON-Beetle-v1
9	DryGASCON-v1	DryGASCON-v1	PHOTON-Beetle-v1	Gimli_GT-v2
10	Elephant-v2	Elephant-v2	GIFT-COFB-v1	ESTATE-v1
11	ISAP-v1	ISAP-v1	Elephant-v2	KNOT-v2
12	Spook-v2-v1	Spook-v2-v1	Spook-v2-v1	Elephant-v2
13	PHOTON-Beetle-v1	PHOTON-Beetle-v1	SCHWAEMM-v1	Spook-v2-v1
14	SCHWAEMM-v1	SCHWAEMM-v1	ESTATE-v1	Saturnin-v2
15	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	SCHWAEMM-v1
16	Oribatida-v1	ESTATE-v1	ISAP-v1	COMET_CI-v1
17	ESTATE-v1	Oribatida-v1	Oribatida-v1	Oribatida-v1
18	COMET_CI-v1	COMET_CI-v1	COMET_CI-v1	ISAP-v1
19	LOCUS-v1	LOCUS-v1	LOCUS-v1	LOCUS-v1
20	Pyjamask-v2	Pyjamask-v2	SpoC-v1	SpoC-v1
21	SpoC-v1	SpoC-v1	Pyjamask-v2	Pyjamask-v2
22	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 54: Intel Cyclone 10 LP Encryption AD+PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	Subterranean-v1
2	Xoodyak_XT-v1	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_VT-v1
3	Ascon_Graz-v2	Xoodyak_XT-v1	Xoodyak_XT-v1	TinyJAMBU_TJT-v3
4	Gimli_GT-v6	Gimli_GT-v6	TinyJAMBU_TJT-v3	Romulus-v2
5	KNOT-v2	KNOT-v2	Gimli_GT-v3	Xoodyak_XT-v1
6	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	KNOT-v2	DryGASCON-v1
7	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1	GIFT-COFB-v1
8	Romulus-v2	Romulus-v2	Romulus-v2	PHOTON-Beetle-v1
9	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	KNOT-v2
10	Spook-v2-v1	Spook-v2-v1	GIFT-COFB-v1	Gimli_GT-v2
11	ISAP-v1	Elephant-v2	Spook-v2-v1	Elephant-v2
12	Elephant-v2	PHOTON-Beetle-v1	Elephant-v2	ESTATE-v1
13	PHOTON-Beetle-v1	ISAP-v1	Saturnin-v2	Spook-v2-v1
14	SCHWAEMM-v1	GIFT-COFB-v1	SCHWAEMM-v1	Saturnin-v2
15	GIFT-COFB-v1	SCHWAEMM-v1	ISAP-v1	COMET_CI-v1
16	Oribatida-v1	Oribatida-v1	ESTATE-v1	SCHWAEMM-v1
17	ESTATE-v1	ESTATE-v1	COMET_CI-v1	Oribatida-v1
18	COMET_CI-v1	COMET_CI-v1	Oribatida-v1	ISAP-v1
19	Pyjamask-v2	Pyjamask-v2	SpoC-v1	SpoC-v1
20	SpoC-v1	SpoC-v1	LOCUS-v1	LOCUS-v1
21	LOCUS-v1	LOCUS-v1	Pyjamask-v2	Pyjamask-v2
22	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 55: Lattice ECP5 Encryption PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	DryGASCON-v1
2	Gimli_GT-v4	Gimli_GT-v4	Xoodyak_XT-v2	Ascon_VT-v1
3	Xoodyak_XT-v2	Xoodyak_XT-v2	DryGASCON-v1	TinyJAMBU_TJT-v3
4	KNOT-v2	DryGASCON-v1	Ascon_VT-v1	PHOTON-Beetle-v1
5	DryGASCON-v1	KNOT-v2	Gimli_GT-v4	Xoodyak_XT-v2
6	Ascon_VT-v1	Ascon_VT-v1	TinyJAMBU_TJT-v3	Subterranean-v1
7	Spook-v2-v1	Spook-v2-v1	PHOTON-Beetle-v1	Elephant-v2
8	PHOTON-Beetle-v1	PHOTON-Beetle-v1	KNOT-v2	Romulus-v3
9	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Spook-v2-v1	Gimli_GT-v4
10	SCHWAEMM-v1	SCHWAEMM-v1	Romulus-v3	GIFT-COFB-v1
11	Saturnin-v2	Saturnin-v2	GIFT-COFB-v1	KNOT-v2
12	Romulus-v3	Romulus-v3	Elephant-v2	ESTATE-v1
13	Elephant-v2	Elephant-v2	SCHWAEMM-v1	Spook-v2-v1
14	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	SCHWAEMM-v1
15	ISAP-v1	ISAP-v1	ESTATE-v1	COMET_CI-v1
16	COMET_VT-v2	COMET_VT-v2	COMET_VT-v2	Oribatida-v1
17	ESTATE-v1	ESTATE-v1	Oribatida-v1	Saturnin-v2
18	Oribatida-v1	Oribatida-v1	ISAP-v2	SpoC-v1
19	Pyjamask-v2	Pyjamask-v2	SpoC-v1	LOCUS-v1
20	SpoC-v1	SpoC-v1	Pyjamask-v2	ISAP-v2
21	WAGE-v1	WAGE-v1	LOCUS-v1	Pyjamask-v2
22	LOCUS-v1	LOCUS-v1	WAGE-v1	WAGE-v1

Table 56: Lattice ECP5 Encryption AD Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
2	Xoodyak_XT-v2	Xoodyak_XT-v2	Subterranean-v1	DryGASCON-v1
3	Gimli_GT-v4	TinyJAMBU_TJT-v3	Xoodyak_XT-v2	PHOTON-Beetle-v1
4	TinyJAMBU_TJT-v3	Gimli_GT-v4	DryGASCON-v1	Xoodyak_XT-v2
5	Saturnin-v2	Saturnin-v2	Ascon_VT-v1	Ascon_VT-v1
6	KNOT-v2	DryGASCON-v1	PHOTON-Beetle-v1	Subterranean-v1
7	DryGASCON-v1	KNOT-v2	Gimli_GT-v4	GIFT-COFB-v1
8	Elephant-v2	Elephant-v2	Elephant-v2	ESTATE-v1
9	Ascon_VT-v1	Ascon_VT-v1	Romulus-v3	Romulus-v3
10	Romulus-v3	Romulus-v3	GIFT-COFB-v1	Gimli_GT-v4
11	PHOTON-Beetle-v1	PHOTON-Beetle-v1	KNOT-v2	Elephant-v2
12	SCHWAEMM-v1	SCHWAEMM-v1	ESTATE-v1	KNOT-v2
13	Spook-v2-v1	Spook-v2-v1	SCHWAEMM-v1	Spook-v2-v1
14	ISAP-v1	ISAP-v1	Spook-v2-v1	SCHWAEMM-v1
15	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	Saturnin-v2
16	ESTATE-v1	ESTATE-v1	Oribatida-v1	COMET_CI-v1
17	Oribatida-v1	Oribatida-v1	COMET_CI-v1	Oribatida-v1
18	COMET_CI-v1	COMET_CI-v1	ISAP-v2	LOCUS-v1
19	Pyjamask-v2	Pyjamask-v2	LOCUS-v1	ISAP-v2
20	LOCUS-v1	LOCUS-v1	SpoC-v1	SpoC-v1
21	SpoC-v1	SpoC-v1	Pyjamask-v2	Pyjamask-v2
22	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Table 57: Lattice ECP5 Encryption AD+PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	Xoodyak_XT-v2
2	Xoodyak_XT-v2	Xoodyak_XT-v2	Xoodyak_XT-v2	TinyJAMBU_TJT-v3
3	Gimli_GT-v4	Gimli_GT-v4	Gimli_GT-v4	DryGASCON-v1
4	KNOT-v2	DryGASCON-v1	DryGASCON-v1	Subterranean-v1
5	DryGASCON-v1	KNOT-v2	TinyJAMBU_TJT-v3	PHOTON-Beetle-v1
6	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Ascon_VT-v1	Ascon_VT-v1
7	Ascon_VT-v1	Ascon_VT-v1	PHOTON-Beetle-v1	Romulus-v3
8	Saturnin-v2	Saturnin-v2	KNOT-v2	GIFT-COFB-v1
9	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Romulus-v3	Gimli_GT-v4
10	Spook-v2-v1	Spook-v2-v1	Elephant-v2	Elephant-v2
11	Elephant-v2	Elephant-v2	Spook-v2-v1	KNOT-v2
12	SCHWAEMM-v1	Romulus-v3	GIFT-COFB-v1	ESTATE-v1
13	Romulus-v3	SCHWAEMM-v1	SCHWAEMM-v1	Saturnin-v2
14	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	Spook-v2-v1
15	ISAP-v1	ISAP-v1	ESTATE-v1	SCHWAEMM-v1
16	ESTATE-v1	ESTATE-v1	COMET_VT-v2	COMET_CI-v1
17	COMET_VT-v2	COMET_VT-v2	Oribatida-v1	Oribatida-v1
18	Oribatida-v1	Oribatida-v1	ISAP-v2	LOCUS-v1
19	Pyjamask-v2	Pyjamask-v2	Pyjamask-v2	SpoC-v1
20	LOCUS-v1	LOCUS-v1	LOCUS-v1	ISAP-v2
21	SpoC-v1	SpoC-v1	SpoC-v1	Pyjamask-v2
22	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1

Changelog

1.0.0 (September 26, 2020) — First version of the paper published

1.0.1 (September 29, 2020)

Fixed

- Table 1: HDL of SpoC changed from VHDL to Verilog (CryptoCore)
  Reason: Mistake in the original version

Added

- Section 5.4: DryGASCON added to the list of algorithms that rank higher for short messages than for long messages
  Reason: Omission in the original version

1.0.2 (September 30, 2020)

Changed

- Table 2: Max Length [bytes] for Spook-v1 changed from $2^{16} - 1$ to unlimited
  Reason: Correction by the Spook Team

Removed

- Section 4: "The designers of Spook-v1 declared the maximum length as unlimited from the implementation point of view, but constrained to $2^{16} - 1$ due to the security bounds derived in [1]."
  Reason: Correction by the Spook Team

1.0.3 (October 2, 2020)

Changed

- Spook-v1 replaced by Spook-v2-v1
  Reason: v2 indicates a new version of the Spook algorithm announced on March 15, 2020

Added

- Figures 6 to 8 and Tables 8 to 10, 16, 17, 23, 34 to 42 and 52 to 54: Added results for ISAP-v2 on Cyclone 10 LP
  Reason: Miscommunication regarding the source list for ISAP-v2

1.0.4 (October 4, 2020)

Removed

- Section 5.1: WAGE removed from the list of algorithms that did not pass all tests.
  Reason: Miscommunication regarding the version of reference software implementation to be used for generating test vectors

1.0.5 (October 23, 2020)

Added

- New hardware design submissions: Gimli_GT (12 variants), Saturnin (2 variants), and TinyJAMBU_TJT (3 variants). The previous submissions renamed: Gimli to Gimli_TUM and TinyJAMBU to TinyJAMBU_GMU.
  Reason: Phase 2 Submissions

- New variants: Romulus-v5 and Oribatida-v2.
  Reason: Phase 2 Submissions
- New design-space exploration diagrams for Gimli and TinyJAMBU.
  Reason: Phase 2 Submissions
- Average, minimum, and maximum values added in Tables 22-51.
  Reason: Additional information helpful in analysis of results

Changed

- The fully-debugged code submitted for ESTATE and SpoC. Improved code submitted for LOCUS-v1.
  Reason: Phase 2 Submissions
- Listing of results in the ranking by throughput tables limited to the best two per hardware design submission.
  Reason: Attempt to limit each result table to one page.
- Section 1 Introduction is split into two sections: Section 1: Introduction and Section 2: Previous Work.
  Reason: Improve readability.

1.0.6 (October 25, 2020)

Fixed

- Added missing hashing throughput results for SCHWAEMM-v2 in Figures 9 and 13
  Reason: Results were missing due to a bug in the table and figure generation script.