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. Twenty five Round 2 candidates in the NIST Lightweight Cryptography (LWC) process have been implemented in hardware by groups from all over the world. All implementations compliant with the LWC Hardware API, proposed in 2019, have been submitted for hardware benchmarking to George Mason University's LWC benchmarking team. The received submissions were first verified for correct functionality and compliance with the hardware API's specification. Then, the execution times in clock cycles, as a function of input sizes, have been determined using behavioral simulation. 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 has 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 a 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.

Despite 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. 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 the 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.

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

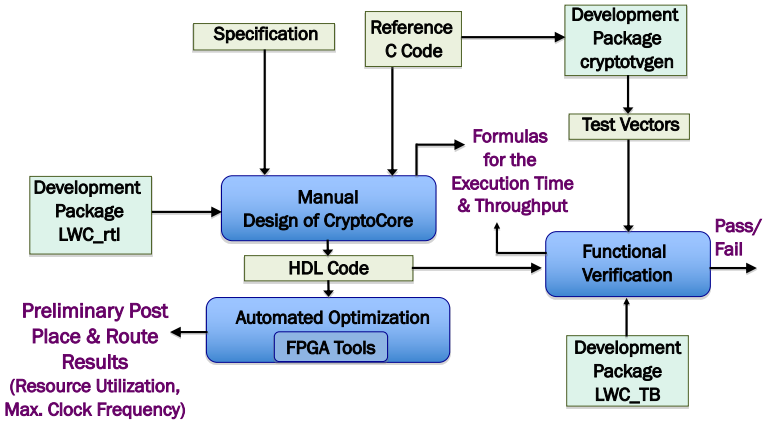

Figure 1: The API-Compliant Code Development using the Development Package

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 the 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, the 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. 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.

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 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.

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 dependent 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 synthesizable 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. The 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 that 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 a single optimization strategy (i.e., the collection of flow settings), targeting optimal timing, was considered. The synthesis was performed using both the Lattice Synthesis Engine (LSE) and Synplify Pro. Only the better of the two results were reported.

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 design packages submitted for benchmarking is given in Table 1. A total of 31 design packages were received (including three for Xoodyak). These designs covered 25 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 hardware design package. In particular,

- George Mason University Cryptographic Engineering Research Group (CERG), USA, implemented 7 candidates: Elephant, mixFeed, 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 design packages submitted for FPGA benchmarking

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designers	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
1	ACE	ComSec Lab University of Waterloo Canada	Mark Aagaard https://ece.uwaterloo.ca/ ∼maagaard maagaard@uwaterloo.ca Nusa Zidaric nzidaric@uwaterloo.ca	Mark Aagaard https://ece.uwaterloo.ca/ ∼maagaard maagaard@uwaterloo.ca Guang Gong https://ece.uwaterloo.ca/ ∼ggong ggong@uwaterloo.ca	Yes, Modified	VHDL	1
2a	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
2b	Ascon	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
3a	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	3
3b	COMET	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@ vt.edu	Yes, Modified	VHDL	2
4	DryGASCON	Independent (previously CERG GMU)	Ekawat Homsirikamol ekawat@gmail.com		Yes, Unmodified	Verilog (CryptoCore)	1
5	Elephant	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/ team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
6	ESTATE	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas Lopez cuauhtemoc.mancillas@ cinvestav.mx http://www.cs.cinvestav.mx/ Investigadores/Cmancillas		Yes, Modified	VHDL	4

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
7	ForkAE	ForkAE Team	Antoon Purnal antoon.purnal@kuleuven.be Jowan Pittevils r0626755@student.kuleuven.be		Yes, Unmodified	Verilog (CryptoCore)	2
8	GIFT-COFB	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Behnaz Rezvani behnaz@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	1
9a	Gimli	Gimli Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	7
9b	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
10	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
11	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)	16
12	LOCUS-AEAD & LOTUS-AEAD	CINVESTAV-IPN, Mexico	Brisbane Ovilla Martinez brisbane@cinvestav.mx		Yes, Unmodified	VHDL	4
13	mixFeed	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Eduardo R. Ferrufino https://cryptography.gmu.edu/ team/eferruf.php eferruf@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	1
14	Oribatida	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas López cuauhtemoc.mancillas@ cinvestav.mx, Alberto F. Martínez Herrera alberto.herrera.tec@gmail.com		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
15	PHOTON-Beetle	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Vivian Ledynh vledynh@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	1
16	Pyjamask	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/team/rishub.php rnagpal2@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
17	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
18	Saturnin	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/team/rishub.php rnagpal2@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
19	SCHWAEMM & ESCH	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Flora Coleman googly2@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
20	SpoC	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	William Diehl wdiehl@vt.edu		Yes, Modified	Verilog (CryptoCore)	1
21	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
22	Subterranean 2.0	Subterranean 2.0 Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	1

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
23a	TinyJAMBU	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Sammy Lin https://cryptography.gmu.edu/team/slin5.php slin5@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	3
23b	TinyJAMBU	TinyJAMBU Team	Tao Huang huangtaochn@gmail.com	Hongjun Wu https://www3.ntu.edu.sg/home/wuhj wuhongjun@gmail.com	Yes, Unmodified	VHDL	3
24	WAGE	ComSec Lab University of Waterloo Canada	Mark Aagaard https://ece.uwaterloo.ca/∼maagaard maagaard@uwaterloo.ca Nusa Zidaric nzidaric@uwaterloo.ca	Mark Aagaard https://ece.uwaterloo.ca/∼maagaard maagaard@uwaterloo.ca Guang Gong https://ece.uwaterloo.ca/∼ggong ggong@uwaterloo.ca	Yes, Modified	VHDL	1
25a	Xoodyak	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	Yes, Unmodified	VHDL	2
25b	Xoodyak	Xoodyak Team + Silvia	Silvia Mella silvia.mella@st.com		Yes, Unmodified	VHDL	12
25c	Xoodyak	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Kamyar Mohajerani https://crytpography.gmu.edu/team/mmohajer.php mmohajer@gmu.edu	Kris Gaj, kgaj@gmu.edu, https://ece.gmu.edu/profiles/kgaj Jens-Peter Kaps, jkaps@gmu.edu https://ece.gmu.edu/profiles/jkaps	No	Bluespec SystemVerilog	2
						Total	**92**

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

The implementation of DryGASCON was developed by an independent researcher, Ekawat Homsirikamol, in close collaboration with the author of the algorithm. An additional 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.

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. The submission Xoodyak_GMU2 (containing two variants) has been implemented purely in Bluespec SystemVerilog, depending on its own Bluespec LWC development package [25]. Three implementations modeled only the part unique to a given algorithm, its CryptoCore, in Verilog. These designs included DryGASCON, KNOT, and SpoC. 17 hardware design packages used VHDL pre-processing and post-processing units, provided as a part of the LWC Development Package without any modifications, 9 with modifications, and 5 did not use them at all.

Nine submissions contained a single variant. In the remaining, the number of variants varied between 2 and 16, with an average of 3.1 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 92. In Table 2, we summarize the 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-v2. In this name, the first v2 indicates version 2 of Spook proposed in [26]. This version is known to have higher security margins at the cost of relatively small performance overheads [26]. The second v2 indicates that it is the second, improved submission, received in Phase 3 of the benchmarking process, in November 2020.

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 [27]. Some were submitted as a part of the hardware package (KNOT and WAGE) or were provided through the 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), ForkAE, and COMET_CI.

The following designs do not support key reuse between consecutive inputs: Gimli_GT (v1-v7), Subterranean-v2, TinyJAMBU_GMU (v1-v3), Xoodyak_XT (v1-v12), and Xoodyak_GMU2 (v1-v2). For algorithms that support key reuse, we list in a 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 overhead of 4 clock cycles was obtained 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]
1	ACE-v1	ACE-AE-128 & ACE-H-256	aceae128v1 (aead) acehash256v1 (hash)	Y	7	N/A
2a	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
2b	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
3a	COMET_CI-v1	Folded architecture	comet128aesv1	Y	8	$2^{16}-1$
	COMET_CI-v2	Folded architecture	comet128aesv1	Y	23	$2^{16}-1$
	COMET_CI-v3	Folded architecture	comet128aesv1	Y	5	$2^{16}-1$
3b	COMET_VT-v1	Basic iterative architecture	comet128aesv1	Y	7	N/A
	COMET_VT-v2	Basic iterative architecture	comet128chamv1	Y	8	N/A
4	DryGASCON-v1	Basic iterative architecture, support for hashing	drygascon128k32 (aead) drygascon128 (hash)	Y	4	N/A
5	Elephant-v1	Basic iterative architecture	elephant160v1	Y	84	unlimited
	Elephant-v2	×5 Unrolled	elephant160v1	Y	20	unlimited
6	ESTATE-v1	Two-pass AES-based, 32-bit datapath	estatetweaes128v1	Y	8	$2^{16}-1$

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	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	$2^{16}-1$
7	ForkAE-v1	Area-focused	paefforkskinnyb-128t288n104v1	Y	23	$2^{16}-1$
	ForkAE-v2	Basic iterative	paefforkskinnyb-128t288n104v1	Y	23	$2^{16}-1$
8	GIFT-COFB-v1	Basic iterative architecture	giftcofb128v1	Y	8	N/A
9a	Gimli_GT-v1	1 combinational round	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v2	2 combinational rounds	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v3	3 combinational rounds	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v4	4 combinational rounds	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v5	6 combinational rounds	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v6	8 combinational rounds	gimli24v1	N		$2^{50}-1$
	Gimli_GT-v7	12 combinational rounds	gimli24v1	N		$2^{50}-1$
9b	Gimli_TUM-v1	Customized FSM based on 3×32-bit register, RAM-based state-memory, 32-bit datapath	gimli24v1	Y	3	N/A
	Gimli_TUM-v2	Customized FSM based on 3×32-bit register, RAM-based state-memory, 16-bit datapath	gimli24v1	Y	3	N/A
	Gimli_TUM-v3	Customized FSM based on 3×32-bit register, RAM-based state-memory, 8-bit datapath	gimli24v1	Y	3	N/A
10	ISAP-v1	Two-pass implementation, Folded architecture	isapk128av20	Y	9	$2^{16}-1$
	ISAP-v2	Two-pass implementation, Folded architecture	isapa128av20	Y	4	$2^{16}-1$
11	KNOT-v1×1	KNOT-AEAD (128, 256, 64), Basic iterative	submitted with HW package	Y	7	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]
	KNOT-v1×1h	KNOT-AEAD (128, 256, 64), Basic iterative support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v1×2	KNOT-AEAD (128, 256, 64), ×2 Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v1×2h	KNOT-AEAD (128, 256, 64), ×2 Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v1×4	KNOT-AEAD (128, 256, 64), ×4 Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v1×4h	KNOT-AEAD (128, 256, 64), ×4 Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v2×1	KNOT-AEAD (128, 384, 192), Basic iterative	submitted with HW package	Y	7	unlimited
	KNOT-v2×1h	KNOT-AEAD (128, 384, 192), Basic iterative support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v2×2	KNOT-AEAD (128, 384, 192), ×2 Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v2×2h	KNOT-AEAD (128, 384, 192), ×2 Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v2×4	KNOT-AEAD (128, 384, 192), ×4 Unrolled	submitted with HW package	Y	7	unlimited
	KNOT-v2×4h	KNOT-AEAD (128, 384, 192), ×4 Unrolled support for hashing	submitted with HW package	Y	7	unlimited
	KNOT-v3	KNOT-AEAD (192, 384, 96), Basic iterative	submitted with HW package	Y	9	unlimited
	KNOT-v3h	KNOT-AEAD (192, 384, 96), Basic iterative support for hashing	submitted with HW package	Y	9	unlimited
	KNOT-v4	KNOT-AEAD (256, 512, 128), Basic iterative	submitted with HW package	Y	11	unlimited
	KNOT-v4h	KNOT-AEAD (256, 512, 128), Basic iterative support for hashing	submitted with HW package	Y	11	unlimited
12	LOCUS-v1	LOCUS, 32-bit datapath	twegift-64locusaeadv1	Y	4	unlimited
	LOCUS-v2	LOCUS, 64-bit datapath	twegift-64locusaeadv1	Y	4	unlimited
	LOTUS-v1	LOTUS, 32-bit datapath	twegift-64lotusaeadv1	Y	4	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]
	LOTUS-v2	LOTUS, 64-bit datapath	twegift-64lotusaeadv1	Y	4	unlimited
13	mixFeed-v1	Folded architecture	mixfeed	Y	8	$2^{50}-1$
14	Oribatida-v1	Oribatida256 256-bit datapath	oribatida256v12	Y	8	unlimited
	Oribatida-v2	Oribatida192 192-bit datapath	oribatida192v12	Y	8	unlimited
15	PHOTON-Beetle-v1	AEAD+Hash	photonbeetle-aead128rate128v1, photonbeetle-hash256rate32v1	Y	6	$2^{50}-1$
16	Pyjamask-v1	Pyjamask128d16, folded architecture	pyjamask 128aeadv1	Y	433	$2^{16}-1$
	Pyjamask-v2	Pipeline implementation of MixRows	pyjamask 128aeadv1	Y	245	$2^{16}-1$
17	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	$2^{50}-1$
18	Saturnin-v1	Folded architecture	saturninctrcascadev2 saturninhashv2	Y	20	$2^{16}-1$
	Saturnin-v2	Unrolled SuperRound	saturninctrcascadev2 saturninhashv2	Y	20	$2^{16}-1$
19	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
20	SpoC-v1	spoc64, Basic iterative architecture	spoc64 sliscplight 192v1	Y	7	N/A
21	Spook-v2-v2	Folded architecture resource sharing Clyde128 Shadow512	spook 128su512v2	Y	7	unlimited
22	Subterranean-v2	32-bit bus	Candidate website	N		$2^{50}-1$
23a	TinyJAMBU_GMU-v1	32-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU_GMU-v2	16-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$

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_GMU-v3	Bit-serial NLFSR	tinyjambu128	N		$2^{50}-1$
23b	TinyJAMBU_TJT-v1	8-step state update	tinyjambu128	Y	15	$2^{50}-1$
	TinyJAMBU_TJT-v2	32-step state update	tinyjambu128	Y	4	$2^{50}-1$
	TinyJAMBU_TJT-v3	128-step state update	tinyjambu128	Y	4	$2^{50}-1$
24	WAGE-v1	Baseline	submitted with HW package	Y	7	N/A
25a	Xoodyak_GMU-v1	384-bit datapath AEAD+Hash	xoodyakv1	Y	18	unlimited
	Xoodyak_GMU-v2	128-bit datapath AEAD+Hash	xoodyakv1	Y	266	unlimited
25b	Xoodyak_XT-v1	Basic iterative architecture, AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v2	×2 Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v3	×3 Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v4	×4 Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v5	×6 Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v6	×12 Unrolled AEAD	xoodyakv1	N		unlimited
	Xoodyak_XT-v7	Basic iterative architecture, AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v8	×2 Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v9	×3 Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v10	×4 Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v11	×6 Unrolled AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_XT-v12	×12 Unrolled AEAD+Hash	xoodyakv1	N		unlimited
25c	Xoodyak_GMU2-v1	Basic iterative 384-bit datapath AEAD+Hash	xoodyakv1	N		unlimited
	Xoodyak_GMU2-v2	×2 Unrolled 384-bit datapath AEAD+Hash	xoodyakv1	N		unlimited
S1	AESGCM-v1	Basic iterative architecture	aes128gcmv1	Y	N/A	unlimited
	AESGCM-v2	GF Multiplier folded by a factor of 32	aes128gcmv1	Y	N/A	unlimited
S2	SHA2-v1	SHA-256 Basic iterative	sha256	N/A	N/A	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]
S3	SHA3-v1	SHA3-256 Folded by a factor of 8	sha3256	N/A	N/A	unlimited

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	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
1	ACE-v1	64	130	64	130	64	130	1.00	1.00	1.00	1.00
2a	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
2b	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
3a	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	
	COMET_CI-v3	128	56	128	66			1.18	1.00	1.08	
3b	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	
4	DryGASCON-v1	128	21	128	21	128	21	1.00	1.00	1.00	1.00
5	Elephant-v1	160	88	160	171			1.94	1.00	1.32	
	Elephant-v2	160	24	160	43			1.79	1.00	1.28	
6	ESTATE-v1	128	44	128	88			2.00	1.00	1.33	

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	AD Enc Thr / PT Enc Thr	PT Dec Thr / PT Enc Thr	AD+PT Enc Thr / PT Enc Thr	Hash Thr / PT Enc Thr
	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	
7	ForkAE-v1	128	1209	128	3194			2.64	1.00	1.45	
	ForkAE-v2	128	106	128	123			1.16	1.00	1.07	
8	GIFT-COFB-v1	128	49	128	47			0.96	1.00	0.98	
9a	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
9b	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
10	ISAP-v1	144	25	144	42			1.68	1.00	1.25	
	ISAP-v2	64	14	64	22			1.57	1.00	1.22	
11	KNOT-v1x1	64	28	64	28			1.00	1.00	1.00	
	KNOT-v1x1h	64	56	64	56	32	544	1.00	1.00	1.00	0.05
	KNOT-v1x2	64	14	64	14			1.00	1.00	1.00	
	KNOT-v1x2h	64	28	64	28	32	272	1.00	1.00	1.00	0.05
	KNOT-v1x4	64	7	64	7			1.00	1.00	1.00	
	KNOT-v1x4h	64	14	64	14	32	136	1.00	1.00	1.00	0.05
	KNOT-v2x1	192	28	192	28			1.00	1.00	1.00	
	KNOT-v2x1h	192	28	192	28	128	160	1.00	1.00	1.00	0.12
	KNOT-v2x2	192	14	192	14			1.00	1.00	1.00	
	KNOT-v2x2h	192	14	192	14	128	80	1.00	1.00	1.00	0.12
	KNOT-v2x4	192	7	192	13			1.00	1.00	1.00	
	KNOT-v2x4h	192	7	192	13	128	40	1.00	1.00	1.00	0.22
	KNOT-v3	96	40	96	40			1.00	1.00	1.00	
	KNOT-v3h	96	80	96	80	48	832	1.00	1.00	1.00	0.05
	KNOT-v4	128	52	128	52			1.00	1.00	1.00	
	KNOT-v4h	128	104	128	104	64	1120	1.00	1.00	1.00	0.05
12	LOCUS-v1	64	57	64	114			2.00	0.95	1.33	
	LOCUS-v2	64	30	64	60			2.00	0.95	1.33	
	LOTUS-v1	64	57	64	114			2.00	1.00	1.33	
	LOTUS-v2	64	30	64	60			2.00	1.00	1.33	
13	mixFeed-v1	128	53	128	57			1.08	1.00	1.04	
14	Oribatida-v1	128	69	128	137			1.99	1.00	1.33	
	Oribatida-v2	96	53	96	105			1.98	1.00	1.33	
15	PHOTON-Beetle-v1	128	28	128	33	32	25	1.18	1.00	1.08	0.33
16	Pyjamask-v1	128	258	128	262			1.02	0.96	1.01	
	Pyjamask-v2	128	98	128	102			1.04	1.00	1.02	
17	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	
	Romulus-v5	128	660	128	1304			1.98	1.00	1.33	
18	Saturnin-v1	256	197	256	394	256	197	2.00	1.00	1.33	2.00

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	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
	Saturnin-v2	256	27	256	54	256	27	2.00	1.00	1.33	2.00
19	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	
20	SpoC-v1	64	109	64	111			1.02	1.00	1.01	
21	Spook-v2-v2	256	48	256	48			1.00	1.00	1.00	
22	Subterranean-v2	8	0.25	8	0.25	8	2	1.00	1.00	1.00	0.13
23a	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	
23b	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	
24	WAGE-v1	64	114	64	114			1.00	1.00	1.00	
25a	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
25b	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
25c	Xoodyak_GMU2-v1	352	13	192	13	128	13	1.83	1.00	1.42	0.67
	Xoodyak_GMU2-v2	352	12	192	7	128	7	1.07	1.00	1.04	0.67
S1	AESGCM-v1	128	9	128	11			1.22	1.00	1.10	
	AESGCM-v2	128	33	128	33			1.00	1.00	1.00	
S2	SHA2-v1					512	65				
S3	SHA3-v1					1088	233				

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, ForkAE (only for v1), ESTATE, LOCUS & LOTUS, Saturnin, Oribatida, Romulus, and Xoodyak.

The ratio of the hashing throughput to the plaintext processing throughput is 2.00 for Saturnin, 1.00 for ACE, DryGASCON, and Gimli, and the smallest for KNOT and Subterranean 2.0.

4.1 Implementations of current standards

For comparison with the current standards, we are including in our report results for the current NIST standard in the area of authenticated encryption with associated data,

AES-GCM, and implementations of two current hash function standards, SHA-256 (representing the SHA-2 family) and SHA3-256 (representing the SHA-3 family). All of these implementations were developed by Ekawat Homsirikamol in the period 2011-2016, when he was a Ph.D. student at George Mason University. Their features are summarized at the end of Tables 2 and Tables 3.

None of these implementations is fully compliant with the LWC Hardware API. However, both variants of AES-GCM are compliant with the very similar CAESAR Hardware API [28]. Additionally, implementations of hash functions follow a similar interface and communication protocol, limited to the PDI and DO ports and to the hashing functionality.

The basic iterative architecture of AES-GCM, AESGCM-v1, does not meet the area threshold selected for LWC candidates. The second variant, AESGCM-v2, contains the Galois Field multiplier folded by a factor of 32. As a result, for Artix-7 FPGAs, the area of this implementation is 2520 LUTs, which is similar to the area of multiple hardware submissions to the LWC FPGA benchmarking study and only 26% higher than the original threshold of 2000 LUTs. As a result, this implementation was judged sufficient for the preliminary comparison.

The basic iterative architecture of SHA-256 (from the SHA-2 family) uses only about 1050 LUTs. The basic iterative architecture of SHA3-256 (from the SHA-3 family) is by far larger. Therefore, in our study, SHA-3 is represented by an architecture folded by a factor of 8. Its area is only about 1250 LUTs. In its current form, this architecture does not support padding. However, adding padding is not likely to affect significantly either throughput or area of this design.

Multiple LWC candidates support resource sharing between authenticated encryption and hashing. For the current standards, this sharing is limited to preprocessing and postprocessing only. As a result, a fair comparison is somewhat challenging, especially for hashing. All implementations of LWC candidates supporting hashing, combine both functionalities in a single unit. Thus, in terms of area, it might be fairer to compare them to the joint implementation of AES-GCM and a hash function standard (SHA-2 or SHA-3). Additionally, in terms of speed, preserving the same maximum clock frequency after combining two units may be challenging to achieve. Either two different clock domains would have to be used, or the circuit would have the maximum clock frequency equal to the minimum of the frequencies of component units (AEAD and Hash).

Additionally, better compact implementations of AES-GCM, SHA-2, and SHA-3 may already exist or be developed in the future. As a result, all comparisons with the current standards presented in Section 5 should be treated as preliminary.

4.2 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 compatibility with other API-compliant implementations of Subterranean 2.0, 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

All variants of all hardware design packages passed all GMU known-answer tests (KATs) and produced reliable timing measurements.

5.1 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 1.91. 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, COMET_VT-v1, mixFeed-v1, Pyjamask-v2, and COMET_VT-v2. The average ratios of the numbers of FFs and clock frequencies, in Cyclone 10 LP vs. Artix-7, are 1.82 and 1.65, 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 1.75 for LUTs, 1.10 for FFs, and 2.58 for frequencies. However, the actual ratios vary in a relatively wide range. For example, the ratio of LUTs varies between 0.69 for Subterranean-v2 and 2.65 for ISAP-v2. In particular, the following designs have significantly larger areas in LUTs for ECP5 as compared to Artix-7: ISAP-v2, mixFeed, TinyJAMBU_GMU-v3, Xoodyak_XT-v7, Ascon_Graz-v2, and Romulus-v5.

5.2 Throughputs for Long Inputs

5.2.1 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 the symbol to the 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 2520 LUTs (the area of the smallest implementation of AES-GCM available to us), the fastest variant meeting this criterion is selected. If a candidate does not have a variant with the area below 2520 LUTs, a variant with the smallest area is selected.

The threshold of 2520 LUTs (26% 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 2520 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 remains still incomplete for the majority of candidates.

The winner for the PT only is Subterranean 2.0. Its implementation reaches the throughput of 6 Gbit/s and is the second smallest in terms of the number of LUTs. The second fastest is Xoodyak, with a throughput of about 4.5 Gbit/s. The next group includes three algorithms, KNOT, Gimli, and Ascon, with the throughputs between 2.3 and 3.2 Gbits/s. Out of these three, the implementation of KNOT is the fastest and the implementation of Ascon the smallest. The third group includes three algorithms with throughputs between 1 and 2 Gbits/s: DryGASCON, COMET, and Spook-v2. Their areas are in the range between 2000 and 2500 LUTs. The implementation of DryGASCON is the fastest, and the implementation of Spook-v2 the smallest in this group. The next algorithm in the ranking is TinyJAMBU, which reaches a speed very close to 1 Gbit/s and at the same time has by far the smallest area, around 600 LUTs. The first dozen candidates in terms of throughput, with the area below 2520 LUTs, also include Romulus, Saturnin, and GIFT-COFB. The design of SCHWAEMM is by far the largest, above 3000 LUTs, yet still only average (rank 13) in terms of throughput. More effort is required to demonstrate the competitiveness of this algorithm with the first 12 candidates mentioned above. All remaining algorithms have throughputs below 700 Mbits/s. Out of them, ISAP, Pyjamask, and ForkAE already have areas exceeding 2000 LUTs.

The designs for GIFT-COFB, Spoc, WAGE, and ACE 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 a lower extent, the designs for mixFeed, ESTATE and Oribatida, all slightly below 1500 LUTs, are also too small to be fairly compared with others. As a result, it might be too premature to assign any negative evaluation to these candidates.

For AD only, the following changes in the rankings are the most significant. Subterranean 2.0 and Xoodyak swap their positions. Xoodyak is the fastest, with a speed exceeding 8 Gbit/s. The next group includes KNOT and Gimli, with the throughputs around 4 Gbit/s and 3 Gbits/s, respectively. TinyJAMBU moves from position 9 for processing plaintext only to position 5 for AD only, followed closely by Ascon at position 6. The new algorithms with throughputs in the range between 1 and 2 Gbit/s include Saturnin, Romulus, and Elephant. Among the first dozen algorithms in the ranking, there is only one change, GIFT-COFB is replaced by Elephant. All first 12 algorithms have throughputs for AD greater than 1 Gbit/s.

Only 10 out of 25 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 Xoodyak and Gimli, with throughputs approximately equal to 3.5 and 3 Gbits/s, respectively. Very close behind are Saturnin and DryGASCON, with the throughputs between 1.4 and 1.6 Gbits/s. They are followed by Ascon at about 1 Gbit/s and Subterranean at around 750 Mbits/s. SCHWAEMM (ESCH) reaches slightly less than 500 Mbit/s. The three remaining algorithms, KNOT, PHOTON-Beetle, and ACE have throughputs below 450 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 an area exceeding the threshold, its rank is marked with *, and the area is given in bold font.

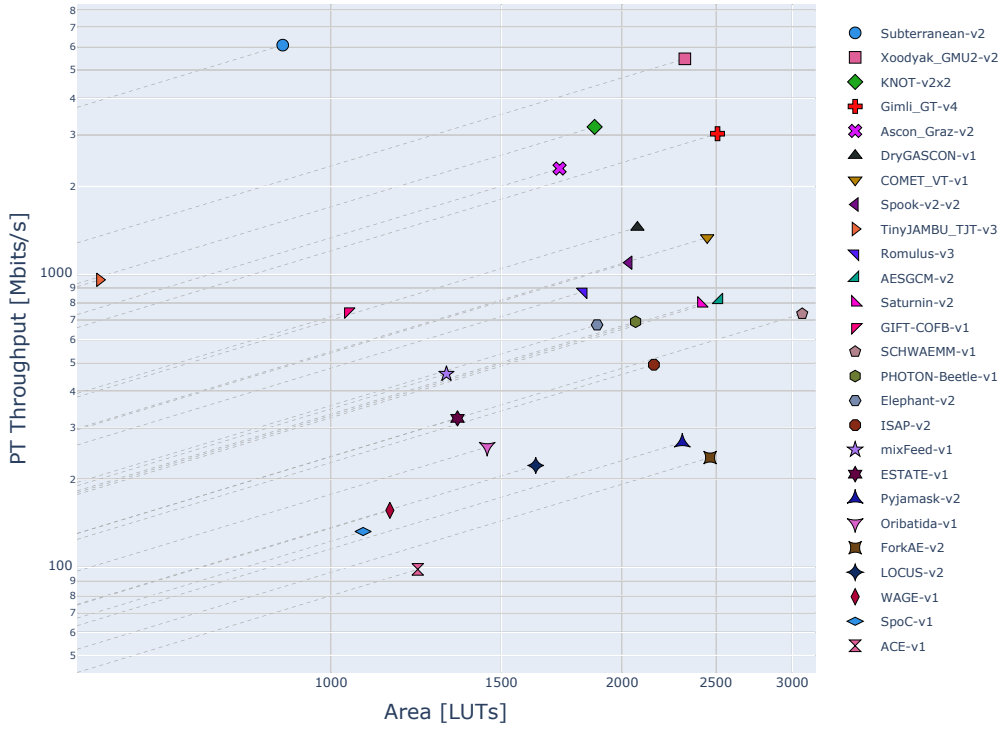

Figure 2: Artix-7 Encryption PT Throughput for Long Messages vs LUTs

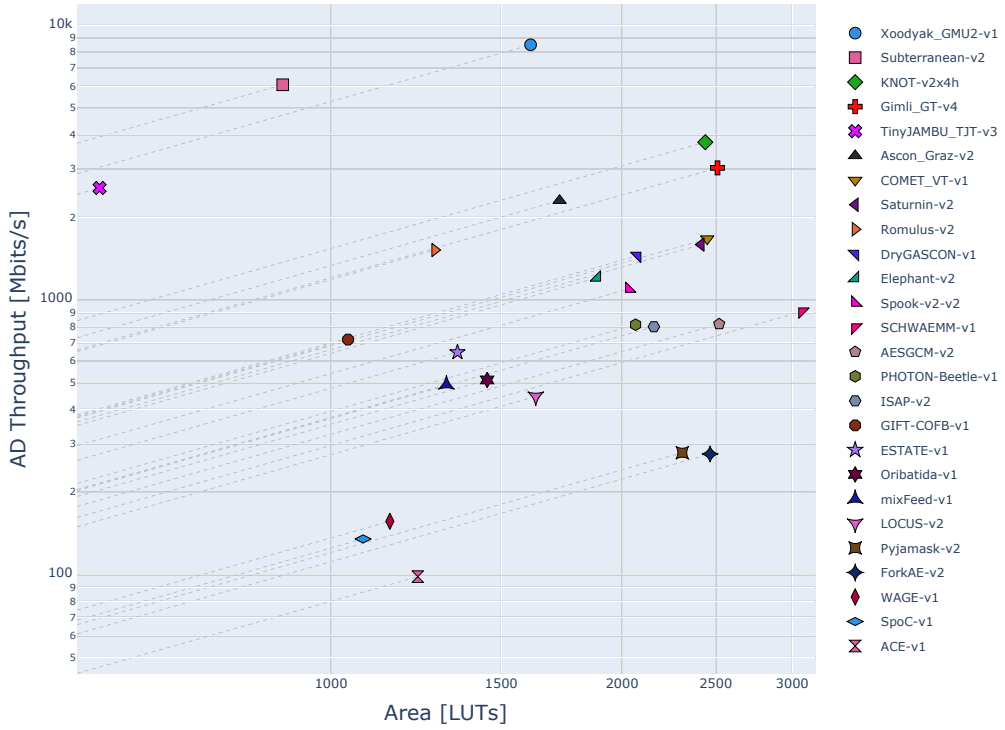

Figure 3: Artix-7 Encryption AD Throughput for Long Messages vs LUTs

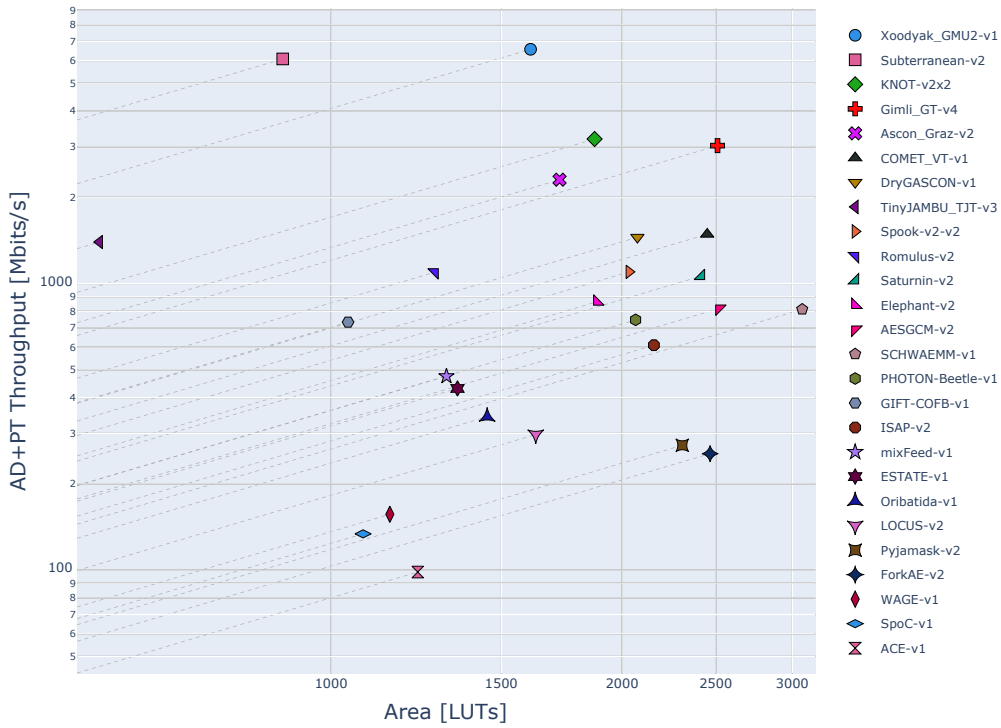

Figure 4: Artix-7 Encryption AD+PT Throughput for Long Messages vs LUTs

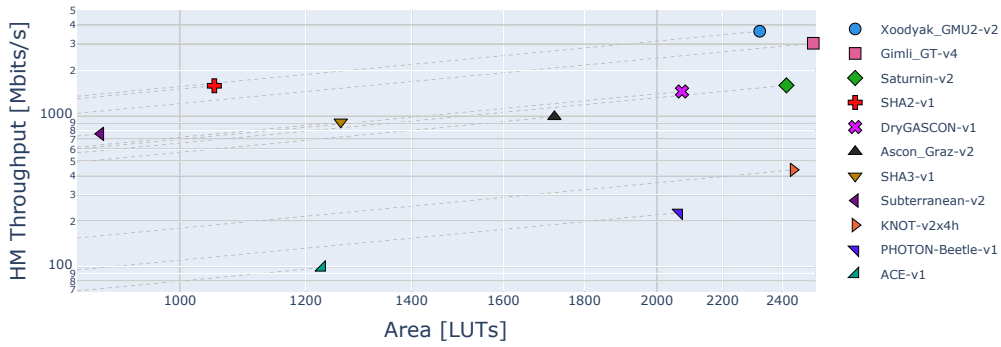

Figure 5: Artix-7 Hashing Throughput for Long Messages vs LUTs

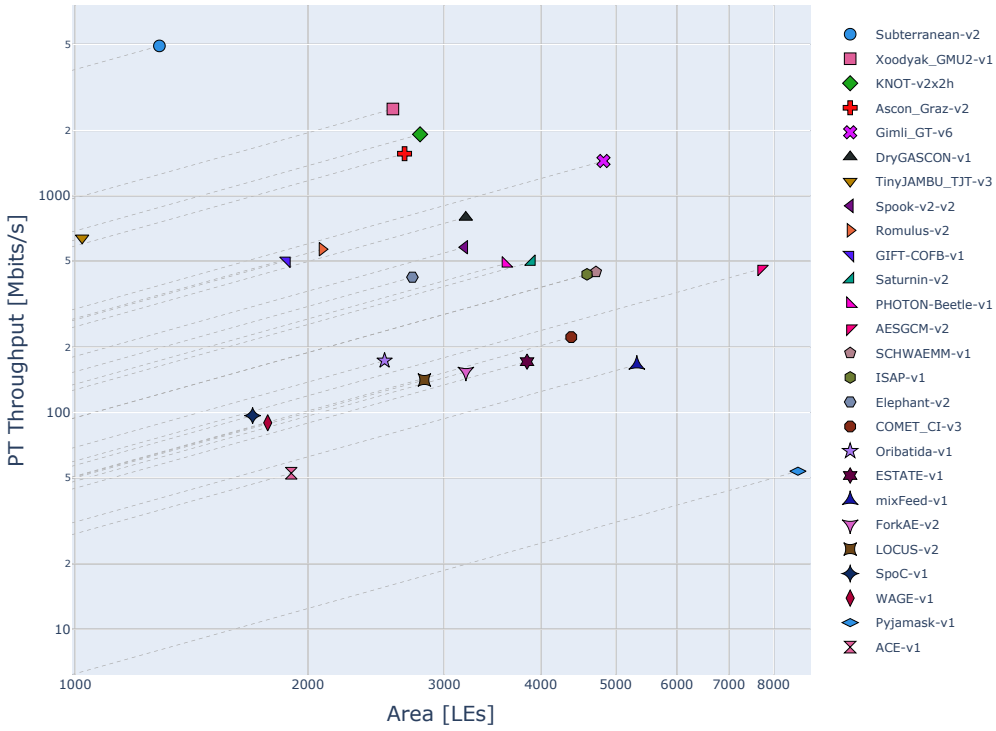

Figure 6: Cyclone-10-LP Encryption PT Throughput for Long Messages vs LEs

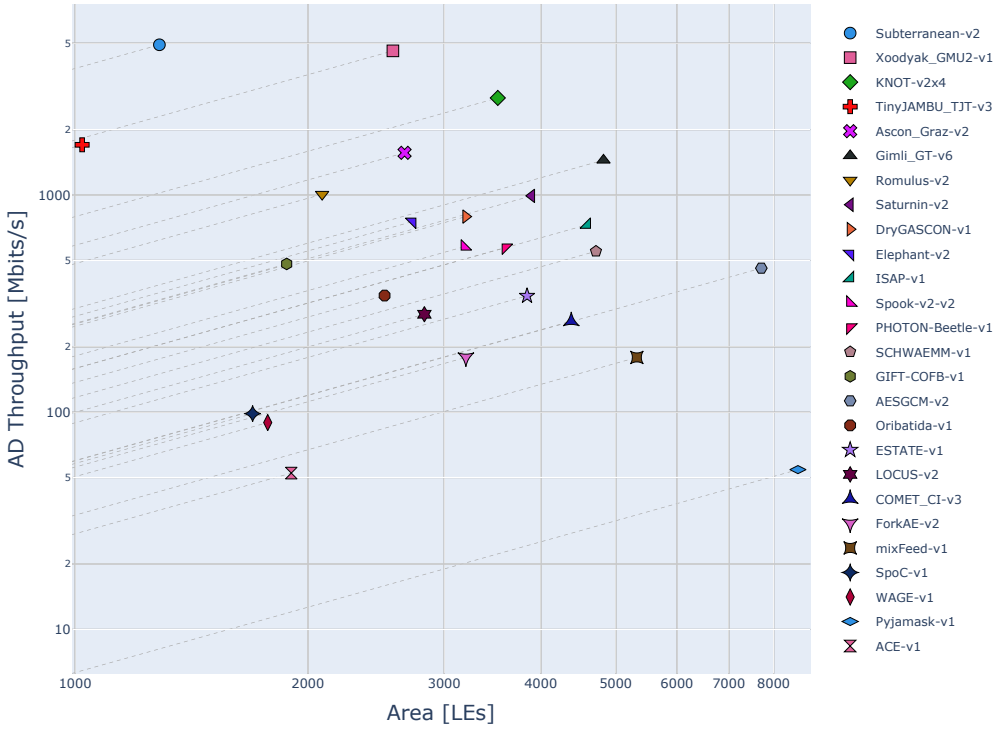

Figure 7: Cyclone-10-LP Encryption AD Throughput for Long Messages vs LEs

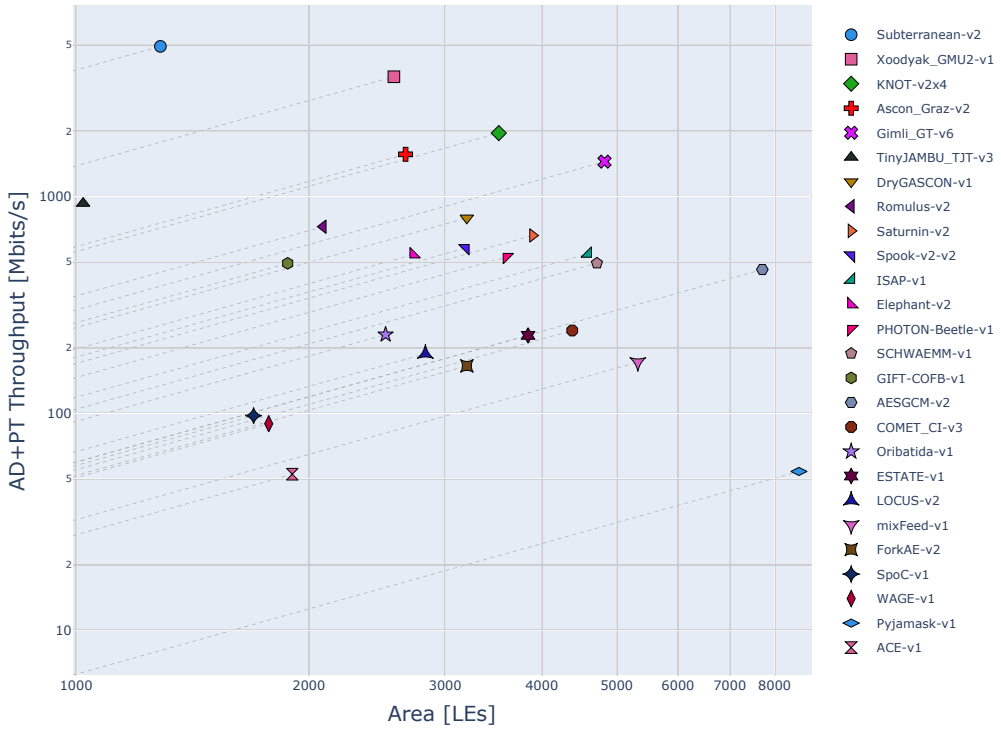

Figure 8: Cyclone-10-LP Encryption AD+PT Throughput for Long Messages vs LEs

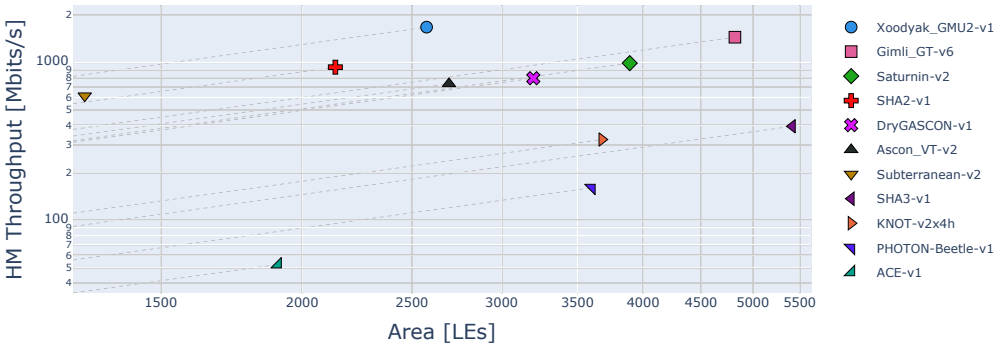

Figure 9: Cyclone-10-LP Hashing Throughput for Long Messages vs LEs

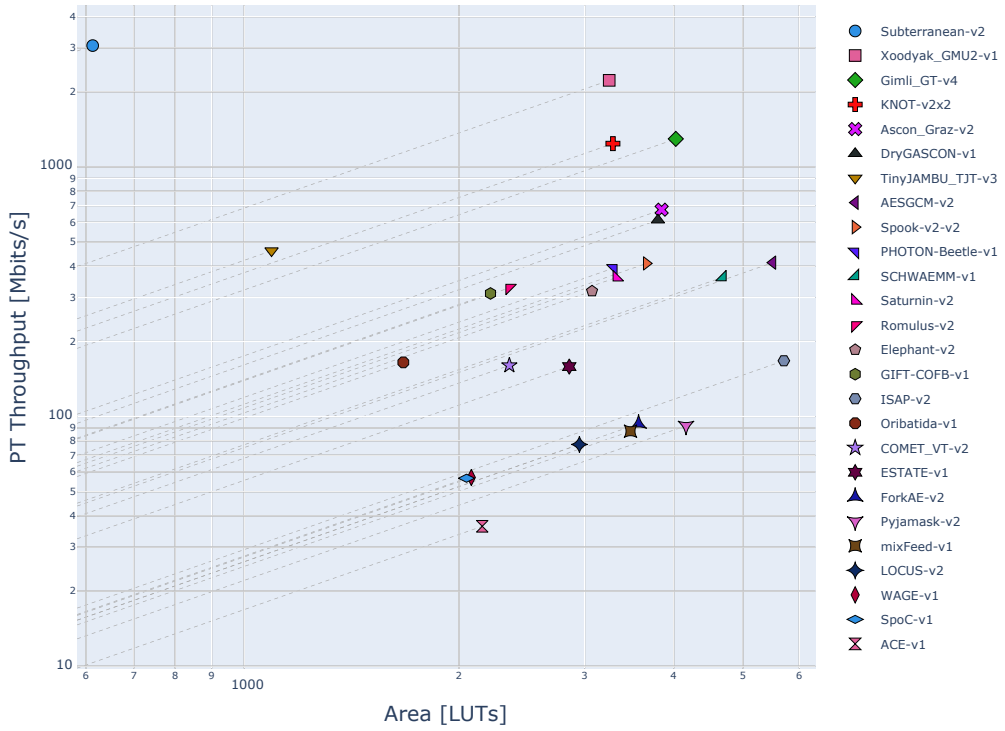

Figure 10: ECP5 Encryption PT Throughput for Long Messages vs LUTs

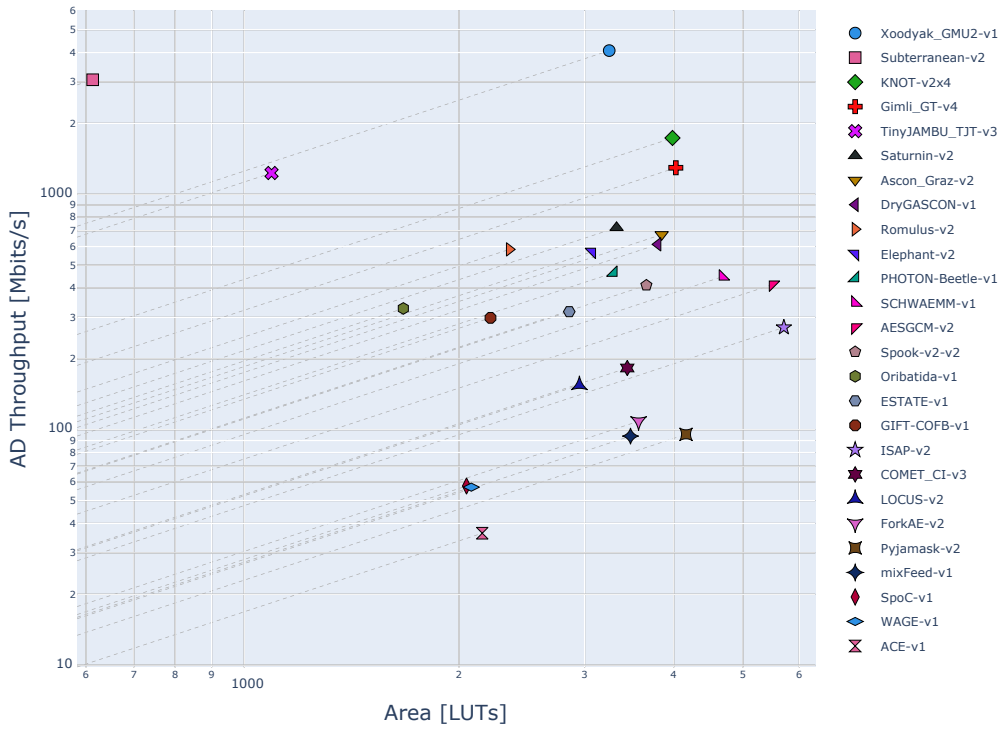

Figure 11: ECP5 Encryption AD Throughput for Long Messages vs LUTs

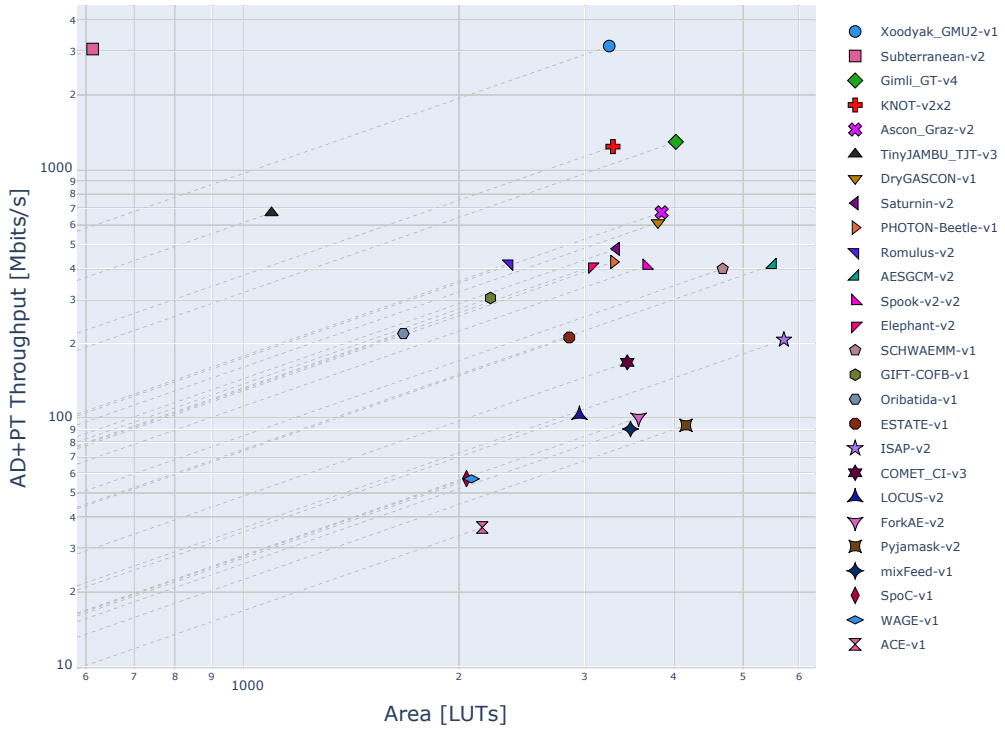

Figure 12: ECP5 Encryption AD+PT Throughput for Long Messages vs LUTs

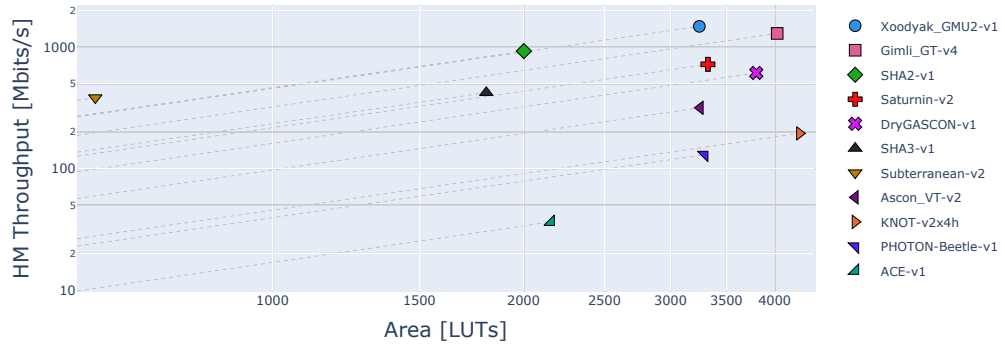

Figure 13: ECP5 Hashing Throughput for Long Messages vs LUTs

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-v2	6,080.0	1	891	190	0.25
Xoodyak_GMU2-v2	5,458.3	2	2,322	199	7
Xoodyak_GMU2-v1	4,637.5		1,608	314	13
KNOT-v2x2	3,195.4	3	1,873	233	14
KNOT-v2x2h	3,044.6		2,112	222	14
Gimli_GT-v4	3,029.3	4	2,510	142	6
Xoodyak_XT-v8	2,393.6		2,040	187	15
Xoodyak_XT-v2	2,342.4		2,071	183	15
Ascon_Graz-v2	2,304.0	5	1,723	216	12
Gimli_GT-v2	1,866.7		1,909	175	12
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
COMET_VT-v1	1,337.6	7	2,449	209	20
Spook-v2-v2	1,098.7	8	2,033	206	48
TinyJAMBU_TJT-v3	960.0	9	576	240	8
Romulus-v3	874.7	10	1,824	123	18
Romulus-v2	856.0		1,280	214	32
AESGCM-v2	818.4	11	2,520	211	33
Saturnin-v2	796.4	12	2,414	168	54
GIFT-COFB-v1	748.9	13	1,041	275	47
SCHWAEMM-v1	735.3	14*	**3,071**	135	47
PHOTON-Beetle-v1	690.4	15	2,065	178	33
Elephant-v2	673.5	16	1,884	181	43
ISAP-v2	492.3	17	2,157	200	26
mixFeed-v1	458.1	18	1,316	204	57
COMET_CI-v3	417.0		1,841	215	66
COMET_CI-v1	407.8		1,884	223	70
COMET_VT-v2	336.5		1,703	234	89
ESTATE-v1	322.9	19	1,351	222	88
TinyJAMBU_TJT-v2	305.5		461	315	33
Pyjamask-v2	267.3	20	2,308	213	102
Oribatida-v1	257.9	21	1,450	276	137
Oribatida-v2	252.3		1,450	276	105
TinyJAMBU_GMU-v1	250.4		591	266	34
ForkAE-v2	237.3	22	2,466	228	123
LOCUS-v2	222.9	23	1,628	209	60
Elephant-v1	214.3		1,291	229	171
WAGE-v1	156.6	24	1,150	279	114
LOTUS-v2	150.4		1,487	141	60
SpoC-v1	132.6	25	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
Pyjamask-v1	111.9		1,979	229	262
ACE-v1	98.5	26	1,229	200	130
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
ForkAE-v1	8.3		1,191	208	3,194

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**
Xoodyak_GMU2-v1	8,502.2	1	1,608	314	13
Subterranean-v2	6,080.0	2	891	190	0.25
Xoodyak_GMU2-v2	5,837.3		2,322	199	12
KNOT-v2x4h	3,757.7	3	2,438	137	7
Xoodyak_XT-v8	3,291.2		2,040	187	20
Xoodyak_XT-v2	3,220.8		2,071	183	20
KNOT-v2x2	3,195.4		1,873	233	14
Gimli_GT-v4	3,029.3	4	2,510	142	6
TinyJAMBU_TJT-v3	2,560.0	5	576	240	3
Xoodyak_GMU-v1	2,493.3		1,808	170	24
Ascon_Graz-v2	2,304.0	6	1,723	216	12
Gimli_GT-v2	1,866.7		1,909	175	12
COMET_VT-v1	1,672.0	7	2,449	209	16
Ascon_Graz-v1	1,672.0		1,551	209	8
Saturnin-v2	1,592.9	8	2,414	168	27
Romulus-v2	1,521.8	9	1,280	214	18
Ascon_VT-v1	1,491.2		1,913	233	10
DryGASCON-v1	1,450.7	10	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	11	1,884	181	24
Spook-v2-v2	1,098.7	12	2,033	206	48
SCHWAEMM-v1	909.5	13*	**3,071**	135	38
AESGCM-v2	818.4	14	2,520	211	33
PHOTON-Beetle-v1	813.7	15	2,065	178	28
ISAP-v2	800.0	16	2,157	200	16
TinyJAMBU_TJT-v2	775.4		461	315	13
GIFT-COFB-v1	718.4	17	1,041	275	49
ESTATE-v1	645.8	18	1,351	222	44
TinyJAMBU_GMU-v1	608.0		591	266	14
Oribatida-v1	512.0	19	1,450	276	69
Oribatida-v2	499.9		1,450	276	53
mixFeed-v1	492.7	20	1,316	204	53
COMET_CI-v3	491.4		1,841	215	56
COMET_CI-v1	475.7		1,884	223	60
LOCUS-v2	445.9	21	1,628	209	30
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
LOTUS-v2	300.8		1,487	141	30
Pyjamask-v2	278.2	22	2,308	213	98
ForkAE-v2	275.3	23	2,466	228	106
Saturnin-v1	249.5		2,020	192	197
Xoodyak_GMU-v2	222.3		1,234	168	266
ESTATE-v3	162.5		1,130	259	204
WAGE-v1	156.6	24	1,150	279	114
SpoC-v1	135.0	25	1,079	230	109
Pyjamask-v1	113.6		1,979	229	258
ACE-v1	98.5	26	1,229	200	130
Gimli_TUM-v1	39.2		933	241	786
ForkAE-v1	22.0		1,191	208	1,209
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**
Xoodyak_GMU2-v1	6,569.8	1	1,608	314	26
Subterranean-v2	6,080.0	2	891	190	0.5
Xoodyak_GMU2-v2	5,697.7		2,322	199	19
KNOT-v2x2	3,195.4	3	1,873	233	28
KNOT-v2x2h	3,044.6		2,112	222	28
Gimli_GT-v4	3,029.3	4	2,510	142	12
Xoodyak_XT-v8	2,906.5		2,040	187	35
Xoodyak_XT-v2	2,844.3		2,071	183	35
Ascon_Graz-v2	2,304.0	5	1,723	216	24
Xoodyak_GMU-v1	2,150.7		1,808	170	43
Gimli_GT-v2	1,866.7		1,909	175	24
Ascon_Graz-v1	1,672.0		1,551	209	16
Ascon_VT-v1	1,491.2		1,913	233	20
COMET_VT-v1	1,486.2	6	2,449	209	36
Ascon_VT-v2	1,475.4		1,928	219	19
DryGASCON-v1	1,450.7	7	2,074	238	42
TinyJAMBU_TJT-v3	1,396.4	8	576	240	11
Spook-v2-v2	1,098.7	9	2,033	206	96
Romulus-v2	1,095.7	10	1,280	214	50
Romulus-v3	1,085.8		1,824	123	29
Saturnin-v2	1,061.9	11	2,414	168	81
Elephant-v2	864.5	12	1,884	181	67
AESGCM-v2	818.4	13	2,520	211	66
SCHWAEMM-v1	813.2	14*	**3,071**	135	85
PHOTON-Beetle-v1	747.0	15	2,065	178	61
GIFT-COFB-v1	733.3	16	1,041	275	96
ISAP-v2	609.5	17	2,157	200	42
mixFeed-v1	474.8	18	1,316	204	110
COMET_CI-v3	451.1		1,841	215	122
COMET_CI-v1	439.1		1,884	223	130
TinyJAMBU_TJT-v2	438.3		461	315	46
ESTATE-v1	430.5	19	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	20	1,450	276	206
Oribatida-v2	335.4		1,450	276	158
LOCUS-v2	297.2	21	1,628	209	90
Elephant-v1	282.9		1,291	229	259
Pyjamask-v2	272.6	22	2,308	213	200
ForkAE-v2	254.9	23	2,466	228	229
LOTUS-v2	200.5		1,487	141	90
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
WAGE-v1	156.6	24	1,150	279	228
SpoC-v1	133.8	25	1,079	230	220
Pyjamask-v1	112.7		1,979	229	520
ESTATE-v3	108.3		1,130	259	612
ACE-v1	98.5	26	1,229	200	260
Gimli_TUM-v1	39.2		933	241	1,575
Gimli_TUM-v2	21.1		905	244	2,955
ForkAE-v1	12.1		1,191	208	4,403

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**
Xoodyak_GMU2-v2	3,638.9	1	2,322	199	7
Xoodyak_GMU2-v1	3,091.7		1,608	314	13
Gimli_GT-v4	3,029.3	2	2,510	142	6
Gimli_GT-v2	1,866.7		1,909	175	12
Xoodyak_XT-v8	1,841.2		2,040	187	13
Saturnin-v2	1,592.9	3	2,414	168	27
SHA2-v1	1,583.3	4	1,051	201	65
Xoodyak_XT-v7	1,536.0		1,405	228	19
DryGASCON-v1	1,450.7	5	2,074	238	21
Ascon_Graz-v2	987.4	6	1,723	216	14
Ascon_VT-v2	934.4		1,928	219	15
SHA3-v1	910.6	7	1,263	195	233
Subterranean-v2	760.0	8	891	190	2
Xoodyak_GMU-v1	640.0		1,808	170	34
KNOT-v2x4h	438.4	9	2,438	137	40
KNOT-v2x2h	355.2		2,112	222	80
Saturnin-v1	249.5		2,020	192	197
PHOTON-Beetle-v1	227.8	10	2,065	178	25
ACE-v1	98.5	11	1,229	200	130
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-v2	4,917.8	1	1,285	153.7	0.25
Xoodyak_GMU2-v1	2,515.2	2	2,575	170.3	13
KNOT-v2x2h	1,921.8	3	2,792	140.1	14
KNOT-v2x2	1,902.4		2,472	138.7	14
Ascon_Graz-v2	1,564.3	4	2,666	146.7	12
Gimli_GT-v6	1,447.4	5	4,820	45.2	4
Gimli_GT-v3	1,372.2		3,651	85.8	8
Xoodyak_XT-v1	1,285.0		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
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-v2	578.8	8	3,188	108.5	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
AESGCM-v2	460.5	13*	**7,711**	118.7	33
SCHWAEMM-v1	445.3	14	4,713	81.8	47
ISAP-v1	434.1	15	4,589	126.6	42
Elephant-v2	421.0	16	2,729	113.2	43
ISAP-v2	335.7		3,852	136.4	26
COMET_CI-v3	222.7	17	4,379	114.8	66
COMET_CI-v1	211.7		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	18	2,512	185.7	137
ESTATE-v1	171.6	19	3,839	118.0	88
mixFeed-v1	166.2	20*	**5,323**	74.0	57
Oribatida-v2	159.5		2,221	174.5	105
ForkAE-v2	154.1	21	3,200	148.1	123
Elephant-v1	152.6		2,056	163.1	171
LOCUS-v2	141.2	22	2,828	132.4	60
LOTUS-v2	106.3		2,445	99.6	60
SpoC-v1	96.7	23	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	24	1,774	159.6	114
ESTATE-v3	56.5		2,279	180.2	408
Pyjamask-v1	53.6	25*	**8,599**	109.7	262
ACE-v1	52.4	26	1,903	106.5	130
ForkAE-v1	5.4		2,129	135.7	3,194

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-v2	4,917.8	1	1,285	153.7	0.25
Xoodyak_GMU2-v1	4,611.2	2	2,575	170.3	13
KNOT-v2x4	2,799.1	3	3,519	102.0	7
KNOT-v2x4h	2,785.1		3,678	101.5	7
Xoodyak_XT-v1	1,902.8		2,282	140.6	26
Xoodyak_XT-v7	1,811.9		2,253	133.8	26
TinyJAMBU_TJT-v3	1,703.4	4	1,021	159.7	3
Xoodyak_GMU-v1	1,566.3		3,135	106.8	24
Ascon_Graz-v2	1,564.3	5	2,666	146.7	12
Gimli_GT-v6	1,447.4	6	4,820	45.2	4
Gimli_GT-v3	1,372.2		3,651	85.8	8
Ascon_Graz-v1	1,222.3		2,484	152.8	8
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-v2	578.8	12	3,188	108.5	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
AESGCM-v2	460.5	16*	**7,711**	118.7	33
TinyJAMBU_GMU-v1	449.9		856	196.8	14
Oribatida-v1	344.4	17	2,512	185.7	69
ESTATE-v1	343.2	18	3,839	118.0	44
Oribatida-v2	316.1		2,221	174.5	53
Elephant-v1	296.5		2,056	163.1	88
LOCUS-v2	282.5	19	2,828	132.4	30
COMET_CI-v3	262.5	20	4,379	114.8	56
COMET_CI-v1	246.9		4,663	115.8	60
TinyJAMBU_GMU-v2	241.4		841	196.2	26
LOTUS-v2	212.6		2,445	99.6	30
Saturnin-v1	188.4		3,802	145.0	197
ForkAE-v2	178.8	21	3,200	148.1	106
mixFeed-v1	178.7	22*	**5,323**	74.0	53
ESTATE-v3	113.1		2,279	180.2	204
SpoC-v1	98.5	23	1,696	167.7	109
WAGE-v1	89.6	24	1,774	159.6	114
Pyjamask-v1	54.4	25*	**8,599**	109.7	258
ACE-v1	52.4	26	1,903	106.5	130
ForkAE-v1	14.4		2,129	135.7	1,209

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-v2	4,917.8	1	1,285	153.7	0.5
Xoodyak_GMU2-v1	3,563.2	2	2,575	170.3	26
KNOT-v2x4	1,959.4	3	3,519	102.0	20
KNOT-v2x4h	1,949.6		3,678	101.5	20
Xoodyak_XT-v1	1,626.8		2,282	140.6	47
Ascon_Graz-v2	1,564.3	4	2,666	146.7	24
Xoodyak_XT-v7	1,549.0		2,253	133.8	47
Gimli_GT-v6	1,447.4	5	4,820	45.2	8
Gimli_GT-v3	1,372.2		3,651	85.8	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
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-v2	578.8	10	3,188	108.5	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
AESGCM-v2	460.5	16*	**7,711**	118.7	66
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
COMET_CI-v3	241.0	17	4,379	114.8	122
Oribatida-v1	230.7	18	2,512	185.7	206
ESTATE-v1	228.8	19	3,839	118.0	132
COMET_CI-v1	227.9		4,663	115.8	130
Oribatida-v2	212.0		2,221	174.5	158
Elephant-v1	201.5		2,056	163.1	259
LOCUS-v2	188.3	20	2,828	132.4	90
mixFeed-v1	172.2	21*	**5,323**	74.0	110
ForkAE-v2	165.5	22	3,200	148.1	229
LOTUS-v2	141.7		2,445	99.6	90
TinyJAMBU_GMU-v2	136.5		841	196.2	92
Saturnin-v1	125.6		3,802	145.0	591
SpoC-v1	97.6	23	1,696	167.7	220
WAGE-v1	89.6	24	1,774	159.6	228
ESTATE-v3	75.4		2,279	180.2	612
Pyjamask-v1	54.0	25*	**8,599**	109.7	520
ACE-v1	52.4	26	1,903	106.5	260
ForkAE-v1	7.9		2,129	135.7	4,403

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
Xoodyak_GMU2-v1	1,676.8	1	2,575	170.3	13
Gimli_GT-v6	1,447.4	2	4,820	45.2	4
Gimli_GT-v3	1,372.2		3,651	85.8	8
Saturnin-v2	991.4	3	3,892	104.6	27
SHA2-v1	934.4	4	2,139	118.6	65
Xoodyak_XT-v7	901.6		2,253	133.8	19
Xoodyak_XT-v8	899.4		4,337	91.3	13
DryGASCON-v1	795.6	5	3,199	130.5	21
Ascon_VT-v2	733.9	6	2,695	172.0	15
Ascon_Graz-v2	670.4		2,666	146.7	14
Subterranean-v2	614.7	7	1,285	153.7	2
Xoodyak_GMU-v1	402.0		3,135	106.8	34
SHA3-v1	394.3	8*	**5,417**	84.5	233
KNOT-v2x4h	324.9	9	3,678	101.5	40
KNOT-v2x2h	224.2		2,792	140.1	80
Saturnin-v1	188.4		3,802	145.0	197
PHOTON-Beetle-v1	160.6	10	3,602	125.4	25
ACE-v1	52.4	11	1,903	106.5	130

5.2.2 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 and mixFeed are the only candidates with no variant fitting within 5000 LEs. In the case of Artix-7 FPGAs, the only candidate exceeding the corresponding area threshold was SCHWAEMM.

For PT only, Subterranean is about two times faster than the second candidate in the ranking, Xoodyak. KNOT, Ascon, and Gimli are the only algorithms with speeds between 1 and 2 Gbit/s. Out of them, Gimli has by far the largest area, approaching 5000 LEs. For AD only, the speed of Xoodyak is only about 20% lower than the speed of Subterranean 2.0. KNOT is the distinct third. TinyJAMBU, Ascon, and Gimli have comparable throughputs, but very different areas. Out of them, TinyJAMBU is by far the smallest, and Gimli the largest. Romulus and Saturnin are very close behind, with throughputs approaching 1 Gbit/s.

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. ISAP is the only algorithm without design within 5000 LUTs. Other than that, the conclusions from these tables and graphs are relatively close to the conclusions based on the results for the Artix-7 FPGA.

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-v2	3,063.4	1	613	95.7	0.25
Xoodyak_GMU2-v1	2,222.5	2	3,248	150.5	13
Xoodyak_GMU2-v2	1,888.7		4,077	68.9	7
Gimli_GT-v4	1,295.6	3	4,027	60.7	6
KNOT-v2x2	1,239.9	4	3,287	90.4	14
KNOT-v2x2h	1,032.7		3,373	75.3	14
Xoodyak_XT-v2	905.0		4,302	70.7	15
Gimli_GT-v3	890.4		4,451	55.6	8
Xoodyak_XT-v8	845.2		3,507	66.0	15
Xoodyak_GMU-v1	747.8		3,172	74.0	19
Ascon_Graz-v2	674.2	5	3,847	63.2	12
DryGASCON-v1	612.8	6	3,801	100.5	21
Ascon_VT-v1	543.4		3,130	84.9	10
Ascon_VT-v2	527.6		3,256	74.2	9
Ascon_Graz-v1	505.4		2,947	63.2	8
TinyJAMBU_TJT-v3	461.6	7	1,092	115.4	8
AESGCM-v2	413.8	8*	**5,507**	106.7	33
Spook-v2-v2	410.7	9	3,662	77.0	48
PHOTON-Beetle-v1	393.5	10	3,294	101.4	33
SCHWAEMM-v1	361.3	11	4,685	66.3	47
Saturnin-v2	360.8	12	3,326	76.1	54
Romulus-v2	328.0	13	2,353	82.0	32
Romulus-v3	320.0		3,847	45.0	18
Elephant-v2	318.1	14	3,073	85.5	43
GIFT-COFB-v1	311.3	15	2,214	114.3	47
ISAP-v2	167.3	16*	**5,708**	68.0	26
Oribatida-v1	164.9	17	1,671	176.5	137
COMET_VT-v2	160.3	18	2,353	111.5	89
ESTATE-v1	158.6	19	2,855	109.0	88
COMET_CI-v3	155.2		3,443	80.0	66
COMET_CI-v1	147.9		3,255	80.9	70
TinyJAMBU_TJT-v2	121.6		689	125.4	33
TinyJAMBU_GMU-v1	117.5		720	124.8	34
Oribatida-v2	104.4		2,497	114.2	105
ForkAE-v2	93.6	20	3,571	90.0	123
Pyjamask-v2	91.9	21	4,162	73.2	102
Elephant-v1	91.2		2,368	97.5	171
mixFeed-v1	87.4	22	3,479	38.9	57
LOCUS-v2	77.3	23	2,950	72.5	60
TinyJAMBU_GMU-v2	62.2		908	128.3	66
Saturnin-v1	61.1		3,093	94.0	394
WAGE-v1	57.0	24	2,081	101.6	114
SpoC-v1	56.6	25	2,049	98.2	111
LOTUS-v2	56.2		2,208	52.7	60
Xoodyak_GMU-v2	55.0		2,316	74.8	261
Pyjamask-v1	45.3		3,897	92.7	262
ACE-v1	36.3	26	2,156	73.8	130
ESTATE-v3	33.6		1,820	107.1	408
ForkAE-v1	2.7		2,022	67.9	3,194

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**
Xoodyak_GMU2-v1	4,074.5	1	3,248	150.5	13
Subterranean-v2	3,063.4	2	613	95.7	0.25
Xoodyak_GMU2-v2	2,019.9		4,077	68.9	12
KNOT-v2x4	1,733.8	3	3,984	63.2	7
KNOT-v2x4h	1,669.6		4,283	60.9	7
Gimli_GT-v4	1,295.6	4	4,027	60.7	6
Xoodyak_XT-v2	1,244.3		4,302	70.7	20
TinyJAMBU_TJT-v3	1,230.8	5	1,092	115.4	3
Xoodyak_XT-v8	1,162.1		3,507	66.0	20
Xoodyak_GMU-v1	1,085.3		3,172	74.0	24
Gimli_GT-v3	890.4		4,451	55.6	8
Saturnin-v2	721.5	6	3,326	76.1	27
Ascon_Graz-v2	674.2	7	3,847	63.2	12
DryGASCON-v1	612.8	8	3,801	100.5	21
Romulus-v2	583.1	9	2,353	82.0	18
Elephant-v2	570.0	10	3,073	85.5	24
Ascon_VT-v1	543.4		3,130	84.9	10
Romulus-v3	523.6		3,847	45.0	11
Ascon_Graz-v1	505.4		2,947	63.2	8
Ascon_VT-v2	474.9		3,256	74.2	10
PHOTON-Beetle-v1	463.7	11	3,294	101.4	28
SCHWAEMM-v1	446.9	12	4,685	66.3	38
AESGCM-v2	413.8	13*	**5,507**	106.7	33
Spook-v2-v2	410.7	14	3,662	77.0	48
Oribatida-v1	327.3	15	1,671	176.5	69
ESTATE-v1	317.1	16	2,855	109.0	44
TinyJAMBU_TJT-v2	308.7		689	125.4	13
GIFT-COFB-v1	298.6	17	2,214	114.3	49
TinyJAMBU_GMU-v1	285.3		720	124.8	14
ISAP-v2	271.9	18*	**5,708**	68.0	16
Oribatida-v2	206.9		2,497	114.2	53
COMET_CI-v3	182.9	19	3,443	80.0	56
Elephant-v1	177.3		2,368	97.5	88
COMET_CI-v1	172.6		3,255	80.9	60
COMET_VT-v2	167.8		2,353	111.5	85
TinyJAMBU_GMU-v2	157.9		908	128.3	26
LOCUS-v2	154.7	20	2,950	72.5	30
Saturnin-v1	122.2		3,093	94.0	197
LOTUS-v2	112.4		2,208	52.7	30
ForkAE-v2	108.7	21	3,571	90.0	106
Xoodyak_GMU-v2	99.0		2,316	74.8	266
Pyjamask-v2	95.6	22	4,162	73.2	98
mixFeed-v1	93.9	23	3,479	38.9	53
ESTATE-v3	67.2		1,820	107.1	204
SpoC-v1	57.7	24	2,049	98.2	109
WAGE-v1	57.0	25	2,081	101.6	114
Pyjamask-v1	46.0		3,897	92.7	258
ACE-v1	36.3	26	2,156	73.8	130
ForkAE-v1	7.2		2,022	67.9	1,209

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
Xoodyak_GMU2-v1	3,148.5	1	3,248	150.5	26
Subterranean-v2	3,063.4	2	613	95.7	0.5
Xoodyak_GMU2-v2	1,971.6		4,077	68.9	19
Gimli_GT-v4	1,295.6	3	4,027	60.7	12
KNOT-v2x2	1,239.9	4	3,287	90.4	28
KNOT-v2x4	1,213.6		3,984	63.2	20
Xoodyak_XT-v2	1,098.9		4,302	70.7	35
Xoodyak_XT-v8	1,026.3		3,507	66.0	35
Xoodyak_GMU-v1	936.2		3,172	74.0	43
Gimli_GT-v3	890.4		4,451	55.6	16
Ascon_Graz-v2	674.2	5	3,847	63.2	24
TinyJAMBU_TJT-v3	671.4	6	1,092	115.4	11
DryGASCON-v1	612.8	7	3,801	100.5	42
Ascon_VT-v1	543.4		3,130	84.9	20
Ascon_Graz-v1	505.4		2,947	63.2	16
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
Romulus-v2	419.8	10	2,353	82.0	50
AESGCM-v2	413.8	11*	**5,507**	106.7	66
Spook-v2-v2	410.7	12	3,662	77.0	96
Elephant-v2	408.4	13	3,073	85.5	67
SCHWAEMM-v1	399.6	14	4,685	66.3	85
Romulus-v3	397.2		3,847	45.0	29
GIFT-COFB-v1	304.8	15	2,214	114.3	96
Oribatida-v1	219.3	16	1,671	176.5	206
ESTATE-v1	211.4	17	2,855	109.0	132
ISAP-v2	207.1	18*	**5,708**	68.0	42
TinyJAMBU_TJT-v2	174.5		689	125.4	46
COMET_CI-v3	167.9	19	3,443	80.0	122
TinyJAMBU_GMU-v1	166.4		720	124.8	48
COMET_VT-v2	164.0		2,353	111.5	174
COMET_CI-v1	159.3		3,255	80.9	130
Oribatida-v2	138.8		2,497	114.2	158
Elephant-v1	120.5		2,368	97.5	259
LOCUS-v2	103.1	20	2,950	72.5	90
ForkAE-v2	100.6	21	3,571	90.0	229
Pyjamask-v2	93.7	22	4,162	73.2	200
mixFeed-v1	90.5	23	3,479	38.9	110
TinyJAMBU_GMU-v2	89.3		908	128.3	92
Saturnin-v1	81.4		3,093	94.0	591
Xoodyak_GMU-v2	77.2		2,316	74.8	527
LOTUS-v2	74.9		2,208	52.7	90
SpoC-v1	57.1	24	2,049	98.2	220
WAGE-v1	57.0	25	2,081	101.6	228
Pyjamask-v1	45.6		3,897	92.7	520
ESTATE-v3	44.8		1,820	107.1	612
ACE-v1	36.3	26	2,156	73.8	260
ForkAE-v1	3.9		2,022	67.9	4,403

Table 15: Lattice ECP5 Hash Throughput for Long Messages

Variant	Throughput HM [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per Block
Xoodyak_GMU2-v1	1,481.6	1	3,248	150.5	13
Gimli_GT-v4	1,295.6	2	4,027	60.7	6
Xoodyak_GMU2-v2	1,259.2		4,077	68.9	7
SHA2-v1	927.4	3	2,001	117.7	65
Gimli_GT-v3	890.4		4,451	55.6	8
Saturnin-v2	721.5	4	3,326	76.1	27
Xoodyak_XT-v8	650.1		3,507	66.0	13
DryGASCON-v1	612.8	5	3,801	100.5	21
Xoodyak_XT-v7	450.4		3,272	66.9	19
SHA3-v1	421.9	6	1,804	90.3	233
Subterranean-v2	382.9	7	613	95.7	2
Ascon_VT-v2	316.6	8	3,256	74.2	15
Ascon_Graz-v2	289.0		3,847	63.2	14
Xoodyak_GMU-v1	278.6		3,172	74.0	34
KNOT-v2x4h	194.8	9	4,283	60.9	40
PHOTON-Beetle-v1	129.8	10	3,294	101.4	25
Saturnin-v1	122.2		3,093	94.0	197
KNOT-v2x2h	120.5		3,373	75.3	80
ACE-v1	36.3	11	2,156	73.8	130
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-v2	Subterranean-v2	Subterranean-v2
2	Xoodyak_GMU2-v2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	KNOT-v2x2	KNOT-v2x2h	Gimli_GT-v4
4	Gimli_GT-v4	Ascon_Graz-v2	KNOT-v2x2
5	Ascon_Graz-v2	Gimli_GT-v6	Ascon_Graz-v2
6	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1
7	COMET_VT-v1	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
8	Spook-v2-v2	Spook-v2-v2	AESGCM-v2
9	TinyJAMBU_TJT-v3	Romulus-v2	Spook-v2-v2
10	Romulus-v3	GIFT-COFB-v1	PHOTON-Beetle-v1
11	AESGCM-v2	Saturnin-v2	SCHWAEMM-v1
12	Saturnin-v2	PHOTON-Beetle-v1	Saturnin-v2
13	GIFT-COFB-v1	AESGCM-v2	Romulus-v2
14	SCHWAEMM-v1	SCHWAEMM-v1	Elephant-v2
15	PHOTON-Beetle-v1	ISAP-v1	GIFT-COFB-v1
16	Elephant-v2	Elephant-v2	ISAP-v2
17	ISAP-v2	COMET_CI-v3	Oribatida-v1
18	mixFeed-v1	Oribatida-v1	COMET_VT-v2
19	ESTATE-v1	ESTATE-v1	ESTATE-v1
20	Pyjamask-v2	mixFeed-v1	ForkAE-v2
21	Oribatida-v1	ForkAE-v2	Pyjamask-v2
22	ForkAE-v2	LOCUS-v2	mixFeed-v1
23	LOCUS-v2	SpoC-v1	LOCUS-v2
24	WAGE-v1	WAGE-v1	WAGE-v1
25	SpoC-v1	Pyjamask-v1	SpoC-v1
26	ACE-v1	ACE-v1	ACE-v1
27	SHA2-v1	SHA2-v1	SHA2-v1
28	SHA3-v1	SHA3-v1	SHA3-v1

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

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Xoodyak_GMU2-v1	Subterranean-v2	Xoodyak_GMU2-v1
2	Subterranean-v2	Xoodyak_GMU2-v1	Subterranean-v2
3	KNOT-v2x4h	KNOT-v2x4	KNOT-v2x4
4	Gimli_GT-v4	TinyJAMBU_TJT-v3	Gimli_GT-v4
5	TinyJAMBU_TJT-v3	Ascon_Graz-v2	TinyJAMBU_TJT-v3
6	Ascon_Graz-v2	Gimli_GT-v6	Saturnin-v2
7	COMET_VT-v1	Romulus-v2	Ascon_Graz-v2
8	Saturnin-v2	Saturnin-v2	DryGASCON-v1
9	Romulus-v2	DryGASCON-v1	Romulus-v2
10	DryGASCON-v1	Elephant-v2	Elephant-v2
11	Elephant-v2	ISAP-v1	PHOTON-Beetle-v1
12	Spook-v2-v2	Spook-v2-v2	SCHWAEMM-v1
13	SCHWAEMM-v1	PHOTON-Beetle-v1	AESGCM-v2
14	AESGCM-v2	SCHWAEMM-v1	Spook-v2-v2
15	PHOTON-Beetle-v1	GIFT-COFB-v1	Oribatida-v1
16	ISAP-v2	AESGCM-v2	ESTATE-v1
17	GIFT-COFB-v1	Oribatida-v1	GIFT-COFB-v1
18	ESTATE-v1	ESTATE-v1	ISAP-v2
19	Oribatida-v1	LOCUS-v2	COMET_CI-v3
20	mixFeed-v1	COMET_CI-v3	LOCUS-v2
21	LOCUS-v2	ForkAE-v2	ForkAE-v2
22	Pyjamask-v2	mixFeed-v1	Pyjamask-v2
23	ForkAE-v2	SpoC-v1	mixFeed-v1
24	WAGE-v1	WAGE-v1	SpoC-v1
25	SpoC-v1	Pyjamask-v1	WAGE-v1
26	ACE-v1	ACE-v1	ACE-v1
27	SHA2-v1	SHA2-v1	SHA2-v1
28	SHA3-v1	SHA3-v1	SHA3-v1

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

Rank	Artix-7	Cyclone 10 LP	ECP5
1	Xoodyak_GMU2-v1	Subterranean-v2	Xoodyak_GMU2-v1
2	Subterranean-v2	Xoodyak_GMU2-v1	Subterranean-v2
3	KNOT-v2x2	KNOT-v2x4	Gimli_GT-v4
4	Gimli_GT-v4	Ascon_Graz-v2	KNOT-v2x2
5	Ascon_Graz-v2	Gimli_GT-v6	Ascon_Graz-v2
6	COMET_VT-v1	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
7	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1
8	TinyJAMBU_TJT-v3	Romulus-v2	Saturnin-v2
9	Spook-v2-v2	Saturnin-v2	PHOTON-Beetle-v1
10	Romulus-v2	Spook-v2-v2	Romulus-v2
11	Saturnin-v2	ISAP-v1	AESGCM-v2
12	Elephant-v2	Elephant-v2	Spook-v2-v2
13	AESGCM-v2	PHOTON-Beetle-v1	Elephant-v2
14	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1
15	PHOTON-Beetle-v1	GIFT-COFB-v1	GIFT-COFB-v1
16	GIFT-COFB-v1	AESGCM-v2	Oribatida-v1
17	ISAP-v2	COMET_CI-v3	ESTATE-v1
18	mixFeed-v1	Oribatida-v1	ISAP-v2
19	ESTATE-v1	ESTATE-v1	COMET_CI-v3
20	Oribatida-v1	LOCUS-v2	LOCUS-v2
21	LOCUS-v2	mixFeed-v1	ForkAE-v2
22	Pyjamask-v2	ForkAE-v2	Pyjamask-v2
23	ForkAE-v2	SpoC-v1	mixFeed-v1
24	WAGE-v1	WAGE-v1	SpoC-v1
25	SpoC-v1	Pyjamask-v1	WAGE-v1
26	ACE-v1	ACE-v1	ACE-v1
27	SHA2-v1	SHA2-v1	SHA2-v1
28	SHA3-v1	SHA3-v1	SHA3-v1

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. For the processing of PT, the top two candidates are the same for all families. They are Subterranean 2.0 and Xoodyak. On positions 3 to 5, the order depends on a particular family. KNOT is the third for Artix-7 and Cyclone 10 LP, while Gimli the third for ECP5. DryGASCON is consistently the 6th for all families. The list of algorithms at positions from 7 to 10 vary but includes consistently Spook and TinyJAMBU. On Artix-7, 10 algorithms offer performance better than AES-GCM. On Cyclone 10 LP, this number is 12, and on ECP5 7.

For the processing of AD, Xoodyak outperforms Subterranean 2.0 for Artix-7 and ECP5, but the opposite is true for Cyclone 10 LP. KNOT is consistently the third for all FPGA families. The order of algorithms at positions 4 to 11 vary but includes consistently Gimli, TinyJAMBU, Ascon, Saturnin, Romulus, DryGASCON, and Elephant. The following algorithms appear among the first 11 only in the case of a single FPGA family: COMET for Artix-7, ISAP for Cyclone 10 LP, and PHOTON-Beetle for ECP5. Spook-v2 is at position 12 for Artix-7 and Cyclone 10 LP and at position 13 for ECP5 (without counting AES-GCM).

5.2.3 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 v2.0 for PT and Xoodyak for AD), smallest area (TinyJAMBU), and largest area (SCHWAEMM).

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 the 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 five designs of COMET. COMET_VT-v1, COMET_CI-v1, COMET_CI-v2, and COMET_CI-v3 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 four mentioned above variants comes from using different hardware architectures. COMET_VT-v1 uses the basic iterative architecture, while COMET_CI-v1, COMET_CI-v2, and COMET_CI-v3 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. COMET_CI-v3 is a minor improvement over COMET_CI-v1. COMET_CI-v2 is over 4 times slower and about 42% smaller.

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 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 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, Gimli_GT-v2, and Gimli_GT-v4 have areas smaller than the area of AES-GCM (2520 LUTs). Out of these three, Gimli_GT-v4 is by far the fastest. 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-v3, with 3 rounds unrolled. The designs from the Technical University of Munich (TUM) have a 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 the area below 1000 LUTs, which may be important in some applications. For hashing, Gimli_GT-v4 is the fastest design with an area smaller than the area of AES-GCM, at about 3 Gbit/s, followed by Gimli_GT-v2 at about 1.9 Gbit/s. Gimli_GT-v5 is the fastest overall, but its area is close to 4000 LUTs.

In Figs. 23 and 24, the Artix-7 results are presented for six variants of KNOT, representing 6 different architectures, implementing the parameter set KNOT-AEAD(128, 384, 192). The parameter sets of KNOT are 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. The parameter set KNOT-AEAD(128, 384, 192) has a substantial advantage in terms of throughput over the parameter sets KNOT-AEAD(128, 256, 64), KNOT-AEAD(192, 384, 96), and KNOT-AEAD(256, 512, 128), with 10 variants summarized in Table 2. For processing PT, KNOT-v2x2 is the fastest, and its area does not exceed 2000 LUTs. Adding hashing to this architecture increases its area by about 13%. For processing AD, KNOT-v2x4h is the fastest among architectures not exceeding 2500 LUTs. The FPGA options have been selected to optimize throughput/area, rather than throughput itself. Only this way, this architecture could be implemented using less than 2500 LUTs. The choice of tool options for KNOT-v2x4 has led to a larger design despite not supporting hashing functionality. The smaller area could be accomplished only at the cost of a significant decrease in the circuit throughput and some decrease in the throughput/area ratio. Basic iterative architectures KNOT-v2x1 and KNOT-v2x1h are the smallest but also the slowest.

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 eight variants of Xoodyak. Four of these designs were submitted by the Xoodyak Team + Silvia, with Silvia Mella as the primary designer. Two sets, with two different variants in each, were submitted by two different GMU primary designers. Variants Xoodyak_XT-v7, Xoodyak_XT-v8, and all variants from GMU 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 2× unrolled architecture) is slightly faster than the basic iterative architecture, but it also takes over 600 more LUTs. For the processing of PT, Xoodyak_GMU2-v2 outperforms Xoodyak_XT-v8 by over 3 Gbit/s and a factor of 2.2. For the processing of AD, Xoodyak_GMU2-v1 outperforms Xoodyak_XT-v8 by over 5 Gbit/s and a factor of 2.5. Xoodyak_GMU2-v1 is smaller than Xoodyak_GMU2-v2 by about 700 LUTs. However, even the larger of the two designs has only 2322 LUTs. Xoodyak_GMU2-v1 is a preferred choice for applications with a large size of AD. Xoodyak_GMU2-v2 should be used when the input consists mostly of plaintext. 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. For hashing, Xoodyak_GMU2-v2 offers throughput about 3.6 Gbits/s and Xoodyak_GMU2-v1 about 3 Gbit/s. The throughput of Xoodyak_XT-v8 exceeds 1.8 Gbit/s, Xoodyak_XT-v7 1.5 Gbit/s, and Xoodyak_GMU-v1 640 Mbit/s.

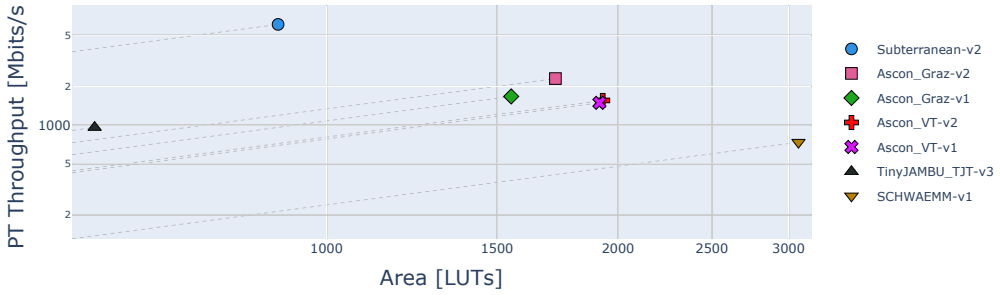

Figure 14: Artix-7 Ascon PT Throughput for Long Messages vs LUTs

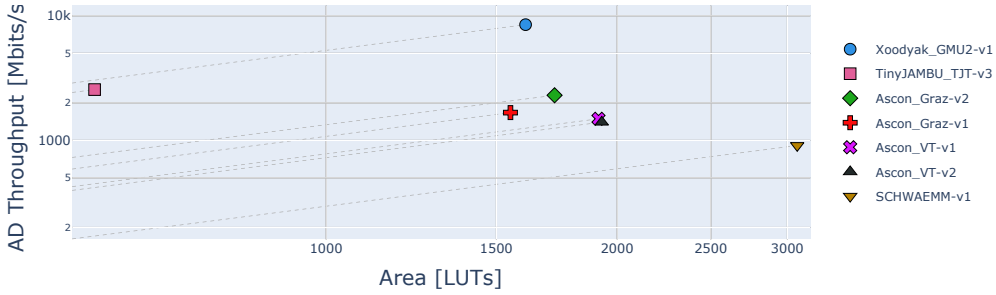

Figure 15: Artix-7 Ascon AD Throughput for Long Messages vs LUTs

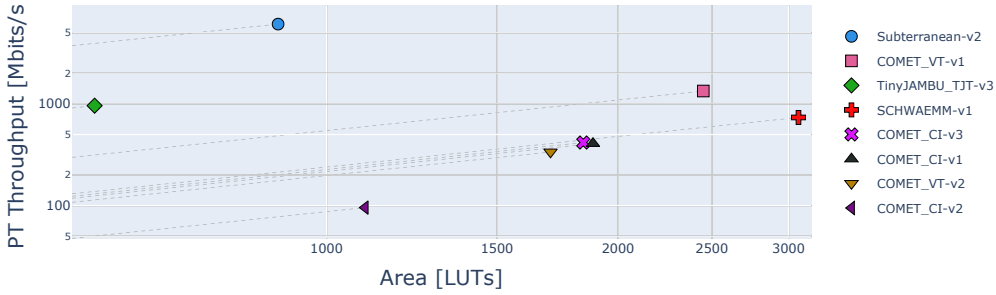

Figure 16: Artix-7 COMET PT Throughput for Long Messages vs LUTs

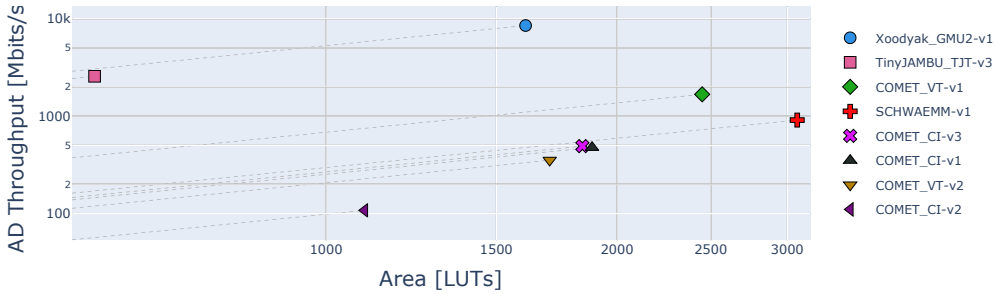

Figure 17: Artix-7 COMET AD Throughput for Long Messages vs LUTs

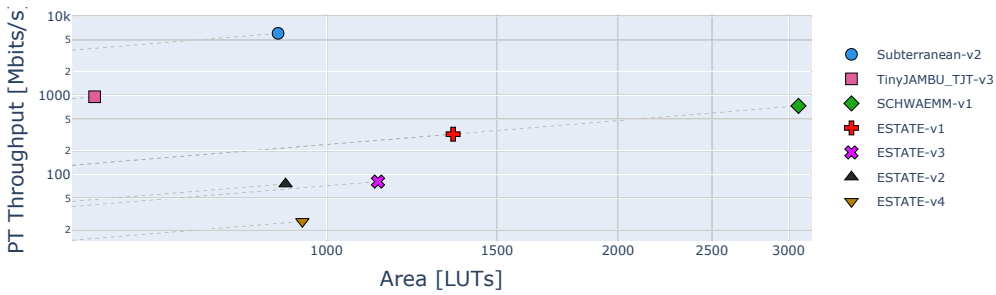

Figure 18: Artix-7 ESTATE PT Throughput for Long Messages vs LUTs

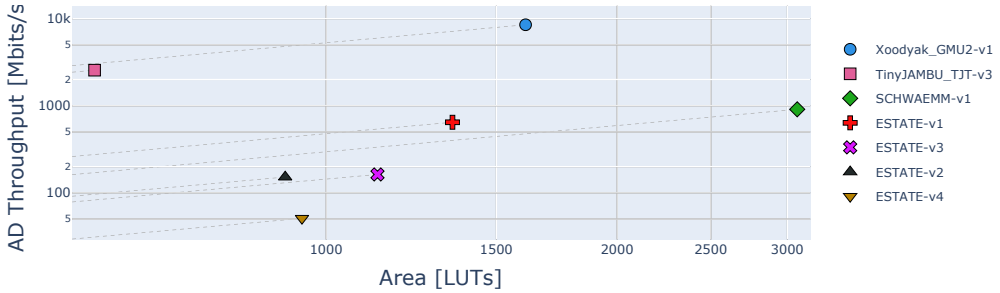

Figure 19: Artix-7 ESTATE AD Throughput for Long Messages vs LUTs

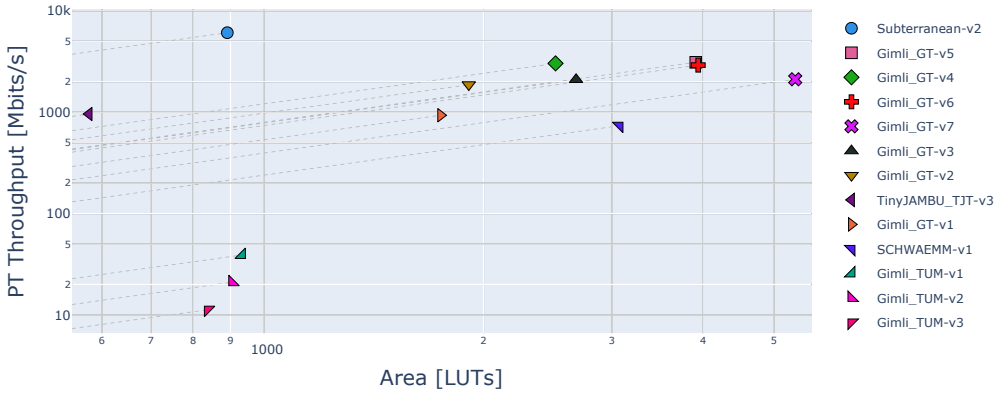

Figure 20: Artix-7 Gimli PT Throughput for Long Messages vs LUTs

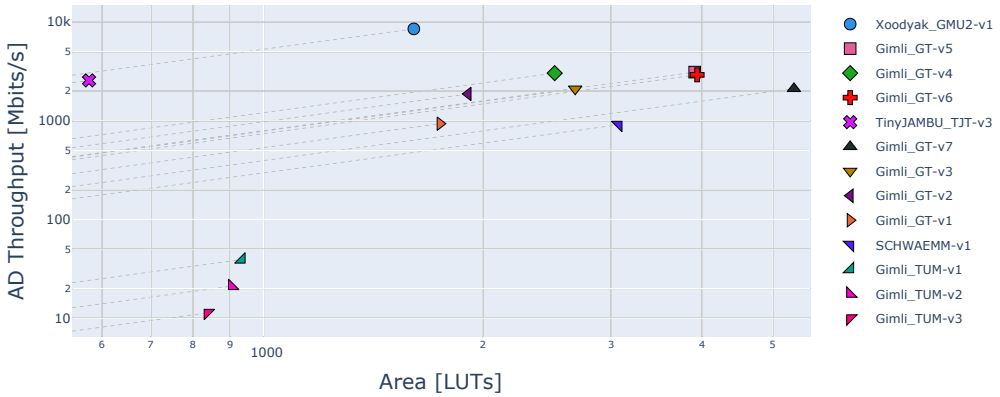

Figure 21: Artix-7 Gimli AD Throughput for Long Messages vs LUTs

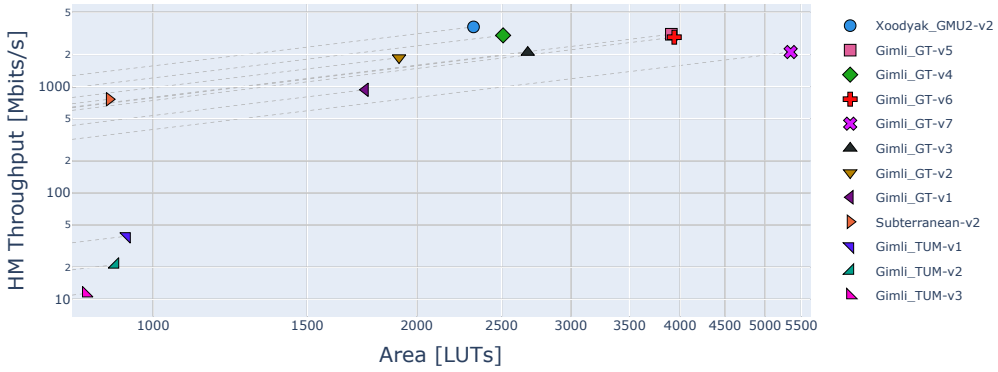

Figure 22: Artix-7 Gimli Hash Throughput for Long Messages vs LUTs

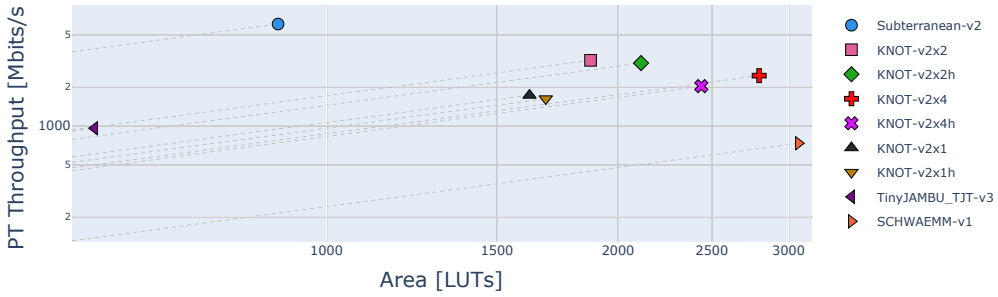

Figure 23: Artix-7 KNOT PT Throughput for Long Messages vs LUTs

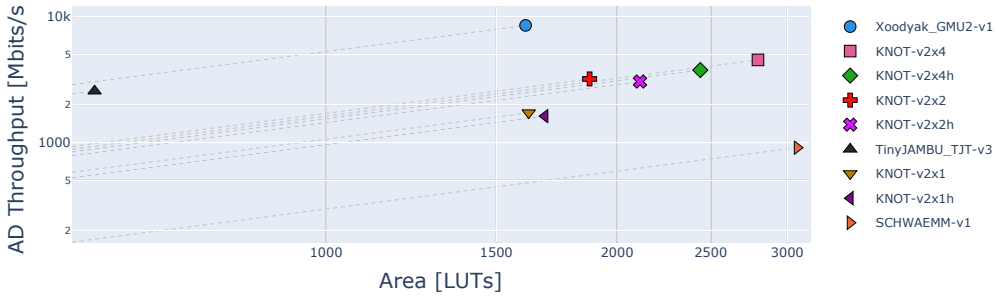

Figure 24: Artix-7 KNOT AD Throughput for Long Messages vs LUTs

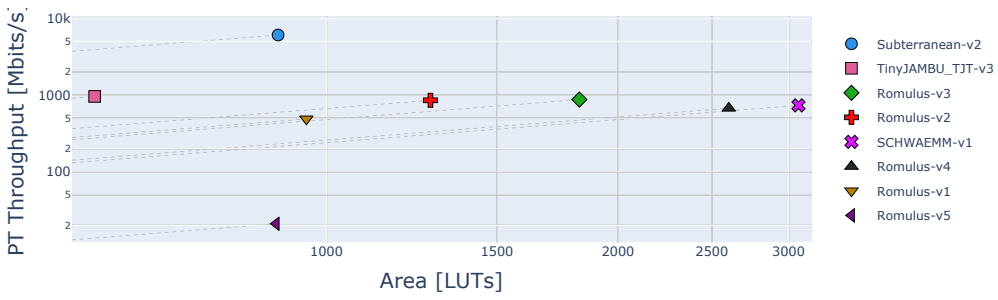

Figure 25: Artix-7 Romulus PT Throughput for Long Messages vs LUTs

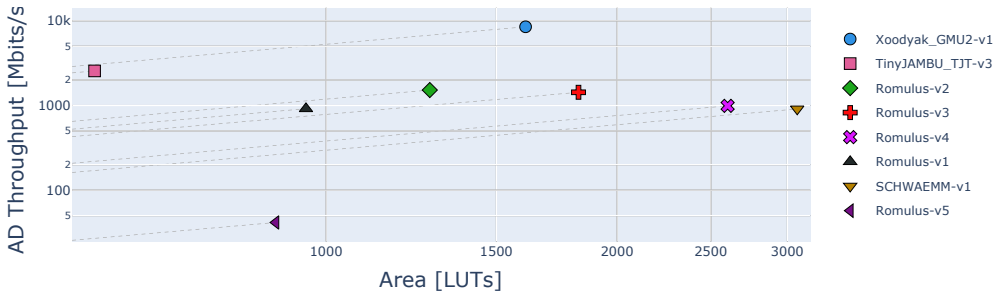

Figure 26: Artix-7 Romulus AD Throughput for Long Messages vs LUTs

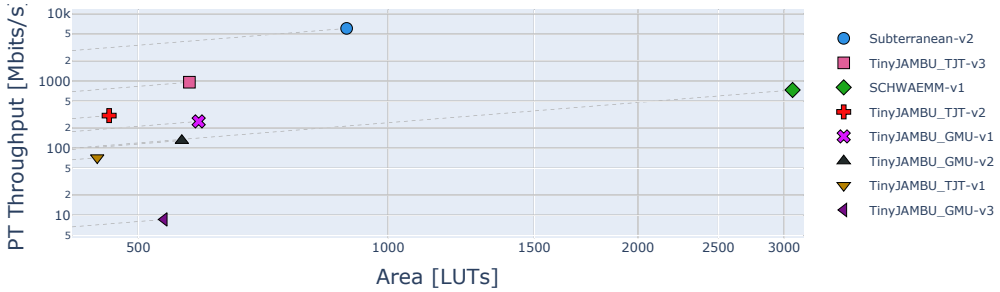

Figure 27: Artix-7 TinyJAMBU PT Throughput for Long Messages vs LUTs

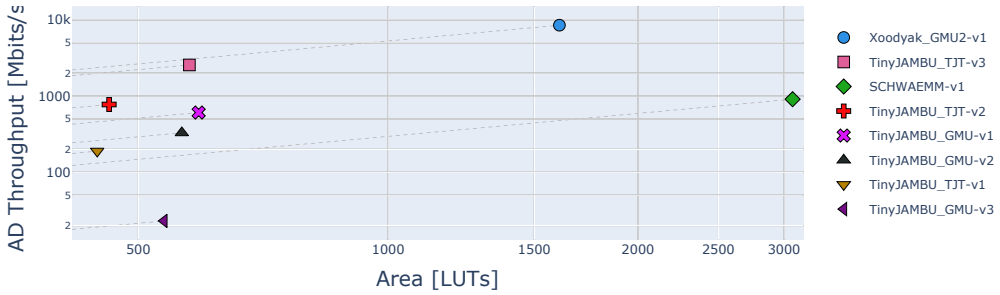

Figure 28: Artix-7 TinyJAMBU AD Throughput for Long Messages vs LUTs

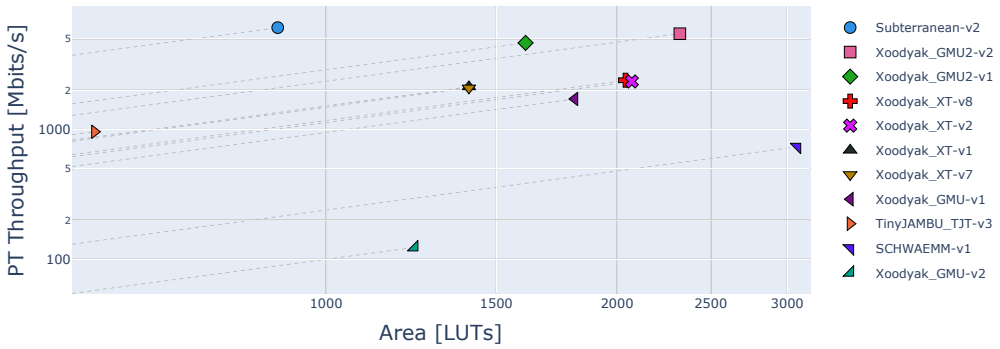

Figure 29: Artix-7 Xoodyak PT Throughput for Long Messages vs LUTs

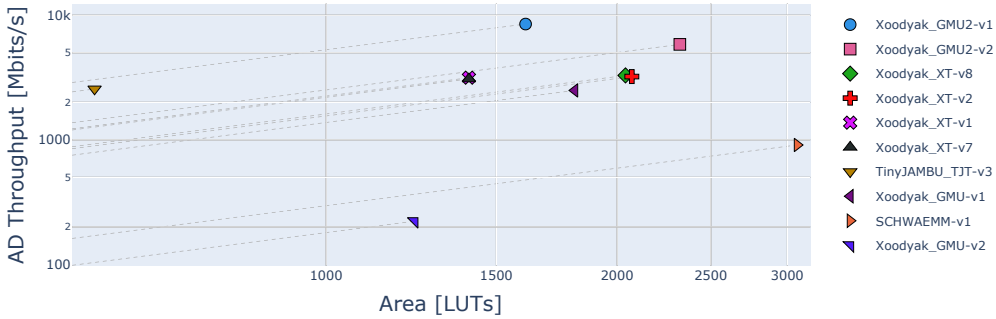

Figure 30: Artix-7 Xoodyak AD Throughput for Long Messages vs LUTs

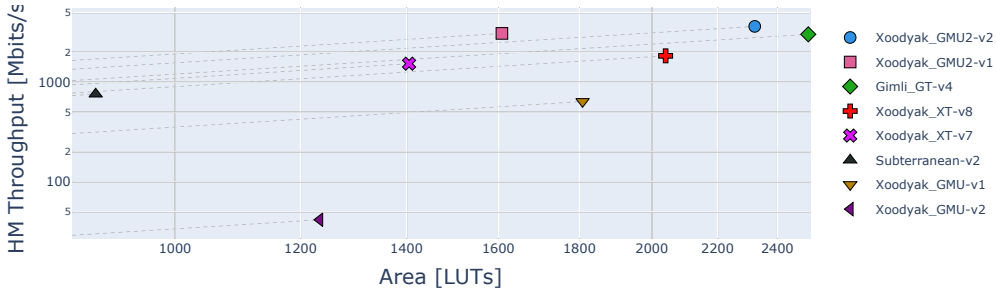

Figure 31: Artix-7 Xoodyak Hash Throughput for Long Messages vs LUTs

Table 19: Xilinx Artix-7 Encryption PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v2	Subterranean-v2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
2	Xoodyak_GMU2-v2	Xoodyak_GMU2-v2	Subterranean-v2	Subterranean-v2
3	KNOT-v2x2	KNOT-v2x2	KNOT-v2x2	Ascon_VT-v1
4	Gimli_GT-v4	Gimli_GT-v4	Ascon_Graz-v2	COMET_VT-v1
5	Ascon_Graz-v2	Ascon_Graz-v2	DryGASCON-v1	DryGASCON-v1
6	DryGASCON-v1	DryGASCON-v1	Gimli_GT-v4	KNOT-v2x2
7	COMET_VT-v1	COMET_VT-v1	COMET_VT-v1	TinyJAMBU_TJT-v3
8	Spook-v2-v2	Spook-v2-v2	TinyJAMBU_TJT-v3	Romulus-v2
9	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Romulus-v2	Gimli_GT-v4
10	Romulus-v3	Romulus-v3	Spook-v2-v2	PHOTON-Beetle-v1
11	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	Elephant-v2
12	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1
13	SCHWAEMM-v1	SCHWAEMM-v1	Elephant-v2	ESTATE-v1
14	PHOTON-Beetle-v1	PHOTON-Beetle-v1	SCHWAEMM-v1	Spook-v2-v2
15	Elephant-v2	Elephant-v2	Saturnin-v2	ForkAE-v2
16	ISAP-v2	ISAP-v2	ESTATE-v1	SCHWAEMM-v1
17	mixFeed-v1	mixFeed-v1	mixFeed-v1	Oribatida-v1
18	ESTATE-v1	ESTATE-v1	ForkAE-v2	LOCUS-v2
19	Pyjamask-v2	Pyjamask-v2	Oribatida-v1	Saturnin-v2
20	Oribatida-v1	Oribatida-v1	LOCUS-v2	mixFeed-v1
21	ForkAE-v2	ForkAE-v2	ISAP-v2	SpoC-v1
22	LOCUS-v2	LOCUS-v2	Pyjamask-v2	ISAP-v2
23	WAGE-v1	WAGE-v1	SpoC-v1	Pyjamask-v2
24	SpoC-v1	SpoC-v1	WAGE-v1	WAGE-v1
25	ACE-v1	ACE-v1	ACE-v1	ACE-v1

Table 20: Xilinx Artix-7 Encryption AD Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	TinyJAMBU_TJT-v3
2	Subterranean-v2	Subterranean-v2	Subterranean-v2	Xoodyak_GMU2-v1
3	KNOT-v2x4h	KNOT-v2x4h	TinyJAMBU_TJT-v3	Subterranean-v2
4	Gimli_GT-v4	Gimli_GT-v4	KNOT-v2x4h	COMET_VT-v1
5	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Ascon_Graz-v2	DryGASCON-v1
6	Ascon_Graz-v2	Ascon_Graz-v2	COMET_VT-v1	Ascon_VT-v1
7	COMET_VT-v1	COMET_VT-v1	Gimli_GT-v4	KNOT-v2x2
8	Saturnin-v2	Romulus-v2	DryGASCON-v1	Romulus-v2
9	Romulus-v2	Saturnin-v2	Romulus-v2	GIFT-COFB-v1
10	DryGASCON-v1	DryGASCON-v1	PHOTON-Beetle-v1	PHOTON-Beetle-v1
11	Elephant-v2	Elephant-v2	Spook-v2-v2	Gimli_GT-v4
12	Spook-v2-v2	Spook-v2-v2	Elephant-v2	ESTATE-v1
13	SCHWAEMM-v1	SCHWAEMM-v1	GIFT-COFB-v1	Elephant-v2
14	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ESTATE-v1	Spook-v2-v2
15	ISAP-v2	ISAP-v2	SCHWAEMM-v1	ForkAE-v2
16	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	LOCUS-v2
17	ESTATE-v1	ESTATE-v1	LOCUS-v2	SCHWAEMM-v1
18	Oribatida-v1	Oribatida-v1	Oribatida-v1	Saturnin-v2
19	mixFeed-v1	mixFeed-v1	ISAP-v2	Oribatida-v2
20	LOCUS-v2	LOCUS-v2	mixFeed-v1	mixFeed-v1
21	Pyjamask-v2	ForkAE-v2	ForkAE-v2	ISAP-v2
22	ForkAE-v2	Pyjamask-v2	Pyjamask-v2	SpoC-v1
23	WAGE-v1	WAGE-v1	SpoC-v1	Pyjamask-v2
24	SpoC-v1	SpoC-v1	WAGE-v1	WAGE-v1
25	ACE-v1	ACE-v1	ACE-v1	ACE-v1

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

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
2	Subterranean-v2	Subterranean-v2	Subterranean-v2	Subterranean-v2
3	KNOT-v2x2	KNOT-v2x2	KNOT-v2x2	TinyJAMBU_TJT-v3
4	Gimli_GT-v4	Gimli_GT-v4	Ascon_Graz-v2	COMET_VT-v1
5	Ascon_Graz-v2	Ascon_Graz-v2	Gimli_GT-v4	KNOT-v2x2
6	COMET_VT-v1	COMET_VT-v1	COMET_VT-v1	Ascon_Graz-v2
7	DryGASCON-v1	DryGASCON-v1	TinyJAMBU_TJT-v3	DryGASCON-v1
8	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	DryGASCON-v1	Romulus-v2
9	Spook-v2-v2	Romulus-v2	Romulus-v2	Gimli_GT-v4
10	Romulus-v2	Spook-v2-v2	Spook-v2-v2	GIFT-COFB-v1
11	Saturnin-v2	Saturnin-v2	GIFT-COFB-v1	PHOTON-Beetle-v1
12	Elephant-v2	Elephant-v2	Elephant-v2	Elephant-v2
13	SCHWAEMM-v1	SCHWAEMM-v1	PHOTON-Beetle-v1	ESTATE-v1
14	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Saturnin-v2	Spook-v2-v2
15	GIFT-COFB-v1	GIFT-COFB-v1	SCHWAEMM-v1	Saturnin-v2
16	ISAP-v2	ISAP-v2	ESTATE-v1	ForkAE-v2
17	mixFeed-v1	mixFeed-v1	mixFeed-v1	LOCUS-v2
18	ESTATE-v1	ESTATE-v1	ISAP-v2	SCHWAEMM-v1
19	Oribatida-v1	Oribatida-v1	Oribatida-v1	Oribatida-v1
20	LOCUS-v2	LOCUS-v2	LOCUS-v2	mixFeed-v1
21	Pyjamask-v2	Pyjamask-v2	ForkAE-v2	ISAP-v2
22	ForkAE-v2	ForkAE-v2	Pyjamask-v2	SpoC-v1
23	WAGE-v1	WAGE-v1	SpoC-v1	Pyjamask-v2
24	SpoC-v1	SpoC-v1	WAGE-v1	WAGE-v1
25	ACE-v1	ACE-v1	ACE-v1	ACE-v1

5.3 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-v2). Multiple algorithms reach 99%. For 64-byte plaintexts, this ratio varies from 25% for Subterranean-v2 to 99% for ForkAE-v1, with an average of 60%. For 16-byte plaintexts, the ratio varies from 8% for Subterranean-v2 to 98% for ForkAE-v1, with an average of 32%. For 1536-byte ADs, the average percentage is 96%, the minimum 88% (Subterranean-v2). Multiple algorithms reach 99%. For 64-byte ADs, this ratio varies from 25% for Subterranean-v2 to 99% for ForkAE-v1, with an average of 53%. For 16-byte ADs, the ratio varies from 6% for Xoodyak_GMU2-v1 to 95% for ForkAE-v1, with an average of 25%. All mentioned above percentages are dependent only on the algorithm and its hardware architecture. They do not depend on a particular FPGA device.

In Tables 19, 20, and 21, we summarize the relative changes in rankings for Artix-7. For processing of PT only, the following algorithms rank higher for short messages than for long messages: Xoodyak, Ascon, DryGASCON, COMET, TinyJAMBU, Romulus, PHOTON-Beetle, Elephant, ESTATE, Oribatida, ForkAE, LOCUS, and SpoC. The opposite is true for the following candidates: Subterranean 2.0, KNOT, Gimli, Spook, SCHWAEMM, Saturnin, ISAP, Pyjamask, and WAGE. The following 9 algorithms remain among the best 10, independently of the size of inputs: Subterranean 2.0, Xoodyak, KNOT, Gimli, Ascon, DryGASCON, COMET, TinyJAMBU, and Romulus. For the shortest considered plaintext of the size of 16 bytes, Spook-v2 drops to position 14. Out of these 9 algorithms, the following 6 also support hashing: Xoodyak, Gimli, DryGASCON, Ascon, Subterranean 2.0, and KNOT (with the first four at least two times faster than KNOT). A candidate particularly fast in hashing but not so good for processing small plaintexts is Saturnin.

For processing of AD only, the following algorithms rank consistently higher for short messages than for long messages: TinyJAMBU, COMET, DryGASCON, GIFT-COFB, PHOTON-Beetle, ESTATE, LOCUS, ForkAE, and SpoC. The opposite is true for the following candidates: KNOT, Elephant, Gimli, SCHWAEMM, Saturnin, ISAP, and Pyjamask. The following 8 algorithms remain among the best 10, independently of the size of inputs: Xoodyak, Subterranean 2.0, KNOT, TinyJAMBU, Ascon, COMET, Romulus, and DryGASCON. For 16-byte ADs, Gimli drops to position 11 and Saturnin to position 16,

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

6 Conclusions and Future Work

For the processing of long plaintexts on Xilinx Artix-7 FPGAs, with a budget of 2520 LUTs or less, 10 candidates outperform the current standard AES-GCM. These candidates, in the order of Throughput, include Subterranean 2.0, Xoodyak, KNOT, Gimli, Ascon, DryGASCON, COMET, Spook-v2, TinyJAMBU, and Romulus. All these algorithms, as well as Saturnin and Elephant, outperform AES-GCM also for the processing of long ADs while meeting the area limit. Out of them, only Xoodyak, Gimli, and Saturnin support hashing faster than SHA-2. Two additional ones, DryGASCON and Ascon, perform hashing faster than the folded implementation of SHA-3.

When the same designs are implemented using Intel Cyclone 10 LP, 12 candidates outperform AES-GCM for processing of plaintexts. These candidates are Subterranean v2.0, Xoodyak, KNOT, Ascon, Gimli, DryGASCON, TinyJAMBU, Spook, Romulus, GIFT-COFB, Saturnin, and PHOTON-Beetle. All of them also outperform AES-GCM for

processing of AD. However, it should be noted that the implementation of AES-GCM uses 7711 LEs, about 54% more than the limit of 5000 LEs imposed on LWC candidates. Out of the mentioned above candidates, only Xoodyak, Gimli, and Saturnin support hashing faster than SHA-2. Additionally, DryGASCON, Ascon, and Subterranean v2.0 perform hashing faster than the implementation of SHA-3 adhering to similar resource utilization constraints (taking 5417 LEs).

When all candidates are implemented using Lattice Semiconductor ECP5, 7 candidates perform faster than AES-GCM for processing of PT only. These candidates are Subterranean v2.0, Xoodyak, Gimli, KNOT, Ascon, DryGASCON, and TinyJAMBU. All of them perform faster also for the processing of AD. However, it should be noted that the implementation of AES-GCM uses 5507 LUTs, about 10% more than the limit of 5000 LUTs imposed on LWC candidates. For hashing, only Xoodyak and Gimli perform faster than SHA-2. Additionally, Saturnin and DryGASCON perform faster than the folded implementation of SHA-3.

Future work in Round 2 will include extending the study with additional candidates and ranking of all investigated candidates in terms of energy per bit. In Round 3, the evaluation should focus on the ranking of implementations protected against side-channel attacks.

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 of Lightweight Cryptography," Tech. Rep. 1273, 2019.

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

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

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

[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," Cryptology ePrint Archive 2019/824, Feb. 2020.

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

[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," Cryptology ePrint Archive 2018/573, Jun. 2018.

[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)*, Washington, DC, USA: IEEE, May 2018.

[18] W. Diehl, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Comparing the Cost of Protecting Selected Lightweight Block Ciphers against Differential Power Analysis in Low-Cost FPGAs," en, *Computers*, vol. 7, no. 2, p. 28, Apr. 2018.

[19] W. Diehl, A. Abdulgadir, F. Farahmand, J.-P. Kaps, and K. Gaj, "Comparison of Cost of Protection against Differential Power Analysis of Selected Authenticated Ciphers," *Cryptography*, vol. 2, no. 3, p. 26, Sep. 2018.

[20] W. Diehl, F. Farahmand, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "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*, https://cryptography.gmu.edu/athena/index.php?id=LWC, 2019.

[22] F. Farahmand, W. Diehl, and K. Gaj, "Minerva: Automated hardware optimization tool," in *International Conference on ReConfigureable Computing and FPGAs (ReConfig)*, Cancun, Mexico, 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] K. Mohajerani, *BlueLight: Bluespec implementations of Lightweight Cryptography Candidates*, Dec. 9, 2020. [Online]. Available: https://github.com/kammoh/bluelight.

[26] D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, C. Momin, O. Pereira, T. Peters, F.-X. Standaert, 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.

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

[28] 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.

A Additional Results

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

Variant	**LUTs**	**FFs**	**Slices**	**Freq. [MHz]**
ACE-v1	1,229	894	400	200
AESGCM-v1	3,270	1,498	1,008	211
AESGCM-v2	2,520	1,611	810	211
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
COMET_CI-v2	1,096	1,034	372	222
COMET_CI-v3	1,841	1,453	553	215
COMET_VT-v1	2,449	947	695	209
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
ForkAE-v1	1,191	808	361	208
ForkAE-v2	2,466	1,343	720	228
GIFT-COFB-v1	1,041	604	321	275
Gimli_GT-v1	1,747	1,169	502	175
Gimli_GT-v2	1,909	1,164	528	175
Gimli_GT-v3	2,678	1,163	752	131
Gimli_GT-v4	2,510	1,161	717	142
Gimli_GT-v5	3,907	1,162	1,057	97
Gimli_GT-v6	3,937	1,160	1,075	91
Gimli_GT-v7	5,347	1,161	1,418	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

Table 22 continued from previous page

Variant	LUTs	FFs	Slices	Freq. [MHz]
ISAP-v2	2,157	1,005	618	200
KNOT-v2x1	1,620	853	474	251
KNOT-v2x1h	1,684	857	504	236
KNOT-v2x2	1,873	855	525	233
KNOT-v2x2h	2,112	858	584	222
KNOT-v2x4	2,797	856	740	165
KNOT-v2x4h	2,438	859	675	137
LOCUS-v1	1,824	1,037	613	216
LOCUS-v2	1,628	789	492	209
LOTUS-v1	1,652	916	469	145
LOTUS-v2	1,487	788	462	141
mixFeed-v1	1,316	187	382	204
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
SHA2-v1	1,051	937	345	201
SHA3-v1	1,263	277	351	195
SpoC-v1	1,079	805	348	230
Spook-v2-v2	2,033	1,517	597	206
Subterranean-v2	891	610	253	190
TinyJAMBU_GMU-v1	591	428	212	266
TinyJAMBU_GMU-v2	564	430	197	268
TinyJAMBU_GMU-v3	537	433	191	278
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_GMU2-v1	1,608	1,249	513	314
Xoodyak_GMU2-v2	2,322	1,228	692	199
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	**1,782**	**841**	**518**	**208.0**
MINIMUM	**446**	**98**	**136**	**58.0**

Table 22 continued from previous page

Variant	LUTs	FFs	Slices	Freq. [MHz]
MAXIMUM	**5,347**	**1,611**	**1,418**	**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]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
ACE-v1	1,903	1.55	918	1.03	106.5	1.88
AESGCM-v1	8,754	2.68	1,585	1.06	121.0	1.74
AESGCM-v2	7,711	3.06	1,699	1.05	118.7	1.78
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_CI-v3	4,379	2.38	1,768	1.22	114.8	1.87
COMET_VT-v1	10,200	4.17	955	1.01	88.9	2.35
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
ForkAE-v1	2,129	1.79	1,194	1.48	135.7	1.53
ForkAE-v2	3,200	1.30	1,415	1.05	148.1	1.54
GIFT-COFB-v1	1,877	1.80	774	1.28	184.4	1.49
Gimli_GT-v1	2,378	1.36	1,156	0.99	142.8	1.23
Gimli_GT-v2	3,145	1.65	1,155	0.99	114.8	1.52
Gimli_GT-v3	3,651	1.36	1,156	0.99	85.8	1.53
Gimli_GT-v4	5,010	2.00	1,154	0.99	88.2	1.61
Gimli_GT-v5	5,948	1.52	1,155	0.99	58.6	1.66
Gimli_GT-v6	4,820	1.22	1,153	0.99	45.2	2.01
Gimli_GT-v7	6,379	1.19	1,154	0.99	32.3	2.05
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
KNOT-v2x1	2,059	1.27	957	1.12	161.7	1.55
KNOT-v2x1h	2,532	1.50	963	1.12	159.4	1.48
KNOT-v2x2	2,472	1.32	958	1.12	138.7	1.68
KNOT-v2x2h	2,792	1.32	964	1.12	140.1	1.58
KNOT-v2x4	3,519	1.26	960	1.12	102.0	1.62
KNOT-v2x4h	3,678	1.51	966	1.12	101.5	1.35

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]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
LOCUS-v1	2,978	1.63	1,045	1.01	125.8	1.72
LOCUS-v2	2,828	1.74	804	1.02	132.4	1.58
LOTUS-v1	2,642	1.60	1,010	1.10	103.5	1.40
LOTUS-v2	2,445	1.64	895	1.14	99.6	1.42
mixFeed-v1	5,323	4.04	1,625	8.69	74.0	2.76
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
SHA2-v1	2,139	2.04	1,191	1.27	118.6	1.69
SHA3-v1	5,417	4.29	3,444	12.43	84.5	2.31
SpoC-v1	1,696	1.57	820	1.02	167.7	1.37
Spook-v2-v2	3,188	1.57	1,485	0.98	108.5	1.90
Subterranean-v2	1,285	1.44	601	0.98	153.7	1.24
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_GMU2-v1	2,575	1.60	1,256	1.01	170.3	1.84
Xoodyak_GMU2-v2	5,058	2.18	1,237	1.01	97.2	2.05
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	**3,502**	**1.91**	**1,174**	**1.81**	**125.0**	**1.66**

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]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
MINIMUM	**686**	**1.19**	**429**	**0.91**	**32.3**	**1.23**
MAXIMUM	**10,200**	**4.76**	**6,236**	**22.83**	**200.8**	**2.76**

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]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
ACE-v1	2,156	1.75	923	1.03	1,379	73.8	2.71
AESGCM-v1	6,740	2.06	1,403	0.94	3,903	108.2	1.95
AESGCM-v2	5,507	2.19	1,512	0.94	3,226	106.7	1.98
Ascon_Graz-v1	2,947	1.90	674	1.01	1,723	63.2	3.31
Ascon_Graz-v2	3,847	2.23	673	1.01	2,263	63.2	3.42
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	3,255	1.73	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_CI-v3	3,443	1.87	1,677	1.15	2,198	80.0	2.69
COMET_VT-v1	5,266	2.15	877	0.93	3,001	98.4	2.12
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	2,855	2.11	1,017	1.39	1,895	109.0	2.04
ESTATE-v2	1,689	1.86	762	1.83	1,135	115.4	2.32
ESTATE-v3	1,820	1.61	1,137	1.34	1,349	107.1	2.42
ESTATE-v4	1,329	1.41	832	1.49	911	118.1	2.35
ForkAE-v1	2,022	1.70	1,024	1.27	1,357	67.9	3.06
ForkAE-v2	3,571	1.45	1,371	1.02	2,184	90.0	2.53
GIFT-COFB-v1	2,214	2.13	689	1.14	1,248	114.3	2.41
Gimli_GT-v1	2,537	1.45	1,165	1.00	1,570	78.2	2.24
Gimli_GT-v2	2,852	1.49	1,166	1.00	1,631	76.2	2.30
Gimli_GT-v3	4,451	1.66	1,170	1.01	2,479	55.6	2.35
Gimli_GT-v4	4,027	1.60	1,168	1.01	2,231	60.7	2.34
Gimli_GT-v5	5,738	1.47	1,127	0.97	3,214	23.3	4.16
Gimli_GT-v6	6,341	1.61	1,126	0.97	3,466	31.5	2.89
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-v2x1	2,275	1.40	864	1.01	1,329	85.5	2.94
KNOT-v2x1h	2,446	1.45	872	1.02	1,445	78.9	2.99

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]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
KNOT-v2x2	3,287	1.75	870	1.02	1,809	90.4	2.58
KNOT-v2x2h	3,373	1.60	877	1.02	1,866	75.3	2.95
KNOT-v2x4	3,984	1.42	872	1.02	2,144	63.2	2.61
KNOT-v2x4h	4,283	1.76	879	1.02	2,342	60.9	2.25
LOCUS-v1	2,857	1.57	882	0.85	1,691	73.0	2.96
LOCUS-v2	2,950	1.81	759	0.96	1,757	72.5	2.88
LOTUS-v1	2,413	1.46	935	1.02	1,400	54.6	2.66
LOTUS-v2	2,208	1.49	807	1.02	1,324	52.7	2.68
mixFeed-v1	3,479	2.64	517	2.77	1,833	38.9	5.24
Oribatida-v1	1,671	1.15	987	0.75	1,128	176.5	1.56
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	1,998	2.10	508	1.01	1,198	80.5	2.84
Romulus-v2	2,353	1.84	508	1.01	1,353	82.0	2.61
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	3,093	1.53	1,588	1.21	1,939	94.0	2.04
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
SCHWAEMM-v2	5,947	1.59	1,546	1.00	3,839	63.8	2.04
SHA2-v1	2,001	1.90	844	0.90	1,142	117.7	1.71
SHA3-v1	1,804	1.43	249	0.90	1,008	90.3	2.16
SpoC-v1	2,049	1.90	740	0.92	1,314	98.2	2.34
Spook-v2-v2	3,662	1.80	1,494	0.98	2,258	77.0	2.67
Subterranean-v2	613	0.69	613	1.00	828	95.7	1.99
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	580	1.30	397	1.90	451	111.3	2.61
TinyJAMBU_TJT-v2	689	1.50	351	1.08	488	125.4	2.51
TinyJAMBU_TJT-v3	1,092	1.90	348	0.81	661	115.4	2.08
WAGE-v1	2,081	1.81	825	1.09	1,287	101.6	2.75
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_GMU2-v1	3,248	2.02	1,261	1.01	1,834	150.5	2.09
Xoodyak_GMU2-v2	4,077	1.76	1,233	1.00	2,369	68.9	2.89
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

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]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
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	**3,426**	**1.75**	**899**	**1.10**	**2,000**	**80.3**	**2.58**
MINIMUM	**580**	**0.69**	**114**	**0.75**	**451**	**16.4**	**1.56**
MAXIMUM	**9,447**	**2.65**	**1,937**	**2.76**	**4,799**	**176.5**	**5.24**

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-v2	5,392.0	89%	1	891	190	433
Xoodyak_GMU2-v2	4,960.1	91%	2	2,322	199	493
Xoodyak_GMU2-v1	4,325.6	93%		1,608	314	892
KNOT-v2x2	2,954.7	92%	3	1,873	233	969
KNOT-v2x2h	2,815.2	92%		2,112	222	969
Gimli_GT-v4	2,756.5	91%	4	2,510	142	633
Xoodyak_XT-v8	2,288.7	96%		2,040	187	1,004
Xoodyak_XT-v2	2,239.7	96%		2,071	183	1,004
Ascon_Graz-v2	2,210.0	96%	5	1,723	216	1,201
Gimli_GT-v2	1,744.0	93%		1,909	175	1,233
Xoodyak_GMU-v1	1,642.3	96%		1,808	170	1,272
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
COMET_VT-v1	1,309.0	98%	7	2,449	209	1,962
Spook-v2-v2	1,055.6	96%	8	2,033	206	2,398
TinyJAMBU_TJT-v3	946.4	99%	9	576	240	3,116
Romulus-v3	855.8	98%	10	1,824	123	1,766
Romulus-v2	841.8	98%		1,280	214	3,124
Saturnin-v2	747.2	94%	11	2,414	168	2,763
GIFT-COFB-v1	731.9	98%	12	1,041	275	4,617
SCHWAEMM-v1	708.6	96%	13*	**3,071**	135	2,341
PHOTON-Beetle-v1	680.3	99%	14	2,065	178	3,215
Elephant-v2	661.4	98%	15	1,884	181	3,363
ISAP-v2	456.5	93%	16	2,157	200	5,384
mixFeed-v1	444.4	97%	17	1,316	204	5,641
COMET_CI-v3	409.9	98%		1,841	215	6,446
COMET_CI-v1	400.8	98%		1,884	223	6,837
COMET_VT-v2	329.6	98%		1,703	234	8,725
ESTATE-v1	320.5	99%	18	1,351	222	8,512
TinyJAMBU_TJT-v2	302.3	99%		461	315	12,803
Pyjamask-v2	255.0	95%	19	2,308	213	10,263
Oribatida-v1	255.0	99%	20	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
ForkAE-v2	235.9	99%	21	2,466	228	11,878
LOCUS-v2	221.0	99%	22	1,628	209	11,619
Elephant-v1	210.8	98%		1,291	229	13,347
WAGE-v1	151.7	97%	23	1,150	279	22,600
LOTUS-v2	149.1	99%		1,487	141	11,619
SpoC-v1	131.2	99%	24	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
Xoodyak_GMU-v2	118.0	95%		1,234	168	17,495
Pyjamask-v1	107.7	96%		1,979	229	26,131
ACE-v1	95.4	97%	25	1,229	200	25,756
ESTATE-v3	80.8	99%		1,130	259	39,392
Gimli_TUM-v1	37.9	97%		933	241	78,117
Gimli_TUM-v2	20.4	97%		905	244	146,617
ForkAE-v1	8.3	100%		1,191	208	306,694
Average		**97%**				
Minimum		**89%**				
Maximum		**100%**				

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
Xoodyak_GMU2-v1	1,623.9	35%	1	1,608	314	99
Xoodyak_GMU2-v2	1,543.8	28%		2,322	199	66
Subterranean-v2	1,496.6	25%	2	891	190	65
KNOT-v2x2	1,181.1	37%	3	1,873	233	101
Ascon_Graz-v2	1,140.1	49%	4	1,723	216	97
KNOT-v2x2h	1,125.4	37%		2,112	222	101
Xoodyak_XT-v8	1,100.5	46%		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%	5	2,074	238	135
Gimli_GT-v4	897.6	30%	6	2,510	142	81
COMET_VT-v1	877.1	66%	7	2,449	209	122
Xoodyak_GMU-v1	784.1	46%		1,808	170	111
TinyJAMBU_TJT-v3	714.4	74%	8	576	240	172
Gimli_GT-v2	694.6	37%		1,909	175	129
Romulus-v2	608.7	71%	9	1,280	214	180
Romulus-v3	572.5	65%		1,824	123	110
Spook-v2-v2	555.1	51%	10	2,033	206	190
PHOTON-Beetle-v1	509.1	74%	11	2,065	178	179
GIFT-COFB-v1	480.5	64%	12	1,041	275	293
Elephant-v2	413.7	61%	13	1,884	181	224
SCHWAEMM-v1	386.1	53%	14*	**3,071**	135	179
Saturnin-v2	308.3	39%	15	2,414	168	279
COMET_CI-v3	294.3	71%		1,841	215	374
COMET_CI-v1	287.6	71%		1,884	223	397
ESTATE-v1	273.2	85%	16	1,351	222	416
mixFeed-v1	263.1	57%	17	1,316	204	397
TinyJAMBU_TJT-v2	244.7	80%		461	315	659
COMET_VT-v2	223.1	66%		1,703	234	537
ForkAE-v2	207.7	88%	18	2,466	228	562
Oribatida-v1	202.7	79%	19	1,450	276	697
TinyJAMBU_GMU-v1	201.2	80%		591	266	677
Oribatida-v2	187.4	74%		1,450	276	754
LOCUS-v2	184.8	83%	20	1,628	209	579
ISAP-v2	171.0	35%	21	2,157	200	599
Elephant-v1	135.7	63%		1,291	229	864
LOTUS-v2	124.7	83%		1,487	141	579
Pyjamask-v2	124.1	46%	22	2,308	213	879
TinyJAMBU_GMU-v2	105.5	81%		564	268	1,301
SpoC-v1	105.0	79%	23	1,079	230	1,121
WAGE-v1	88.0	56%	24	1,150	279	1,624
ESTATE-v3	71.4	88%		1,130	259	1,856
Saturnin-v1	66.9	54%		2,020	192	1,469
Pyjamask-v1	57.8	52%		1,979	229	2,027
ACE-v1	55.8	57%	25	1,229	200	1,836
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
ForkAE-v1	8.3	99%		1,191	208	12,846
Average		**60%**				
Minimum		**25%**				
Maximum		**99%**				

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
Xoodyak_GMU2-v1	550.6	12%	1	1,608	314	73
Xoodyak_GMU2-v2	489.8	9%		2,322	199	52
Subterranean-v2	458.9	8%	2	891	190	53
Ascon_VT-v1	458.8	31%	3	1,913	233	65
Ascon_Graz-v2	453.2	20%		1,723	216	61
Ascon_VT-v2	438.0	28%		1,928	219	64
COMET_VT-v1	431.5	32%	4	2,449	209	62
DryGASCON-v1	423.1	29%	5	2,074	238	72
Xoodyak_XT-v8	419.9	18%		2,040	187	57
Ascon_Graz-v1	411.6	25%		1,551	209	65
Xoodyak_XT-v2	410.9	18%		2,071	183	57
KNOT-v2x2	408.5	13%	6	1,873	233	73
TinyJAMBU_TJT-v3	404.2	42%	7	576	240	76
KNOT-v2x2h	389.3	13%		2,112	222	73
Romulus-v2	326.1	38%	8	1,280	214	84
Xoodyak_GMU-v1	298.1	17%		1,808	170	73
Gimli_GT-v4	288.5	10%	9	2,510	142	63
PHOTON-Beetle-v1	284.8	41%	10	2,065	178	80
Romulus-v3	281.1	32%		1,824	123	56
Elephant-v2	243.9	36%	11	1,884	181	95
Gimli_GT-v2	240.9	13%		1,909	175	93
GIFT-COFB-v1	231.6	31%	12	1,041	275	152
ESTATE-v1	186.9	58%	13	1,351	222	152
Spook-v2-v2	185.7	17%	14	2,033	206	142
COMET_CI-v3	156.4	38%		1,841	215	176
TinyJAMBU_TJT-v2	153.3	50%		461	315	263
COMET_CI-v1	152.6	37%		1,884	223	187
ForkAE-v2	151.2	64%	15	2,466	228	193
SCHWAEMM-v1	135.0	18%	16*	**3,071**	135	128
TinyJAMBU_GMU-v1	126.6	51%		591	266	269
Oribatida-v1	123.5	48%	17	1,450	276	286
LOCUS-v2	122.2	55%	18	1,628	209	219
Saturnin-v2	118.2	15%	19	2,414	168	182
mixFeed-v1	115.5	25%	20	1,316	204	226
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
LOTUS-v2	82.4	55%		1,487	141	219
TinyJAMBU_GMU-v2	67.4	52%		564	268	509
SpoC-v1	64.7	49%	21	1,079	230	455
ISAP-v2	57.8	12%	22	2,157	200	443
ESTATE-v3	52.5	65%		1,130	259	632
Pyjamask-v2	47.6	18%	23	2,308	213	573
WAGE-v1	38.0	24%	24	1,150	279	940
Saturnin-v1	28.5	23%		2,020	192	862
ACE-v1	24.2	25%	25	1,229	200	1,056
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
ForkAE-v1	8.2	98%		1,191	208	3,264
Gimli_TUM-v2	5.3	25%		905	244	5,922
Average		**32%**				
Minimum		**8%**				
Maximum		**98%**				

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
Xoodyak_GMU2-v1	7,492.1	88%	1	1,608	314	515
Subterranean-v2	5,404.4	89%	2	891	190	432
Xoodyak_GMU2-v2	5,315.9	91%		2,322	199	460
KNOT-v2x4h	3,366.9	90%	3	2,438	137	500
Xoodyak_XT-v8	3,096.8	94%		2,040	187	742
Xoodyak_XT-v2	3,030.6	94%		2,071	183	742
KNOT-v2x2	2,915.6	91%		1,873	233	982
Gimli_GT-v4	2,760.9	91%	4	2,510	142	632
TinyJAMBU_TJT-v3	2,467.9	96%	5	576	240	1,195
Xoodyak_GMU-v1	2,334.0	94%		1,808	170	895
Ascon_Graz-v2	2,195.4	95%	6	1,723	216	1,209
Gimli_GT-v2	1,744.0	93%		1,909	175	1,233
COMET_VT-v1	1,627.5	97%	7	2,449	209	1,578
Ascon_Graz-v1	1,614.2	97%		1,551	209	1,591
Romulus-v2	1,451.2	95%	8	1,280	214	1,812
Ascon_VT-v1	1,451.1	97%		1,913	233	1,973
Saturnin-v2	1,422.7	89%	9	2,414	168	1,451
DryGASCON-v1	1,414.9	98%	10	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%	11	1,884	181	1,943
Spook-v2-v2	1,055.6	96%	12	2,033	206	2,398
SCHWAEMM-v1	869.0	96%	13*	**3,071**	135	1,909
PHOTON-Beetle-v1	799.1	98%	14	2,065	178	2,737
TinyJAMBU_TJT-v2	755.7	97%		461	315	5,122
ISAP-v2	741.8	93%	15	2,157	200	3,313
GIFT-COFB-v1	709.3	99%	16	1,041	275	4,764
ESTATE-v1	636.9	99%	17	1,351	222	4,283
TinyJAMBU_GMU-v1	593.4	98%		591	266	5,508
Oribatida-v1	495.8	97%	18	1,450	276	6,841
Oribatida-v2	487.3	97%		1,450	276	6,960
COMET_CI-v3	481.6	98%		1,841	215	5,486
mixFeed-v1	476.9	97%	19	1,316	204	5,256
COMET_CI-v1	466.3	98%		1,884	223	5,877
LOCUS-v2	438.3	98%	20	1,628	209	5,859
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
LOTUS-v2	295.7	98%		1,487	141	5,859
ForkAE-v2	273.6	99%	21	2,466	228	10,239
Pyjamask-v2	264.7	95%	22	2,308	213	9,887
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
WAGE-v1	150.9	96%	23	1,150	279	22,713
SpoC-v1	133.6	99%	24	1,079	230	21,161
Pyjamask-v1	109.3	96%		1,979	229	25,755
ACE-v1	94.9	96%	25	1,229	200	25,885
Gimli_TUM-v1	38.1	97%		933	241	77,829
ForkAE-v1	22.0	100%		1,191	208	116,127
Gimli_TUM-v2	20.5	97%		905	244	145,945
Average		**96%**				
Minimum		**88%**				
Maximum		**100%**				

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
Xoodyak_GMU2-v1	1,869.4	22%	1	1,608	314	86
Xoodyak_GMU2-v2	1,592.0	27%		2,322	199	64
Subterranean-v2	1,520.0	25%	2	891	190	64
TinyJAMBU_TJT-v3	1,350.3	53%	3	576	240	91
Xoodyak_XT-v8	1,243.4	38%		2,040	187	77
Xoodyak_XT-v2	1,216.8	38%		2,071	183	77
KNOT-v2x4h	1,062.8	28%	4	2,438	137	66
Ascon_Graz-v2	1,053.3	46%	5	1,723	216	105
KNOT-v2x2	1,046.5	33%		1,873	233	114
COMET_VT-v1	1,009.5	60%	6	2,449	209	106
Gimli_GT-v4	908.8	30%	7	2,510	142	80
DryGASCON-v1	902.6	62%	8	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%	9	1,280	214	156
Gimli_GT-v2	694.6	37%		1,909	175	129
Romulus-v3	629.8	44%		1,824	123	100
PHOTON-Beetle-v1	566.1	70%	10	2,065	178	161
Spook-v2-v2	555.1	51%	11	2,033	206	190
Elephant-v2	554.9	46%	12	1,884	181	167
GIFT-COFB-v1	550.0	77%	13	1,041	275	256
ESTATE-v1	483.7	75%	14	1,351	222	235
TinyJAMBU_TJT-v2	477.2	62%		461	315	338
SCHWAEMM-v1	429.3	47%	15*	**3,071**	135	161
Saturnin-v2	411.6	26%	16	2,414	168	209
TinyJAMBU_GMU-v1	382.6	63%		591	266	356
COMET_CI-v3	329.6	67%		1,841	215	334
COMET_CI-v1	319.8	67%		1,884	223	357
LOCUS-v2	315.7	71%	17	1,628	209	339
Oribatida-v1	286.6	56%	18	1,450	276	493
Oribatida-v2	286.1	57%		1,450	276	494
ISAP-v2	277.5	35%	19	2,157	200	369
mixFeed-v1	274.9	56%	20	1,316	204	380
ForkAE-v2	239.7	87%	21	2,466	228	487
COMET_VT-v2	230.0	65%		1,703	234	521
LOTUS-v2	213.0	71%		1,487	141	339
TinyJAMBU_GMU-v2	207.9	63%		564	268	660
Elephant-v1	190.6	46%		1,291	229	615
ESTATE-v3	128.1	79%		1,130	259	1,035
Pyjamask-v2	125.2	45%	22	2,308	213	871
SpoC-v1	106.6	79%	23	1,079	230	1,105
Saturnin-v1	92.8	37%		2,020	192	1,059
WAGE-v1	82.2	53%	24	1,150	279	1,737
Xoodyak_GMU-v2	65.3	29%		1,234	168	1,317
Pyjamask-v1	58.1	51%		1,979	229	2,019
ACE-v1	52.1	53%	25	1,229	200	1,965
Gimli_TUM-v1	22.4	57%		933	241	5,517
ForkAE-v1	21.7	99%		1,191	208	4,899
Gimli_TUM-v2	12.1	57%		905	244	10,337
Average		**53%**				
Minimum		**22%**				
Maximum		**99%**				

Table 30: Xilinx Artix-7 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	558.5	22%	1	576	240	55
Xoodyak_GMU2-v1	550.6	6%	2	1,608	314	73
Xoodyak_GMU2-v2	489.8	8%		2,322	199	52
Subterranean-v2	467.7	8%	3	891	190	52
COMET_VT-v1	461.2	28%	4	2,449	209	58
Xoodyak_XT-v8	427.4	13%		2,040	187	56
DryGASCON-v1	423.1	29%	5	2,074	238	72
Xoodyak_XT-v2	418.3	13%		2,071	183	56
Ascon_VT-v1	408.5	27%	6	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
KNOT-v2x2	346.8	11%	7	1,873	233	86
KNOT-v2x4h	337.2	9%		2,438	137	52
Romulus-v2	326.1	21%	8	1,280	214	84
GIFT-COFB-v1	322.9	45%	9	1,041	275	109
Xoodyak_GMU-v1	298.1	12%		1,808	170	73
PHOTON-Beetle-v1	295.9	36%	10	2,065	178	77
Gimli_GT-v4	293.2	10%	11	2,510	142	62
Romulus-v3	281.1	20%		1,824	123	56
ESTATE-v1	275.9	43%	12	1,351	222	103
Gimli_GT-v2	240.9	13%		1,909	175	93
TinyJAMBU_TJT-v2	221.5	29%		461	315	182
Elephant-v2	194.7	16%	13	1,884	181	119
Spook-v2-v2	185.7	17%	14	2,033	206	142
TinyJAMBU_GMU-v1	181.1	30%		591	266	188
ForkAE-v2	172.7	63%	15	2,466	228	169
LOCUS-v2	168.3	38%	16	1,628	209	159
COMET_CI-v3	165.8	34%		1,841	215	166
COMET_CI-v1	161.3	34%		1,884	223	177
SCHWAEMM-v1	140.5	15%	17*	**3,071**	135	123
Saturnin-v2	138.7	9%	18	2,414	168	155
Oribatida-v2	125.3	25%	19	1,450	276	282
Oribatida-v1	123.5	24%		1,450	276	286
mixFeed-v1	118.2	24%	20	1,316	204	221
LOTUS-v2	113.5	38%		1,487	141	159
COMET_VT-v2	112.6	32%		1,703	234	266
TinyJAMBU_GMU-v2	98.6	30%		564	268	348
ISAP-v2	93.8	12%	21	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%	22	1,079	230	451
Pyjamask-v2	47.3	17%	23	2,308	213	577
Saturnin-v1	37.0	15%		2,020	192	665
WAGE-v1	33.9	22%	24	1,150	279	1,053
Pyjamask-v1	23.5	21%		1,979	229	1,245
ACE-v1	21.6	22%	25	1,229	200	1,185
ForkAE-v1	20.9	95%		1,191	208	1,272
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		**25%**				
Minimum		**6%**				
Maximum		**95%**				

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

Variant	Throughput 1536B [Mbits/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 1536B
Xoodyak_GMU2-v1	2,892.4	44%	1	1,608	314	1,334
Subterranean-v2	2,861.2	47%	2	891	190	816
Xoodyak_GMU2-v2	2,714.0	48%		2,322	199	901
KNOT-v2x2	1,523.7	48%	3	1,873	233	1,879
KNOT-v2x2h	1,451.8	48%		2,112	222	1,879
Gimli_GT-v4	1,444.5	48%	4	2,510	142	1,208
Xoodyak_XT-v8	1,357.3	47%		2,040	187	1,693
Xoodyak_XT-v2	1,328.2	47%		2,071	183	1,693
Ascon_Graz-v2	1,124.2	49%	5	1,723	216	2,361
Xoodyak_GMU-v1	996.2	46%		1,808	170	2,097
Gimli_GT-v2	901.6	48%		1,909	175	2,385
Ascon_Graz-v1	822.9	49%		1,551	209	3,121
Ascon_VT-v1	735.4	49%		1,913	233	3,893
COMET_VT-v1	734.2	49%	6	2,449	209	3,498
Ascon_VT-v2	726.9	49%		1,928	219	3,702
DryGASCON-v1	716.3	49%	7	2,074	238	4,083
TinyJAMBU_TJT-v3	691.1	49%	8	576	240	4,267
Romulus-v2	542.0	49%	9	1,280	214	4,852
Spook-v2-v2	538.4	49%	10	2,033	206	4,702
Romulus-v3	535.6	49%		1,824	123	2,822
Saturnin-v2	508.6	48%	11	2,414	168	4,059
Elephant-v2	426.8	49%	12	1,884	181	5,211
SCHWAEMM-v1	396.8	49%	13*	**3,071**	135	4,181
PHOTON-Beetle-v1	370.4	50%	14	2,065	178	5,905
GIFT-COFB-v1	364.3	50%	15	1,041	275	9,276
ISAP-v2	290.6	48%	16	2,157	200	8,456
mixFeed-v1	232.6	49%	17	1,316	204	10,778
COMET_CI-v3	223.5	50%		1,841	215	11,822
COMET_CI-v1	217.5	50%		1,884	223	12,597
TinyJAMBU_TJT-v2	217.5	50%		461	315	17,795
ESTATE-v1	214.2	50%	18	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%	19	1,450	276	19,995
Oribatida-v2	166.2	50%		1,450	276	20,400
LOCUS-v2	147.8	50%	20	1,628	209	17,379
Elephant-v1	139.8	49%		1,291	229	20,123
Pyjamask-v2	133.0	49%	21	2,308	213	19,680
ForkAE-v2	127.1	50%	22	2,466	228	22,050
LOTUS-v2	99.7	50%		1,487	141	17,379
TinyJAMBU_GMU-v2	92.6	50%		564	268	35,572
Saturnin-v1	81.2	49%		2,020	192	29,049
Xoodyak_GMU-v2	77.8	45%		1,234	168	26,548
WAGE-v1	76.9	49%	23	1,150	279	44,601
SpoC-v1	66.5	50%	24	1,079	230	42,473
Pyjamask-v1	55.3	49%		1,979	229	50,908
ESTATE-v3	54.0	50%		1,130	259	58,976
ACE-v1	48.3	49%	25	1,229	200	50,845
Gimli_TUM-v1	19.3	49%		933	241	153,573
Gimli_TUM-v2	10.4	49%		905	244	288,121
ForkAE-v1	6.0	50%		1,191	208	422,754
Average		**49%**				
Minimum		**44%**				
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**
Xoodyak_GMU2-v1	1,435.4	22%	1	1,608	314	112
Xoodyak_GMU2-v2	1,306.3	23%		2,322	199	78
Subterranean-v2	1,216.0	20%	2	891	190	80
Xoodyak_XT-v8	862.6	30%		2,040	187	111
Xoodyak_XT-v2	844.1	30%		2,071	183	111
KNOT-v2x2	834.2	26%	3	1,873	233	143
KNOT-v2x2h	794.9	26%		2,112	222	143
Ascon_Graz-v2	722.8	31%	4	1,723	216	153
Gimli_GT-v4	699.1	23%	5	2,510	142	104
Xoodyak_GMU-v1	626.2	29%		1,808	170	139
Ascon_Graz-v1	604.6	36%		1,551	209	177
COMET_VT-v1	575.3	39%	6	2,449	209	186
TinyJAMBU_TJT-v3	561.1	40%	7	576	240	219
Ascon_VT-v1	560.1	38%		1,913	233	213
DryGASCON-v1	556.4	38%	8	2,074	238	219
Ascon_VT-v2	544.3	37%		1,928	219	206
Gimli_GT-v2	506.2	27%		1,909	175	177
Romulus-v2	434.8	40%	9	1,280	214	252
Romulus-v3	408.9	38%		1,824	123	154
Spook-v2-v2	368.8	34%	10	2,033	206	286
GIFT-COFB-v1	317.1	43%	11	1,041	275	444
Elephant-v2	313.1	36%	12	1,884	181	296
PHOTON-Beetle-v1	311.0	42%	13	2,065	178	293
Saturnin-v2	258.3	24%	14	2,414	168	333
SCHWAEMM-v1	255.1	31%	15*	**3,071**	135	271
ESTATE-v1	192.0	45%	16	1,351	222	592
TinyJAMBU_TJT-v2	186.0	42%		461	315	867
COMET_CI-v3	184.1	41%		1,841	215	598
COMET_CI-v1	179.2	41%		1,884	223	637
mixFeed-v1	158.7	33%	17	1,316	204	658
TinyJAMBU_GMU-v1	151.3	43%		591	266	900
ISAP-v2	140.7	23%	18	2,157	200	728
COMET_VT-v2	136.6	40%		1,703	234	877
Oribatida-v1	135.5	40%	19	1,450	276	1,043
LOCUS-v2	130.7	44%	20	1,628	209	819
Oribatida-v2	125.7	37%		1,450	276	1,124
ForkAE-v2	118.9	47%	21	2,466	228	982
Elephant-v1	103.9	37%		1,291	229	1,128
LOTUS-v2	88.1	44%		1,487	141	819
Pyjamask-v2	85.2	31%	22	2,308	213	1,280
TinyJAMBU_GMU-v2	80.0	43%		564	268	1,716
SpoC-v1	59.1	44%	23	1,079	230	1,993
WAGE-v1	53.9	34%	24	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
Xoodyak_GMU-v2	46.7	27%		1,234	168	1,842
Pyjamask-v1	38.2	34%		1,979	229	3,068
ACE-v1	34.1	35%	25	1,229	200	3,005
Gimli_TUM-v1	14.2	36%		933	241	8,673
Gimli_TUM-v2	7.7	36%		905	244	16,261
ForkAE-v1	6.0	50%		1,191	208	17,678
Average		**35%**				
Minimum		**20%**				
Maximum		**50%**				

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
Xoodyak_GMU2-v1	550.6	8%	1	1,608	314	73
Xoodyak_GMU2-v2	489.8	9%		2,322	199	52
Subterranean-v2	434.3	7%	2	891	190	56
Xoodyak_XT-v8	398.9	14%		2,040	187	60
Xoodyak_XT-v2	390.4	14%		2,071	183	60
TinyJAMBU_TJT-v3	353.1	25%	3	576	240	87
COMET_VT-v1	343.0	23%	4	2,449	209	78
KNOT-v2x2	342.8	11%	5	1,873	233	87
Ascon_Graz-v2	341.3	15%	6	1,723	216	81
KNOT-v2x4h	330.9	13%		2,438	137	53
Ascon_Graz-v1	330.3	20%		1,551	209	81
DryGASCON-v1	327.6	23%	7	2,074	238	93
Romulus-v2	326.1	30%	8	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
Gimli_GT-v4	267.3	9%	9	2,510	142	68
GIFT-COFB-v1	225.6	31%	10	1,041	275	156
Gimli_GT-v2	213.3	11%		1,909	175	105
PHOTON-Beetle-v1	207.1	28%	11	2,065	178	110
Elephant-v2	194.7	23%	12	1,884	181	119
ESTATE-v1	145.0	34%	13	1,351	222	196
Spook-v2-v2	138.8	13%	14	2,033	206	190
TinyJAMBU_TJT-v2	128.0	29%		461	315	315
COMET_CI-v3	118.6	26%		1,841	215	232
Saturnin-v2	118.2	11%	15	2,414	168	182
COMET_CI-v1	115.6	26%		1,884	223	247
TinyJAMBU_GMU-v1	105.1	30%		591	266	324
ForkAE-v2	98.9	39%	16	2,466	228	295
LOCUS-v2	95.9	32%	17	1,628	209	279
SCHWAEMM-v1	94.9	12%	18*	**3,071**	135	182
COMET_VT-v2	84.4	25%		1,703	234	355
Oribatida-v1	83.1	24%	19	1,450	276	425
mixFeed-v1	79.6	17%	20	1,316	204	328
Oribatida-v2	71.8	21%		1,450	276	492
Elephant-v1	66.8	24%		1,291	229	439
LOTUS-v2	64.7	32%		1,487	141	279
TinyJAMBU_GMU-v2	56.1	30%		564	268	612
ISAP-v2	53.8	9%	21	2,157	200	476
SpoC-v1	43.7	33%	22	1,079	230	673
Pyjamask-v2	40.1	15%	23	2,308	213	680
ESTATE-v3	39.7	37%		1,130	259	836
Saturnin-v1	28.5	17%		2,020	192	862
WAGE-v1	27.9	18%	24	1,150	279	1,281
Xoodyak_GMU-v2	20.4	12%		1,234	168	1,053
Pyjamask-v1	19.4	17%		1,979	229	1,508
ACE-v1	17.7	18%	25	1,229	200	1,445
Gimli_TUM-v1	7.8	20%		933	241	3,948
ForkAE-v1	6.0	49%		1,191	208	4,469
Gimli_TUM-v2	4.2	20%		905	244	7,396
Average		**21%**				
Minimum		**7%**				
Maximum		**49%**				

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

Variant	**Throughput 1536B [Mbits/s]**	**Thr PT 1536B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 1536B**
Subterranean-v2	4,361.2	89%	1	1,285	153.7	433
Xoodyak_GMU2-v1	2,346.0	93%	2	2,575	170.3	892
KNOT-v2x2h	1,777.0	92%	3	2,792	140.1	969
KNOT-v2x2	1,759.1	92%		2,472	138.7	969
Ascon_Graz-v2	1,500.4	96%	4	2,666	146.7	1,201
Gimli_GT-v6	1,274.7	88%	5	4,820	45.2	436
Gimli_GT-v3	1,259.0	92%		3,651	85.8	837
Xoodyak_XT-v1	1,228.4	96%		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
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
Romulus-v2	557.4	98%	8	2,086	141.7	3,124
Spook-v2-v2	556.1	96%	9	3,188	108.5	2,398
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
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-v3	218.9	98%	16	4,379	114.8	6,446
COMET_CI-v1	208.0	98%		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
mixFeed-v1	161.2	97%	19*	**5,323**	74.0	5,641
Oribatida-v2	158.1	99%		2,221	174.5	13,564
ForkAE-v2	153.2	99%	20	3,200	148.1	11,878
Elephant-v1	150.1	98%		2,056	163.1	13,347
LOCUS-v2	140.0	99%	21	2,828	132.4	11,619
LOTUS-v2	105.4	99%		2,445	99.6	11,619
SpoC-v1	95.7	99%	22	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%	23	1,774	159.6	22,600
ESTATE-v3	56.2	99%		2,279	180.2	39,392
Pyjamask-v1	51.6	96%	24*	**8,599**	109.7	26,131
ACE-v1	50.8	97%	25	1,903	106.5	25,756
ForkAE-v1	5.4	100%		2,129	135.7	306,694
Average		**97%**				
Minimum		**88%**				
Maximum		**100%**				

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

Variant	Through-put 64B [Mbits/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 64B
Subterranean-v2	1,210.5	25%	1	1,285	153.7	65
Xoodyak_GMU2-v1	880.7	35%	2	2,575	170.3	99
Ascon_Graz-v2	774.1	49%	3	2,666	146.7	97
Ascon_VT-v2	746.3	61%		2,695	172.0	118
KNOT-v2x4	725.7	48%	4	3,519	102.0	72
Ascon_VT-v1	723.4	64%		2,432	176.6	125
KNOT-v2x4h	722.1	48%		3,678	101.5	72
Ascon_Graz-v1	692.3	57%		2,484	152.8	113
Xoodyak_XT-v1	585.1	46%		2,282	140.6	123
Xoodyak_XT-v7	557.1	46%		2,253	133.8	123
DryGASCON-v1	495.0	62%	5	3,199	130.5	135
Xoodyak_GMU-v1	492.6	46%		3,135	106.8	111
TinyJAMBU_TJT-v3	475.4	74%	6	1,021	159.7	172
Gimli_GT-v2	455.6	37%	7	3,145	114.8	129
Gimli_GT-v3	434.7	32%		3,651	85.8	101
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-v2	292.4	51%	11	3,188	108.5	190
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
COMET_CI-v3	157.2	71%	15	4,379	114.8	374
TinyJAMBU_TJT-v2	152.5	80%		777	196.2	659
COMET_CI-v1	149.3	71%		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
ForkAE-v2	134.9	88%	18	3,200	148.1	562
ISAP-v1	124.2	29%	19	4,589	126.6	522
Oribatida-v2	118.5	74%		2,221	174.5	754
LOCUS-v2	117.1	83%	20	2,828	132.4	579
ISAP-v2	116.6	35%		3,852	136.4	599
Elephant-v1	96.6	63%		2,056	163.1	864
mixFeed-v1	95.4	57%	21*	**5,323**	74.0	397
LOTUS-v2	88.1	83%		2,445	99.6	579
TinyJAMBU_GMU-v2	77.2	81%		841	196.2	1,301
SpoC-v1	76.6	79%	22	1,696	167.7	1,121
Saturnin-v1	50.5	54%		3,802	145.0	1,469
WAGE-v1	50.3	56%	23	1,774	159.6	1,624
ESTATE-v3	49.7	88%		2,279	180.2	1,856
ACE-v1	29.7	57%	24	1,903	106.5	1,836
Pyjamask-v1	27.7	52%	25*	**8,599**	109.7	2,027
ForkAE-v1	5.4	99%		2,129	135.7	12,846
Average		**61%**				
Minimum		**25%**				
Maximum		**99%**				

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-v2	371.2	8%	1	1,285	153.7	53
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
Xoodyak_GMU2-v1	298.6	12%	3	2,575	170.3	73
KNOT-v2x4	284.0	19%	4	3,519	102.0	46
KNOT-v2x4h	282.5	19%		3,678	101.5	46
TinyJAMBU_TJT-v3	269.0	42%	5	1,021	159.7	76
DryGASCON-v1	232.1	29%	6	3,199	130.5	72
Xoodyak_XT-v1	222.1	17%		2,282	140.6	81
Romulus-v2	215.9	38%	7	2,086	141.7	84
Xoodyak_XT-v7	211.5	17%		2,253	133.8	81
PHOTON-Beetle-v1	200.7	41%	8	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
Gimli_GT-v2	158.0	13%	9	3,145	114.8	93
GIFT-COFB-v1	155.3	31%	10	1,877	184.4	152
Elephant-v2	152.5	36%	11	2,729	113.2	95
Gimli_GT-v3	142.6	10%		3,651	85.8	77
ESTATE-v1	99.4	58%	12	3,839	118.0	152
ForkAE-v2	98.2	64%	13	3,200	148.1	193
Spook-v2-v2	97.8	17%	14	3,188	108.5	142
TinyJAMBU_TJT-v2	95.5	50%		777	196.2	263
TinyJAMBU_GMU-v1	93.6	51%		856	196.8	269
COMET_CI-v3	83.5	38%	15	4,379	114.8	176
Oribatida-v1	83.1	48%	16	2,512	185.7	286
SCHWAEMM-v1	81.8	18%	17	4,713	81.8	128
COMET_CI-v1	79.2	37%		4,663	115.8	187
LOCUS-v2	77.4	55%	18	2,828	132.4	219
Saturnin-v2	73.5	15%	19	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
LOTUS-v2	58.2	55%		2,445	99.6	219
TinyJAMBU_GMU-v2	49.3	52%		841	196.2	509
SpoC-v1	47.2	49%	20	1,696	167.7	455
mixFeed-v1	41.9	25%	21*	**5,323**	74.0	226
ISAP-v1	40.3	9%	22	4,589	126.6	402
ISAP-v2	39.4	12%		3,852	136.4	443
ESTATE-v3	36.5	65%		2,279	180.2	632
WAGE-v1	21.7	24%	23	1,774	159.6	940
Saturnin-v1	21.5	23%		3,802	145.0	862
ACE-v1	12.9	25%	24	1,903	106.5	1,056
Pyjamask-v1	11.3	21%	25*	**8,599**	109.7	1,241
ForkAE-v1	5.3	98%		2,129	135.7	3,264
Average		**33%**				
Minimum		**8%**				
Maximum		**98%**				

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-v2	4,371.3	89%	1	1,285	153.7	432
Xoodyak_GMU2-v1	4,063.4	88%	2	2,575	170.3	515
KNOT-v2x4	2,508.0	90%	3	3,519	102.0	500
KNOT-v2x4h	2,495.4	90%		3,678	101.5	500
Xoodyak_XT-v1	1,780.5	94%		2,282	140.6	970
Xoodyak_XT-v7	1,695.4	94%		2,253	133.8	970
TinyJAMBU_TJT-v3	1,642.1	96%	4	1,021	159.7	1,195
Ascon_Graz-v2	1,490.5	95%	5	2,666	146.7	1,209
Xoodyak_GMU-v1	1,466.2	94%		3,135	106.8	895
Gimli_GT-v6	1,274.7	88%	6	4,820	45.2	436
Gimli_GT-v3	1,257.5	92%		3,651	85.8	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
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
PHOTON-Beetle-v1	563.2	98%	12	3,602	125.4	2,737
Spook-v2-v2	556.1	96%	13	3,188	108.5	2,398
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
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
LOCUS-v2	277.7	98%	18	2,828	132.4	5,859
COMET_CI-v3	257.2	98%	19	4,379	114.8	5,486
COMET_CI-v1	242.0	98%		4,663	115.8	5,877
TinyJAMBU_GMU-v2	235.7	98%		841	196.2	10,228
LOTUS-v2	209.0	98%		2,445	99.6	5,859
ForkAE-v2	177.7	99%	20	3,200	148.1	10,239
Saturnin-v1	176.0	93%		3,802	145.0	10,121
mixFeed-v1	173.0	97%	21*	**5,323**	74.0	5,256
ESTATE-v3	111.8	99%		2,279	180.2	19,803
SpoC-v1	97.4	99%	22	1,696	167.7	21,161
WAGE-v1	86.3	96%	23	1,774	159.6	22,713
Pyjamask-v1	52.3	96%	24*	**8,599**	109.7	25,755
ACE-v1	50.6	96%	25	1,903	106.5	25,885
ForkAE-v1	14.4	100%		2,129	135.7	116,127
Average		**95%**				
Minimum		**88%**				
Maximum		**100%**				

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

Variant	**Through-put 64B [Mbits/s]**	**Thr AD 64B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 64B**
Subterranean-v2	1,229.4	25%	1	1,285	153.7	64
Xoodyak_GMU2-v1	1,013.9	22%	2	2,575	170.3	86
TinyJAMBU_TJT-v3	898.5	53%	3	1,021	159.7	91
KNOT-v2x4	791.7	28%	4	3,519	102.0	66
KNOT-v2x4h	787.7	28%		3,678	101.5	66
Ascon_Graz-v2	715.1	46%	5	2,666	146.7	105
Ascon_VT-v1	679.9	60%		2,432	176.6	133
Xoodyak_XT-v1	672.5	35%		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%	6	3,199	130.5	135
Romulus-v2	465.1	46%	7	2,086	141.7	156
Gimli_GT-v2	455.6	37%	8	3,145	114.8	129
Gimli_GT-v3	430.5	31%		3,651	85.8	102
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
TinyJAMBU_TJT-v2	297.2	62%		777	196.2	338
Spook-v2-v2	292.4	51%	12	3,188	108.5	190
TinyJAMBU_GMU-v1	283.1	63%		856	196.8	356
SCHWAEMM-v1	260.0	47%	13	4,713	81.8	161
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
LOCUS-v2	200.0	71%	17	2,828	132.4	339
Oribatida-v1	192.8	56%	18	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-v3	176.0	67%	19	4,379	114.8	334
COMET_CI-v1	166.0	67%		4,663	115.8	357
ForkAE-v2	155.7	87%	20	3,200	148.1	487
TinyJAMBU_GMU-v2	152.2	63%		841	196.2	660
LOTUS-v2	150.5	71%		2,445	99.6	339
Elephant-v1	135.7	46%		2,056	163.1	615
mixFeed-v1	99.7	56%	21*	**5,323**	74.0	380
ESTATE-v3	89.1	79%		2,279	180.2	1,035
SpoC-v1	77.7	79%	22	1,696	167.7	1,105
Saturnin-v1	70.1	37%		3,802	145.0	1,059
WAGE-v1	47.0	53%	23	1,774	159.6	1,737
Pyjamask-v1	27.8	51%	24*	**8,599**	109.7	2,019
ACE-v1	27.8	53%	25	1,903	106.5	1,965
ForkAE-v1	14.2	99%		2,129	135.7	4,899
Average		**53%**				
Minimum		**22%**				
Maximum		**99%**				

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-v2	378.3	8%	1	1,285	153.7	52
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
Xoodyak_GMU2-v1	298.6	6%	4	2,575	170.3	73
Ascon_Graz-v1	275.5	23%		2,484	152.8	71
Ascon_Graz-v2	272.0	17%		2,666	146.7	69
KNOT-v2x4	251.2	9%	5	3,519	102.0	52
KNOT-v2x4h	249.9	9%		3,678	101.5	52
DryGASCON-v1	232.1	29%	6	3,199	130.5	72
Xoodyak_XT-v1	224.9	12%		2,282	140.6	80
GIFT-COFB-v1	216.5	45%	7	1,877	184.4	109
Romulus-v2	215.9	21%	8	2,086	141.7	84
Xoodyak_XT-v7	214.1	12%		2,253	133.8	80
PHOTON-Beetle-v1	208.5	36%	9	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	158.0	13%	10	3,145	114.8	93
ESTATE-v1	146.6	43%	11	3,839	118.0	103
Gimli_GT-v3	140.7	10%		3,651	85.8	78
TinyJAMBU_TJT-v2	138.0	29%		777	196.2	182
TinyJAMBU_GMU-v1	134.0	30%		856	196.8	188
Elephant-v2	121.7	16%	12	2,729	113.2	119
ForkAE-v2	112.2	63%	13	3,200	148.1	169
LOCUS-v2	106.6	38%	14	2,828	132.4	159
Spook-v2-v2	97.8	17%	15	3,188	108.5	142
COMET_CI-v3	88.6	34%	16	4,379	114.8	166
Saturnin-v2	86.3	9%	17	3,892	104.6	155
SCHWAEMM-v1	85.1	15%	18	4,713	81.8	123
COMET_CI-v1	83.7	34%		4,663	115.8	177
Oribatida-v1	83.1	24%	19	2,512	185.7	286
LOTUS-v2	80.2	38%		2,445	99.6	159
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%	20	4,589	126.6	244
ISAP-v2	63.9	12%		3,852	136.4	273
ESTATE-v3	54.5	48%		2,279	180.2	423
SpoC-v1	47.6	48%	21	1,696	167.7	451
Elephant-v1	47.5	16%		2,056	163.1	439
mixFeed-v1	42.9	24%	22*	**5,323**	74.0	221
Saturnin-v1	27.9	15%		3,802	145.0	665
WAGE-v1	19.4	22%	23	1,774	159.6	1,053
ForkAE-v1	13.7	95%		2,129	135.7	1,272
ACE-v1	11.5	22%	24	1,903	106.5	1,185
Pyjamask-v1	11.3	21%	25*	**8,599**	109.7	1,245
Average		**25%**				
Minimum		**6%**				
Maximum		**95%**				

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

Variant	**Through-put 64B [Mbits/s]**	**Thr AD+PT 64B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 64B**
Subterranean-v2	983.6	20%	1	1,285	153.7	80
Xoodyak_GMU2-v1	778.5	22%	2	2,575	170.3	112
KNOT-v2x4	561.8	29%	3	3,519	102.0	93
KNOT-v2x4h	559.0	29%		3,678	101.5	93
Ascon_Graz-v2	490.8	31%	4	2,666	146.7	153
Xoodyak_XT-v1	470.3	29%		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%	5	1,021	159.7	219
Gimli_GT-v2	332.1	27%	6	3,145	114.8	177
Gimli_GT-v3	327.7	24%		3,651	85.8	134
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
Elephant-v2	195.7	36%	11	2,729	113.2	296
Spook-v2-v2	194.3	34%	12	3,188	108.5	286
Saturnin-v2	160.8	24%	13	3,892	104.6	333
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
COMET_CI-v3	98.3	41%	17	4,379	114.8	598
ISAP-v2	95.9	23%		3,852	136.4	728
COMET_CI-v1	93.0	41%		4,663	115.8	637
Oribatida-v1	91.1	40%	18	2,512	185.7	1,043
LOCUS-v2	82.8	44%	19	2,828	132.4	819
Oribatida-v2	79.5	37%		2,221	174.5	1,124
ForkAE-v2	77.2	47%	20	3,200	148.1	982
Elephant-v1	74.0	37%		2,056	163.1	1,128
LOTUS-v2	62.3	44%		2,445	99.6	819
TinyJAMBU_GMU-v2	58.5	43%		841	196.2	1,716
mixFeed-v1	57.6	33%	21*	**5,323**	74.0	658
SpoC-v1	43.1	44%	22	1,696	167.7	1,993
Saturnin-v1	39.8	32%		3,802	145.0	1,863
ESTATE-v3	34.5	46%		2,279	180.2	2,672
WAGE-v1	30.8	34%	23	1,774	159.6	2,649
Pyjamask-v1	18.3	34%	24*	**8,599**	109.7	3,068
ACE-v1	18.1	35%	25	1,903	106.5	3,005
ForkAE-v1	3.9	50%		2,129	135.7	17,678
Average		**36%**				
Minimum		**20%**				
Maximum		**50%**				

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

Variant	Through-put 1536B [Mbits/s]	Thr AD+PT 1536B / Thr Long	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per 1536B
Subterranean-v2	2,314.2	47%	1	1,285	153.7	816
Xoodyak_GMU2-v1	1,568.7	44%	2	2,575	170.3	1,334
KNOT-v2x4	940.7	48%	3	3,519	102.0	1,333
KNOT-v2x4h	936.0	48%		3,678	101.5	1,333
Ascon_Graz-v2	763.3	49%	4	2,666	146.7	2,361
Xoodyak_XT-v1	751.2	46%		2,282	140.6	2,299
Xoodyak_XT-v7	715.3	46%		2,253	133.8	2,299
Gimli_GT-v6	679.4	47%	5	4,820	45.2	818
Gimli_GT-v3	656.2	48%		3,651	85.8	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
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-v2	283.6	49%	10	3,188	108.5	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
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
COMET_CI-v3	119.4	50%	16	4,379	114.8	11,822
Oribatida-v1	114.1	49%	17	2,512	185.7	19,995
ESTATE-v1	113.8	50%	18	3,839	118.0	12,736
COMET_CI-v1	112.9	50%		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
LOCUS-v2	93.6	50%	19	2,828	132.4	17,379
mixFeed-v1	84.4	49%	20*	**5,323**	74.0	10,778
ForkAE-v2	82.5	50%	21	3,200	148.1	22,050
LOTUS-v2	70.5	50%		2,445	99.6	17,379
TinyJAMBU_GMU-v2	67.8	50%		841	196.2	35,572
Saturnin-v1	61.3	49%		3,802	145.0	29,049
SpoC-v1	48.5	50%	22	1,696	167.7	42,473
WAGE-v1	44.0	49%	23	1,774	159.6	44,601
ESTATE-v3	37.5	50%		2,279	180.2	58,976
Pyjamask-v1	26.5	49%	24*	**8,599**	109.7	50,908
ACE-v1	25.7	49%	25	1,903	106.5	50,845
ForkAE-v1	3.9	50%		2,129	135.7	422,754
Average		**49%**				
Minimum		**44%**				
Maximum		**50%**				

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

Variant	**Through-put 16B [Mbits/s]**	**Thr AD+PT 16B / Thr Long**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per 16B**
Subterranean-v2	351.3	7%	1	1,285	153.7	56
Xoodyak_GMU2-v1	298.6	8%	2	2,575	170.3	73
KNOT-v2x4	246.5	13%	3	3,519	102.0	53
KNOT-v2x4h	245.2	13%		3,678	101.5	53
Ascon_VT-v1	243.1	22%	4	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%	5	1,021	159.7	87
Ascon_Graz-v2	231.7	15%		2,666	146.7	81
Romulus-v2	215.9	30%	6	2,086	141.7	84
Xoodyak_XT-v1	214.2	13%		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%	7	3,199	130.5	93
GIFT-COFB-v1	151.3	31%	8	1,877	184.4	156
PHOTON-Beetle-v1	146.0	28%	9	3,602	125.4	110
Gimli_GT-v2	139.9	11%	10	3,145	114.8	105
Gimli_GT-v3	127.6	9%		3,651	85.8	86
Elephant-v2	121.7	23%	11	2,729	113.2	119
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
Saturnin-v2	73.5	11%	13	3,892	104.6	182
Spook-v2-v2	73.1	13%	14	3,188	108.5	190
ForkAE-v2	64.3	39%	15	3,200	148.1	295
COMET_CI-v3	63.4	26%	16	4,379	114.8	232
LOCUS-v2	60.8	32%	17	2,828	132.4	279
COMET_CI-v1	60.0	26%		4,663	115.8	247
SCHWAEMM-v1	57.5	12%	18	4,713	81.8	182
Oribatida-v1	55.9	24%	19	2,512	185.7	425
Elephant-v1	47.5	24%		2,056	163.1	439
LOTUS-v2	45.7	32%		2,445	99.6	279
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%	20	4,589	126.6	411
ISAP-v2	36.7	9%		3,852	136.4	476
SpoC-v1	31.9	33%	21	1,696	167.7	673
mixFeed-v1	28.9	17%	22*	**5,323**	74.0	328
ESTATE-v3	27.6	37%		2,279	180.2	836
Saturnin-v1	21.5	17%		3,802	145.0	862
WAGE-v1	15.9	18%	23	1,774	159.6	1,281
ACE-v1	9.4	18%	24	1,903	106.5	1,445
Pyjamask-v1	9.3	17%	25*	**8,599**	109.7	1,508
ForkAE-v1	3.9	49%		2,129	135.7	4,469
Average		**21%**				
Minimum		**7%**				
Maximum		**49%**				

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-v2	2,716.7	89%	1	613	95.7	433
Xoodyak_GMU2-v1	2,073.0	93%	2	3,248	150.5	892
Xoodyak_GMU2-v2	1,716.3	91%		4,077	68.9	493
Gimli_GT-v4	1,178.9	91%	3	4,027	60.7	633
KNOT-v2x2	1,146.5	92%	4	3,287	90.4	969
KNOT-v2x2h	954.9	92%		3,373	75.3	969
Xoodyak_XT-v2	865.3	96%		4,302	70.7	1,004
Gimli_GT-v3	817.0	92%		4,451	55.6	837
Xoodyak_XT-v8	808.1	96%		3,507	66.0	1,004
Xoodyak_GMU-v1	714.9	96%		3,172	74.0	1,272
Ascon_Graz-v2	646.7	96%	5	3,847	63.2	1,201
DryGASCON-v1	597.6	98%	6	3,801	100.5	2,067
Ascon_VT-v1	530.9	98%		3,130	84.9	1,965
Ascon_VT-v2	514.0	97%		3,256	74.2	1,774
Ascon_Graz-v1	489.7	97%		2,947	63.2	1,585
TinyJAMBU_TJT-v3	455.0	99%	7	1,092	115.4	3,116
Spook-v2-v2	394.6	96%	8	3,662	77.0	2,398
PHOTON-Beetle-v1	387.7	99%	9	3,294	101.4	3,215
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-v2	322.5	98%	12	2,353	82.0	3,124
Romulus-v3	313.1	98%		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
Oribatida-v1	163.0	99%	15	1,671	176.5	13,301
ESTATE-v1	157.4	99%	16	2,855	109.0	8,512
COMET_VT-v2	157.0	98%	17	2,353	111.5	8,725
ISAP-v2	155.1	93%	18*	**5,708**	68.0	5,384
COMET_CI-v3	152.5	98%		3,443	80.0	6,446
COMET_CI-v1	145.4	98%		3,255	80.9	6,837
TinyJAMBU_TJT-v2	120.4	99%		689	125.4	12,803
TinyJAMBU_GMU-v1	116.3	99%		720	124.8	13,189
Oribatida-v2	103.5	99%		2,497	114.2	13,564
ForkAE-v2	93.1	99%	19	3,571	90.0	11,878
Elephant-v1	89.8	98%		2,368	97.5	13,347
Pyjamask-v2	87.6	95%	20	4,162	73.2	10,263
mixFeed-v1	84.7	97%	21	3,479	38.9	5,641
LOCUS-v2	76.7	99%	22	2,950	72.5	11,619
TinyJAMBU_GMU-v2	61.6	99%		908	128.3	25,589
Saturnin-v1	59.0	97%		3,093	94.0	19,593
SpoC-v1	56.0	99%	23	2,049	98.2	21,545
LOTUS-v2	55.7	99%		2,208	52.7	11,619
WAGE-v1	55.2	97%	24	2,081	101.6	22,600
Xoodyak_GMU-v2	52.5	95%		2,316	74.8	17,495
Pyjamask-v1	43.6	96%		3,897	92.7	26,131
ACE-v1	35.2	97%	25	2,156	73.8	25,756
ESTATE-v3	33.4	99%		1,820	107.1	39,392
ForkAE-v1	2.7	100%		2,022	67.9	306,694
Average		**97%**				
Minimum		**89%**				
Maximum		**100%**				

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

Variant	Throughput 64B [Mbits/s]	Thr PT 64B / Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per 64B
Xoodyak_GMU2-v1	778.2	35%	1	3,248	150.5	99
Subterranean-v2	754.1	25%	2	613	95.7	65
Xoodyak_GMU2-v2	534.2	28%		4,077	68.9	66
KNOT-v2x2	458.3	37%	3	3,287	90.4	101
KNOT-v2x4	449.5	48%		3,984	63.2	72
Xoodyak_XT-v2	416.1	46%		4,302	70.7	87
Xoodyak_XT-v8	388.6	46%		3,507	66.0	87
Gimli_GT-v4	383.9	30%	4	4,027	60.7	81
DryGASCON-v1	381.3	62%	5	3,801	100.5	135
Ascon_VT-v1	347.8	64%	6	3,130	84.9	125
TinyJAMBU_TJT-v3	343.5	74%	7	1,092	115.4	172
Xoodyak_GMU-v1	341.3	46%		3,172	74.0	111
Ascon_Graz-v2	333.6	49%		3,847	63.2	97
Ascon_VT-v2	322.0	61%		3,256	74.2	118
Gimli_GT-v2	302.4	37%		2,852	76.2	129
PHOTON-Beetle-v1	290.2	74%	8	3,294	101.4	179
Ascon_Graz-v1	286.2	57%		2,947	63.2	113
Romulus-v2	233.2	71%	9	2,353	82.0	180
Romulus-v3	209.5	65%		3,847	45.0	110
Spook-v2-v2	207.5	51%	10	3,662	77.0	190
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
Saturnin-v2	139.7	39%	14	3,326	76.1	279
ESTATE-v1	134.2	85%	15	2,855	109.0	416
Oribatida-v1	129.6	79%	16	1,671	176.5	697
COMET_CI-v3	109.5	71%	17	3,443	80.0	374
COMET_VT-v2	106.3	66%		2,353	111.5	537
COMET_CI-v1	104.3	71%		3,255	80.9	397
TinyJAMBU_TJT-v2	97.4	80%		689	125.4	659
TinyJAMBU_GMU-v1	94.4	80%		720	124.8	677
ForkAE-v2	82.0	88%	18	3,571	90.0	562
Oribatida-v2	77.5	74%		2,497	114.2	754
LOCUS-v2	64.1	83%	19	2,950	72.5	579
ISAP-v2	58.1	35%	20*	**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
mixFeed-v1	50.2	57%	21	3,479	38.9	397
LOTUS-v2	46.6	83%		2,208	52.7	579
SpoC-v1	44.9	79%	22	2,049	98.2	1,121
Pyjamask-v2	42.6	46%	23	4,162	73.2	879
Saturnin-v1	32.8	54%		3,093	94.0	1,469
WAGE-v1	32.0	56%	24	2,081	101.6	1,624
ESTATE-v3	29.6	88%		1,820	107.1	1,856
Xoodyak_GMU-v2	24.4	44%		2,316	74.8	1,572
Pyjamask-v1	23.4	52%		3,897	92.7	2,027
ACE-v1	20.6	57%	25	2,156	73.8	1,836
ForkAE-v1	2.7	99%		2,022	67.9	12,846
Average		**60%**				
Minimum		**25%**				
Maximum		**99%**				

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
Xoodyak_GMU2-v1	263.9	12%	1	3,248	150.5	73
Subterranean-v2	231.2	8%	2	613	95.7	53
TinyJAMBU_TJT-v3	194.3	42%	3	1,092	115.4	76
DryGASCON-v1	178.7	29%	4	3,801	100.5	72
KNOT-v2x4	175.9	19%	5	3,984	63.2	46
Xoodyak_GMU2-v2	169.5	9%		4,077	68.9	52
KNOT-v2x4h	169.4	19%		4,283	60.9	46
Ascon_VT-v1	167.2	31%	6	3,130	84.9	65
PHOTON-Beetle-v1	162.3	41%	7	3,294	101.4	80
Xoodyak_XT-v2	158.8	18%		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
Ascon_Graz-v2	132.6	20%		3,847	63.2	61
Xoodyak_GMU-v1	129.8	17%		3,172	74.0	73
Romulus-v2	125.0	38%	8	2,353	82.0	84
Ascon_Graz-v1	124.4	25%		2,947	63.2	65
Gimli_GT-v4	123.4	10%	9	4,027	60.7	63
Elephant-v2	115.2	36%	10	3,073	85.5	95
Gimli_GT-v2	104.9	13%		2,852	76.2	93
Romulus-v3	102.9	32%		3,847	45.0	56
GIFT-COFB-v1	96.3	31%	11	2,214	114.3	152
ESTATE-v1	91.8	58%	12	2,855	109.0	152
Oribatida-v1	79.0	48%	13	1,671	176.5	286
Spook-v2-v2	69.4	17%	14	3,662	77.0	142
SCHWAEMM-v1	66.3	18%	15	4,685	66.3	128
TinyJAMBU_TJT-v2	61.0	50%		689	125.4	263
ForkAE-v2	59.7	64%	16	3,571	90.0	193
TinyJAMBU_GMU-v1	59.4	51%		720	124.8	269
COMET_CI-v3	58.2	38%	17	3,443	80.0	176
COMET_CI-v1	55.4	37%		3,255	80.9	187
Saturnin-v2	53.5	15%	18	3,326	76.1	182
COMET_VT-v2	52.8	33%		2,353	111.5	270
Oribatida-v2	43.8	42%		2,497	114.2	334
LOCUS-v2	42.4	55%	19	2,950	72.5	219
Elephant-v1	35.6	39%		2,368	97.5	351
TinyJAMBU_GMU-v2	32.3	52%		908	128.3	509
LOTUS-v2	30.8	55%		2,208	52.7	219
SpoC-v1	27.6	49%	20	2,049	98.2	455
mixFeed-v1	22.0	25%	21	3,479	38.9	226
ESTATE-v3	21.7	65%		1,820	107.1	632
ISAP-v2	19.6	12%	22*	**5,708**	68.0	443
Pyjamask-v2	16.4	18%	23	4,162	73.2	573
Saturnin-v1	14.0	23%		3,093	94.0	862
WAGE-v1	13.8	24%	24	2,081	101.6	940
Pyjamask-v1	9.6	21%		3,897	92.7	1,241
Xoodyak_GMU-v2	9.1	17%		2,316	74.8	1,050
ACE-v1	8.9	25%	25	2,156	73.8	1,056
ForkAE-v1	2.7	98%		2,022	67.9	3,264
Average		**32%**				
Minimum		**8%**				
Maximum		**98%**				

Table 46: Lattice ECP5 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
Xoodyak_GMU2-v1	3,590.5	88%	1	3,248	150.5	515
Subterranean-v2	2,723.0	89%	2	613	95.7	432
Xoodyak_GMU2-v2	1,839.5	91%		4,077	68.9	460
KNOT-v2x4	1,553.4	90%	3	3,984	63.2	500
KNOT-v2x4h	1,495.9	90%		4,283	60.9	500
TinyJAMBU_TJT-v3	1,186.5	96%	4	1,092	115.4	1,195
Gimli_GT-v4	1,180.8	91%	5	4,027	60.7	632
Xoodyak_XT-v2	1,170.8	94%		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
Gimli_GT-v3	816.0	92%		4,451	55.6	838
Saturnin-v2	644.5	89%	6	3,326	76.1	1,451
Ascon_Graz-v2	642.5	95%	7	3,847	63.2	1,209
DryGASCON-v1	597.6	98%	8	3,801	100.5	2,067
Romulus-v2	556.1	95%	9	2,353	82.0	1,812
Elephant-v2	540.7	95%	10	3,073	85.5	1,943
Ascon_VT-v1	528.8	97%		3,130	84.9	1,973
Romulus-v3	497.3	95%		3,847	45.0	1,112
Ascon_Graz-v1	487.9	97%		2,947	63.2	1,591
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
SCHWAEMM-v1	427.0	96%	12	4,685	66.3	1,909
Spook-v2-v2	394.6	96%	13	3,662	77.0	2,398
Oribatida-v1	317.0	97%	14	1,671	176.5	6,841
ESTATE-v1	312.8	99%	15	2,855	109.0	4,283
TinyJAMBU_TJT-v2	300.9	97%		689	125.4	5,122
GIFT-COFB-v1	294.8	99%	16	2,214	114.3	4,764
TinyJAMBU_GMU-v1	278.4	98%		720	124.8	5,508
ISAP-v2	252.1	93%	17*	**5,708**	68.0	3,313
Oribatida-v2	201.6	97%		2,497	114.2	6,960
COMET_CI-v3	179.2	98%	18	3,443	80.0	5,486
COMET_CI-v1	169.2	98%		3,255	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
LOCUS-v2	152.1	98%	19	2,950	72.5	5,859
Saturnin-v1	114.1	93%		3,093	94.0	10,121
LOTUS-v2	110.5	98%		2,208	52.7	5,859
ForkAE-v2	108.0	99%	20	3,571	90.0	10,239
Xoodyak_GMU-v2	91.0	92%		2,316	74.8	10,100
Pyjamask-v2	91.0	95%	21	4,162	73.2	9,887
mixFeed-v1	90.9	97%	22	3,479	38.9	5,256
ESTATE-v3	66.5	99%		1,820	107.1	19,803
SpoC-v1	57.0	99%	23	2,049	98.2	21,161
WAGE-v1	54.9	96%	24	2,081	101.6	22,713
Pyjamask-v1	44.2	96%		3,897	92.7	25,755
ACE-v1	35.0	96%	25	2,156	73.8	25,885
ForkAE-v1	7.2	100%		2,022	67.9	116,127
Average		**95%**				
Minimum		**88%**				
Maximum		**100%**				

Table 47: Lattice ECP5 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
Xoodyak_GMU2-v1	895.9	22%	1	3,248	150.5	86
Subterranean-v2	765.8	25%	2	613	95.7	64
TinyJAMBU_TJT-v3	649.2	53%	3	1,092	115.4	91
Xoodyak_GMU2-v2	550.9	27%		4,077	68.9	64
KNOT-v2x4	490.4	28%	4	3,984	63.2	66
KNOT-v2x4h	472.2	28%		4,283	60.9	66
Xoodyak_XT-v2	470.1	38%		4,302	70.7	77
Xoodyak_XT-v8	439.1	38%		3,507	66.0	77
Gimli_GT-v4	388.7	30%	5	4,027	60.7	80
Xoodyak_GMU-v1	386.6	36%		3,172	74.0	98
DryGASCON-v1	381.3	62%	6	3,801	100.5	135
Ascon_VT-v1	326.8	60%	7	3,130	84.9	133
PHOTON-Beetle-v1	322.6	70%	8	3,294	101.4	161
Ascon_Graz-v2	308.2	46%		3,847	63.2	105
Gimli_GT-v2	302.4	37%		2,852	76.2	129
Ascon_VT-v2	285.6	60%		3,256	74.2	133
Ascon_Graz-v1	271.8	54%		2,947	63.2	119
Romulus-v2	269.1	46%	9	2,353	82.0	156
Elephant-v2	262.1	46%	10	3,073	85.5	167
ESTATE-v1	237.5	75%	11	2,855	109.0	235
Romulus-v3	230.4	44%		3,847	45.0	100
GIFT-COFB-v1	228.6	77%	12	2,214	114.3	256
SCHWAEMM-v1	211.0	47%	13	4,685	66.3	161
Spook-v2-v2	207.5	51%	14	3,662	77.0	190
TinyJAMBU_TJT-v2	190.0	62%		689	125.4	338
Saturnin-v2	186.4	26%	15	3,326	76.1	209
Oribatida-v1	183.3	56%	16	1,671	176.5	493
TinyJAMBU_GMU-v1	179.5	63%		720	124.8	356
COMET_CI-v3	122.6	67%	17	3,443	80.0	334
Oribatida-v2	118.4	57%		2,497	114.2	494
COMET_CI-v1	116.0	67%		3,255	80.9	357
COMET_VT-v2	109.5	65%		2,353	111.5	521
LOCUS-v2	109.5	71%	18	2,950	72.5	339
TinyJAMBU_GMU-v2	99.5	63%		908	128.3	660
ForkAE-v2	94.6	87%	19	3,571	90.0	487
ISAP-v2	94.3	35%	20*	**5,708**	68.0	369
Elephant-v1	81.2	46%		2,368	97.5	615
LOTUS-v2	79.5	71%		2,208	52.7	339
ESTATE-v3	53.0	79%		1,820	107.1	1,035
mixFeed-v1	52.4	56%	21	3,479	38.9	380
SpoC-v1	45.5	79%	22	2,049	98.2	1,105
Saturnin-v1	45.5	37%		3,093	94.0	1,059
Pyjamask-v2	43.0	45%	23	4,162	73.2	871
WAGE-v1	29.9	53%	24	2,081	101.6	1,737
Xoodyak_GMU-v2	29.1	29%		2,316	74.8	1,317
Pyjamask-v1	23.5	51%		3,897	92.7	2,019
ACE-v1	19.2	53%	25	2,156	73.8	1,965
ForkAE-v1	7.1	99%		2,022	67.9	4,899
Average		**52%**				
Minimum		**22%**				
Maximum		**99%**				

Table 48: Lattice ECP5 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	268.5	22%	1	1,092	115.4	55
Xoodyak_GMU2-v1	263.9	6%	2	3,248	150.5	73
Subterranean-v2	235.6	8%	3	613	95.7	52
DryGASCON-v1	178.7	29%	4	3,801	100.5	72
Xoodyak_GMU2-v2	169.5	8%		4,077	68.9	52
PHOTON-Beetle-v1	168.6	36%	5	3,294	101.4	77
Xoodyak_XT-v2	161.6	13%		4,302	70.7	56
KNOT-v2x4	155.6	9%	6	3,984	63.2	52
Xoodyak_XT-v8	150.9	13%		3,507	66.0	56
KNOT-v2x4h	149.8	9%		4,283	60.9	52
Ascon_VT-v1	148.9	27%	7	3,130	84.9	73
ESTATE-v1	135.5	43%	8	2,855	109.0	103
GIFT-COFB-v1	134.2	45%	9	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
Gimli_GT-v4	125.4	10%	10	4,027	60.7	62
Romulus-v2	125.0	21%	11	2,353	82.0	84
Ascon_Graz-v2	117.3	17%		3,847	63.2	69
Ascon_Graz-v1	113.9	23%		2,947	63.2	71
Gimli_GT-v2	104.9	13%		2,852	76.2	93
Romulus-v3	102.9	20%		3,847	45.0	56
Elephant-v2	92.0	16%	12	3,073	85.5	119
TinyJAMBU_TJT-v2	88.2	29%		689	125.4	182
TinyJAMBU_GMU-v1	85.0	30%		720	124.8	188
Oribatida-v1	79.0	24%	13	1,671	176.5	286
Spook-v2-v2	69.4	17%	14	3,662	77.0	142
SCHWAEMM-v1	69.0	15%	15	4,685	66.3	123
ForkAE-v2	68.2	63%	16	3,571	90.0	169
Saturnin-v2	62.8	9%	17	3,326	76.1	155
COMET_CI-v3	61.7	34%	18	3,443	80.0	166
COMET_CI-v1	58.5	34%		3,255	80.9	177
LOCUS-v2	58.4	38%	19	2,950	72.5	159
COMET_VT-v2	53.6	32%		2,353	111.5	266
Oribatida-v2	51.8	25%		2,497	114.2	282
TinyJAMBU_GMU-v2	47.2	30%		908	128.3	348
LOTUS-v2	42.4	38%		2,208	52.7	159
ESTATE-v3	32.4	48%		1,820	107.1	423
ISAP-v2	31.9	12%	20*	**5,708**	68.0	273
Elephant-v1	28.4	16%		2,368	97.5	439
SpoC-v1	27.9	48%	21	2,049	98.2	451
mixFeed-v1	22.5	24%	22	3,479	38.9	221
Saturnin-v1	18.1	15%		3,093	94.0	665
Pyjamask-v2	16.2	17%	23	4,162	73.2	577
WAGE-v1	12.3	22%	24	2,081	101.6	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
ACE-v1	8.0	22%	25	2,156	73.8	1,185
ForkAE-v1	6.8	95%		2,022	67.9	1,272
Average		**25%**				
Minimum		**6%**				
Maximum		**95%**				

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-v2	1,441.6	47%	1	613	95.7	816
Xoodyak_GMU2-v1	1,386.1	44%	2	3,248	150.5	1,334
Xoodyak_GMU2-v2	939.1	48%		4,077	68.9	901
Gimli_GT-v4	617.8	48%	3	4,027	60.7	1,208
KNOT-v2x2	591.2	48%	4	3,287	90.4	1,879
KNOT-v2x4	582.7	48%		3,984	63.2	1,333
Xoodyak_XT-v2	513.1	47%		4,302	70.7	1,693
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	425.8	48%		4,451	55.6	1,606
TinyJAMBU_TJT-v3	332.3	49%	5	1,092	115.4	4,267
Ascon_Graz-v2	329.0	49%	6	3,847	63.2	2,361
DryGASCON-v1	302.6	49%	7	3,801	100.5	4,083
Ascon_VT-v1	268.0	49%		3,130	84.9	3,893
Ascon_Graz-v1	248.7	49%		2,947	63.2	3,121
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
Romulus-v2	207.7	49%	10	2,353	82.0	4,852
Elephant-v2	201.6	49%	11	3,073	85.5	5,211
Spook-v2-v2	201.2	49%	12	3,662	77.0	4,702
Romulus-v3	195.9	49%		3,847	45.0	2,822
SCHWAEMM-v1	195.0	49%	13	4,685	66.3	4,181
GIFT-COFB-v1	151.4	50%	14	2,214	114.3	9,276
Oribatida-v1	108.4	49%	15	1,671	176.5	19,995
ESTATE-v1	105.2	50%	16	2,855	109.0	12,736
ISAP-v2	98.8	48%	17*	**5,708**	68.0	8,456
TinyJAMBU_TJT-v2	86.6	50%		689	125.4	17,795
COMET_CI-v3	83.2	50%	18	3,443	80.0	11,822
TinyJAMBU_GMU-v1	82.6	50%		720	124.8	18,564
COMET_VT-v2	81.1	49%		2,353	111.5	16,885
COMET_CI-v1	78.9	50%		3,255	80.9	12,597
Oribatida-v2	68.8	50%		2,497	114.2	20,400
Elephant-v1	59.5	49%		2,368	97.5	20,123
LOCUS-v2	51.3	50%	19	2,950	72.5	17,379
ForkAE-v2	50.1	50%	20	3,571	90.0	22,050
Pyjamask-v2	45.7	49%	21	4,162	73.2	19,680
mixFeed-v1	44.3	49%	22	3,479	38.9	10,778
TinyJAMBU_GMU-v2	44.3	50%		908	128.3	35,572
Saturnin-v1	39.8	49%		3,093	94.0	29,049
LOTUS-v2	37.2	50%		2,208	52.7	17,379
Xoodyak_GMU-v2	34.6	45%		2,316	74.8	26,548
SpoC-v1	28.4	50%	23	2,049	98.2	42,473
WAGE-v1	28.0	49%	24	2,081	101.6	44,601
Pyjamask-v1	22.4	49%		3,897	92.7	50,908
ESTATE-v3	22.3	50%		1,820	107.1	58,976
ACE-v1	17.8	49%	25	2,156	73.8	50,845
ForkAE-v1	2.0	50%		2,022	67.9	422,754
Average		**49%**				
Minimum		**44%**				
Maximum		**50%**				

Table 50: Lattice ECP5 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
Xoodyak_GMU2-v1	687.9	22%	1	3,248	150.5	112
Subterranean-v2	612.7	20%	2	613	95.7	80
Xoodyak_GMU2-v2	452.0	23%		4,077	68.9	78
KNOT-v2x4	348.0	29%	3	3,984	63.2	93
KNOT-v2x4h	335.1	29%		4,283	60.9	93
Xoodyak_XT-v2	326.1	30%		4,302	70.7	111
Xoodyak_XT-v8	304.6	30%		3,507	66.0	111
Gimli_GT-v4	299.0	23%	4	4,027	60.7	104
Xoodyak_GMU-v1	272.6	29%		3,172	74.0	139
TinyJAMBU_TJT-v3	269.8	40%	5	1,092	115.4	219
DryGASCON-v1	235.0	38%	6	3,801	100.5	219
Gimli_GT-v2	220.4	27%		2,852	76.2	177
Ascon_Graz-v2	211.5	31%	7	3,847	63.2	153
Ascon_VT-v1	204.1	38%		3,130	84.9	213
Ascon_VT-v2	184.4	37%		3,256	74.2	206
Ascon_Graz-v1	182.7	36%		2,947	63.2	177
PHOTON-Beetle-v1	177.3	42%	8	3,294	101.4	293
Romulus-v2	166.6	40%	9	2,353	82.0	252
Romulus-v3	149.6	38%		3,847	45.0	154
Elephant-v2	147.9	36%	10	3,073	85.5	296
Spook-v2-v2	137.8	34%	11	3,662	77.0	286
GIFT-COFB-v1	131.8	43%	12	2,214	114.3	444
SCHWAEMM-v1	125.3	31%	13	4,685	66.3	271
Saturnin-v2	117.0	24%	14	3,326	76.1	333
ESTATE-v1	94.3	45%	15	2,855	109.0	592
Oribatida-v1	86.6	40%	16	1,671	176.5	1,043
TinyJAMBU_TJT-v2	74.1	42%		689	125.4	867
TinyJAMBU_GMU-v1	71.0	43%		720	124.8	900
COMET_CI-v3	68.5	41%	17	3,443	80.0	598
COMET_VT-v2	65.1	40%		2,353	111.5	877
COMET_CI-v1	65.0	41%		3,255	80.9	637
Oribatida-v2	52.0	37%		2,497	114.2	1,124
ISAP-v2	47.8	23%	18*	**5,708**	68.0	728
ForkAE-v2	46.9	47%	19	3,571	90.0	982
LOCUS-v2	45.3	44%	20	2,950	72.5	819
Elephant-v1	44.3	37%		2,368	97.5	1,128
TinyJAMBU_GMU-v2	38.3	43%		908	128.3	1,716
LOTUS-v2	32.9	44%		2,208	52.7	819
mixFeed-v1	30.3	33%	21	3,479	38.9	658
Pyjamask-v2	29.3	31%	22	4,162	73.2	1,280
Saturnin-v1	25.8	32%		3,093	94.0	1,863
SpoC-v1	25.2	44%	23	2,049	98.2	1,993
Xoodyak_GMU-v2	20.8	27%		2,316	74.8	1,842
ESTATE-v3	20.5	46%		1,820	107.1	2,672
WAGE-v1	19.6	34%	24	2,081	101.6	2,649
Pyjamask-v1	15.5	34%		3,897	92.7	3,068
ACE-v1	12.6	35%	25	2,156	73.8	3,005
ForkAE-v1	2.0	50%		2,022	67.9	17,678
Average		**35%**				
Minimum		**20%**				
Maximum		**50%**				

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_GMU2-v1	263.9	8%	1	3,248	150.5	73
Subterranean-v2	218.8	7%	2	613	95.7	56
TinyJAMBU_TJT-v3	169.8	25%	3	1,092	115.4	87
Xoodyak_GMU2-v2	169.5	9%		4,077	68.9	52
KNOT-v2x4	152.7	13%	4	3,984	63.2	53
Xoodyak_XT-v2	150.8	14%		4,302	70.7	60
KNOT-v2x4h	147.0	13%		4,283	60.9	53
Xoodyak_XT-v8	140.9	14%		3,507	66.0	60
DryGASCON-v1	138.4	23%	5	3,801	100.5	93
Romulus-v2	125.0	30%	6	2,353	82.0	84
Xoodyak_GMU-v1	124.6	13%		3,172	74.0	76
PHOTON-Beetle-v1	118.0	28%	7	3,294	101.4	110
Ascon_VT-v1	116.9	22%	8	3,130	84.9	93
Gimli_GT-v4	114.3	9%	9	4,027	60.7	68
Ascon_VT-v2	103.2	21%		3,256	74.2	92
Romulus-v3	102.9	26%		3,847	45.0	56
Ascon_Graz-v2	99.9	15%		3,847	63.2	81
Ascon_Graz-v1	99.8	20%		2,947	63.2	81
GIFT-COFB-v1	93.8	31%	10	2,214	114.3	156
Gimli_GT-v2	92.9	11%		2,852	76.2	105
Elephant-v2	92.0	23%	11	3,073	85.5	119
ESTATE-v1	71.2	34%	12	2,855	109.0	196
Saturnin-v2	53.5	11%	13	3,326	76.1	182
Oribatida-v1	53.1	24%	14	1,671	176.5	425
Spook-v2-v2	51.9	13%	15	3,662	77.0	190
TinyJAMBU_TJT-v2	51.0	29%		689	125.4	315
TinyJAMBU_GMU-v1	49.3	30%		720	124.8	324
SCHWAEMM-v1	46.7	12%	16	4,685	66.3	182
COMET_CI-v3	44.1	26%	17	3,443	80.0	232
COMET_CI-v1	41.9	26%		3,255	80.9	247
COMET_VT-v2	40.2	25%		2,353	111.5	355
ForkAE-v2	39.0	39%	18	3,571	90.0	295
LOCUS-v2	33.3	32%	19	2,950	72.5	279
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
LOTUS-v2	24.2	32%		2,208	52.7	279
SpoC-v1	18.7	33%	20	2,049	98.2	673
ISAP-v2	18.3	9%	21*	**5,708**	68.0	476
ESTATE-v3	16.4	37%		1,820	107.1	836
mixFeed-v1	15.2	17%	22	3,479	38.9	328
Saturnin-v1	14.0	17%		3,093	94.0	862
Pyjamask-v2	13.8	15%	23	4,162	73.2	680
WAGE-v1	10.1	18%	24	2,081	101.6	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
ACE-v1	6.5	18%	25	2,156	73.8	1,445
ForkAE-v1	1.9	49%		2,022	67.9	4,469
Average		**21%**				
Minimum		**7%**				
Maximum		**49%**				

Table 52: Intel Cyclone 10 LP Encryption PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v2	Subterranean-v2	Subterranean-v2	Subterranean-v2
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Ascon_VT-v1
3	KNOT-v2x2h	KNOT-v2x2h	Ascon_Graz-v2	Xoodyak_GMU2-v1
4	Ascon_Graz-v2	Ascon_Graz-v2	KNOT-v2x4	KNOT-v2x4
5	Gimli_GT-v6	Gimli_GT-v6	DryGASCON-v1	TinyJAMBU_TJT-v3
6	DryGASCON-v1	DryGASCON-v1	TinyJAMBU_TJT-v3	DryGASCON-v1
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Gimli_GT-v2	Romulus-v2
8	Spook-v2-v2	Romulus-v2	Romulus-v2	PHOTON-Beetle-v1
9	Romulus-v2	Spook-v2-v2	PHOTON-Beetle-v1	Gimli_GT-v2
10	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1	GIFT-COFB-v1
11	Saturnin-v2	PHOTON-Beetle-v1	Spook-v2-v2	Elephant-v2
12	PHOTON-Beetle-v1	Saturnin-v2	Elephant-v2	ESTATE-v1
13	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	ForkAE-v2
14	ISAP-v1	Elephant-v2	Saturnin-v2	Spook-v2-v2
15	Elephant-v2	ISAP-v1	COMET_CI-v3	COMET_CI-v3
16	COMET_CI-v3	COMET_CI-v3	ESTATE-v1	Oribatida-v1
17	Oribatida-v1	Oribatida-v1	Oribatida-v1	SCHWAEMM-v1
18	ESTATE-v1	ESTATE-v1	ForkAE-v2	LOCUS-v2
19	mixFeed-v1	mixFeed-v1	ISAP-v1	Saturnin-v2
20	ForkAE-v2	ForkAE-v2	LOCUS-v2	SpoC-v1
21	LOCUS-v2	LOCUS-v2	mixFeed-v1	mixFeed-v1
22	SpoC-v1	SpoC-v1	SpoC-v1	ISAP-v1
23	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
24	Pyjamask-v1	Pyjamask-v1	ACE-v1	ACE-v1
25	ACE-v1	ACE-v1	Pyjamask-v1	Pyjamask-v1

Table 53: Intel Cyclone 10 LP Encryption AD Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v2	Subterranean-v2	Subterranean-v2	Subterranean-v2
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	TinyJAMBU_TJT-v3
3	KNOT-v2x4	KNOT-v2x4	TinyJAMBU_TJT-v3	Ascon_VT-v1
4	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	KNOT-v2x4	Xoodyak_GMU2-v1
5	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_Graz-v2	KNOT-v2x4
6	Gimli_GT-v6	Gimli_GT-v6	DryGASCON-v1	DryGASCON-v1
7	Romulus-v2	Romulus-v2	Romulus-v2	GIFT-COFB-v1
8	Saturnin-v2	Saturnin-v2	Gimli_GT-v2	Romulus-v2
9	DryGASCON-v1	DryGASCON-v1	PHOTON-Beetle-v1	PHOTON-Beetle-v1
10	Elephant-v2	Elephant-v2	GIFT-COFB-v1	Gimli_GT-v2
11	ISAP-v1	ISAP-v1	Elephant-v2	ESTATE-v1
12	Spook-v2-v2	PHOTON-Beetle-v1	Spook-v2-v2	Elephant-v2
13	PHOTON-Beetle-v1	Spook-v2-v2	SCHWAEMM-v1	ForkAE-v2
14	SCHWAEMM-v1	SCHWAEMM-v1	ESTATE-v1	LOCUS-v2
15	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	Spook-v2-v2
16	Oribatida-v1	ESTATE-v1	ISAP-v1	COMET_CI-v3
17	ESTATE-v1	Oribatida-v1	LOCUS-v2	Saturnin-v2
18	LOCUS-v2	LOCUS-v2	Oribatida-v1	SCHWAEMM-v1
19	COMET_CI-v3	COMET_CI-v3	COMET_CI-v3	Oribatida-v1
20	ForkAE-v2	ForkAE-v2	ForkAE-v2	ISAP-v1
21	mixFeed-v1	mixFeed-v1	mixFeed-v1	SpoC-v1
22	SpoC-v1	SpoC-v1	SpoC-v1	mixFeed-v1
23	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
24	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1	ACE-v1
25	ACE-v1	ACE-v1	ACE-v1	Pyjamask-v1

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

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v2	Subterranean-v2	Subterranean-v2	Subterranean-v2
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
3	KNOT-v2x4	KNOT-v2x4	KNOT-v2x4	KNOT-v2x4
4	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_VT-v1
5	Gimli_GT-v6	Gimli_GT-v6	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3
6	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	Gimli_GT-v2	Romulus-v2
7	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1	DryGASCON-v1
8	Romulus-v2	Romulus-v2	Romulus-v2	GIFT-COFB-v1
9	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	PHOTON-Beetle-v1
10	Spook-v2-v2	Spook-v2-v2	GIFT-COFB-v1	Gimli_GT-v2
11	ISAP-v1	Elephant-v2	Elephant-v2	Elephant-v2
12	Elephant-v2	PHOTON-Beetle-v1	Spook-v2-v2	ESTATE-v1
13	PHOTON-Beetle-v1	ISAP-v1	Saturnin-v2	Saturnin-v2
14	SCHWAEMM-v1	GIFT-COFB-v1	SCHWAEMM-v1	Spook-v2-v2
15	GIFT-COFB-v1	SCHWAEMM-v1	ISAP-v1	ForkAE-v2
16	COMET_CI-v3	COMET_CI-v3	ESTATE-v1	COMET_CI-v3
17	Oribatida-v1	Oribatida-v1	COMET_CI-v3	LOCUS-v2
18	ESTATE-v1	ESTATE-v1	Oribatida-v1	SCHWAEMM-v1
19	LOCUS-v2	LOCUS-v2	LOCUS-v2	Oribatida-v1
20	mixFeed-v1	mixFeed-v1	ForkAE-v2	ISAP-v1
21	ForkAE-v2	ForkAE-v2	mixFeed-v1	SpoC-v1
22	SpoC-v1	SpoC-v1	SpoC-v1	mixFeed-v1
23	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
24	Pyjamask-v1	Pyjamask-v1	Pyjamask-v1	ACE-v1
25	ACE-v1	ACE-v1	ACE-v1	Pyjamask-v1

Table 55: Lattice ECP5 Encryption PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Subterranean-v2	Subterranean-v2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Subterranean-v2	Subterranean-v2
3	Gimli_GT-v4	Gimli_GT-v4	KNOT-v2x2	TinyJAMBU_TJT-v3
4	KNOT-v2x2	KNOT-v2x2	Gimli_GT-v4	DryGASCON-v1
5	Ascon_Graz-v2	Ascon_Graz-v2	DryGASCON-v1	KNOT-v2x4
6	DryGASCON-v1	DryGASCON-v1	Ascon_VT-v1	Ascon_VT-v1
7	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	PHOTON-Beetle-v1
8	Spook-v2-v2	Spook-v2-v2	PHOTON-Beetle-v1	Romulus-v2
9	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Romulus-v2	Gimli_GT-v4
10	SCHWAEMM-v1	SCHWAEMM-v1	Spook-v2-v2	Elephant-v2
11	Saturnin-v2	Saturnin-v2	GIFT-COFB-v1	GIFT-COFB-v1
12	Romulus-v2	Romulus-v2	Elephant-v2	ESTATE-v1
13	Elephant-v2	Elephant-v2	SCHWAEMM-v1	Oribatida-v1
14	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	Spook-v2-v2
15	ISAP-v2	Oribatida-v1	ESTATE-v1	SCHWAEMM-v1
16	Oribatida-v1	ESTATE-v1	Oribatida-v1	ForkAE-v2
17	COMET_VT-v2	COMET_VT-v2	COMET_CI-v3	COMET_CI-v3
18	ESTATE-v1	ISAP-v2	ForkAE-v2	Saturnin-v2
19	ForkAE-v2	ForkAE-v2	LOCUS-v2	LOCUS-v2
20	Pyjamask-v2	Pyjamask-v2	ISAP-v2	SpoC-v1
21	mixFeed-v1	mixFeed-v1	mixFeed-v1	mixFeed-v1
22	LOCUS-v2	LOCUS-v2	SpoC-v1	ISAP-v2
23	WAGE-v1	SpoC-v1	Pyjamask-v2	Pyjamask-v2
24	SpoC-v1	WAGE-v1	WAGE-v1	WAGE-v1
25	ACE-v1	ACE-v1	ACE-v1	ACE-v1

Table 56: Lattice ECP5 Encryption AD Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1	TinyJAMBU_TJT-v3
2	Subterranean-v2	Subterranean-v2	Subterranean-v2	Xoodyak_GMU2-v1
3	KNOT-v2x4	KNOT-v2x4	TinyJAMBU_TJT-v3	Subterranean-v2
4	Gimli_GT-v4	TinyJAMBU_TJT-v3	KNOT-v2x4	DryGASCON-v1
5	TinyJAMBU_TJT-v3	Gimli_GT-v4	Gimli_GT-v4	PHOTON-Beetle-v1
6	Saturnin-v2	Saturnin-v2	DryGASCON-v1	KNOT-v2x4
7	Ascon_Graz-v2	Ascon_Graz-v2	Ascon_VT-v1	Ascon_VT-v1
8	DryGASCON-v1	DryGASCON-v1	PHOTON-Beetle-v1	ESTATE-v1
9	Romulus-v2	Romulus-v2	Romulus-v2	GIFT-COFB-v1
10	Elephant-v2	Elephant-v2	Elephant-v2	Gimli_GT-v4
11	PHOTON-Beetle-v1	PHOTON-Beetle-v1	ESTATE-v1	Romulus-v2
12	SCHWAEMM-v1	SCHWAEMM-v1	GIFT-COFB-v1	Elephant-v2
13	Spook-v2-v2	Spook-v2-v2	SCHWAEMM-v1	Oribatida-v1
14	Oribatida-v1	Oribatida-v1	Spook-v2-v2	Spook-v2-v2
15	ESTATE-v1	ESTATE-v1	Saturnin-v2	SCHWAEMM-v1
16	GIFT-COFB-v1	GIFT-COFB-v1	Oribatida-v1	ForkAE-v2
17	ISAP-v2	ISAP-v2	COMET_CI-v3	Saturnin-v2
18	COMET_CI-v3	COMET_CI-v3	LOCUS-v2	COMET_CI-v3
19	LOCUS-v2	LOCUS-v2	ForkAE-v2	LOCUS-v2
20	ForkAE-v2	ForkAE-v2	ISAP-v2	ISAP-v2
21	Pyjamask-v2	Pyjamask-v2	mixFeed-v1	SpoC-v1
22	mixFeed-v1	mixFeed-v1	SpoC-v1	mixFeed-v1
23	SpoC-v1	SpoC-v1	Pyjamask-v2	Pyjamask-v2
24	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
25	ACE-v1	ACE-v1	ACE-v1	ACE-v1

Table 57: Lattice ECP5 Encryption AD+PT Throughput Rankings

Rank	Long	1536 Byte	64 Byte	16 Byte
1	Xoodyak_GMU2-v1	Subterranean-v2	Xoodyak_GMU2-v1	Xoodyak_GMU2-v1
2	Subterranean-v2	Xoodyak_GMU2-v1	Subterranean-v2	Subterranean-v2
3	Gimli_GT-v4	Gimli_GT-v4	KNOT-v2x4	TinyJAMBU_TJT-v3
4	KNOT-v2x2	KNOT-v2x2	Gimli_GT-v4	KNOT-v2x4
5	Ascon_Graz-v2	TinyJAMBU_TJT-v3	TinyJAMBU_TJT-v3	DryGASCON-v1
6	TinyJAMBU_TJT-v3	Ascon_Graz-v2	DryGASCON-v1	Romulus-v2
7	DryGASCON-v1	DryGASCON-v1	Ascon_Graz-v2	PHOTON-Beetle-v1
8	Saturnin-v2	Saturnin-v2	PHOTON-Beetle-v1	Ascon_VT-v1
9	PHOTON-Beetle-v1	PHOTON-Beetle-v1	Romulus-v2	Gimli_GT-v4
10	Romulus-v2	Romulus-v2	Elephant-v2	GIFT-COFB-v1
11	Spook-v2-v2	Elephant-v2	Spook-v2-v2	Elephant-v2
12	Elephant-v2	Spook-v2-v2	GIFT-COFB-v1	ESTATE-v1
13	SCHWAEMM-v1	SCHWAEMM-v1	SCHWAEMM-v1	Saturnin-v2
14	GIFT-COFB-v1	GIFT-COFB-v1	Saturnin-v2	Oribatida-v1
15	Oribatida-v1	Oribatida-v1	ESTATE-v1	Spook-v2-v2
16	ESTATE-v1	ESTATE-v1	Oribatida-v1	SCHWAEMM-v1
17	ISAP-v2	ISAP-v2	COMET_CI-v3	COMET_CI-v3
18	COMET_CI-v3	COMET_CI-v3	ISAP-v2	ForkAE-v2
19	LOCUS-v2	LOCUS-v2	ForkAE-v2	LOCUS-v2
20	ForkAE-v2	ForkAE-v2	LOCUS-v2	SpoC-v1
21	Pyjamask-v2	Pyjamask-v2	mixFeed-v1	ISAP-v2
22	mixFeed-v1	mixFeed-v1	Pyjamask-v2	mixFeed-v1
23	SpoC-v1	SpoC-v1	SpoC-v1	Pyjamask-v2
24	WAGE-v1	WAGE-v1	WAGE-v1	WAGE-v1
25	ACE-v1	ACE-v1	ACE-v1	ACE-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 5.3: 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 3.6: 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.

1.0.7 (December 23, 2020)

Added

- New hardware design submissions: ACE (1 variant), ForkAE (2 variants), mixFeed (1 variant), and Xoodyak_GMU2 (2 variants).
  Reason: Phase 3 Submissions
- New variants replacing previous variants: KNOT (16 new variants replacing previous 4 variants). New variants added on top of previous variants: COMET_CI-v3, LOCUS-v2, and LOTUS-v2.
  Reason: Phase 3 Submissions
- Results reported for the implementations of the current standards: AES-GCM (2 variants), SHA-2 (SHA-256, 1 variant), and SHA-3 (SHA3-256, 1 variant).
  Reason: The first attempt at the comparison with the current standards
- New sections: 4.1 Implementations of current standards, 6 Conclusions and Future Work.
  Reason: The first attempt at comparison with the current standards. Conclusions from Phases 1-3.

Changed

- The fully-debugged code submitted for COMET_VT-v1. Improved code submitted for Gimli (7 new variants replacing previous variants with the same names), Spook-v2-v2 (replacing Spook-v2-v1), and Subterranean-v2 (replacing Subterranean-v2)
  Reason: Phase 3 Submissions

- Revised space-exploration graphs for COMET, Gimli, KNOT, and Xoodyak.
  Reason: Phase 3 Submissions
- Revised sections: 4 Hardware Designs, 5 Results and Their Analysis, Appendix A Additional Results
  Reason: Phase 3 Submissions. Comparison with the current standards.