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

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

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

Abstract. Over 20 Round 2 candidates in the NIST Lightweight Cryptography (LWC) process have been implemented in hardware by groups from all over the world. In August and September 2020, all implementations compliant with the LWC Hardware API, proposed in 2019, have been submitted for FPGA benchmarking to George Mason University's LWC benchmarking team, who co-authored this report. The received submissions were first verified for correct functionality and compliance with the hardware API's specification. Then, formulas for the execution times in clock cycles, as a function of input sizes, have been confirmed using behavioral simulation. If needed, appropriate corrections were introduced in collaboration with the submission teams. 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 overhead of modifying vs. reusing a key between two consecutive inputs was quantified. 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

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 [1].

The first version of the proposed hardware API for CAESAR was reported in [2]. This version was later substantially revised, endorsed by the CAESAR Committee in May 2016, and published as a Cryptology ePrint Archive in June 2016 [3]. A relatively minor addendum was proposed in the same month, and endorsed by the CAESAR Committee in November 2016 [4].

The commonly accepted CAESAR Hardware API provided the foundation for the GMU Development Package, released in May and June 2016 [5], [6]. 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 [7]. A few relatively minor weaknesses of this version of the package, discovered when performing experimental testing using general-purpose prototyping boards, were reported in [8], [9].

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 [5], [10]. 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, [7] 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 [5], [6] by just following the specification [3] directly.

In spite of being non-mandatory and the lack of official endorsement by the CAESAR Committee, the CAESAR Development Package played a significant role in increasing the number of implementations developed during Round 2 of the CAESAR contest. Out of 43 implementations reported before the end of Round 2, 32 were fully compliant, and one partially compliant with the CAESAR Hardware API. All fully compliant code used the GMU Development Package. The fully and partially compliant implementations covered 28 out of 29 Round 2 candidates (all except Tiaoxin) [5]. 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 [5]. 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 [11]. In [12]–[15], several other implementations were enhanced with countermeasures against Differential Power Analysis. In order to facilitate this enhancement, an additional Random Data Input (RDI) port was added to the CAESAR Hardware API.

A comprehensive framework for fair and efficient benchmarking of hardware implementations of lightweight cryptography was proposed in [16]. Major differences between the proposed Lightweight Cryptography Hardware API and the CAESAR Hardware API, defined in [3], [4], 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.

The corresponding LWC Development Package has been built as a major revision of the CAESAR Development Package 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 three times, including the most recent revision in June 2020. The advantages of the LWC Development Package over the CAESAR Development Package in terms of the smaller area overhead was demonstrated in [17]. 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 [18].

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

2 Methodology

2.1 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 [20]. The major parts of this API include the minimum compliance criteria, interface, and communication protocol supported by the LWC core. The proposed API is intended to meet the requirements of all candidates submitted to the NIST Lightweight Cryptography standardization process, as well as all CAESAR candidates and current authenticated cipher and hash function standards. The main reasons for defining a common API for all hardware implementations of candidates submitted to the NIST Lightweight Cryptography standardization project [19] 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.

2.2 LWC Hardware Development Package

To make the benchmarking framework more efficient in terms of the hardware development time, the designers are provided with the following resources, compliant with the use of the proposed LWC Hardware API:
a) VHDL code supporting the API protocol, common to all Lightweight Cryptography standardization process candidates, as well as all CAESAR candidates and AES-GCM (LWCsrc)

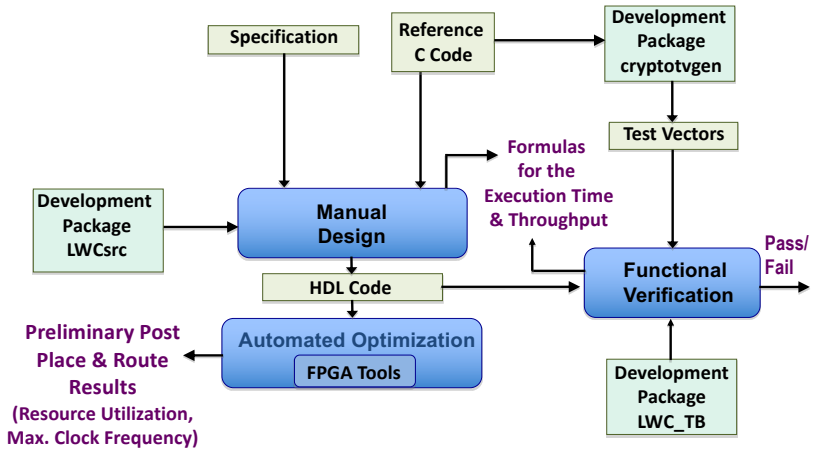

Figure 1: The API-Compliant Code Development using the Development Package

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
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 LWCsrc 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 verification is used to confirm the required functionality. 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. Functional verification can also be used to confirm formulas for the Execution Time and Throughput derived during the timing analysis phase of the Manual Design.

2.3 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, low-energy FPGA families
2. capable of holding SCA-protected designs (possibly using up to 4 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.

2.4 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 between 3 and 4 times more LUTs than unprotected implementations, our unprotected design should take no more than one fourth of the total number of LUTs, i.e., 2000 LUTs. At the same time, we assume that the benchmarked implementations are not permitted to use any family-specific embedded resources, such as Block RAMs, DSP units, or embedded multipliers. Any storage should be implemented using either flip-flops or distributed memory, which, in case of Xilinx FPGAs, is built out of LUTs. The number of Artix-7 flip-flops is limited to 4000, as in this FPGA family each LUT is accompanied by two flip-flops. The designs are also prohibited from using any family-specific primitives or megafunctions.

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

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

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

   of Xilinx Artix-7 FPGAs.
   Other limits, such as 1500 LUTs, 500 LUTs, etc. are welcome too.
4. Maximum throughput, assuming
   - 1000 or less LUTs
   - 2000 or less FFs
   - No BRAMs and no DSP units

   of Xilinx Artix-7 FPGAs, for the input composed of empty Associated Data and n bytes of plaintext, for n=16, 64, or 1536 bytes.

2.5 Deliverables

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

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

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

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

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

2.6 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 ([20], Fig. 2) and the use of an external FIFO was expected from two-pass implementations.

Then, a comprehensive set of new test vectors, unknown in advance to hardware designers, was generated separately for each variant of each algorithm. These tests included multiple special cases, such as empty AD, empty plaintext, various widths of an incomplete last block, etc. If these test vectors passed, the implementation was judged functionally correct and compliant with the LWC Hardware API. If these test vectors failed, the source of failure was investigated in close collaboration with hardware designers. The designers were allowed to submit revised versions of their code as late as September 23, 2020. In some cases, an error was on the side of the benchmarking team. For example, an incorrect version of the reference implementation was used, or an incorrect order of segments (such as Npub, AD, plaintext, ciphertext, tag) at the PDI input to the LWC core was assumed. In other cases, the previously-submitted HDL code had to be modified by the designers.

If the code did not pass all tests until the final deadline, it was still included in our study. However, our description of the corresponding hardware design, included in Section 3, clearly indicates that such a problem occurred.

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

2.7 Timing Measurements

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

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

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

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

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

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

2.8 Synthesis, Implementation, and Optimization of Tool Options

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

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

The determination of the maximum clock frequency and the corresponding resource utilization was performed using tools specific for each FPGA vendor. For Artix-7 FPGAs, Minerva: An Automated Hardware Optimization Tool described in [22], was used. An average time required to find the optimum requested clock frequency and the best optimization strategy was close to 4 hours per algorithm variant. Still, in some cases, hardware design teams were able to generate better results by themselves. The source of such discrepancies is still under investigation, but possible reasons include different versions of Vivado, use vs. no use of the out-of-context mode, limited time that could be devoted to each Minerva run (affecting tool options), etc.

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

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

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

2.9 Performance Metrics

The following performance metrics have been evaluated as a part of Phase 1 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 = $d\cdot$ 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.

3 Hardware Designs

An overview of hardware designs submitted for benchmarking is given in Table 1. A total of 24 designs were received. These designs covered 21 out of 32 Round 2 candidates. The only candidates implemented independently by two different groups were Ascon, COMET, and Xoodyak.

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

- Virginia Tech Signatures Analysis Lab, USA, contributed implementations of 5 candidates: Ascon, COMET, GIFT-COFB, SCHWAEMM & ESCH, and Spoc;
- George Mason University Cryptographic Engineering Research Group (CERG), USA, implemented 5 candidates: Elephant, PHOTON-Beetle, Pyjamask, TinyJAMBU, and Xoodyak;
- 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.

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

Table 1: Overview of hardware designs submitted for FPGA benchmarking

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

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	Gimli	Chair of Security in Information Technology, Technical University of Munich, Germany	Patrick Karl patrick.karl@tum.de	Michael Tempelmeier michael.tempelmeier@ tum.de	Yes, Unmodified	VHDL	3
8	ISAP	Institute of Applied Information Processing and Communications, TU Graz, Austria	Robert Primas https://rprimas.github.io rprimas@gmail.com	Stefan Mangard https://www.iaik.tugraz.at/ person/stefan-mangard stefan.mangard@ iaik.tugraz.at	Yes, Modified	VHDL	2
9	KNOT	KNOT Team, Tsinghua University, China	Bohan Yang bohanyang@tsinghua.edu.cn, Zhengdong Li lizd@tsinghua.edu.cn	Wentao Zhang zhangwentao@iie.ac.cn, Leibo Liu liulb@ tsinghua.edu.cn	Yes, Unmodified	Verilog (CryptoCore)	4
10	LOCUS-AEAD & LOTUS-AEAD	CINVESTAV-IPN, Mexico	Brisbane Ovilla Martinez brisbane@cinvestav.mx		Yes, Unmodified	VHDL	2
11	Oribatida	CINVESTAV-IPN, Mexico	Cuauhtemoc Mancillas López cuauhtemoc.mancillas@ cinvestav.mx, Alberto F. Martínez Herrera alberto.herrera.tec@gmail.com		Yes, Unmodified	VHDL	1
12	PHOTON-Beetle	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Vivian Ledynh vledynh@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	1
13	Pyjamask	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Rishub Nagpal https://cryptography.gmu.edu/ team/rishub.php rnagpal2@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	2

Table 1 continued from previous page

No.	LWC Candidate	Hardware Design Group	Primary Hardware Designer	Academic Advisors/ Program Managers	LWC Development Package	HDL	Number of Variants
14	Romulus	Romulus-Team, Symmetric Key and Lightweight Cryptography Lab (SyLLab), Nanyang Technological University, Singapore	Mustafa Khairallah http://www.mustafa-khairallah.com mustafam001@e.ntu.edu.sg	Thomas Peyrin https://thomaspeyrin.github.io/web/ thomas.peyrin@ntu.edu.sg	No	Verilog (LWC)	4
15	SCHWAEMM & ESCH	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	Flora Coleman googly2@vt.edu	William Diehl wdiehl@vt.edu	Yes, Modified	VHDL	2
16	SpoC	Virginia Tech Signatures Analysis Lab, Virginia Tech, USA	William Diehl wdiehl@vt.edu		Yes, Modified	Verilog (CryptoCore)	1
17	Spook	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
18	Subterranean 2.0	Subterranean 2.0 Team	Pedro Maat Costa Massolino https://www.pmassolino.xyz pmaat@protonmail.com		No	Verilog (LWC)	1
19	TinyJAMBU	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Sammy Lin https://cryptography.gmu.edu/team/slin5.php slin5@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	3
20	WAGE	WAGE Team	Nusa Zidaric nzidaric@uwaterloo.ca	Mark Aagaard https://ece.uwaterloo.ca/∼maagaard maagaard@uwaterloo.ca	Yes, Modified	VHDL	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
21a	Xoodyak	Cryptographic Engineering Research Group (CERG), George Mason University, USA	Richard Haeussler https://crytpography.gmu.edu/team/rhaeuss.php rhaeussl@gmu.edu	Kris Gaj https://ece.gmu.edu/∼kgaj kgaj@gmu.edu Jens-Peter Kaps https://ece.gmu.edu/∼jkaps jkaps@gmu.edu	Yes, Unmodified	VHDL	2
21b	Xoodyak	Xoodyak Team + Silvia	Silvia Mella silvia.mella@st.com		Yes, Unmodified	VHDL	12
						Total	**59**

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

Most groups used VHDL. Three 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 Romulus, Spook, and Subterranean 2.0. Three implementations modeled only the part unique to a given algorithm, its CryptoCore, in Verilog. These designs included DryGASCON, KNOT, and SpoC. Altogether, 13 implementations used VHDL pre-processing and post-processing units, provided as a part of the LWC Development Package without any modifications, 8 with modifications, and 3 did not use them at all.

Eight submissions contained a single variant. In the remaining, the number of variants varied between 2 and 12. 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 56. In Table 2, we summarize basic features of each variant, and assign each variant a unique name used in the rest of the paper. For algorithms implemented by a single group, this name consists of the name of the algorithm followed by "-<variant_number>". For algorithms implemented by two groups we add "_<Group_Name_Abbreviation>" after the algorithm name. The abbreviations used are: Graz - TU Graz, Austria, VT - Virginia Tech, CI - CINVESTAV-IPN, GMU - George Mason University, and XT - Xoodyak Team + Silvia. For Spook, exceptionally, the name of the variant is Spook-v2-v1. In this name, v2 indicates version 2 of Spook, proposed in [25]. This version is known to have higher security margins at the cost of minimum performance overheads [25]. For each variant, we also list the name of the corresponding reference implementation. Most of these implementations can be found in the most recent version of SUPERCOP [26]. Some were submitted as a part of the hardware package (KNOT and WAGE) or were provided through candidate's website (Subterranean 2.0).

The maximum length of inputs processed by the implementations is often unlimited by the hardware design itself. In such cases, the authors either stated the maximum length required by the NIST Submission Requirements and Evaluation Criteria [19], $2^{50} - 1$, 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 and ISAP), implementations performing precomputations dependent on the maximum input size (Pyjamask), and COMET_CI (v1 and v2).

The following designs explicitly do not support key reuse between consecutive inputs: Subterranean-v1, TinyJAMBU (v1-v3), and Xoodyak_XT (v1-v12). The following submissions did not provide information regarding this support: Ascon_VT and SpoC-v1. For algorithms that support key reuse, we list in the separate column the number of additional clock cycles required to load a new key. This number has been determined experimentally through our own measurements and often differed from the value provided as a part of the submission package. The highest overhead for loading a new key was observed in the case of Pyjamask-v1 (433 cycles), Xoodyak_GMU-v2 (266 cycles), and Pyjamask-v2 (245 cycles). The smallest overhead of 3 clock cycles was measured for Ascon_Graz (v1 and v2) and Gimli (v1-v3). The second smallest, in the amount of 4 clock cycles, for DryGASCON-v1, LOCUS-v1, and LOTUS-v1.

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

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
1a	Ascon_Graz-v1	Ascon-128+ Ascon-Hash, Folded architecture	ascon128v12, asconhashv12	Y	3	unlimited
	Ascon_Graz-v2	Ascon-128a+ Ascon-Hash, Folded architecture	ascon128av12, asconhashv12	Y	3	unlimited
1b	Ascon_VT-v1	Ascon-128, Basic iterative architecture	ascon128v12	N/A		N/A
	Ascon_VT-v2	Ascon-128+ Ascon-Hash Basic iterative architecture	ascon128v12, asconhashv12	N/A		N/A
2a	COMET_CI-v1	Folded architecture	comet128aesv1	Y	8	$2^{16}-1$
	COMET_CI-v2	Folded architecture	comet128aesv1	Y	23	$2^{16}-1$
2b	COMET_VT-v1	Basic iterative architecture	comet128aesv1	Y	7	N/A
	COMET_VT-v2	Basic iterative architecture	comet128chamv1	Y	8	N/A
3	DryGASCON-v1	Basic iterative architecture, support for hashing	drygascon128k32(aead) drygascon128(hash)	Y	4	N/A
4	Elephant-v1	Basic iterative architecture	elephant160v1	Y	84	unlimited
	Elephant-v2	x5 Unrolled	elephant160v1	Y	20	unlimited
5	ESTATE-v1	Two-pass AES-based, 32-bit datapath	estatetweaes128v1	Y	8	$2^{16}-1$
	ESTATE-v2	Two-pass AES-based, 8-bit datapath	estatetweaes128v1	Y	23	$2^{16}-1$
	ESTATE-v3	Two-pass Gift-based, 32-bit datapath	estatetwegift128v1	Y	8	$2^{16}-1$
	ESTATE-v4	Two-pass, Gift-based, 8-bit datapath	estatetwegift128v1	Y	16	$2^{16}-1$
6	GIFT-COFB-v1	Basic iterative architecture	giftcofb128v1	Y	8	N/A
7	Gimli-v1	Customized FSM based on 3x32-bit register, RAM-based state-memory, 32-bit datapath	gimli24v1	Y	3	N/A
	Gimli-v2	Customized FSM based on 3x32-bit register, RAM-based state-memory, 16-bit datapath	gimli24v1	Y	3	N/A

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	Gimli-v3	Customized FSM based on 3x32-bit register, RAM-based state-memory, 8-bit datapath	gimli24v1	Y	3	N/A
8	ISAP-v1	Two-pass implementation, Folded architecture	isapk128av20	Y	9	$2^{16}-1$
	ISAP-v2	Two-pass implementation, Folded architecture	isapa128av20	Y	5	$2^{16}-1$
9	KNOT-v1	KNOT-AEAD (128, 256, 64), Basic iterative architecture	submitted with HW package	Y	7	unlimited
	KNOT-v2	KNOT-AEAD (128, 384, 192), Basic iterative architecture	submitted with HW package	Y	7	unlimited
	KNOT-v3	KNOT-AEAD (192, 384, 96), Basic iterative architecture	submitted with HW package	Y	9	unlimited
	KNOT-v4	KNOT-AEAD (256, 512, 128), Basic iterative architecture	submitted with HW package	Y	11	unlimited
10	LOCUS-v1	LOCUS, 32-bit datapath	twegift-64locusaeadv1	Y	4	unlimited
	LOTUS-v1	LOTUS, 32-bit datapath	twegift-64lotusaeadv1	Y	4	unlimited
11	Oribatida-v1	Oribatida256 256-bit datapath	oribatida256v12	Y	8	unlimited
12	PHOTON-Beetle-v1	AEAD+Hash	photonbeetle-aead128rate128v1, photonbeetle-hash256rate32v1	Y	6	$2^{50}-1$
13	Pyjamask-v1	Pyjamask128d16, folded architecture	pyjamask 128aeadv1	Y	433	$2^{16}-1$
	Pyjamask-v2	Pipeline implementation of MixRows	pyjamask 128aeadv1	Y	245	$2^{16}-1$
14	Romulus-v1	Round based architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v2	Two-Round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v3	Four-round architecture	romulusn1v12	Y	7	$2^{50}-1$
	Romulus-v4	Eight-round architecture	romulusn1v12	Y	7	$2^{50}-1$
15	SCHWAEMM-v1	Schwaemm-256128, AEAD only, Basic iterative architecture	schwaemm-256128v1	Y	8	N/A

Table 2 continued from previous page

No.	Variant Name	Variant Features	Reference Software	Key Reuse	Cycles New Key vs. Key Reuse	Max Length [bytes]
	SCHWAEMM-v2	Schwaemm-256128 and Esch256 AEAD+HASH	schwaemm-256128v1, esch256v1	Y	8	N/A
16	SpoC-v1	spoc64, Basic iterative architecture	spoc64 sliscplight 192v1	N/A	N/A	N/A
17	Spook-v2-v1	Folded architecture resource sharing Clyde128 Shadow512	spook 128su512v2	Y	7	unlimited
18	Subterranean-v1	32-bit bus	Candidate website	N		$2^{50}-1$
19	TinyJAMBU-v1	32-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU-v2	16-bit concurrent NLFSR	tinyjambu128	N		$2^{50}-1$
	TinyJAMBU-v3	Bit-serial NLFSR	tinyjambu128	N		$2^{50}-1$
20	WAGE-v1	Baseline	submitted with HW package	Y	7	N/A
21a	Xoodyak_GMU-v1	384-bit datapath AEAD+Hash	xoodyakv1	Y	18	unlimited
	Xoodyak_GMU-v2	128-bit datapath AEAD+Hash	xoodyakv1	Y	266	unlimited
21b	Xoodyak_XT-v1	Basic iterative architecture, AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v2	x2 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v3	x3 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v4	x4 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v5	x6 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v6	x12 Unrolled AEAD	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v7	Basic iterative architecture, AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v8	x2 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v9	x3 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v10	x4 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v11	x6 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$
	Xoodyak_XT-v12	x12 Unrolled AEAD+Hash	xoodyakv1	N		$2^{50}-1$

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

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

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

Table 3 continued from previous page

No.	Variant Name	AD Block Size [bits]	Cycles per AD Block	PT-CT Block Size [bits]	Cycles per PT-CT Block	Hash Msg. Block Size [bits]	Cycles per Hash Msg Block	$\frac{\text{AD Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{PT Dec Thr}}{\text{PT Enc Thr}}$	$\frac{\text{AD+PT Enc Thr}}{\text{PT Enc Thr}}$	$\frac{\text{Hash Thr}}{\text{PT Enc Thr}}$
	Romulus-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	
15	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	
16	SpoC-v1	64	109	64	111			1.02	1.00	1.01	
17	Spook-v2-v1	256	48	256	48			1.00	1.00	1.00	
18	Subterranean-v1	8	0.25	8	0.25	8	2	1.00	1.00	1.00	0.13
19	TinyJAMBU-v1	32	14	32	34			2.43	1.00	1.42	
	TinyJAMBU-v2	32	26	32	66			2.54	1.00	1.43	
	TinyJAMBU-v3	32	386	32	1,026			2.66	1.00	1.45	
20	WAGE-v1	64	114	64	114			1.00	1.00	1.00	
21a	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
21b	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

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.

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

3.1 Unique Features

Most of the designs assume the following standard order of segments provided at the Public Data Input (PDI) ports during encryption: Public Message Number (Npub), Associated

Data (AD), Plaintext (PT). For decryption, the corresponding order is: Public Message Number (Npub), Associated Data (AD), Ciphertext (PT), and Tag. For ESTATE, the order for decryption is changed to Npub, AD, Tag, Ciphertext. For ISAP, the order for encryption is: Npub, Plaintext, AD; the order for decryption is: Npub, AD, Ciphertext, Tag. For Romulus, the order for encryption is: AD, Npub, Plaintext; the order for decryption is: AD, Npub, Ciphertext, Tag.

Subterranean 2.0 is the only design that uses an unconventional maximum segment size of 2^{15}, instead of the recommended $2^{16} - 1$. This feature does not considerably affect the interoperability, 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.

4 Results and Their Analysis

4.1 Results of Functional Verification and Timing Measurements

All variants of 20 out of 24 hardware designs passed all GMU known-answer tests (KATs) and produced reliable timing measurements.

The exceptions were as follows:

- SpoC-v1, ESTATE-v2, and ESTATE-v4 did not pass GMU KATs and did not produce reliable timing measurements. As a result, only their throughputs for long inputs are reported in this paper.
- COMET_VT-v1, ESTATE-v1, and ESTATE-v3 did not pass all tests, but produced consistent timing measurements. All their performance metrics are reported in the subsequent subsections, but should be treated as preliminary, and subject to at least minor changes after these designs are fully debugged.

4.2 Results of Synthesis

ISAP was the only design which did not pass synthesis using Intel Quartus Prime targeting Cyclone 10 LP FPGA. The same code passed synthesis and implementation using Xilinx Vivado and Lattice Diamond Software.

Initial versions of several other 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 three-week benchmarking period.

4.3 Throughputs for Long Inputs

4.3.1 Results for Xilinx Artix-7

The two-dimensional graphs Throughput vs. Number of Used LUTs are shown in Figs. 2, 3, and 4. The throughputs concern the cases of Plaintext (PT) only, Associated Data (AD) only, and equal-size AD+PT, respectively. All three mentioned above graphs concern results for the Xilinx Artix-7 FPGA xc7a12tcsg325-3. The results apply to long inputs. We use the logarithmic scale on both axes. Dashed lines represent the same throughput over area ratio. In the legends of these figures, the algorithms are listed in the order of decreasing throughput. While the order of the symbols remains the same, the mapping of symbol to algorithm changes. The corresponding detailed numerical results can be found in Tables 4, 5, and 6.

The clear winner for all three types of inputs is Subterranean 2.0. Its implementation is approximately two times faster than its closest competitor. Additionally, out of designs shown in these graphs, only TinyJAMBU uses fewer LUTs. The next group include

the fastest architectures of Xoodyak, Ascon, and KNOT, exceeding 1500 Mbits/s for all input types. Out of them, KNOT is the smallest and Xoodyak the largest, but not by a high margin. They are followed by DryGASCON and COMET, separated by 3%-29% from each other in terms of Throughput, and swapping places depending on the input type. DryGASCON is better in processing plaintext, while COMET excels in processing AD. However, the implementation of COMET requires significantly more LUTs compared to the implementation of DryGASCON. Next come Romulus and Spook, with the implementation of Romulus faster in two out of three categories and significantly smaller than the implementation of Spook.

The design of SCHWAEMM-v1 is by far the largest, yet still only average (rank 10 or 11) in terms of Throughput. More effort is required to demonstrate the competitiveness of this algorithm with the first 8 candidates mentioned above.

The designs for LOCUS and Pyjamasks seem to be both aiming at the proposed optimization target of 2000 LUTs, but fail to achieve performance comparable to the first eight algorithms in the rankings. PHOTON-Beetle, Elephant, and ISAP come somewhat closer, but still significantly below at least the first six.

Among the other designs, TinyJAMBU-v1 distinguishes itself from the competition with the smallest area and average Throughput. The designs for Gimli, Spoc, WAGE, and GIFT-COFB are all in the vicinity of 1000 LUTs, and clearly were not optimized for the maximum throughput assuming the resource utilization of 2000 LUTs or less. To the lower extent, the designs for ESTATE and Oribatida, both slightly below 1500 LUTs, are also too small to be fairly compared with others. As a result, it would be too premature to assign any negative evaluation to these candidates.

Only 7 out of 21 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 detailed results are summarized in Table 13. The two fastest designs are Xoodyak_XT-v7 and and DryGASCON-v1, both reaching the throughput of about 1500 Mbits/s. They are followed by Ascon_Graz-v2 at about 1000 Mbit/s and Subterranean-v1 at around 750 Mbits/s. SCHWAEMM-v2 (ESCH) reaches slightly less than 500 Mbit/s, and Photon around 225 Mbits/s. The current implementation of Gimli is by far the slowest at around 40 Mbits. On the other hand, it is also the second smallest, approximately as large as the implementation of Subterranean-v1.

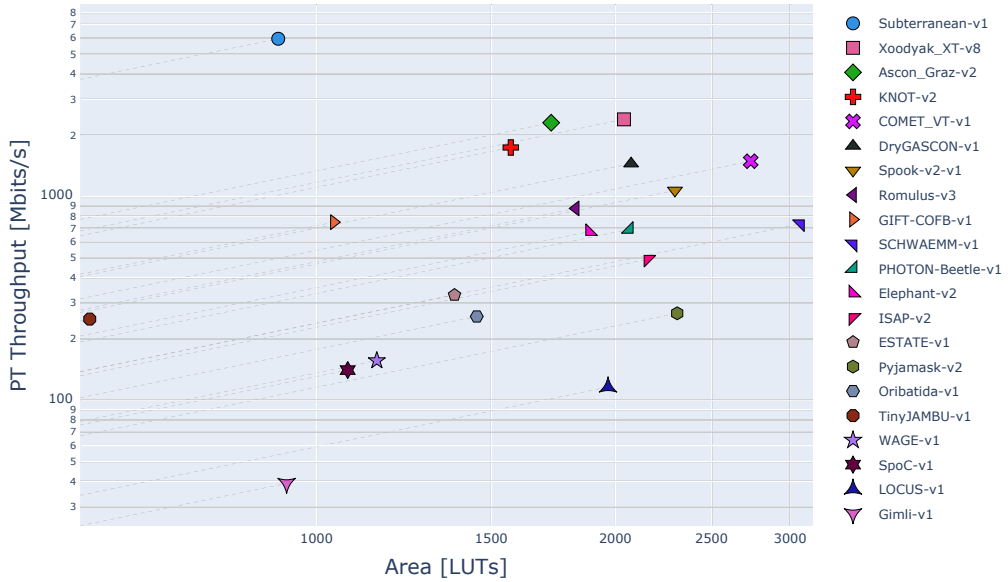

Figure 2: Artix-7 Encryption PT Throughput for Long Messages vs LUTs

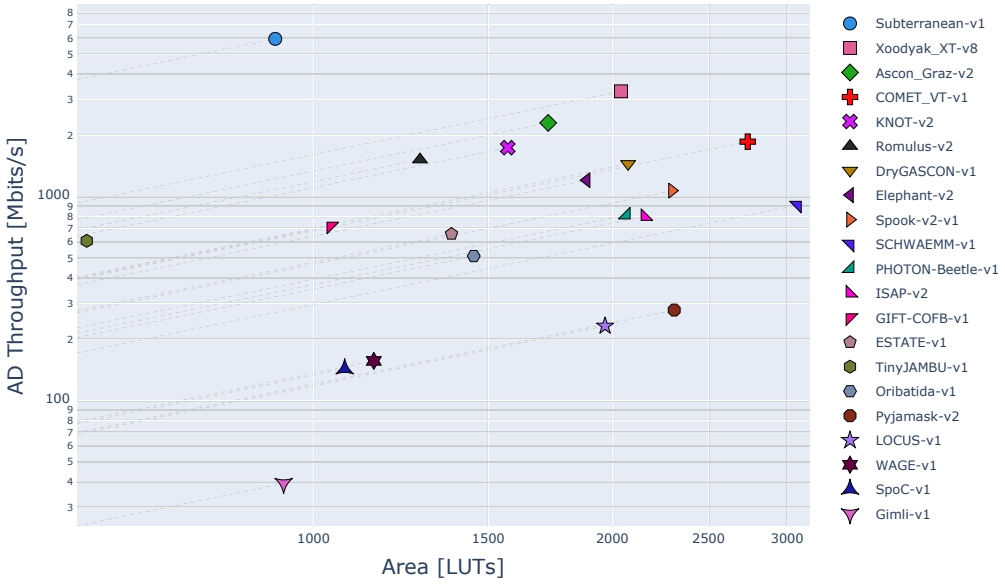

Figure 3: Artix-7 Encryption AD Throughput for Long Messages vs LUTs

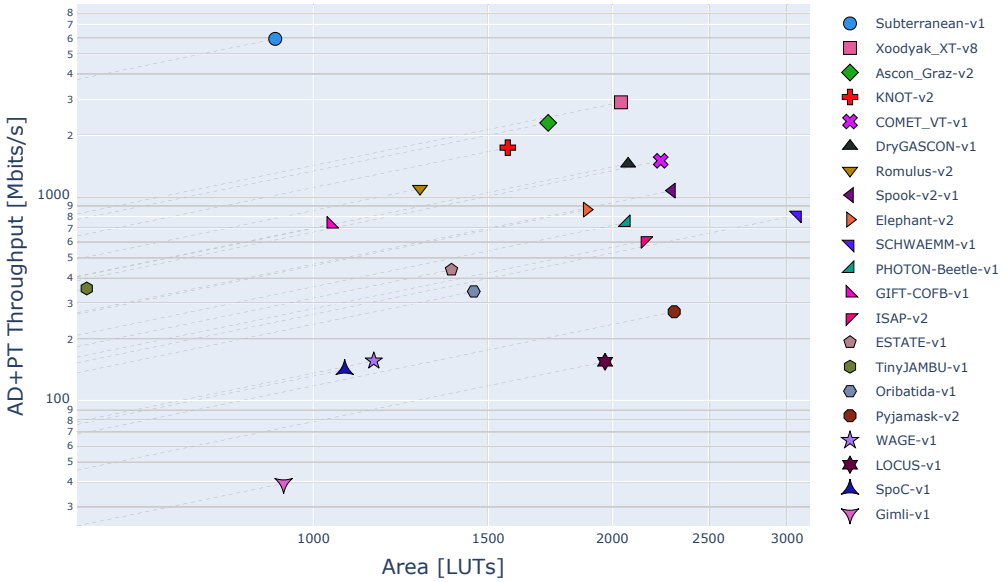

Figure 4: Artix-7 Encryption AD+PT Throughput for Long Messages vs LUTs

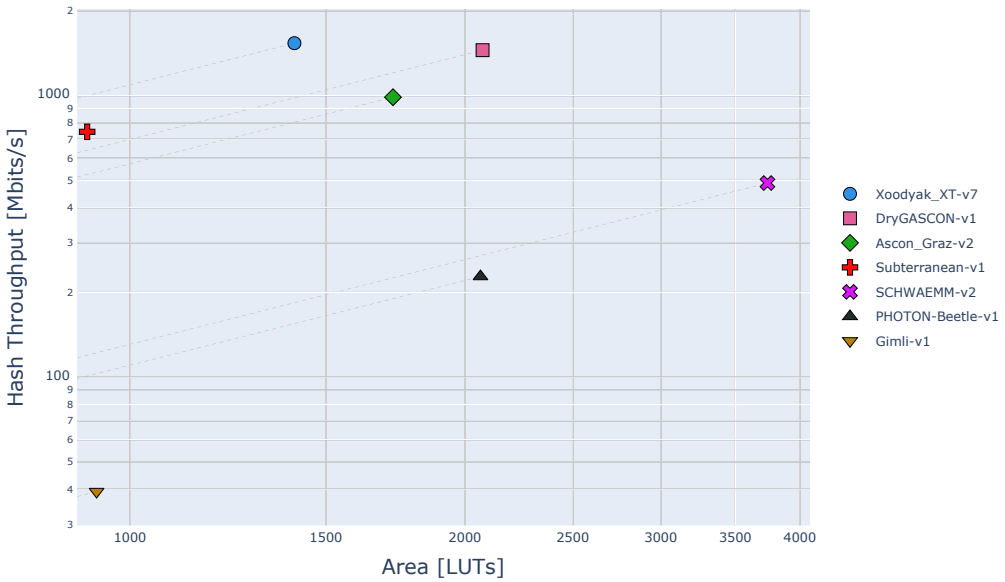

Figure 5: Artix-7 Hashing Throughput for Long Messages vs LUTs

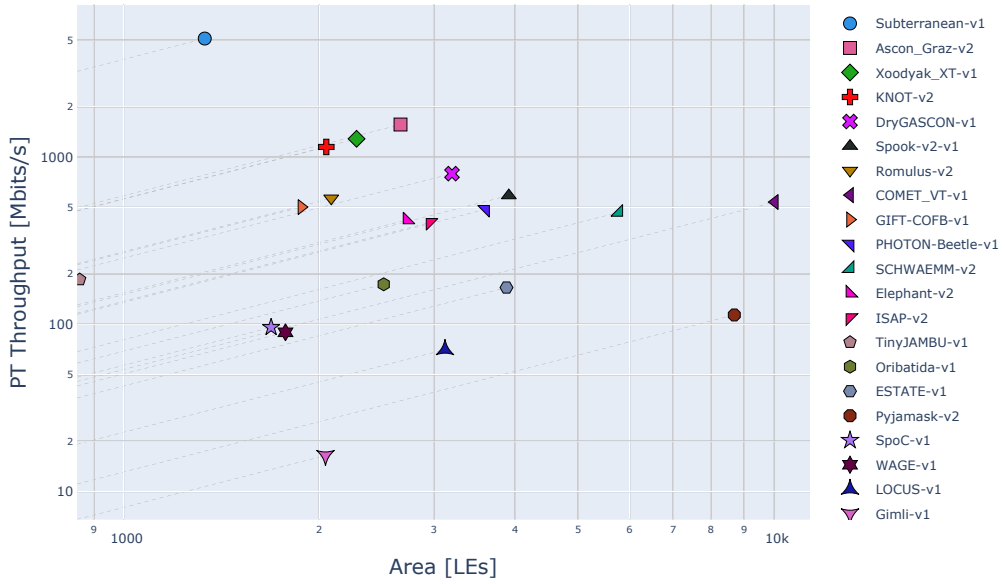

Figure 6: Cyclone-10-LP Encryption PT Throughput for Long Messages vs LEs

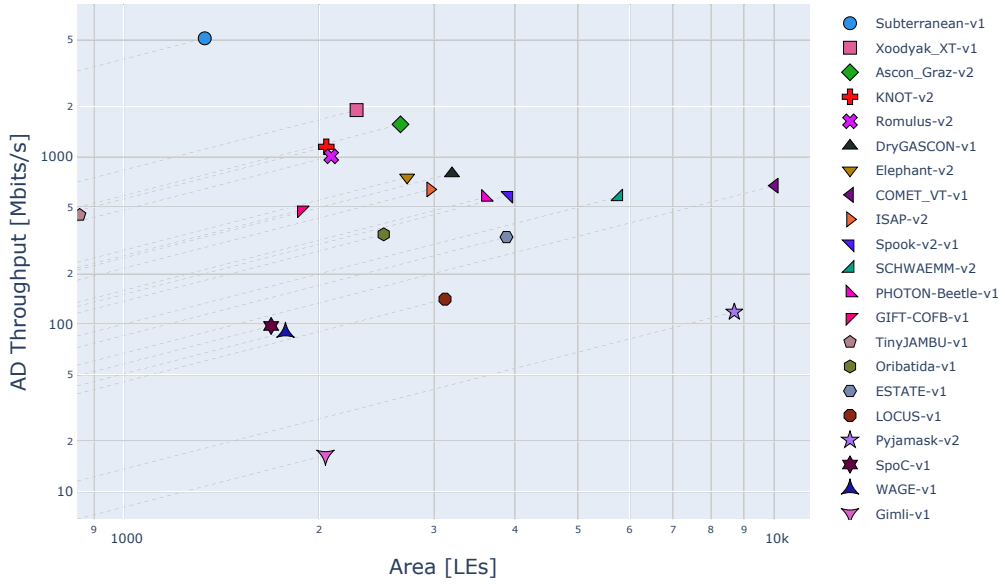

Figure 7: Cyclone-10-LP Encryption AD Throughput for Long Messages vs LEs

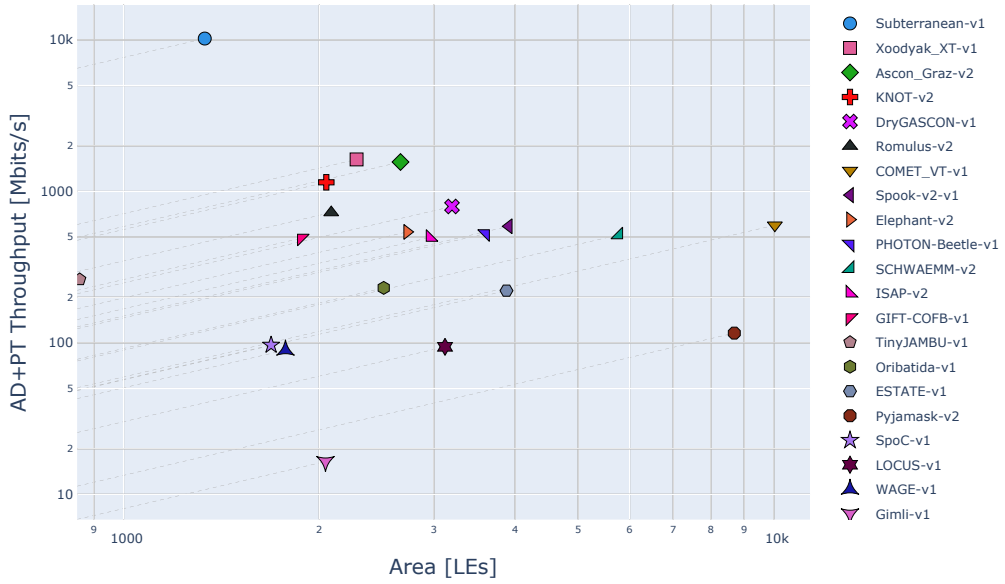

Figure 8: Cyclone-10-LP Encryption AD+PT Throughput for Long Messages vs LEs

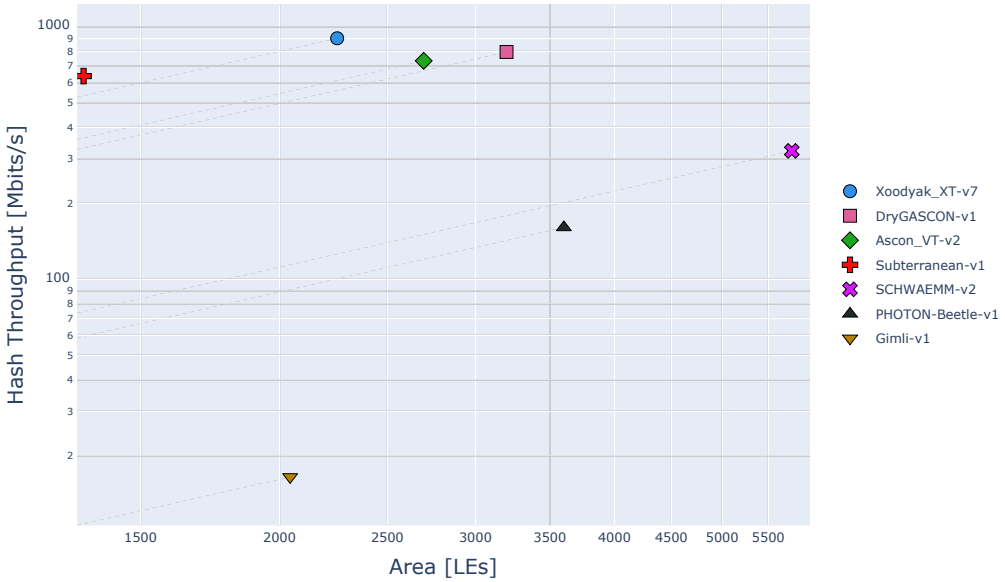

Figure 9: Cyclone-10-LP Hashing Throughput for Long Messages vs LEs

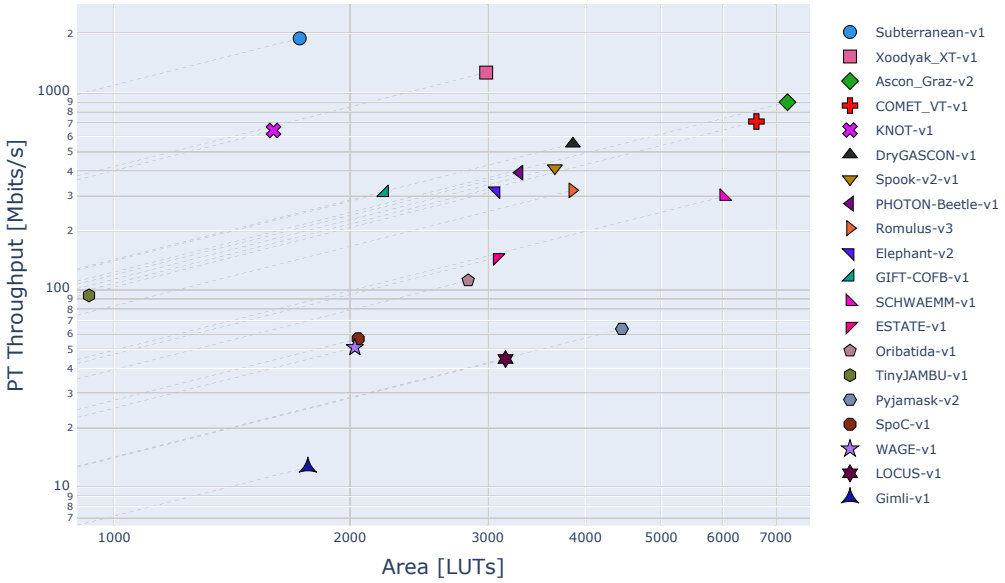

Figure 10: ECP5 Encryption PT Throughput for Long Messages vs LUTs

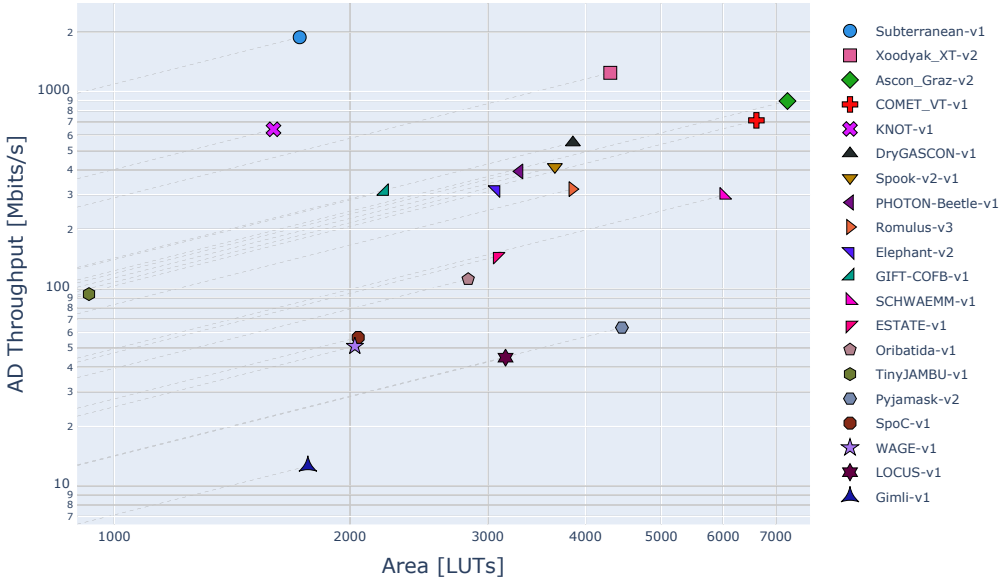

Figure 11: ECP5 Encryption AD Throughput for Long Messages vs LUTs

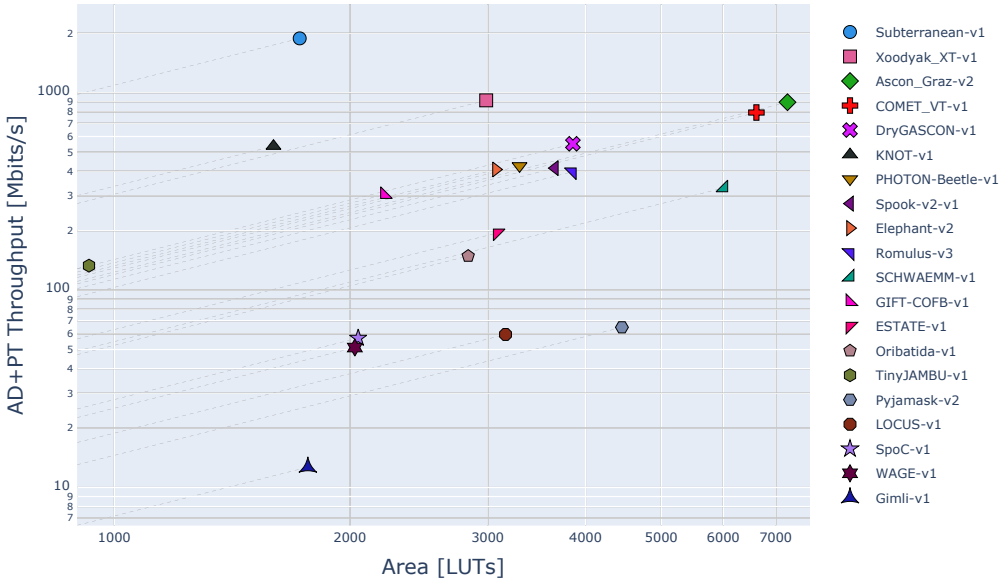

Figure 12: ECP5 Encryption AD+PT Throughput for Long Messages vs LUTs

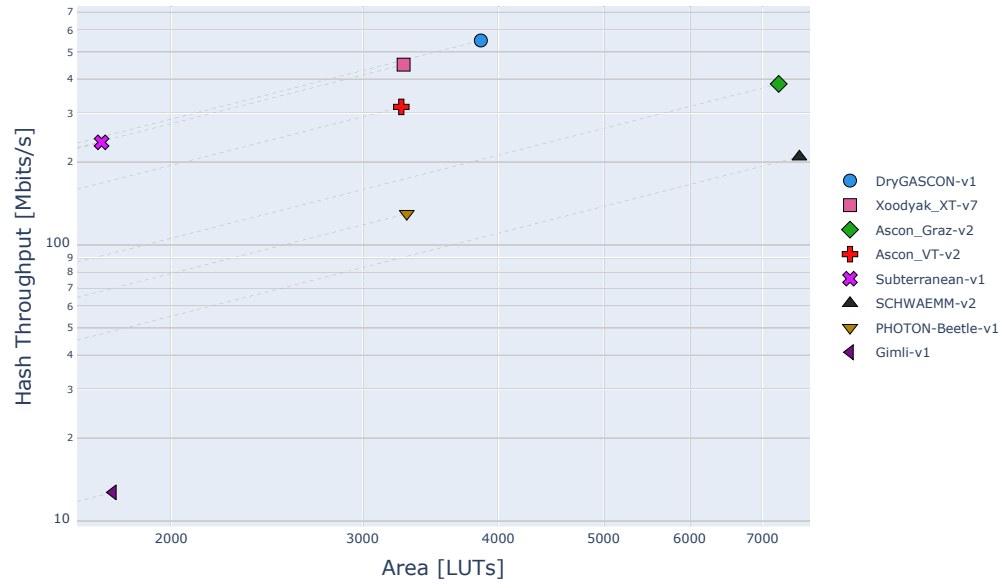

Figure 13: ECP5 Hashing Throughput for Long Messages vs LUTs

4.3.2 Results for Intel Cyclone 10 LP and Lattice Semiconductor ECP5

The equivalent graphs for Intel Cyclone 10 LP are shown in Figs. 6, 7, 8, and 9. The corresponding tables are listed as Tables 7, 8, 9, and 14. The conclusions from these tables and graphs are very close to the conclusions based on the results for the Artix-7 FPGA. The exceptions include the relatively much larger area in the cases of COMET_VT-v1, Pyjamask-v2, and ESTATE-v1. Additionally, the area of Gimli-v1 is not any longer comparable to Subterranean-v1 but rather becomes similar to KNOT-v2. For hashing, the differences in Throughput among the first four algorithms become smaller.

In Table 16, the ratios between the numbers of Cyclone 10 LP LEs vs. Artix-7 LUTs are provided. The average ratio is 1.93. However, the actual ratios vary in a relatively wide range, between 1.27 for Ascon_VT-v1 and 4.76 for Xoodyak_GMU-v2. Additionally, the following designs have significantly larger area in LEs for Cyclone 10 LP FPGAs as compared to the area in LUTs for Artix-7: Xoodyak_GMU-v2, Pyjamask-v1, Pyjamask-v2, COMET_VT-v1, and COMET_VT-v2. The average ratios of the numbers of FFs and clock frequencies, in Cyclone 10 LP vs. Artix-7, are 1.98 and 1.69, respectively.

The two-dimesional graphs for Lattice Semiconductor ECP5 are shown in Figs. 10, 11, 12, and 13. The corresponding tables are listed as Tables 10, 11, 12, and 15. The conclusions from these tables and graphs are relatively close to the conclusions based on the results for the Artix-7 FPGA.

In Table 17, 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 2.01 for LUTs, 1.13 for FFs, and 2.78 for frequencies. However, the actual ratios vary in a relatively wide range. For example, the ratio of LUTs varies between 1.35 for KNOT-v4 and 5.17 for ISAP-v2. In particular, the following designs have significantly larger area in LUTs for ECP5 as compared to Artix-7: ISAP-v2, ISAP-v1, Ascon_Graz-v2, and Ascon_Graz-v1. Additionally, the areas of ISAP-v1 and ISAP-v2 reached 16,179 and 11,158 LUTs, respectively, well above the threshold of 7,500 LUTs used to create graphs shown in Figs. 10, 11, 12.

The ranking of candidates depending on the FPGA family used is summarized in Tables 18, 19, and 20, for PT only, AD only, and AD+PT, respectively. The major differences are as follows: Cyclone 10 LP seems to favor Ascon vs. Xoodyak, but only in the case of processing PT. On Cyclone 10 LP, the ranking of COMET_VT-v1 drops by 3-4 positions vs. Artix-7 and ECP5. At the same time, the ranking of TinyJAMBU-v1 increases by 1-3 positions vs. Artix-7. The ranking of PHOTON-Beetle improves by 3-5 positions and the ranking of ISAP-v1 drops by 0-4 positions between Artix-7 and ECP5. The changes in positions of other algorithms are relatively minor.

4.3.3 Resource Utilization and Maximum Clock Frequency

The details of resource utilization and maximum clock frequency for all evaluated designs are provided in the Appendix, in Tables 24, 25, and 26. In these tables design variants are listed in the order from the lowest to the highest number of LUTs/LEs. The corresponding rankings of candidates are provided as well. It should be stressed that these rankings should not be used to evaluate LWC candidates, as their designs were not optimized for the minimum possible area. They however can be used to see that the implemented architectures of all candidates span a relatively wide range of the resource utilization values, from about 500 to 3750 LUTs in Artix-7 FPGAs, from about 800 to 10,000 LEs in Cyclone 10 LP, and from about 900 to 16,000 LUTs for ECP5.

4.3.4 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.

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

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per PT block**	**PT block size [bits]**
Subterranean-v1	5,952.0	1	915	186	0.2	8
Xoodyak_XT-v8	2,393.6	2	2,040	187	15.0	192
Xoodyak_XT-v2	2,342.4		2,071	183	15.0	192
Ascon_Graz-v2	2,304.0	3	1,723	216	12.0	128
Xoodyak_XT-v1	2,130.3		1,405	233	21.0	192
Xoodyak_XT-v7	2,084.6		1,405	228	21.0	192
KNOT-v2	1,741.7	4	1,569	254	28.0	192
Xoodyak_GMU-v1	1,717.9		1,808	170	19.0	192
Ascon_Graz-v1	1,672.0		1,551	209	8.0	64
Ascon_VT-v2	1,557.3		1,928	219	9.0	64
Ascon_VT-v1	1,491.2		1,913	233	10.0	64
COMET_VT-v1	1,491.2	5	2,737	233	20.0	128
DryGASCON-v1	1,450.7	6	2,074	238	21.0	128
Spook-v2-v1	1,072.0	7	2,296	201	48.0	256
Romulus-v3	874.7	8	1,824	123	18.0	128
Romulus-v2	856.0		1,280	214	32.0	128
GIFT-COFB-v1	748.9	9	1,041	275	47.0	128
SCHWAEMM-v1	735.3	10	3,071	135	47.0	256
SCHWAEMM-v2	708.1		3,740	130	47.0	256
PHOTON-Beetle-v1	690.4	11	2,065	178	33.0	128
Romulus-v4	674.9		2,602	58	11.0	128
Elephant-v2	673.5	12	1,884	181	43.0	160
ISAP-v1	661.7	13	3,491	193	42.0	144
KNOT-v3	633.6		1,367	264	40.0	96
KNOT-v4	630.2		1,783	256	52.0	128
KNOT-v1	594.3		1,092	260	28.0	64
ISAP-v2	492.3		2,157	200	26.0	64
Romulus-v1	488.5		953	229	60.0	128
COMET_CI-v1	407.8		1,884	223	70.0	128
COMET_VT-v2	336.5		1,703	234	89.0	128
ESTATE-v1	328.7	14	1,377	226	88.0	128
Pyjamask-v2	267.3	15	2,308	213	102.0	128
Oribatida-v1	257.9	16	1,450	276	137.0	128
TinyJAMBU-v1	250.4	17	591	266	34.0	32
Elephant-v1	214.3		1,291	229	171.0	160
WAGE-v1	156.6	18	1,150	279	114.0	64
SpoC-v1	140.7	19	1,075	244	111.0	64
TinyJAMBU-v2	129.9		564	268	66.0	32
Xoodyak_GMU-v2	123.6		1,234	168	261.0	192
LOCUS-v1	116.2	20	1,966	207	114.0	64
Pyjamask-v1	111.9		1,979	229	262.0	128
COMET_CI-v2	95.7		1,096	222	297.0	128
LOTUS-v1	81.4		1,652	145	114.0	64
ESTATE-v3	80.0		1,197	255	408.0	128
ESTATE-v2	78.4		893	277	452.0	128
Gimli-v1	39.1	21	933	241	789.0	128
ESTATE-v4	25.5		944	277	1,392.0	128
Gimli-v2	21.1		905	244	1,481.0	128
Gimli-v3	11.3		838	253	2,865.0	128
TinyJAMBU-v3	8.7		537	278	1,026.0	32

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

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per AD Block	AD Block Size [bits]
Subterranean-v1	5,952.0	1	915	186	0.2	8
Xoodyak_XT-v8	3,291.2	2	2,040	187	20.0	352
Xoodyak_XT-v2	3,220.8		2,071	183	20.0	352
Xoodyak_XT-v1	3,154.5		1,405	233	26.0	352
Xoodyak_XT-v7	3,086.8		1,405	228	26.0	352
Xoodyak_GMU-v1	2,493.3		1,808	170	24.0	352
Ascon_Graz-v2	2,304.0	3	1,723	216	12.0	128
COMET_VT-v1	1,864.0	4	2,737	233	16.0	128
KNOT-v2	1,741.7	5	1,569	254	28.0	192
Ascon_Graz-v1	1,672.0		1,551	209	8.0	64
Romulus-v2	1,521.8	6	1,280	214	18.0	128
Ascon_VT-v1	1,491.2		1,913	233	10.0	64
DryGASCON-v1	1,450.7	7	2,074	238	21.0	128
Romulus-v3	1,431.3		1,824	123	11.0	128
Ascon_VT-v2	1,401.6		1,928	219	10.0	64
Elephant-v2	1,206.7	8	1,884	181	24.0	160
ISAP-v1	1,111.7	9	3,491	193	25.0	144
Spook-v2-v1	1,072.0	10	2,296	201	48.0	256
Romulus-v4	989.9		2,602	58	7.5	128
Romulus-v1	916.0		953	229	32.0	128
SCHWAEMM-v1	909.5	11	3,071	135	38.0	256
SCHWAEMM-v2	875.8		3,740	130	38.0	256
PHOTON-Beetle-v1	813.7	12	2,065	178	28.0	128
ISAP-v2	800.0		2,157	200	16.0	64
GIFT-COFB-v1	718.4	13	1,041	275	49.0	128
ESTATE-v1	657.5	14	1,377	226	44.0	128
KNOT-v3	633.6		1,367	264	40.0	96
KNOT-v4	630.2		1,783	256	52.0	128
TinyJAMBU-v1	608.0	15	591	266	14.0	32
KNOT-v1	594.3		1,092	260	28.0	64
Oribatida-v1	512.0	16	1,450	276	69.0	128
COMET_CI-v1	475.7		1,884	223	60.0	128
Elephant-v1	416.4		1,291	229	88.0	160
COMET_VT-v2	352.4		1,703	234	85.0	128
TinyJAMBU-v2	329.8		564	268	26.0	32
Pyjamask-v2	278.2	17	2,308	213	98.0	128
LOCUS-v1	232.4	18	1,966	207	57.0	64
Xoodyak_GMU-v2	222.3		1,234	168	266.0	352
LOTUS-v1	162.8		1,652	145	57.0	64
ESTATE-v3	160.0		1,197	255	204.0	128
ESTATE-v2	156.9		893	277	226.0	128
WAGE-v1	156.6	19	1,150	279	114.0	64
SpoC-v1	143.3	20	1,075	244	109.0	64
Pyjamask-v1	113.6		1,979	229	258.0	128
COMET_CI-v2	107.6		1,096	222	264.0	128
ESTATE-v4	50.9		944	277	696.0	128
Gimli-v1	39.2	21	933	241	786.0	128
TinyJAMBU-v3	23.0		537	278	386.0	32
Gimli-v2	21.2		905	244	1,474.0	128
Gimli-v3	11.4		838	253	2,850.0	128

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

Variant	**Throughput AE AD+PT Long [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles per AD+PT block**	**AD Block Size [bits]**	**PT Block Size [bits]**
Subterranean-v1	5,952.0	1	915	186	0.5	8	8
Xoodyak_XT-v8	2,906.5	2	2,040	187	35.0	352	192
Xoodyak_XT-v2	2,844.3		2,071	183	35.0	352	192
Xoodyak_XT-v1	2,696.9		1,405	233	47.0	352	192
Xoodyak_XT-v7	2,639.0		1,405	228	47.0	352	192
Ascon_Graz-v2	2,304.0	3	1,723	216	24.0	128	128
Xoodyak_GMU-v1	2,150.7		1,808	170	43.0	352	192
KNOT-v2	1,741.7	4	1,569	254	56.0	192	192
Ascon_Graz-v1	1,672.0		1,551	209	16.0	64	64
COMET_VT-v1	1,656.9	5	2,737	233	36.0	128	128
Ascon_VT-v1	1,491.2		1,913	233	20.0	64	64
Ascon_VT-v2	1,475.4		1,928	219	19.0	64	64
DryGASCON-v1	1,450.7	6	2,074	238	42.0	128	128
Romulus-v2	1,095.7	7	1,280	214	50.0	128	128
Romulus-v3	1,085.8		1,824	123	29.0	128	128
Spook-v2-v1	1,072.0	8	2,296	201	96.0	256	256
Elephant-v2	864.5	9	1,884	181	67.0	160	160
ISAP-v1	829.6	10	3,491	193	67.0	144	144
SCHWAEMM-v1	813.2	11	3,071	135	85.0	256	256
Romulus-v4	802.6		2,602	58	18.5	128	128
SCHWAEMM-v2	783.1		3,740	130	85.0	256	256
PHOTON-Beetle-v1	747.0	12	2,065	178	61.0	128	128
GIFT-COFB-v1	733.3	13	1,041	275	96.0	128	128
Romulus-v1	637.2		953	229	92.0	128	128
KNOT-v3	633.6		1,367	264	80.0	96	96
KNOT-v4	630.2		1,783	256	104.0	128	128
ISAP-v2	609.5		2,157	200	42.0	64	64
KNOT-v1	594.3		1,092	260	56.0	64	64
COMET_CI-v1	439.1		1,884	223	130.0	128	128
ESTATE-v1	438.3	14	1,377	226	132.0	128	128
TinyJAMBU-v1	354.7	15	591	266	48.0	32	32
COMET_VT-v2	344.3		1,703	234	174.0	128	128
Oribatida-v1	343.0	16	1,450	276	206.0	128	128
Elephant-v1	282.9		1,291	229	259.0	160	160
Pyjamask-v2	272.6	17	2,308	213	200.0	128	128
TinyJAMBU-v2	186.4		564	268	92.0	32	32
Xoodyak_GMU-v2	173.4		1,234	168	527.0	352	192
WAGE-v1	156.6	18	1,150	279	228.0	64	64
LOCUS-v1	154.9	19	1,966	207	171.0	64	64
SpoC-v1	142.0	20	1,075	244	220.0	64	64
Pyjamask-v1	112.7		1,979	229	520.0	128	128
LOTUS-v1	108.5		1,652	145	171.0	64	64
ESTATE-v3	106.7		1,197	255	612.0	128	128
ESTATE-v2	104.6		893	277	678.0	128	128
COMET_CI-v2	101.3		1,096	222	561.0	128	128
Gimli-v1	39.2	21	933	241	1,575.0	128	128
ESTATE-v4	34.0		944	277	2,088.0	128	128
Gimli-v2	21.1		905	244	2,955.0	128	128
TinyJAMBU-v3	12.6		537	278	1,412.0	32	32
Gimli-v3	11.3		838	253	5,715.0	128	128

Table 7: Intel Cyclone 10 LP Encryption PT Throughput for Long Messages

Variant	**Throughput AE PT Long [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles per PT Block**	**PT Block Size [bits]**
Subterranean-v1	5,108.5	1	1,333	159.6	0.2	8
Ascon_Graz-v2	1,564.3	2	2,666	146.7	12.0	128
Xoodyak_XT-v1	1,285.0	3	2,282	140.6	21.0	192
Xoodyak_XT-v7	1,223.6		2,253	133.8	21.0	192
Ascon_VT-v2	1,223.1		2,695	172.0	9.0	64
Ascon_Graz-v1	1,222.3		2,484	152.8	8.0	64
Xoodyak_XT-v8	1,169.3		4,337	91.3	15.0	192
KNOT-v2	1,148.6	4	2,050	167.5	28.0	192
Ascon_VT-v1	1,130.4		2,432	176.6	10.0	64
Xoodyak_XT-v2	1,124.4		3,518	87.8	15.0	192
Xoodyak_GMU-v1	1,079.1		3,135	106.8	19.0	192
DryGASCON-v1	795.6	5	3,199	130.5	21.0	128
Spook-v2-v1	588.7	6	3,912	110.4	48.0	256
Romulus-v2	566.8	7	2,086	141.7	32.0	128
Romulus-v3	563.9		2,407	79.3	18.0	128
COMET_VT-v1	538.3	8	10,035	84.1	20.0	128
GIFT-COFB-v1	502.2	9	1,877	184.4	47.0	128
PHOTON-Beetle-v1	486.6	10	3,602	125.4	33.0	128
Romulus-v4	469.6		3,409	40.4	11.0	128
SCHWAEMM-v2	467.0	11	5,773	85.7	47.0	256
SCHWAEMM-v1	445.3		4,713	81.8	47.0	256
KNOT-v4	421.8		2,412	171.3	52.0	128
Elephant-v2	421.0	12	2,729	113.2	43.0	160
KNOT-v3	409.6		1,962	170.7	40.0	96
ISAP-v2	406.7	13	2,961	139.8	22.0	64
KNOT-v1	406.6		1,485	177.9	28.0	64
Romulus-v1	305.6		1,735	143.2	60.0	128
COMET_CI-v1	211.7		4,663	115.8	70.0	128
TinyJAMBU-v1	185.2	14	856	196.8	34.0	32
Oribatida-v1	173.5	15	2,512	185.7	137.0	128
ESTATE-v1	165.9	16	3,880	114.1	88.0	128
COMET_VT-v2	159.1		5,204	110.6	89.0	128
Elephant-v1	152.6		2,056	163.1	171.0	160
Pyjamask-v2	113.7	17	8,692	90.6	102.0	128
SpoC-v1	95.9	18	1,686	166.3	111.0	64
TinyJAMBU-v2	95.1		841	196.2	66.0	32
WAGE-v1	89.6	19	1,774	159.6	114.0	64
LOCUS-v1	70.6	20	3,121	125.8	114.0	64
LOTUS-v1	58.1		2,642	103.5	114.0	64
COMET_CI-v2	57.3		2,629	132.9	297.0	128
Xoodyak_GMU-v2	56.7		5,871	77.0	261.0	192
ESTATE-v3	54.4		2,320	173.4	408.0	128
Pyjamask-v1	53.6		8,599	109.7	262.0	128
ESTATE-v2	49.4		1,946	174.3	452.0	128
ESTATE-v4	18.4		1,572	200.1	1,392.0	128
Gimli-v1	16.4	21	2,044	101.3	789.0	128
Gimli-v2	8.4		2,074	97.3	1,481.0	128
TinyJAMBU-v3	6.0		817	191.1	1,026.0	32
Gimli-v3	4.5		2,115	100.5	2,865.0	128

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

Variant	Throughput AE AD Long [Mbits/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per AD Block	AD Block Size [bits]
Subterranean-v1	5,108.5	1	1,333	159.6	0.2	8
Xoodyak_XT-v1	1,902.8	2	2,282	140.6	26.0	352
Xoodyak_XT-v7	1,811.9		2,253	133.8	26.0	352
Xoodyak_XT-v8	1,607.8		4,337	91.3	20.0	352
Xoodyak_GMU-v1	1,566.3		3,135	106.8	24.0	352
Ascon_Graz-v2	1,564.3	3	2,666	146.7	12.0	128
Xoodyak_XT-v2	1,546.0		3,518	87.8	20.0	352
Ascon_Graz-v1	1,222.3		2,484	152.8	8.0	64
KNOT-v2	1,148.6	4	2,050	167.5	28.0	192
Ascon_VT-v1	1,130.4		2,432	176.6	10.0	64
Ascon_VT-v2	1,100.8		2,695	172.0	10.0	64
Romulus-v2	1,007.6	5	2,086	141.7	18.0	128
Romulus-v3	922.8		2,407	79.3	11.0	128
DryGASCON-v1	795.6	6	3,199	130.5	21.0	128
Elephant-v2	754.3	7	2,729	113.2	24.0	160
Romulus-v4	688.8		3,409	40.4	7.5	128
COMET_VT-v1	672.9	8	10,035	84.1	16.0	128
ISAP-v2	639.1	9	2,961	139.8	14.0	64
Spook-v2-v1	588.7	10	3,912	110.4	48.0	256
SCHWAEMM-v2	577.6	11	5,773	85.7	38.0	256
PHOTON-Beetle-v1	573.4	12	3,602	125.4	28.0	128
Romulus-v1	573.0		1,735	143.2	32.0	128
SCHWAEMM-v1	550.7		4,713	81.8	38.0	256
GIFT-COFB-v1	481.7	13	1,877	184.4	49.0	128
TinyJAMBU-v1	449.9	14	856	196.8	14.0	32
KNOT-v4	421.8		2,412	171.3	52.0	128
KNOT-v3	409.6		1,962	170.7	40.0	96
KNOT-v1	406.6		1,485	177.9	28.0	64
Oribatida-v1	344.4	15	2,512	185.7	69.0	128
ESTATE-v1	331.8	16	3,880	114.1	44.0	128
Elephant-v1	296.5		2,056	163.1	88.0	160
COMET_CI-v1	246.9		4,663	115.8	60.0	128
TinyJAMBU-v2	241.4		841	196.2	26.0	32
COMET_VT-v2	166.6		5,204	110.6	85.0	128
LOCUS-v1	141.2	17	3,121	125.8	57.0	64
Pyjamask-v2	118.4	18	8,692	90.6	98.0	128
LOTUS-v1	116.2		2,642	103.5	57.0	64
ESTATE-v3	108.8		2,320	173.4	204.0	128
Xoodyak_GMU-v2	102.0		5,871	77.0	266.0	352
ESTATE-v2	98.7		1,946	174.3	226.0	128
SpoC-v1	97.7	19	1,686	166.3	109.0	64
WAGE-v1	89.6	20	1,774	159.6	114.0	64
COMET_CI-v2	64.5		2,629	132.9	264.0	128
Pyjamask-v1	54.4		8,599	109.7	258.0	128
ESTATE-v4	36.8		1,572	200.1	696.0	128
Gimli-v1	16.5	21	2,044	101.3	786.0	128
TinyJAMBU-v3	15.8		817	191.1	386.0	32
Gimli-v2	8.5		2,074	97.3	1,474.0	128
Gimli-v3	4.5		2,115	100.5	2,850.0	128

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

Variant	Through-put AE AD+PT Long [Mbits/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per AD+PT Block	AD Block Size [bits]	PT Block Size [bits]
Subterranean-v1	10,217.0	1	1,333	159.6	0.2	8	8
Xoodyak_XT-v1	1,626.8	2	2,282	140.6	47.0	352	192
Ascon_Graz-v2	1,564.3	3	2,666	146.7	24.0	128	128
Xoodyak_XT-v7	1,549.0		2,253	133.8	47.0	352	192
Xoodyak_XT-v8	1,419.8		4,337	91.3	35.0	352	192
Xoodyak_XT-v2	1,365.3		3,518	87.8	35.0	352	192
Xoodyak_GMU-v1	1,351.0		3,135	106.8	43.0	352	192
Ascon_Graz-v1	1,222.3		2,484	152.8	16.0	64	64
Ascon_VT-v2	1,158.7		2,695	172.0	19.0	64	64
KNOT-v2	1,148.6	4	2,050	167.5	56.0	192	192
Ascon_VT-v1	1,130.4		2,432	176.6	20.0	64	64
DryGASCON-v1	795.6	5	3,199	130.5	42.0	128	128
Romulus-v2	725.5	6	2,086	141.7	50.0	128	128
Romulus-v3	700.0		2,407	79.3	29.0	128	128
COMET_VT-v1	598.1	7	10,035	84.1	36.0	128	128
Spook-v2-v1	588.7	8	3,912	110.4	96.0	256	256
Romulus-v4	558.5		3,409	40.4	18.5	128	128
Elephant-v2	540.4	9	2,729	113.2	67.0	160	160
PHOTON-Beetle-v1	526.4	10	3,602	125.4	61.0	128	128
SCHWAEMM-v2	516.5	11	5,773	85.7	85.0	256	256
ISAP-v2	497.1	12	2,961	139.8	36.0	64	64
SCHWAEMM-v1	492.4		4,713	81.8	85.0	256	256
GIFT-COFB-v1	491.7	13	1,877	184.4	96.0	128	128
KNOT-v4	421.8		2,412	171.3	104.0	128	128
KNOT-v3	409.6		1,962	170.7	80.0	96	96
KNOT-v1	406.6		1,485	177.9	56.0	64	64
Romulus-v1	398.6		1,735	143.2	92.0	128	128
TinyJAMBU-v1	262.4	14	856	196.8	48.0	32	32
Oribatida-v1	230.7	15	2,512	185.7	206.0	128	128
COMET_CI-v1	227.9		4,663	115.8	130.0	128	128
ESTATE-v1	221.2	16	3,880	114.1	132.0	128	128
Elephant-v1	201.5		2,056	163.1	259.0	160	160
COMET_VT-v2	162.8		5,204	110.6	174.0	128	128
TinyJAMBU-v2	136.5		841	196.2	92.0	32	32
Pyjamask-v2	116.0	17	8,692	90.6	200.0	128	128
SpoC-v1	96.8	18	1,686	166.3	220.0	64	64
LOCUS-v1	94.1	19	3,121	125.8	171.0	64	64
WAGE-v1	89.6	20	1,774	159.6	228.0	64	64
Xoodyak_GMU-v2	79.5		5,871	77.0	527.0	352	192
LOTUS-v1	77.5		2,642	103.5	171.0	64	64
ESTATE-v3	72.5		2,320	173.4	612.0	128	128
ESTATE-v2	65.8		1,946	174.3	678.0	128	128
COMET_CI-v2	60.7		2,629	132.9	561.0	128	128
Pyjamask-v1	54.0		8,599	109.7	520.0	128	128
ESTATE-v4	24.5		1,572	200.1	2,088.0	128	128
Gimli-v1	16.5	21	2,044	101.3	1,575.0	128	128
TinyJAMBU-v3	8.7		817	191.1	1,412.0	32	32
Gimli-v2	8.4		2,074	97.3	2,955.0	128	128
Gimli-v3	4.5		2,115	100.5	5,715.0	128	128

Table 10: Lattice ECP5 Encryption PT Throughput for Long Messages

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per PT block	PT Block Size[bits]
Subterranean-v1	1,884.8	1	1,725	58.9	0.2	8
Xoodyak_XT-v1	1,264.3	2	2,986	79.0	12.0	192
Xoodyak_XT-v2	1,044.2		4,302	70.7	13.0	192
Ascon_Graz-v2	894.9	3	7,246	83.9	12.0	128
Xoodyak_XT-v8	835.8		4,553	65.3	15.0	192
COMET_VT-v1	714.2	4	6,613	111.6	20.0	128
Ascon_Graz-v1	661.6		6,507	82.7	8.0	64
Xoodyak_GMU-v1	645.0		3,474	63.8	19.0	192
KNOT-v1	643.5	5	1,597	93.8	28.0	192
Xoodyak_XT-v7	611.3		3,272	66.9	21.0	192
DryGASCON-v1	551.0	6	3,854	90.4	21.0	128
Ascon_VT-v1	543.4		3,130	84.9	10.0	64
Xoodyak_XT-v9	531.7		5,614	36.0	13.0	192
Ascon_VT-v2	527.6		3,256	74.2	9.0	64
Xoodyak_XT-v10	462.5		6,899	26.5	11.0	192
Xoodyak_XT-v4	427.2		6,839	26.7	12.0	192
Spook-v2-v1	414.9	7	3,655	77.8	48.0	256
PHOTON-Beetle-v1	393.5	8	3,294	101.4	33.0	128
Xoodyak_XT-v3	350.2		5,569	38.3	21.0	192
Romulus-v3	320.0	9	3,847	45.0	18.0	128
Elephant-v2	318.1	10	3,073	85.5	43.0	160
GIFT-COFB-v1	311.3	11	2,214	114.3	47.0	128
SCHWAEMM-v2	302.3	12	7,570	55.5	47.0	256
SCHWAEMM-v1	297.9		6,008	54.7	47.0	256
Xoodyak_XT-v5	289.4		9,386	16.6	11.0	192
Romulus-v2	257.6		3,080	64.4	32.0	128
Romulus-v4	251.3		5,086	21.6	11.0	128
KNOT-v2	218.8		2,241	91.2	40.0	96
Xoodyak_XT-v11	212.4		9,447	16.6	15.0	192
KNOT-v3	204.7		2,037	83.2	52.0	128
ISAP-v1	196.6	13	16,179	57.4	42.0	144
KNOT-v4	195.7		2,408	85.6	28.0	64
Romulus-v1	168.1		2,633	78.8	60.0	128
ISAP-v2	161.2		11,158	65.5	26.0	64
COMET_CI-v1	147.9		3,427	80.9	70.0	128
ESTATE-v1	146.0	14	3,085	100.4	88.0	128
COMET_VT-v2	132.7		3,154	92.2	89.0	128
Oribatida-v1	111.8	15	2,832	119.7	137.0	128
TinyJAMBU-v1	93.9	16	928	99.7	34.0	32
Elephant-v1	91.2		2,368	97.5	171.0	160
Pyjamask-v2	63.5	17	4,452	50.6	102.0	128
SpoC-v1	56.6	18	2,049	98.2	111.0	64
WAGE-v1	51.1	19	2,029	91.1	114.0	64
TinyJAMBU-v2	48.0		913	99.0	66.0	32
Xoodyak_GMU-v2	47.1		2,803	64.0	261.0	192
LOCUS-v1	44.7	20	3,161	79.6	114.0	64
COMET_CI-v2	40.7		1,974	94.3	297.0	128
ESTATE-v3	32.6		2,029	104.0	408.0	128
Pyjamask-v1	32.2		4,094	66.0	262.0	128
LOTUS-v1	31.2		2,820	55.6	114.0	64
ESTATE-v2	25.6		1,691	90.5	452.0	128
Gimli-v1	12.6	21	1,767	78.0	789.0	128
ESTATE-v4	8.8		1,394	96.0	1,392.0	128
Gimli-v2	6.4		1,767	73.5	1,481.0	128
Gimli-v3	3.5		1,772	78.5	2,865.0	128
TinyJAMBU-v3	3.0		881	97.7	1,026.0	32

Table 11: Lattice ECP5 Encryption AD Throughput for Long Messages

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per AD Block	AD Block Size [bits]
Subterranean-v1	1,884.8	1	1,725	58.9	0.2	8
Xoodyak_XT-v2	1,244.3	2	4,302	70.7	20.0	352
Xoodyak_GMU-v1	1,182.5		3,474	63.8	19.0	352
Xoodyak_XT-v8	1,149.3		4,553	65.3	20.0	352
Xoodyak_XT-v1	1,069.8		2,986	79.0	26.0	352
Xoodyak_XT-v7	905.2		3,272	66.9	26.0	352
Ascon_Graz-v2	894.9	3	7,246	83.9	12.0	128
Xoodyak_XT-v3	749.0		5,569	38.3	18.0	352
COMET_VT-v1	714.2	4	6,613	111.6	20.0	128
Xoodyak_XT-v9	704.0		5,614	36.0	18.0	352
Ascon_Graz-v1	661.6		6,507	82.7	8.0	64
KNOT-v1	643.5	5	1,597	93.8	28.0	192
Xoodyak_XT-v4	552.8		6,839	26.7	17.0	352
DryGASCON-v1	551.0	6	3,854	90.4	21.0	128
Xoodyak_XT-v10	548.7		6,899	26.5	17.0	352
Ascon_VT-v1	543.4		3,130	84.9	10.0	64
Ascon_VT-v2	527.6		3,256	74.2	9.0	64
Spook-v2-v1	414.9	7	3,655	77.8	48.0	256
PHOTON-Beetle-v1	393.5	8	3,294	101.4	33.0	128
Xoodyak_XT-v11	365.0		9,447	16.6	16.0	352
Xoodyak_XT-v5	364.8		9,386	16.6	16.0	352
Romulus-v3	320.0	9	3,847	45.0	18.0	128
Elephant-v2	318.1	10	3,073	85.5	43.0	160
GIFT-COFB-v1	311.3	11	2,214	114.3	47.0	128
SCHWAEMM-v2	302.3	12	7,570	55.5	47.0	256
SCHWAEMM-v1	297.9		6,008	54.7	47.0	256
Romulus-v2	257.6		3,080	64.4	32.0	128
Romulus-v4	251.3		5,086	21.6	11.0	128
KNOT-v2	218.8		2,241	91.2	40.0	96
KNOT-v3	204.7		2,037	83.2	52.0	128
ISAP-v1	196.6	13	16,179	57.4	42.0	144
KNOT-v4	195.7		2,408	85.6	28.0	64
Romulus-v1	168.1		2,633	78.8	60.0	128
ISAP-v2	161.2		11,158	65.5	26.0	64
COMET_CI-v1	147.9		3,427	80.9	70.0	128
ESTATE-v1	146.0	14	3,085	100.4	88.0	128
COMET_VT-v2	132.7		3,154	92.2	89.0	128
Oribatida-v1	111.8	15	2,832	119.7	137.0	128
TinyJAMBU-v1	93.9	16	928	99.7	34.0	32
Elephant-v1	91.2		2,368	97.5	171.0	160
Xoodyak_GMU-v2	86.4		2,803	64.0	261.0	352
Pyjamask-v2	63.5	17	4,452	50.6	102.0	128
SpoC-v1	56.6	18	2,049	98.2	111.0	64
WAGE-v1	51.1	19	2,029	91.1	114.0	64
TinyJAMBU-v2	48.0		913	99.0	66.0	32
LOCUS-v1	44.7	20	3,161	79.6	114.0	64
COMET_CI-v2	40.7		1,974	94.3	297.0	128
ESTATE-v3	32.6		2,029	104.0	408.0	128
Pyjamask-v1	32.2		4,094	66.0	262.0	128
LOTUS-v1	31.2		2,820	55.6	114.0	64
ESTATE-v2	25.6		1,691	90.5	452.0	128
Gimli-v1	12.6	21	1,767	78.0	789.0	128
ESTATE-v4	8.8		1,394	96.0	1,392.0	128
Gimli-v2	6.4		1,767	73.5	1,481.0	128
Gimli-v3	3.5		1,772	78.5	2,865.0	128
TinyJAMBU-v3	3.0		881	97.7	1,026.0	32

Table 12: Lattice ECP5 Encryption AD+PT Throughput for Long Messages

Variant	Through-put [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per AD+PT Block	AD Block Size [bits]	PT Block Size [bits]
Subterranean-v1	1,884.8	1	1,725	58.9	0.5	8	8
Xoodyak_XT-v2	1,098.9		4,302	70.7	35.0	352	192
Xoodyak_XT-v8	1,014.9		4,553	65.3	35.0	352	192
Xoodyak_XT-v1	914.6	2	2,986	79.0	47.0	352	192
Ascon_Graz-v2	894.9	3	7,246	83.9	24.0	128	128
Xoodyak_GMU-v1	807.5		3,474	63.8	43.0	352	192
COMET_VT-v1	793.6	4	6,613	111.6	36.0	128	128
Xoodyak_XT-v7	773.9		3,272	66.9	47.0	352	192
Ascon_Graz-v1	661.6		6,507	82.7	16.0	64	64
Xoodyak_XT-v9	631.7		5,614	36.0	31.0	352	192
DryGASCON-v1	551.0	5	3,854	90.4	42.0	128	128
Ascon_VT-v1	543.4		3,130	84.9	20.0	64	64
KNOT-v1	536.3	6	1,597	93.8	56.0	128	192
Xoodyak_XT-v10	533.9		6,899	26.5	27.0	352	192
Xoodyak_XT-v4	500.9		6,839	26.7	29.0	352	192
Ascon_VT-v2	499.9		3,256	74.2	19.0	64	64
Xoodyak_XT-v3	443.3		5,569	38.3	47.0	352	192
PHOTON-Beetle-v1	425.7	7	3,294	101.4	61.0	128	128
Spook-v2-v1	414.9	8	3,655	77.8	96.0	256	256
Elephant-v2	408.4	9	3,073	85.5	67.0	160	160
Romulus-v3	397.2	10	3,847	45.0	29.0	128	128
SCHWAEMM-v2	334.3	11	7,570	55.5	85.0	256	256
Xoodyak_XT-v5	334.1		9,386	16.6	27.0	352	192
Romulus-v2	329.7		3,080	64.4	50.0	128	128
SCHWAEMM-v1	329.5		6,008	54.7	85.0	256	256
GIFT-COFB-v1	304.8	12	2,214	114.3	96.0	128	128
Romulus-v4	298.9		5,086	21.6	18.5	128	128
Xoodyak_XT-v11	257.9		9,447	16.6	35.0	352	192
KNOT-v3	255.8		2,037	83.2	104.0	192	128
ISAP-v1	246.5	13	16,179	57.4	67.0	144	144
KNOT-v4	244.6		2,408	85.6	56.0	96	64
Romulus-v1	219.2		2,633	78.8	92.0	128	128
ISAP-v2	199.6		11,158	65.5	42.0	64	64
ESTATE-v1	194.7	14	3,085	100.4	132.0	128	128
KNOT-v2	182.3		2,241	91.2	80.0	64	96
COMET_CI-v1	159.3		3,427	80.9	130.0	128	128
Oribatida-v1	148.7	15	2,832	119.7	206.0	128	128
COMET_VT-v2	135.7		3,154	92.2	174.0	128	128
TinyJAMBU-v1	133.0	16	928	99.7	48.0	32	32
Elephant-v1	120.5		2,368	97.5	259.0	160	160
Xoodyak_GMU-v2	66.1		2,803	64.0	527.0	352	192
Pyjamask-v2	64.8	17	4,452	50.6	200.0	128	128
LOCUS-v1	59.6	18	3,161	79.6	171.0	64	64
SpoC-v1	57.1	19	2,049	98.2	220.0	64	64
WAGE-v1	51.1	20	2,029	91.1	228.0	64	64
ESTATE-v3	43.5		2,029	104.0	612.0	128	128
COMET_CI-v2	43.0		1,974	94.3	561.0	128	128
LOTUS-v1	41.6		2,820	55.6	171.0	64	64
ESTATE-v2	34.2		1,691	90.5	678.0	128	128
Pyjamask-v1	32.5		4,094	66.0	520.0	128	128
TinyJAMBU-v2	31.7		913	99.0	200.0	32	32
Gimli-v1	12.7	21	1,767	78.0	1,575.0	128	128
ESTATE-v4	11.8		1,394	96.0	2,088.0	128	128
Gimli-v2	6.4		1,767	73.5	2,955.0	128	128
TinyJAMBU-v3	4.4		881	97.7	1,412.0	32	32
Gimli-v3	3.5		1,772	78.5	5,715.0	128	128

Table 13: Xilinx Artix-7 Hashing Throughput for Long Messages

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per HM block	Hash Msg Block Size [bits]
Xoodyak_XT-v7	1,536.0	1	1,405	228	19	128
DryGASCON-v1	1,450.7	2	2,074	238	21	128
Ascon_Graz-v2	987.4	3	1,723	216	14	64
Ascon_VT-v2	934.4		1,928	219	15	64
Xoodyak_XT-v8	920.6		2,040	187	26	128
Subterranean-v1	744.0	4	915	186	2	8
Xoodyak_GMU-v1	640.0		1,808	170	34	128
SCHWAEMM-v2	489.4	5	3,740	130	34	128
PHOTON-Beetle-v1	227.8	6	2,065	178	25	32
Xoodyak_GMU-v2	41.5		1,234	168	518	128
Gimli-v1	39.2	7	933	241	786	128
Gimli-v2	21.2		905	244	1,474	128
Gimli-v3	11.4		838	253	2,850	128

Table 14: Intel Cyclone 10 LP Hashing Throughput for Long Messages

Variant	Throughput Hash Long [Mbits/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles per HM Block	Hash Msg Block Size [bits]
Xoodyak_XT-v7	901.6	1	2,253	133.8	19	128
DryGASCON-v1	795.6	2	3,199	130.5	21	128
Ascon_VT-v2	733.9	3	2,695	172.0	15	64
Ascon_Graz-v2	670.4		2,666	146.7	14	64
Subterranean-v1	638.6	4	1,333	159.6	2	8
Xoodyak_XT-v8	449.7		4,337	91.3	26	128
Xoodyak_GMU-v1	402.0		3,135	106.8	34	128
SCHWAEMM-v2	322.8	5	5,773	85.7	34	128
PHOTON-Beetle-v1	160.6	6	3,602	125.4	25	32
Xoodyak_GMU-v2	19.0		5,871	77.0	518	128
Gimli-v1	16.5	7	2,044	101.3	786	128
Gimli-v2	8.5		2,074	97.3	1,474	128
Gimli-v3	4.5		2,115	100.5	2,850	128

Table 15: Lattice ECP5 Hashing Throughput for Long Messages

Variant	Through-put [Mbits/s]	Candi-date Ranking by Throughput	LUTs	Freq. [MHz]	Cycles per HM block	Hash Msg Block Size [bits]
DryGASCON-v1	551.0	1	3,854	90.4	21	128
Xoodyak_XT-v7	450.4	2	3,272	66.9	19	128
Ascon_Graz-v2	383.5	3	7,246	83.9	14	64
Xoodyak_XT-v8	321.5		4,553	65.3	26	128
Ascon_VT-v2	316.6		3,256	74.2	15	64
Xoodyak_GMU-v1	240.3		3,474	63.8	34	128
Subterranean-v1	235.6	4	1,725	58.9	2	8
Xoodyak_XT-v9	209.5		5,614	36.0	22	128
SCHWAEMM-v2	208.9	5	7,570	55.5	34	128
Xoodyak_XT-v10	169.6		6,899	26.5	20	128
PHOTON-Beetle-v1	129.8	6	3,294	101.4	25	32
Xoodyak_XT-v11	118.0		9,447	16.6	18	128
Xoodyak_GMU-v2	15.8		2,803	64.0	518	128
Gimli-v1	12.7	7	1,767	78.0	786	128
Gimli-v2	6.4		1,767	73.5	1,474	128
Gimli-v3	3.5		1,772	78.5	2,850	128

In the following two-dimensional graphs, apart from points representing variants of an investigated algorithm, we include also points corresponding to the implementations with the highest Throughput (Subterranean-v1), smallest area (TinyJAMBU-v1), and largest area (SCHWAEMM-v1).

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

In Figs. 16 and 17, the Artix-7 results are presented for four designs of COMET. COMET_VT-v1, COMET_CI-v1, and COMET_CI-v2 are realizations of the primary parameter set: COMET-128_AES-128/128. COMET_VT-v2 is the realization of the parameter set COMET-128_CHAM-128/128. The difference in performance between the first three variants comes from using different hardware architectures. COMET_VT-v1 uses the basic iterative architecture, while COMET_CI-v1 and COMET_CI-v2 use folded architectures with different folding factors. For the same basic iterative architecture, the implementation of COMET-128_AES-128/128 (COMET_VT-v1) is both faster and bigger than the implementation of COMET-128_CHAM-128/128 (COMET_VT-v2). As shown in Table 3, the number of clock cycles per block is significantly higher for COMET-128_CHAM-128/128. At the same time, implementing one round of CHAM-128/128 takes significantly less area than implementing one round of AES-128/128.

In Figs. 18 and 19, the Artix-7 results are presented for four designs of ESTATE. ESTATE-v1 and ESTATE-v2 are implementations of the parameter set ESTATE_TweAES-128, obtained by instantiating the ESTATE mode of operation with the TweAES-128 block cipher. ESTATE-v3 and ESTATE-v4 are implementations of the parameter set

Table 16: Intel Cyclone-10-LP Relative Resource Usage and Frequency

Variant	LEs	$\frac{\text{LEs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Frequency [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
Ascon_Graz-v1	2484	1.60	775	1.16	152.8	1.37
Ascon_Graz-v2	2666	1.55	775	1.16	146.7	1.47
Ascon_VT-v1	2432	1.27	634	1.18	176.6	1.32
Ascon_VT-v2	2695	1.40	640	1.18	172.0	1.27
COMET_CI-v1	4663	2.48	1885	1.22	115.8	1.93
COMET_CI-v2	2629	2.40	1632	1.58	132.9	1.67
COMET_VT-v1	10035	**3.67**	1153	1.10	84.1	**2.77**
COMET_VT-v2	5204	**3.06**	826	1.12	110.6	**2.12**
DryGASCON-v1	3199	1.54	1310	1.07	130.5	1.82
Elephant-v1	2056	1.59	1005	1.10	163.1	1.40
Elephant-v2	2729	1.45	998	1.11	113.2	1.60
ESTATE-v1	3880	2.82	1401	1.91	114.1	1.98
ESTATE-v2	1946	2.18	1026	2.45	174.3	1.59
ESTATE-v3	2320	1.94	1442	1.64	173.4	1.47
ESTATE-v4	1572	1.67	1098	1.97	200.1	1.38
GIFT-COFB-v1	1877	1.80	774	1.28	184.4	1.49
Gimli-v1	2044	2.19	1130	**4.33**	101.3	**2.38**
Gimli-v2	2074	2.29	1136	**4.64**	97.4	**2.51**
Gimli-v3	2115	2.52	1143	**4.59**	100.5	**2.52**
ISAP-v2	2961	1.37	1120	1.11	139.8	1.43
KNOT-v1	1485	1.36	674	1.17	177.9	1.46
KNOT-v2	2050	1.31	955	1.12	167.5	1.52
KNOT-v3	1962	1.44	905	1.12	170.7	1.55
KNOT-v4	2412	1.35	1135	1.09	171.4	1.49
LOCUS-v1	3121	1.59	1109	1.09	125.8	1.65
LOTUS-v1	2642	1.60	1010	1.10	103.5	1.40
Oribatida-v1	2512	1.73	1331	1.01	185.7	1.49
PHOTON-Beetle-v1	3602	1.74	836	1.15	125.4	1.42
Pyjamask-v1	8599	**4.35**	6236	**4.77**	109.7	**2.09**
Pyjamask-v2	8692	**3.77**	6092	**4.31**	90.6	**2.35**
Romulus-v1	1735	1.82	500	1.00	143.3	1.60
Romulus-v2	2086	1.63	500	1.00	141.7	1.51
Romulus-v3	2407	1.32	500	0.99	79.3	1.55
Romulus-v4	3409	1.31	500	0.99	40.4	1.44
SCHWAEMM-v2	5773	1.54	1624	1.05	85.7	1.52
SCHWAEMM-v1	4713	1.53	1489	1.07	81.8	1.65
SpoC-v1	1686	1.57	821	1.13	166.3	1.47
Spook-v2-v1	3912	1.70	1485	0.99	110.4	1.82
Subterranean-v1	1333	1.46	578	0.99	159.6	1.17
TinyJAMBU-v1	856	1.45	447	1.04	196.8	1.35
TinyJAMBU-v2	841	1.49	448	1.04	196.2	1.37
TinyJAMBU-v3	817	1.52	452	1.04	191.1	1.45
WAGE-v1	1774	1.54	846	1.11	159.6	1.75
Xoodyak_GMU-v1	3135	1.73	947	1.11	106.8	1.59
Xoodyak_GMU-v2	5871	**4.76**	2237	**22.83**	77.1	**2.18**
Xoodyak_XT-v1	2282	1.62	589	1.23	140.6	1.66
Xoodyak_XT-v2	3518	1.70	589	1.23	87.8	**2.08**
Xoodyak_XT-v7	2253	1.60	602	1.25	133.8	1.70
Xoodyak_XT-v8	4337	**2.13**	602	1.25	91.4	**2.05**

Table 17: Lattice ECP5 Relative Resource Usage and Frequency

Variant	LUTs	$\frac{\text{LUTs}}{\text{Artix-7 LUTs}}$	FFs	$\frac{\text{FFs}}{\text{Artix-7 FFs}}$	Frequency [MHz]	$\frac{\text{Artix-7 Freq}}{\text{Freq}}$
Ascon_Graz-v1	6507	**4.20**	692	1.04	82.70	2.53
Ascon_Graz-v2	7246	**4.21**	692	1.03	83.90	2.57
Ascon_VT-v1	3130	1.64	550	1.02	84.90	2.74
Ascon_VT-v2	3256	1.69	556	1.02	74.20	2.95
COMET_CI-v1	3427	1.82	1798	1.17	80.90	2.76
COMET_CI-v2	1974	1.80	1607	**1.55**	94.34	2.35
COMET_VT-v1	6613	2.42	1154	1.11	111.60	2.09
COMET_VT-v2	3154	1.85	741	1.01	92.25	2.54
DryGASCON-v1	3854	1.86	1226	1.00	90.40	2.63
Elephant-v1	2368	1.83	923	1.01	97.50	2.35
Elephant-v2	3073	1.63	916	1.02	85.50	2.12
ESTATE-v1	3085	2.24	1308	1.78	100.40	2.25
ESTATE-v2	1691	1.89	995	**2.37**	90.50	**3.06**
ESTATE-v3	2029	1.70	1358	1.55	103.95	2.45
ESTATE-v4	1394	1.48	1063	1.91	95.98	2.89
GIFT-COFB-v1	2214	2.13	689	1.14	114.30	2.41
Gimli-v1	1767	1.89	260	1.00	77.96	**3.09**
Gimli-v2	1767	1.95	263	1.07	73.48	**3.32**
Gimli-v3	1772	2.11	272	1.09	78.48	**3.22**
ISAP-v1	16179	**4.63**	1204	1.02	57.35	**3.37**
ISAP-v2	11158	**5.17**	1043	1.04	65.50	**3.05**
KNOT-v1	1597	1.46	581	1.01	93.85	2.77
KNOT-v2	2241	1.43	865	1.01	91.15	2.79
KNOT-v3	2037	1.49	813	1.01	83.15	**3.17**
KNOT-v4	2408	1.35	1043	1.01	85.60	2.99
LOCUS-v1	3161	1.61	1036	1.02	79.60	2.60
LOTUS-v1	2820	1.71	936	1.02	55.60	2.61
Oribatida-v1	2832	1.95	1246	0.94	119.69	2.31
PHOTON-Beetle-v1	3294	1.60	753	1.03	101.44	1.75
Pyjamask-v1	4094	2.07	1808	1.38	65.96	**3.47**
Pyjamask-v2	4452	1.93	1657	1.17	50.60	**4.21**
Romulus-v1	2633	2.76	502	1.00	78.78	2.91
Romulus-v2	3080	2.41	519	1.04	64.40	**3.32**
Romulus-v3	3847	2.11	569	1.13	45.00	2.73
Romulus-v4	5086	1.95	571	1.14	21.60	2.69
SCHWAEMM-v2	7570	2.02	1540	1.00	55.50	2.34
SCHWAEMM-v1	6008	1.96	1405	1.01	54.70	2.47
SpoC-v1	2049	1.91	740	1.02	98.20	2.48
Spook-v2-v1	3655	1.59	1494	0.99	77.80	2.58
Subterranean-v1	1725	1.89	545	0.93	58.90	**3.16**
TinyJAMBU-v1	928	1.57	363	0.85	99.72	2.67
TinyJAMBU-v2	913	1.62	364	0.85	99.00	2.71
TinyJAMBU-v3	881	1.64	368	0.85	97.70	2.85
WAGE-v1	2029	1.76	794	1.04	91.10	**3.06**
Xoodyak_GMU-v1	3474	1.92	865	1.02	63.83	2.66
Xoodyak_GMU-v2	2803	2.27	108	1.10	64.05	2.62
Xoodyak_XT-v1	2986	2.13	528	1.10	79.02	2.95
Xoodyak_XT-v2	4302	2.08	526	1.10	70.70	2.59
Xoodyak_XT-v7	3272	2.33	657	1.37	66.86	**3.41**
Xoodyak_XT-v8	4553	2.23	657	1.37	65.30	2.86

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

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

Table 19: FPGA Rankings based on Encryption AD Throughput for Long Messages

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

Table 20: FPGA Rankings based on Encryption AD+PT Throughput for Long Messages

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

ESTATE_TweGIFT-128, obtained by instantiating the ESTATE mode of operation with the TweGIFT-128 block cipher. Within each pair, the former implementation uses a 32-bit datapath and the latter an 8-bit datapath. For the implementations using the same datapath width, the realizations of ESTATE_TweAES-128 (ESTATE-v1 and ESTATE-v2) are significantly faster. At the same time, both 8-bit architectures (ESTATE-v2 and ESTATE-v4) have their areas smaller than 1000 LUTs.

In Figs. 20 and 21, the Artix-7 results are presented for four designs of KNOT. The four variants correspond to four different parameter sets, denoted as KNOT-AEAD(k, b, r), where k is the key length, b is the state size, and r is the bitrate. The bitrate determines the block size of plaintext and AD. KNOT-v1 and KNOT-v2 represent the parameter sets KNOT-AEAD(128, 256, 64) and KNOT-AEAD (128, 384, 192), respectively. Both are believed to have the same security strength, but the latter uses a higher bitrate due to its bigger state size (permutation width), hence it has a higher throughput. KNOT-v4 represents the parameter set KNOT-AEAD(256, 512, 128) which has the highest security level, and KNOT-v3 represents KNOT-AEAD(192, 384, 96), which has the intermediate security level. Higher security levels come with the penalty of a higher number of clock cycles per block: 40 for KNOT-v3=KNOT-AEAD(192, 384, 96) and 52 for KNOT-v4=KNOT-AEAD(256, 512, 128), vs. 28 for KNOT-v1=KNOT-AEAD(128, 256, 64) and KNOT-v2=KNOT-AEAD (128, 384, 192). As a result, KNOT-v2, which has the highest block size for plaintext and AD (192 bits) is by far the fastest. The remaining variants offer similar speed, but differ in terms of area, which is determined primarily by the state size (permutation width), which is equal to 128 for KNOT-v1, 384 for KNOT-v3, and 512 for KNOT-v4.

In Figs. 22 and 23, the Artix-7 results are presented for four 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

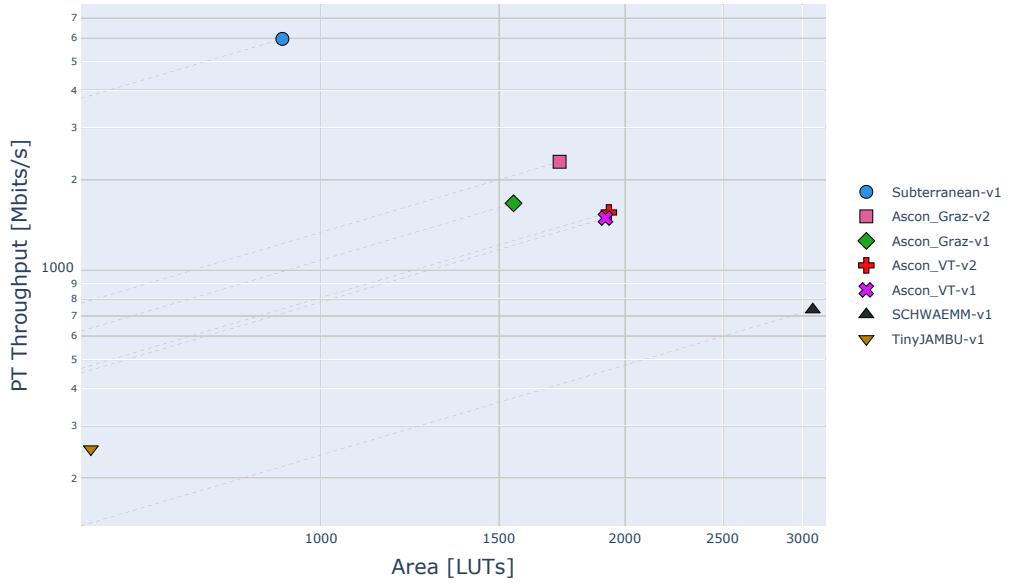

Figure 14: Artix-7 Ascon Throughput PT Long

architecture (Romulus-v1), two-round architecture (Romulus-v2), four-round architecture (Romulus-v3), and eight-round 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 is the slowest of the four, but it is the only architecture with the number of LUTs smaller than 1000. As shown in Tables 7, 8, 9, and 14, 10, 11, 12 for Cyclone 10 LP FPGAs, Romulus-v2 is the also fastest, but for ECP5 FPGAs, it is outperformed by Romulus-v3.

In Figs. 24 and 25, the Artix-7 results are presented for six designs of Xoodyak. Four designs were submitted by the Xoodyak Team + Silvia, with Silvia Mella as the primary designer. Two designs were submitted by GMU. Variants Xoodyak_XT-v7, Xoodyak_XT-v8, Xoodyak_GMU-v1, and Xoodyak_GMU-v2 support hashing. By comparing the throughput and area of Xoodyak_XT-v7 vs. Xoodyak_XT-v1, and Xoodyak_XT-v8 vs. Xoodyak_XT-v2, it can be seen that the support for hashing does not introduce any performance penalty in terms of either area or speed. Xoodyak_XT-v8 (a 2x unrolled architecture) is slightly faster than the basic iterative architecture, but it also takes over 600 more LUTs. One of the GMU designs, Xoodyak_GMU-v1, with the 384-bit datapath, is slightly slower than the four investigated designs from Xoodyak Team. Its area falls between areas of Xoodyak_XT-v7 and Xoodyak_XT-v8, with the same AEAD+Hash functionality. The second design from GMU is very significantly slower, and only about 170 LUTs smaller than Xoodyak_XT-v1. Thus, this design is not really competitive.

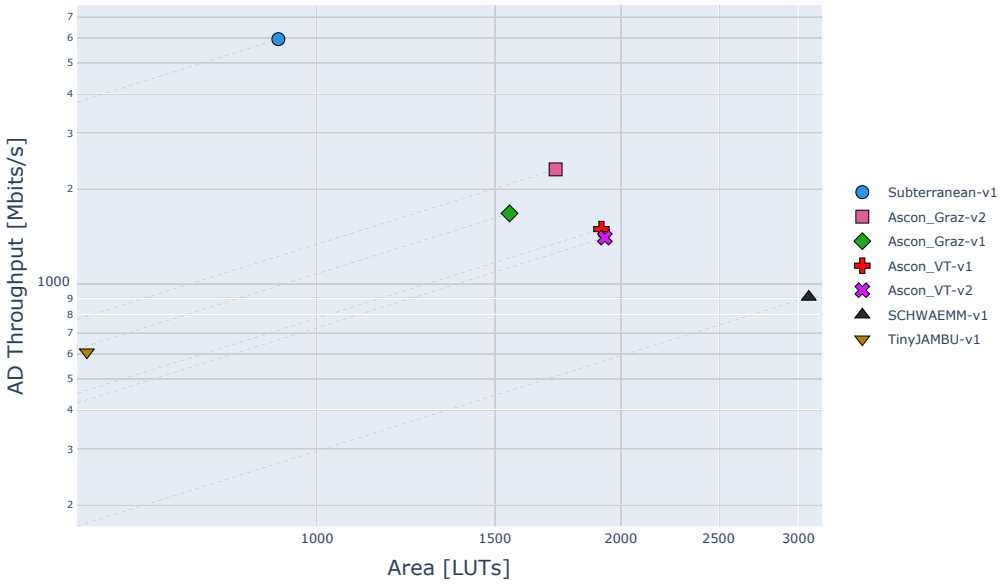

Figure 15: Artix-7 Ascon Throughput AD Long

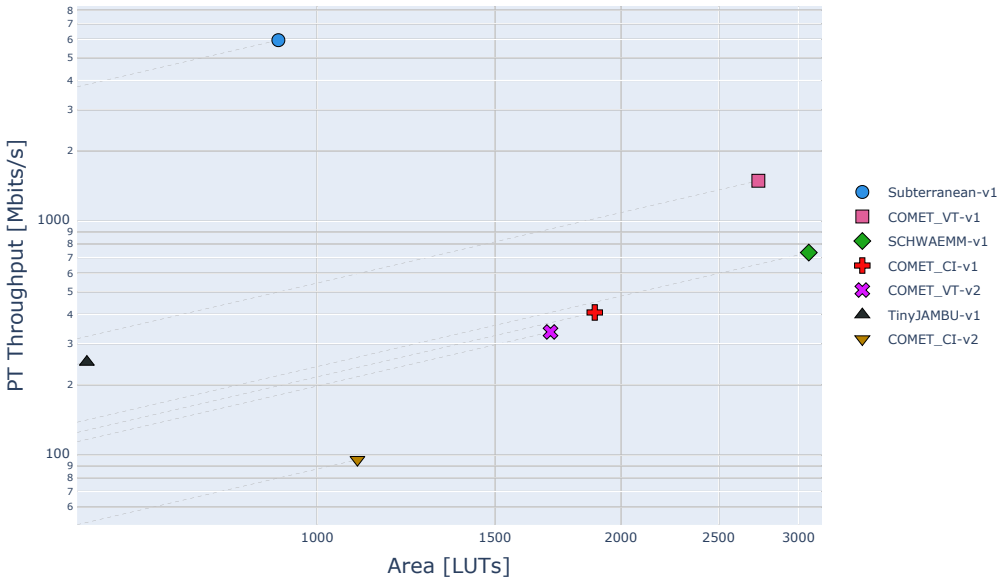

Figure 16: Artix-7 COMET Throughput PT Long

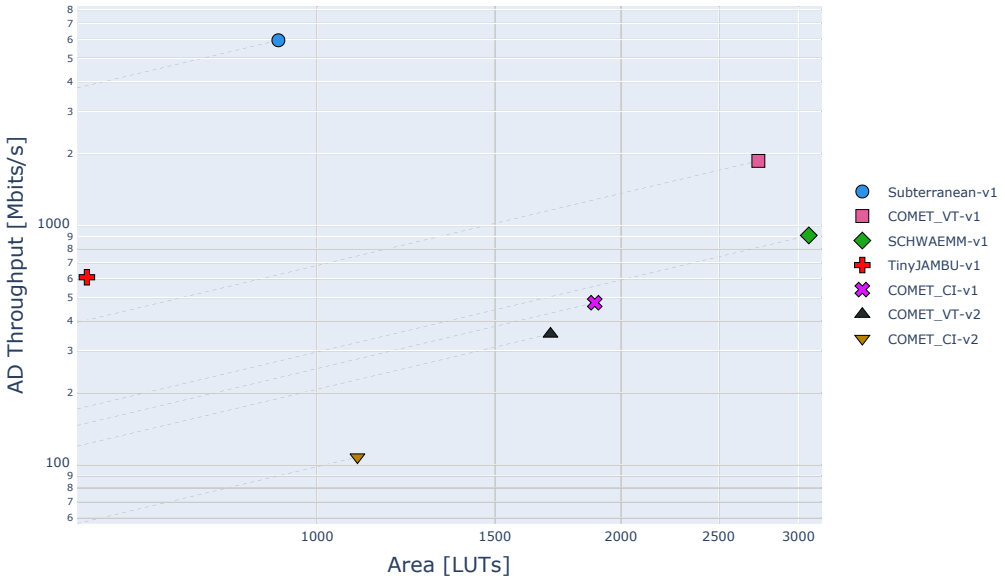

Figure 17: Artix-7 COMET Throughput AD Long

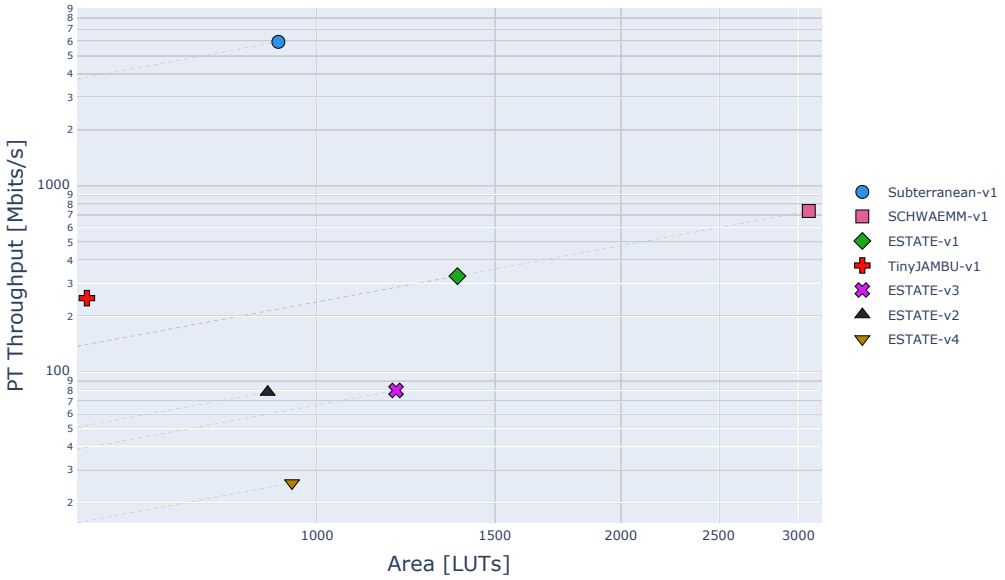

Figure 18: Artix-7 ESTATE Throughput PT Long

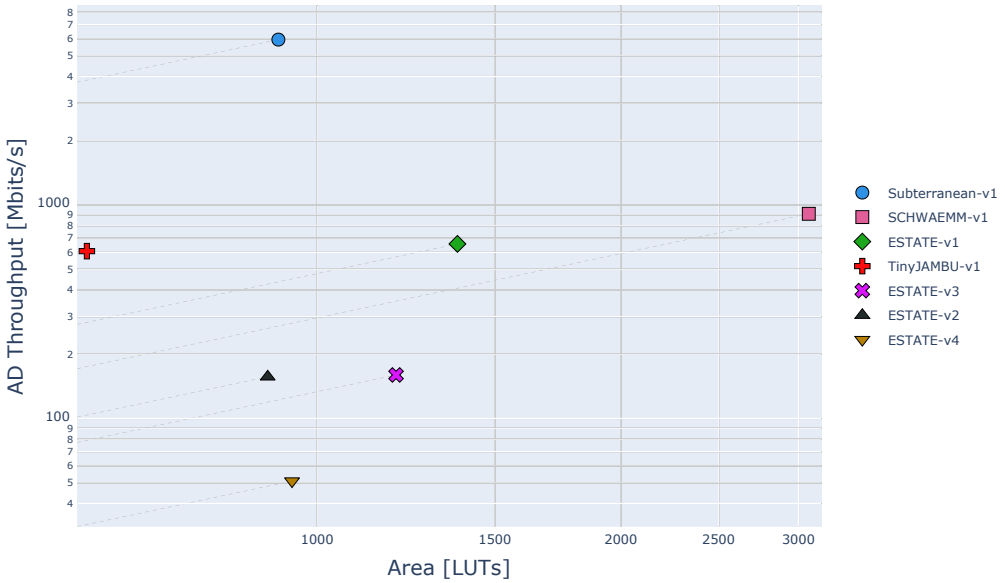

Figure 19: Artix-7 ESTATE Throughput AD Long

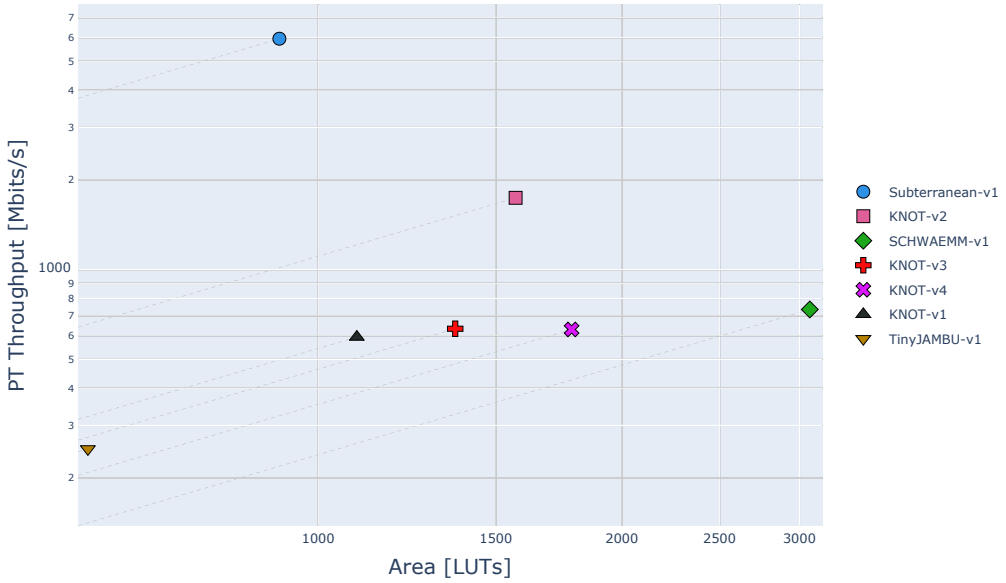

Figure 20: Artix-7 KNOT Throughput PT Long

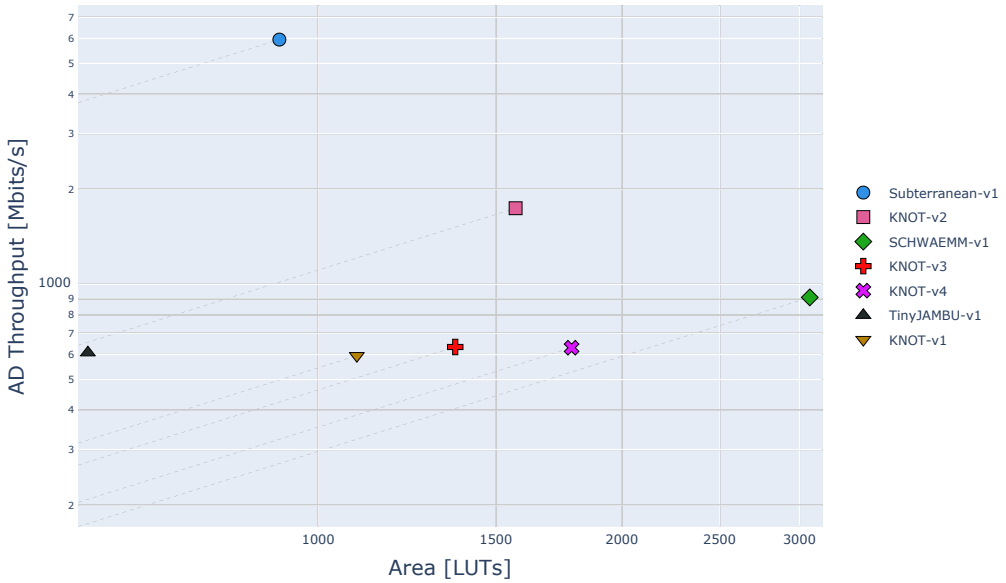

Figure 21: Artix-7 KNOT Throughput AD Long

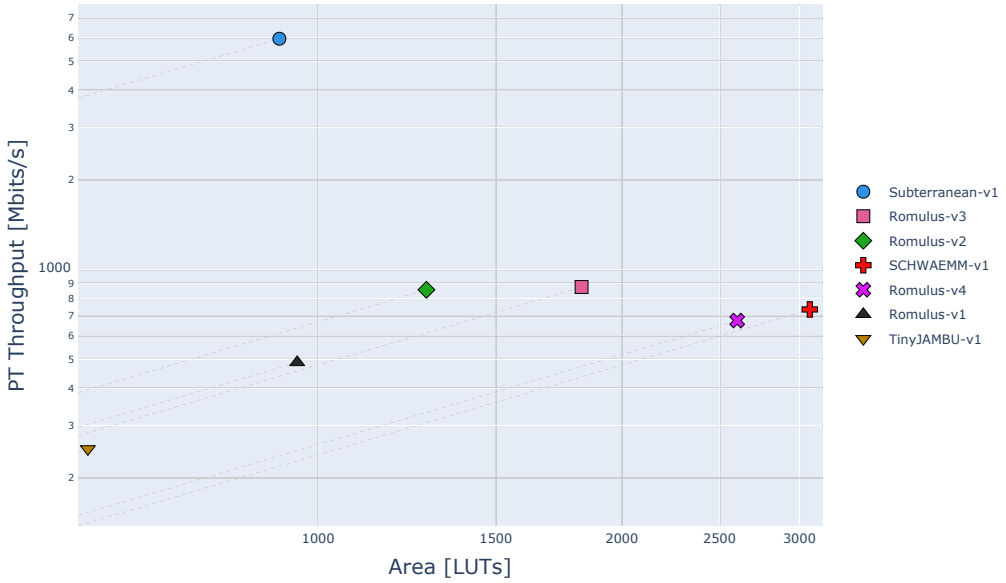

Figure 22: Artix-7 Romulus Throughput PT Long

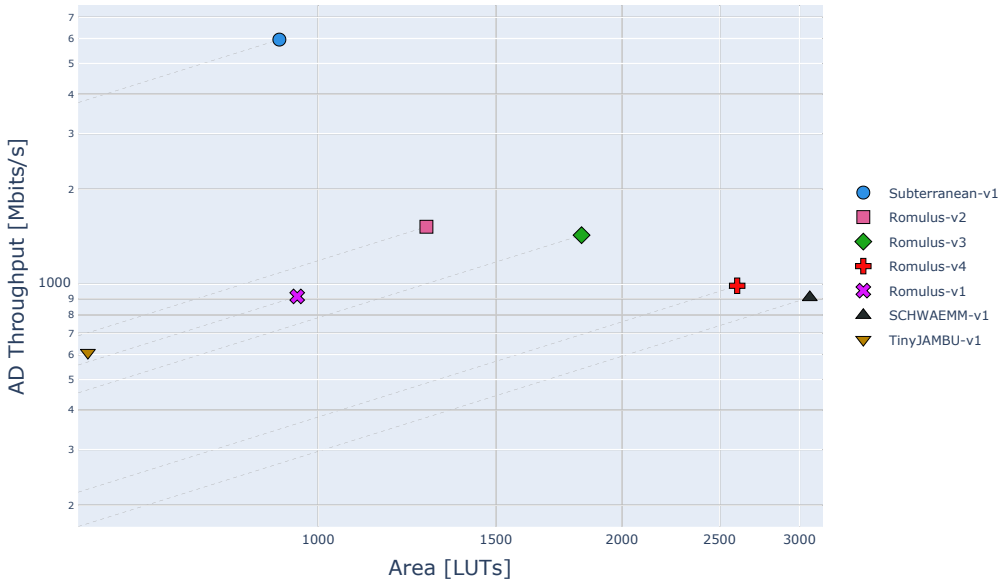

Figure 23: Artix-7 Romulus Throughput AD Long

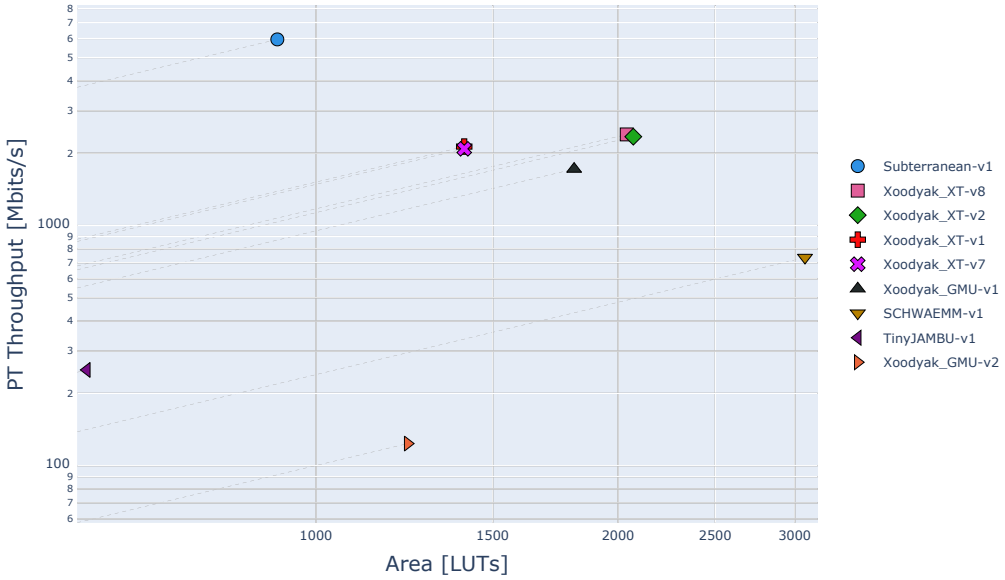

Figure 24: Artix-7 Xoodyak Throughput PT Long

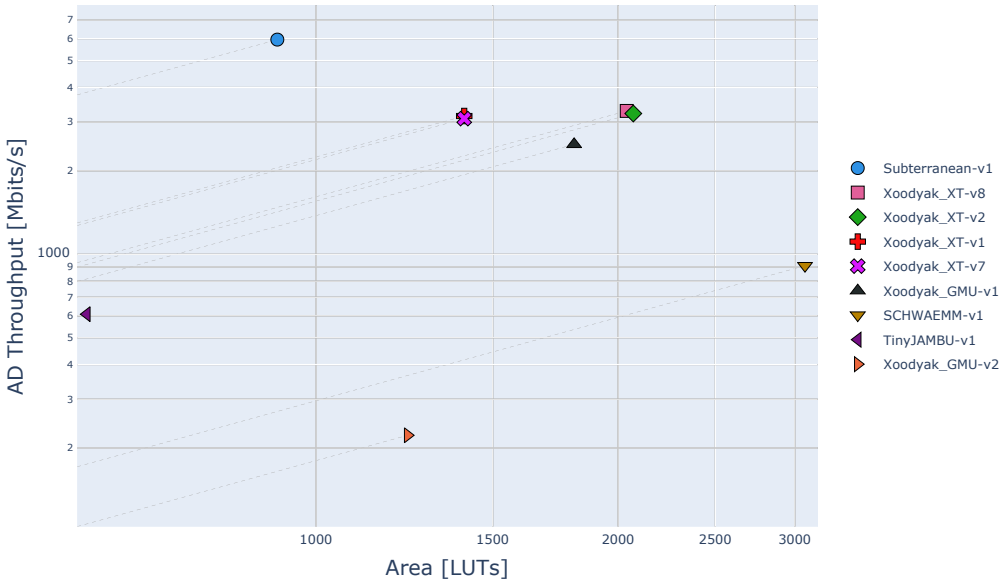

Figure 25: Artix-7 Xoodyak Throughput AD Long

Table 21: Artix-7 Encryption PT Throughput Rankings

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

4.4 Throughputs for Short Inputs

In the Appendix, in Tables 27–53, we provide values of throughputs for short and medium input sizes, such as 16 bytes, 64 bytes, and 1536 bytes. For 1536 byte inputs, the throughputs are very close to throughputs for long inputs. For example for PT, they vary in the range of 89%-99% of throughputs for long plaintexts. For 64 byte plaintexts, this ratio varies from 25% Subterranean-v1 to 88% for ESTATE-v3. For 16 bytes, the ratio varies from 8% for Subterranean-v1 to 65% for ESTATE-v3.

In Tables 21, 22, and 23, we summarize the relative changes in rankings for Artix-7. As shown in all mentioned above tables, the following algorithms rank higher for short messages than for long messages: Ascon, COMET, DryGASCON, Romulus, PHOTON-Beetle, Elephant, ESTATE, TinyJAMBU, and LOCUS. The opposite is true for the following candidates: Xoodyak, KNOT, Spook, Pyjamask, ISAP. The remaining algorithm rank approximately the same. The following 5 algorithms remain among the best 6, for processing of PT only and AD+PT, independently of the size of inputs: Subterranean 2.0, Xoodyak, Ascon, COMET, and DryGASCON. The following 5 algorithms remain among the best 6, for processing of AD only, independently of the size of inputs: Subterranean 2.0, Ascon, Xoodyak, COMET, and Romulus.

In Tables 54–59, we summarize the relative changes in rankings for Cyclone 10 LP and ECP5.

5 Future Work

Before drawing final conclusions, we are planning to perform two additional phases of Round 2 benchmarking, with the submission deadlines at the beginning of October and the beginning of November 2020, respectively. Only after the results of these additional phases are known, final conclusions can be drawn. At the end of this effort, we hope for the full coverage of all 32 Round 2 candidates and the implementation of multiple variants of each candidate. This benchmarking effort should clearly demonstrate the major strengths and weaknesses of unprotected implementations of Round 2 candidates. It should also

Table 22: Artix-7 Encryption AD Throughput Rankings

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

Table 23: Artix-7 Encryption AD+PT Throughput Rankings

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

provide a strong foundation for the fair and comprehensive evaluation of the SCA-protected implementations in Round 3 of the NIST LWC standardization process.

References

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

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

[12] W. Diehl, A. Abdulgadir, F. Farahmand, J.-P. Kaps, and K. Gaj, "Comparison of cost of protection against differential power analysis of selected authenticated ciphers," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018*, Washington, DC: IEEE, Apr. 2018, pp. 147–152.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A Additional Results

Table 24: Xilinx Artix-7 Resource Usage and Maximum Frequency

Variant	**LUTs**	**Candidate Ranking by LUTs**	**FFs**	**Slices**	**Freq. [MHz]**
TinyJAMBU-v3	537	1	433	191	278
TinyJAMBU-v2	564		430	197	268
TinyJAMBU-v1	591		428	212	266
Gimli-v3	838	2	249	252	253
ESTATE-v2	893	3	419	266	277
Gimli-v2	905		245	266	244
Subterranean-v1	915	4	584	260	186
Gimli-v1	933		261	269	241
ESTATE-v4	944		557	292	277
Romulus-v1	953	5	501	271	229
GIFT-COFB-v1	1,041	6	604	321	275
SpoC-v1	1,075	7	728	310	244
KNOT-v1	1,092	8	575	317	260
COMET-CI-v2	1,096	9	1,034	372	222
WAGE	1,150	10	760	332	279
ESTATE-v3	1,197		878	385	255
Xoodyak_GMU-v2	1,234	11	98	323	168
Romulus-v2	1,280		501	344	214
Elephant-v1	1,291	12	910	379	229
KNOT-v3	1,367		806	414	264
ESTATE-v1	1,377		733	408	226
Xoodyak_XT-v1	1,405		480	398	233
Xoodyak_XT-v7	1,405		480	391	228
Oribatida-v1	1,450	13	1,319	466	276
Ascon-Graz-v1	1,551	14	666	438	209
KNOT-v2	1,569		854	467	254
LOTUS-v1	1,652	15	916	469	145
COMET_VT-v2	1,703		736	504	234
Ascon-Graz-v2	1,723		669	487	216
KNOT-v4	1,783		1,037	527	256
Xoodyak_GMU-v1	1,808		851	495	170
Romulus-v3	1,824		504	507	123
COMET-CI-v1	1,884		1,543	639	223
Elephant-v2	1,884		900	541	181
Ascon-VT-v1	1,913		539	518	233
Ascon-VT-v2	1,928		544	515	219
LOCUS-v1	1,966		1,016	592	207
Pyjamask-v1	1,979	16	1,306	592	229
Xoodyak_XT-v8	2,040		480	542	187
PHOTON-Beetle-v1	2,065	17	729	620	178
Xoodyak_XT-v2	2,071		480	564	183
DryGASCON-v1	2,074	18	1,220	596	238
ISAP-v2	2,157	19	1,005	618	200
Spook-v2-v1	2,296	20	1,502	693	201
Pyjamask-v2	2,308		1,415	780	213
Romulus-v4	2,602		503	702	58
COMET_VT-v1	2,737		1,044	734	233
SCHWAEMM-v1	3,071	21	1,396	872	135
ISAP-v1	3,491		1,177	937	193
SCHWAEMM-v2	3,740		1,541	1,004	130

Table 25: Intel Cyclone 10 LP Resource Usage and Maximum Frequency

Variant	LEs	Candidate Ranking by LEs	FFs	Freq. [MHz]
TinyJAMBU-v3	817	1	452	191.1
TinyJAMBU-v2	841		448	196.2
TinyJAMBU-v1	856		447	196.8
Subterranean-v1	1,333	2	578	159.6
KNOT-v1	1,485	3	674	177.9
ESTATE-v4	1,572	4	1,098	200.1
SpoC-v1	1,686	5	821	166.3
Romulus-v1	1,735	6	500	143.2
WAGE-v1	1,774	7	846	159.6
GIFT-COFB-v1	1,877	8	774	184.4
ESTATE-v2	1,946		1,026	174.3
KNOT-v3	1,962		905	170.7
Gimli-v1	2,044	9	1,130	101.3
KNOT-v2	2,050		955	167.5
Elephant-v1	2,056	10	1,005	163.1
Gimli-v2	2,074		1,136	97.3
Romulus-v2	2,086		500	141.7
Gimli-v3	2,115		1,143	100.5
Xoodyak_XT-v7	2,253	11	602	133.8
Xoodyak_XT-v1	2,282		589	140.6
ESTATE-v3	2,320		1,442	173.4
Romulus-v3	2,407		500	79.3
KNOT-v4	2,412		1,135	171.3
Ascon_VT-v1	2,432	12	634	176.6
Ascon_Graz-v1	2,484		775	152.8
Oribatida-v1	2,512	13	1,331	185.7
COMET_CI-v2	2,629	14	1,632	132.9
LOTUS-v1	2,642	15	1,010	103.5
Ascon_Graz-v2	2,666		775	146.7
Ascon_VT-v2	2,695		640	172.0
Elephant-v2	2,729		998	113.2
ISAP-v2	2,961	16	1,120	139.8
LOCUS-v1	3,121		1,109	125.8
Xoodyak_GMU-v1	3,135		947	106.8
DryGASCON-v1	3,199	17	1,310	130.5
Romulus-v4	3,409		500	40.4
Xoodyak_XT-v2	3,518		589	87.8
PHOTON-Beetle-v1	3,602	18	836	125.4
ESTATE-v1	3,880		1,401	114.1
Spook-v2-v1	3,912	19	1,485	110.4
Xoodyak_XT-v8	4,337		602	91.3
COMET_CI-v1	4,663		1,885	115.8
SCHWAEMM-v1	4,713	20	1,489	81.8
COMET_VT-v2	5,204		826	110.6
SCHWAEMM-v2	5,773		1,624	85.7
Xoodyak_GMU-v2	5,871		2,237	77.0
Pyjamask-v1	8,599	21	6,236	109.7
Pyjamask-v2	8,692		6,092	90.6
COMET_VT-v1	10,035		1,153	84.1

Table 26: Lattice ECP5 Resource Frequency

Variant	LUTs	Candidate Ranking by LUTs	FFs	Slices	Freq. [MHz]
TinyJAMBU-v3	881	1	368	552	97.7
TinyJAMBU-v2	913		364	588	99.0
TinyJAMBU-v1	928		363	563	99.7
ESTATE-v4	1,394	2	1,063	1,025	96.0
KNOT-v1	1,597	3	581	930	93.8
ESTATE-v2	1,691		995	1,223	90.5
Subterranean-v1	1,725	4	545	1,069	58.9
Gimli-v1	1,767	5	260	1,072	78.0
Gimli-v2	1,767		263	1,040	73.5
Gimli-v3	1,772		272	1,064	78.5
COMET_CI-v2	1,974	6	1,607	1,662	94.3
ESTATE-v3	2,029		1,358	1,533	104.0
WAGE-v1	2,029	7	794	1,270	91.1
KNOT-v3	2,037		813	1,193	83.2
SpoC-v1	2,049	8	740	1,314	98.2
GIFT-COFB-v1	2,214	9	689	1,248	114.3
KNOT-v2	2,241		865	1,304	91.2
Elephant-v1	2,368	10	923	1,464	97.5
KNOT-v4	2,408		1,043	1,429	85.6
Romulus-v1	2,633	11	502	1,486	78.8
Xoodyak_GMU-v2	2,803	12	108	1,648	64.0
LOTUS-v1	2,820	13	936	1,748	55.6
Oribatida-v1	2,832	14	1,246	1,781	119.7
Xoodyak_XT-v1	2,986		528	1,571	79.0
Elephant-v2	3,073		916	1,823	85.5
Romulus-v2	3,080		519	1,678	64.4
ESTATE-v1	3,085		1,308	2,117	100.4
Ascon_VT-v1	3,130	15	550	1,673	84.9
COMET_VT-v2	3,154		741	1,934	92.2
LOCUS-v1	3,161		1,036	2,019	79.6
Ascon_VT-v2	3,256		556	1,678	74.2
Xoodyak_XT-v7	3,272		657	1,744	66.9
PHOTON-Beetle-v1	3,294	16	753	1,938	101.4
COMET_CI-v1	3,427		1,798	2,175	80.9
Xoodyak_GMU-v1	3,474		865	2,097	63.8
Spook-v2-v1	3,655	17	1,494	2,254	77.8
Romulus-v3	3,847		569	2,092	45.0
DryGASCON-v1	3,854	18	1,226	2,168	90.4
Pyjamask-v1	4,094	19	1,808	2,639	66.0
Xoodyak_XT-v2	4,302		526	2,215	70.7
Pyjamask-v2	4,452		1,657	2,796	50.6
Xoodyak_XT-v8	4,553		657	2,361	65.3
Romulus-v4	5,086		571	2,710	21.6
Xoodyak_XT-v3	5,569		526	2,854	38.3
Xoodyak_XT-v9	5,614		538	2,875	36.0
SCHWAEMM-v1	6,008	20	1,405	3,937	54.7
Ascon_Graz-v1	6,507		692	4,307	82.7
COMET_VT-v1	6,613		1,154	3,698	111.6
Xoodyak_XT-v4	6,839		526	3,492	26.7
Xoodyak_XT-v10	6,899		538	3,520	26.5
Ascon_Graz-v2	7,246		692	4,617	83.9
SCHWAEMM-v2	7,570		1,540	4,864	55.5
Xoodyak_XT-v5	9,386		526	4,775	16.6
Xoodyak_XT-v11	9,447		538	4,799	16.6
ISAP-v2	11,158	21	1,043	6,480	65.5
ISAP-v1	16,179		1,204	9,080	57.4

Table 27: Xilinx Artix-7 Encryption PT Throughput for 1536 Byte Messages

Variant	Throughput PT 1536B [Mbits/s]	Thr PT 1536B/ Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles PT 1536B
Subterranean-v1	5,290.7	89%	1	915	186	432
Xoodyak_XT-v8	2,288.7	96%	2	2,040	187	1,004
Xoodyak_XT-v2	2,239.7	96%		2,071	183	1,004
Ascon_Graz-v2	2,210.0	96%	3	1,723	216	1,201
Xoodyak_XT-v1	2,036.3	96%		1,405	233	1,406
Xoodyak_XT-v7	1,992.6	96%		1,405	228	1,406
Xoodyak_GMU-v1	1,642.3	96%		1,808	170	1,272
KNOT-v2	1,626.4	93%	4	1,569	254	1,919
Ascon_Graz-v1	1,620.3	97%		1,551	209	1,585
Ascon_VT-v2	1,517.0	97%		1,928	219	1,774
COMET_VT-v1	1,459.3	98%	5	2,737	233	1,962
Ascon_VT-v1	1,457.1	98%		1,913	233	1,965
DryGASCON-v1	1,414.9	98%	6	2,074	238	2,067
Spook-v2-v1	1,030.0	96%	7	2,296	201	2,398
Romulus-v3	855.8	98%	8	1,824	123	1,766
Romulus-v2	841.8	98%		1,280	214	3,124
GIFT-COFB-v1	731.9	98%	9	1,041	275	4,617
SCHWAEMM-v1	708.6	96%	10	3,071	135	2,341
SCHWAEMM-v2	682.4	96%		3,740	130	2,341
PHOTON-Beetle-v1	680.3	99%	11	2,065	178	3,215
Elephant-v2	661.4	98%	12	1,884	181	3,363
Romulus-v4	655.7	97%		2,602	58	1,087
KNOT-v3	616.2	97%		1,367	264	5,265
KNOT-v4	607.4	96%		1,783	256	5,179
ISAP-v1	598.6	90%	13	3,491	193	3,962
KNOT-v1	583.1	98%		1,092	260	5,479
Romulus-v1	481.8	99%		953	229	5,840
COMET_CI-v1	400.8	98%		1,884	223	6,837
COMET_VT-v2	329.6	98%		1,703	234	8,725
ESTATE-v1	326.3	99%	14	1,377	226	8,512
Pyjamask-v2	255.0	95%	15	2,308	213	10,263
Oribatida-v1	255.0	99%	16	1,450	276	13,301
TinyJAMBU-v1	247.8	99%	17	591	266	13,189
Elephant-v1	210.8	98%		1,291	229	13,347
WAGE-v1	151.7	97%	18	1,150	279	22,600
TinyJAMBU-v2	128.7	99%		564	268	25,589
Xoodyak_GMU-v2	118.0	95%		1,234	168	17,495
LOCUS-v1	115.3	99%	19	1,966	207	22,068
Pyjamask-v1	107.7	96%		1,979	229	26,131
COMET_CI-v2	94.0	98%		1,096	222	29,031
LOTUS-v1	80.7	99%		1,652	145	22,068
ESTATE-v3	79.5	99%		1,197	255	39,392
Gimli-v1	37.9	97%	20	933	241	78,117
Gimli-v2	20.4	97%		905	244	146,617
Gimli-v3	11.0	97%		838	253	283,617
TinyJAMBU-v3	8.6	99%		537	278	397,589

Table 28: Xilinx Artix-7 Encryption PT Throughput for 64 Byte Messages

Variant	**Throughput PT 64B [Mbits/s]**	**Thr PT 64B/ Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles PT 64B**
Subterranean-v1	1,488.0	25%	1	915	186	64
Ascon_Graz-v2	1,140.1	49%	2	1,723	216	97
Xoodyak_XT-v8	1,100.5	46%	3	2,040	187	87
Xoodyak_XT-v2	1,077.0	46%		2,071	183	87
COMET_VT-v1	977.8	66%	4	2,737	233	122
Xoodyak_XT-v1	969.9	46%		1,405	233	123
Ascon_VT-v1	954.4	64%		1,913	233	125
Ascon_VT-v2	950.2	61%		1,928	219	118
Xoodyak_XT-v7	949.1	46%		1,405	228	123
Ascon_Graz-v1	947.0	57%		1,551	209	113
DryGASCON-v1	902.6	62%	5	2,074	238	135
Xoodyak_GMU-v1	784.1	46%		1,808	170	111
KNOT-v2	710.6	41%	6	1,569	254	183
Romulus-v2	608.7	71%	7	1,280	214	180
Romulus-v3	572.5	65%		1,824	123	110
Spook-v2-v1	541.6	51%	8	2,296	201	190
PHOTON-Beetle-v1	509.1	74%	9	2,065	178	179
GIFT-COFB-v1	480.5	64%	10	1,041	275	293
Elephant-v2	413.7	61%	11	1,884	181	224
KNOT-v1	407.1	69%		1,092	260	327
Romulus-v4	395.9	59%		2,602	58	75
KNOT-v3	391.8	62%		1,367	264	345
SCHWAEMM-v1	386.1	53%	12	3,071	135	179
SCHWAEMM-v2	371.8	53%		3,740	130	179
Romulus-v1	366.4	75%		953	229	320
KNOT-v4	331.8	53%		1,783	256	395
COMET_CI-v1	287.6	71%		1,884	223	397
ESTATE-v1	278.2	85%	13	1,377	226	416
COMET_VT-v2	223.1	66%		1,703	234	537
Oribatida-v1	202.7	79%	14	1,450	276	697
TinyJAMBU-v1	201.2	80%	15	591	266	677
ISAP-v1	189.3	29%	16	3,491	193	522
Elephant-v1	135.7	63%		1,291	229	864
Pyjamask-v2	124.1	46%	17	2,308	213	879
TinyJAMBU-v2	105.5	81%		564	268	1,301
LOCUS-v1	97.1	84%	18	1,966	207	1,092
WAGE-v1	88.0	56%	19	1,150	279	1,624
ESTATE-v3	70.3	88%		1,197	255	1,856
LOTUS-v1	68.0	84%		1,652	145	1,092
COMET_CI-v2	66.6	70%		1,096	222	1,707
Pyjamask-v1	57.8	52%		1,979	229	2,027
Xoodyak_GMU-v2	54.7	44%		1,234	168	1,572
Gimli-v1	22.3	57%	20	933	241	5,529
Gimli-v2	12.1	57%		905	244	10,365
TinyJAMBU-v3	7.1	82%		537	278	20,021
Gimli-v3	6.5	57%		838	253	20,037

Table 29: Xilinx Artix-7 Encryption PT Throughput for 16 Byte Messages

Variant	Through-put PT 16B [Mbits/s]	Thr PT 16B/Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles PT 16B
Ascon_VT-v1	458.8	31%	1	1,913	233	65
Subterranean-v1	457.8	8%	2	915	186	52
Ascon_Graz-v2	453.2	20%		1,723	216	61
Ascon_VT-v2	438.0	28%		1,928	219	64
COMET_VT-v1	481.0	32%	3	2,737	233	62
DryGASCON-v1	423.1	29%	4	2,074	238	72
Xoodyak_XT-v8	419.9	18%	5	2,040	187	57
Ascon_Graz-v1	411.6	25%		1,551	209	65
Xoodyak_XT-v2	410.9	18%		2,071	183	57
Xoodyak_XT-v1	368.2	17%		1,405	233	81
Xoodyak_XT-v7	360.3	17%		1,405	228	81
Romulus-v2	326.1	38%	6	1,280	214	84
Xoodyak_GMU-v1	298.1	17%		1,808	170	73
PHOTON-Beetle-v1	284.8	41%	7	2,065	178	80
Romulus-v3	281.1	32%		1,824	123	56
KNOT-v2	256.0	15%	8	1,569	254	127
Elephant-v2	243.9	36%	9	1,884	181	95
GIFT-COFB-v1	231.6	31%	10	1,041	275	152
Romulus-v1	209.4	43%		953	229	140
KNOT-v1	209.3	35%		1,092	260	159
ESTATE-v1	190.3	58%	11	1,377	226	152
KNOT-v3	182.7	29%		1,367	264	185
Spook-v2-v1	181.2	17%	12	2,296	201	142
Romulus-v4	176.8	26%		2,602	58	42
COMET_CI-v1	152.6	37%		1,884	223	187
KNOT-v4	137.1	22%		1,783	256	239
SCHWAEMM-v1	135.0	18%	13	3,071	135	128
SCHWAEMM-v2	130.0	18%		3,740	130	128
TinyJAMBU-v1	126.6	51%	14	591	266	269
Oribatida-v1	123.5	48%	15	1,450	276	286
COMET_VT-v2	110.9	33%		1,703	234	270
Elephant-v1	83.5	39%		1,291	229	351
TinyJAMBU-v2	67.4	52%		564	268	509
LOCUS-v1	64.9	56%	16	1,966	207	408
ISAP-v1	61.5	9%	17	3,491	193	402
ESTATE-v3	51.6	65%		1,197	255	632
Pyjamask-v2	47.6	18%	18	2,308	213	573
LOTUS-v1	45.5	56%		1,652	145	408
WAGE-v1	38.0	24%	19	1,150	279	940
COMET_CI-v2	34.8	36%		1,096	222	816
Pyjamask-v1	23.6	21%		1,979	229	1,241
Xoodyak_GMU-v2	20.5	17%		1,234	168	1,050
Gimli-v1	9.8	25%	20	933	241	3,162
Gimli-v2	5.3	25%		905	244	5,922
TinyJAMBU-v3	4.6	53%		537	278	7,709
Gimli-v3	2.8	25%		838	253	11,442

Table 30: Xilinx Artix-7 Encryption AD Throughput for 1536 Byte Messages

Variant	**Throughput AD 1536B [Mbits/s]**	**Thr AD 1536B/ Thr Long**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles AD 1536B**
Subterranean-v1	5,302.9	89%	1	915	186	431
Xoodyak_XT-v8	3,096.8	94%	2	2,040	187	742
Xoodyak_XT-v2	3,030.6	94%		2,071	183	742
Xoodyak_XT-v1	2,951.7	93%		1,405	233	970
Xoodyak_XT-v7	2,888.3	93%		1,405	228	970
Xoodyak_GMU-v1	2,334.0	93%		1,808	170	895
Ascon_Graz-v2	2,195.4	95%	3	1,723	216	1,209
COMET_VT-v1	1,814.4	97%	4	2,737	233	1,578
Ascon_Graz-v1	1,614.2	96%		1,551	209	1,591
KNOT-v2	1,603.9	92%	5	1,569	254	1,946
Romulus-v2	1,451.2	95%	6	1,280	214	1,812
Ascon_VT-v1	1,451.1	97%		1,913	233	1,973
DryGASCON-v1	1,414.9	97%	7	2,074	238	2,067
Ascon_VT-v2	1,363.9	97%		1,928	219	1,973
Romulus-v3	1,359.2	94%		1,824	123	1,112
Elephant-v2	1,144.7	94%	8	1,884	181	1,943
Spook-v2-v1	1,030.0	96%	9	2,296	201	2,398
ISAP-v1	1,003.2	90%	10	3,491	193	2,364
Romulus-v4	935.3	94%		2,602	58	762
Romulus-v1	876.1	95%		953	229	3,212
SCHWAEMM-v1	869.0	95%	11	3,071	135	1,909
SCHWAEMM-v2	836.8	95%		3,740	130	1,909
PHOTON-Beetle-v1	799.1	98%	12	2,065	178	2,737
GIFT-COFB-v1	709.3	98%	13	1,041	275	4,764
ESTATE-v1	648.4	98%	14	1,377	226	4,283
KNOT-v3	611.6	96%		1,367	264	5,304
KNOT-v4	601.5	95%		1,783	256	5,230
TinyJAMBU-v1	593.4	97%	15	591	266	5,508
KNOT-v1	580.3	97%		1,092	260	5,506
Oribatida-v1	495.8	96%	16	1,450	276	6,841
COMET_CI-v1	466.3	98%		1,884	223	5,877
Elephant-v1	394.8	94%		1,291	229	7,127
COMET_VT-v2	344.7	97%		1,703	234	8,341
TinyJAMBU-v2	322.0	97%		564	268	10,228
Pyjamask-v2	264.7	95%	17	2,308	213	9,887
LOCUS-v1	228.7	98%	18	1,966	207	11,124
Xoodyak_GMU-v2	204.4	91%		1,234	168	10,100
LOTUS-v1	160.2	98%		1,652	145	11,124
ESTATE-v3	158.2	98%		1,197	255	19,803
ESTATE-v2	154.9	99%		893	277	21,967
WAGE-v1	150.9	96%	19	1,150	279	22,713
Pyjamask-v1	109.3	96%		1,979	229	25,755
COMET_CI-v2	105.5	97%		1,096	222	25,863
ESTATE-v4	50.4	98%		944	277	67,557
Gimli-v1	38.1	96%	20	933	241	77,829
TinyJAMBU-v3	22.5	97%		537	278	151,828
Gimli-v2	20.5	96%		905	244	145,945
Gimli-v3	11.0	96%		838	253	282,177

Table 31: Xilinx Artix-7 Encryption AD Throughput for 64 Byte Messages

Variant	Throughput AD 64B [Mbits/s]	Thr AD 64B/ Thr Long	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles AD 64B
Subterranean-v1	1,511.6	25%	1	915	186	63
Xoodyak_XT-v8	1,243.4	37%	2	2,040	187	77
Xoodyak_XT-v2	1,216.8	37%		2,071	183	77
COMET_VT-v1	1,125.4	60%	3	2,737	233	106
Xoodyak_XT-v1	1,114.9	35%		1,405	233	107
Xoodyak_XT-v7	1,091.0	35%		1,405	228	107
Ascon_Graz-v2	1,053.3	45%	4	1,723	216	105
DryGASCON-v1	902.6	62%	5	2,074	238	135
Ascon_Graz-v1	899.2	53%		1,551	209	119
Ascon_VT-v1	897.0	60%		1,913	233	133
Xoodyak_GMU-v1	888.2	35%		1,808	170	98
Ascon_VT-v2	843.1	60%		1,928	219	133
Romulus-v2	702.4	46%	6	1,280	214	156
Romulus-v3	629.8	44%		1,824	123	100
KNOT-v2	619.3	35%	7	1,569	254	210
PHOTON-Beetle-v1	566.1	69%	8	2,065	178	161
Elephant-v2	554.9	45%	9	1,884	181	167
GIFT-COFB-v1	550.0	76%	10	1,041	275	256
Spook-v2-v1	541.6	50%	11	2,296	201	190
ESTATE-v1	492.4	74%	12	1,377	226	235
Romulus-v1	437.5	47%		953	229	268
SCHWAEMM-v1	429.3	47%	13	3,071	135	161
SCHWAEMM-v2	413.4	47%		3,740	130	161
Romulus-v4	412.4	41%		2,602	58	72
TinyJAMBU-v1	382.6	62%	14	591	266	356
KNOT-v1	376.0	63%		1,092	260	354
KNOT-v3	352.0	55%		1,367	264	384
COMET_CI-v1	319.8	67%		1,884	223	357
ISAP-v1	312.7	28%	15	3,491	193	316
KNOT-v4	293.9	46%		1,783	256	446
Oribatida-v1	286.6	55%	16	1,450	276	493
COMET_VT-v2	230.0	65%		1,703	234	521
TinyJAMBU-v2	207.9	63%		564	268	660
Elephant-v1	190.6	45%		1,291	229	615
LOCUS-v1	166.6	71%	17	1,966	207	636
ESTATE-v3	126.1	78%		1,197	255	1,035
Pyjamask-v2	125.2	45%	18	2,308	213	871
ESTATE-v2	120.7	77%		893	277	1,175
LOTUS-v1	116.7	71%		1,652	145	636
WAGE-v1	82.2	52%	19	1,150	279	1,737
COMET_CI-v2	72.2	67%		1,096	222	1,575
Xoodyak_GMU-v2	65.3	29%		1,234	168	1,317
Pyjamask-v1	58.1	51%		1,979	229	2,019
ESTATE-v4	40.2	78%		944	277	3,525
Gimli-v1	22.4	56%	20	933	241	5,517
TinyJAMBU-v3	14.6	63%		537	278	9,780
Gimli-v2	12.1	57%		905	244	10,337
Gimli-v3	6.5	57%		838	253	19,977

Table 32: Xilinx Artix-7 Encryption AD Throughput for 16 Byte Messages

Variant	Through-put 16B [Mbits/s]	Thr AD 16B/ Thr Long	Candi-date Ranking by Throughput	LUTs	Freq. [MHz]	Cycles AD 16B
COMET_VT-v1	514.2	27%	1	2,737	233	58
Subterranean-v1	466.8	7%	2	915	186	51
Xoodyak_XT-v8	427.4	12%	3	2,040	187	56
DryGASCON-v1	423.1	29%	4	2,074	238	72
Xoodyak_XT-v2	418.3	12%		2,071	183	56
Ascon_VT-v1	408.5	27%	5	1,913	233	73
Ascon_Graz-v2	400.7	17%		1,723	216	69
Ascon_VT-v2	384.0	27%		1,928	219	73
Ascon_Graz-v1	376.8	22%		1,551	209	71
Xoodyak_XT-v1	372.8	11%		1,405	233	80
Xoodyak_XT-v7	364.8	11%		1,405	228	80
Romulus-v2	326.1	21%	6	1,280	214	84
GIFT-COFB-v1	322.9	44%	7	1,041	275	109
Xoodyak_GMU-v1	298.1	11%		1,808	170	73
PHOTON-Beetle-v1	295.9	36%	8	2,065	178	77
Romulus-v3	281.1	19%		1,824	123	56
ESTATE-v1	280.9	42%	9	1,377	226	103
KNOT-v2	211.1	12%	10	1,569	254	154
Romulus-v1	209.4	22%		953	229	140
Elephant-v2	194.7	16%	11	1,884	181	119
Spook-v2-v1	181.2	16%	12	2,296	201	142
TinyJAMBU-v1	181.1	29%	13	591	266	188
KNOT-v1	178.9	30%		1,092	260	186
Romulus-v4	176.8	17%		2,602	58	42
COMET_CI-v1	161.3	33%		1,884	223	177
KNOT-v3	150.9	23%		1,367	264	224
SCHWAEMM-v1	140.5	15%	14	3,071	135	123
SCHWAEMM-v2	135.3	15%		3,740	130	123
Oribatida-v1	123.5	24%	15	1,450	276	286
KNOT-v4	113.0	17%		1,783	256	290
COMET_VT-v2	112.6	31%		1,703	234	266
ISAP-v1	101.2	9%	16	3,491	193	244
TinyJAMBU-v2	98.6	29%		564	268	348
LOCUS-v1	90.1	38%	17	1,966	207	294
ESTATE-v3	77.2	48%		1,197	255	423
ESTATE-v2	71.3	45%		893	277	497
Elephant-v1	66.8	16%		1,291	229	439
LOTUS-v1	63.1	38%		1,652	145	294
Pyjamask-v2	47.3	16%	18	2,308	213	577
COMET_CI-v2	36.3	33%		1,096	222	783
WAGE-v1	33.9	21%	19	1,150	279	1,053
ESTATE-v4	24.7	48%		944	277	1,437
Pyjamask-v1	23.5	20%		1,979	229	1,245
Xoodyak_GMU-v2	20.5	9%		1,234	168	1,050
Gimli-v1	9.8	24%	20	933	241	3,159
TinyJAMBU-v3	6.9	29%		537	278	5,148
Gimli-v2	5.3	24%		905	244	5,915
Gimli-v3	2.8	24%		838	253	11,427

Table 33: Xilinx Artix-7 Encryption AD+PT Throughput for 1536 Byte Messages

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles AD+PT 1536B**
Subterranean-v1	5,608.8	1	915	186	815
Xoodyak_XT-v8	2,714.5	2	2,040	187	1,693
Xoodyak_XT-v2	2,656.5		2,071	183	1,693
Xoodyak_XT-v1	2,490.7		1,405	233	2,299
Xoodyak_XT-v7	2,437.3		1,405	228	2,299
Ascon_Graz-v2	2,248.4	3	1,723	216	2,361
Xoodyak_GMU-v1	1,992.3		1,808	170	2,097
KNOT-v2	1,669.5	4	1,569	254	3,739
Ascon_Graz-v1	1,645.7		1,551	209	3,121
COMET_VT-v1	1,637.0	5	2,737	233	3,498
Ascon_VT-v1	1,470.9		1,913	233	3,893
Ascon_VT-v2	1,453.8		1,928	219	3,702
DryGASCON-v1	1,432.5	6	2,074	238	4,083
Romulus-v2	1,083.9	7	1,280	214	4,852
Romulus-v3	1,071.2		1,824	123	2,822
Spook-v2-v1	1,050.6	8	2,296	201	4,702
Elephant-v2	853.6	9	1,884	181	5,211
SCHWAEMM-v1	793.5	10	3,071	135	4,181
Romulus-v4	788.8		2,602	58	1,807
ISAP-v1	778.7	11	3,491	193	6,091
SCHWAEMM-v2	764.1		3,740	130	4,181
PHOTON-Beetle-v1	740.8	12	2,065	178	5,905
GIFT-COFB-v1	728.6	13	1,041	275	9,276
Romulus-v1	631.5		953	229	8,912
KNOT-v3	622.4		1,367	264	10,425
KNOT-v4	615.4		1,783	256	10,223
KNOT-v1	587.1		1,092	260	10,883
ESTATE-v1	436.1	14	1,377	226	12,736
COMET_CI-v1	435.1		1,884	223	12,597
TinyJAMBU-v1	352.1	15	591	266	18,564
COMET_VT-v2	340.6		1,703	234	16,885
Oribatida-v1	339.2	16	1,450	276	19,995
Elephant-v1	279.7		1,291	229	20,123
Pyjamask-v2	266.0	17	2,308	213	19,680
TinyJAMBU-v2	185.2		564	268	35,572
Xoodyak_GMU-v2	155.5		1,234	168	26,548
LOCUS-v1	154.1	18	1,966	207	33,012
Pyjamask-v1	110.6		1,979	229	50,908
LOTUS-v1	107.9		1,652	145	33,012
ESTATE-v3	106.3		1,197	255	58,976
COMET_CI-v2	100.3		1,096	222	54,375
Gimli-v1	38.6	19	933	241	153,573
Gimli-v2	20.8		905	244	288,121
TinyJAMBU-v3	12.5		537	278	545,812
Gimli-v3	11.2		838	253	557,217

Table 34: Xilinx Artix-7 Encryption AD+PT Throughput for 64 Byte Messages

Variant	**Throughput [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles AD+PT 64B**
Subterranean-v1	2,410.9	1	915	186	79
Xoodyak_XT-v8	1,725.1	2	2,040	187	111
Xoodyak_XT-v2	1,688.2		2,071	183	111
Xoodyak_XT-v1	1,559.4		1,405	233	153
Xoodyak_XT-v7	1,526.0		1,405	228	153
Ascon_Graz-v2	1,445.6	3	1,723	216	153
COMET_VT-v1	1,282.8	4	2,737	233	186
Xoodyak_GMU-v1	1,252.4		1,808	170	139
Ascon_Graz-v1	1,209.1		1,551	209	177
Ascon_VT-v1	1,120.2		1,913	233	213
DryGASCON-v1	1,112.8	5	2,074	238	219
Ascon_VT-v2	1,088.6		1,928	219	206
KNOT-v2	974.1	6	1,569	254	267
Romulus-v2	869.6	7	1,280	214	252
Romulus-v3	817.9		1,824	123	154
Spook-v2-v1	719.7	8	2,296	201	286
GIFT-COFB-v1	634.2	9	1,041	275	444
Elephant-v2	626.2	10	1,884	181	296
PHOTON-Beetle-v1	622.1	11	2,065	178	293
Romulus-v4	565.6		2,602	58	105
Romulus-v1	523.4		953	229	448
SCHWAEMM-v1	510.1	12	3,071	135	271
SCHWAEMM-v2	491.2		3,740	130	271
KNOT-v3	462.1		1,367	264	585
KNOT-v1	459.8		1,092	260	579
KNOT-v4	400.2		1,783	256	655
ESTATE-v1	390.9	13	1,377	226	592
COMET_CI-v1	358.5		1,884	223	637
ISAP-v1	327.7	14	3,491	193	603
TinyJAMBU-v1	302.6	15	591	266	900
COMET_VT-v2	273.2		1,703	234	877
Oribatida-v1	271.0	16	1,450	276	1,043
Elephant-v1	207.9		1,291	229	1,128
Pyjamask-v2	170.4	17	2,308	213	1,280
TinyJAMBU-v2	159.9		564	268	1,716
LOCUS-v1	136.9	18	1,966	207	1,548
ESTATE-v3	97.7		1,197	255	2,672
LOTUS-v1	95.9		1,652	145	1,548
Xoodyak_GMU-v2	93.4		1,234	168	1,842
COMET_CI-v2	82.3		1,096	222	2,763
Pyjamask-v1	76.4		1,979	229	3,068
Gimli-v1	28.5	19	933	241	8,673
Gimli-v2	15.4		905	244	16,261
TinyJAMBU-v3	10.9		537	278	26,196
Gimli-v3	8.2		838	253	31,437

Table 35: Xilinx Artix-7 Encryption AD+PT Throughput for 16 Byte Messages

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles AD+PT 16B**
Subterranean-v1	865.7	1	915	186	55
Xoodyak_XT-v8	797.9	2	2,040	187	60
Xoodyak_XT-v2	780.8		2,071	183	60
COMET_VT-v1	764.7	3	2,737	233	78
Xoodyak_XT-v1	710.1		1,405	233	84
Xoodyak_XT-v7	694.9		1,405	228	84
Ascon_Graz-v2	682.7	4	1,723	216	81
Ascon_Graz-v1	660.5		1,551	209	81
DryGASCON-v1	655.1	5	2,074	238	93
Romulus-v2	652.2	6	1,280	214	84
Ascon_VT-v1	641.4		1,913	233	93
Ascon_VT-v2	609.4		1,928	219	92
Xoodyak_GMU-v1	572.6		1,808	170	76
Romulus-v3	562.3		1,824	123	56
GIFT-COFB-v1	451.3	7	1,041	275	156
KNOT-v2	419.5	8	1,569	254	155
Romulus-v1	418.7		953	229	140
PHOTON-Beetle-v1	414.3	9	2,065	178	110
Elephant-v2	389.4	10	1,884	181	119
Romulus-v4	353.5		2,602	58	42
ESTATE-v1	295.2	11	1,377	226	196
KNOT-v1	273.9		1,092	260	243
Spook-v2-v1	270.8	12	2,296	201	190
KNOT-v3	255.0		1,367	264	265
COMET_CI-v1	231.1		1,884	223	247
TinyJAMBU-v1	210.2	13	591	266	324
KNOT-v4	191.1		1,783	256	343
SCHWAEMM-v1	189.9	14	3,071	135	182
SCHWAEMM-v2	182.9		3,740	130	182
COMET_VT-v2	168.7		1,703	234	355
Oribatida-v1	166.2	15	1,450	276	425
Elephant-v1	133.5		1,291	229	439
ISAP-v1	120.2	16	3,491	193	411
TinyJAMBU-v2	112.1		564	268	612
LOCUS-v1	101.5	17	1,966	207	522
Pyjamask-v2	80.2	18	2,308	213	680
ESTATE-v3	78.1		1,197	255	836
LOTUS-v1	71.1		1,652	145	522
COMET_CI-v2	52.6		1,096	222	1,080
Xoodyak_GMU-v2	40.8		1,234	168	1,053
Pyjamask-v1	38.9		1,979	229	1,508
Gimli-v1	15.6	19	933	241	3,948
Gimli-v2	8.4		905	244	7,396
TinyJAMBU-v3	7.7		537	278	9,252
Gimli-v3	4.5		838	253	14,292

Table 36: Intel Cyclone 10 LP Encryption PT Throughput for 1536 Byte Messages

Variant	**Throughput AE PT 1536B [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles PT 1536B**
Subterranean-v1	4,540.9	1	1,333	159.6	432
Ascon_Graz-v2	1,500.4	2	2,666	146.7	1,201
Xoodyak_XT-v1	1,228.4	3	2,282	140.6	1,406
Ascon_VT-v2	1,191.4		2,695	172.0	1,774
Ascon_Graz-v1	1,184.5		2,484	152.8	1,585
Xoodyak_XT-v7	1,169.6		2,253	133.8	1,406
Xoodyak_XT-v8	1,118.0		4,337	91.3	1,004
Ascon_VT-v1	1,104.5		2,432	176.6	1,965
Xoodyak_XT-v2	1,075.1		3,518	87.8	1,004
KNOT-v2	1,072.6	4	2,050	167.5	1,919
Xoodyak_GMU-v1	1,031.6		3,135	106.8	1,272
DryGASCON-v1	776.0	5	3,199	130.5	2,067
Spook-v2-v1	565.7	6	3,912	110.4	2,398
Romulus-v2	557.4	7	2,086	141.7	3,124
Romulus-v3	551.8		2,407	79.3	1,766
COMET_VT-v1	526.8	8	10,035	84.1	1,962
GIFT-COFB-v1	490.8	9	1,877	184.4	4,617
PHOTON-Beetle-v1	479.4	10	3,602	125.4	3,215
Romulus-v4	456.2		3,409	40.4	1,087
SCHWAEMM-v2	450.1	11	5,773	85.7	2,341
SCHWAEMM-v1	429.1		4,713	81.8	2,341
Elephant-v2	413.4	12	2,729	113.2	3,363
KNOT-v4	406.6		2,412	171.3	5,179
KNOT-v1	399.0		1,485	177.9	5,479
KNOT-v3	398.3		1,962	170.7	5,265
ISAP-v2	374.1	13	2,961	139.8	4,592
Romulus-v1	301.4		1,735	143.2	5,840
COMET_CI-v1	208.0		4,663	115.8	6,837
TinyJAMBU-v1	183.4	14	856	196.8	13,189
Oribatida-v1	171.5	15	2,512	185.7	13,301
ESTATE-v1	164.7	16	3,880	114.1	8,512
COMET_VT-v2	155.8		5,204	110.6	8,725
Elephant-v1	150.1		2,056	163.1	13,347
Pyjamask-v2	108.5	17	8,692	90.6	10,263
WAGE-v1	86.8	18	1,774	159.6	22,600
LOCUS-v1	70.0	19	3,121	125.8	22,068
LOTUS-v1	57.6		2,642	103.5	22,068
COMET_CI-v2	56.3		2,629	132.9	29,031
Xoodyak_GMU-v2	54.1		5,871	77.0	17,495
ESTATE-v3	54.1		2,320	173.4	39,392
Pyjamask-v1	51.6		8,599	109.7	26,131
Gimli-v1	15.9	20	2,044	101.3	78,117
Gimli-v2	8.2		2,074	97.3	146,617
Gimli-v3	4.4		2,115	100.5	283,617

Table 37: Intel Cyclone 10 LP Encryption PT Throughput for 64 Byte Messages

Variant	**Throughput AE PT 64B [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles PT 64B**
Subterranean-v1	1,277.1	1	1,333	159.6	64
Ascon_Graz-v2	774.1	2	2,666	146.7	97
Ascon_VT-v2	746.3		2,695	172.0	118
Ascon_VT-v1	723.4		2,432	176.6	125
Ascon_Graz-v1	692.3		2,484	152.8	113
Xoodyak_XT-v1	585.1	3	2,282	140.6	123
Xoodyak_XT-v7	557.1		2,253	133.8	123
Xoodyak_XT-v8	537.6		4,337	91.3	87
Xoodyak_XT-v2	516.9		3,518	87.8	87
DryGASCON-v1	495.0	4	3,199	130.5	135
Xoodyak_GMU-v1	492.6		3,135	106.8	111
KNOT-v2	468.6	5	2,050	167.5	183
Romulus-v2	403.1	6	2,086	141.7	180
Romulus-v3	369.1		2,407	79.3	110
PHOTON-Beetle-v1	358.8	7	3,602	125.4	179
COMET_VT-v1	353.0	8	10,035	84.1	122
GIFT-COFB-v1	322.2	9	1,877	184.4	293
Spook-v2-v1	297.5	10	3,912	110.4	190
KNOT-v1	278.5		1,485	177.9	327
Romulus-v4	275.5		3,409	40.4	75
Elephant-v2	258.6	11	2,729	113.2	224
KNOT-v3	253.3		1,962	170.7	345
SCHWAEMM-v2	245.2	12	5,773	85.7	179
SCHWAEMM-v1	233.8		4,713	81.8	179
Romulus-v1	229.2		1,735	143.2	320
KNOT-v4	222.1		2,412	171.3	395
COMET_CI-v1	149.3		4,663	115.8	397
TinyJAMBU-v1	148.8	13	856	196.8	677
ESTATE-v1	140.4	14	3,880	114.1	416
Oribatida-v1	136.4	15	2,512	185.7	697
ISAP-v2	131.6	16	2,961	139.8	544
COMET_VT-v2	105.5		5,204	110.6	537
Elephant-v1	96.6		2,056	163.1	864
LOCUS-v1	59.0	17	3,121	125.8	1,092
Pyjamask-v2	52.8	18	8,692	90.6	879
WAGE-v1	50.3	19	1,774	159.6	1,624
LOTUS-v1	48.5		2,642	103.5	1,092
ESTATE-v3	47.8		2,320	173.4	1,856
COMET_CI-v2	39.9		2,629	132.9	1,707
Pyjamask-v1	27.7		8,599	109.7	2,027
Xoodyak_GMU-v2	25.1		5,871	77.0	1,572
Gimli-v1	9.4	20	2,044	101.3	5,529
Gimli-v2	4.8		2,074	97.3	10,365
Gimli-v3	2.6		2,115	100.5	20,037

Table 38: Intel Cyclone 10 LP Encryption PT Throughput for 16 Byte Messages

Variant	**Throughput AE PT 16B [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles PT 16B**
Subterranean-v1	393.0	1	1,333	159.6	52
Ascon_VT-v1	347.8	2	2,432	176.6	65
Ascon_VT-v2	344.0		2,695	172.0	64
Ascon_Graz-v2	307.7		2,666	146.7	61
Ascon_Graz-v1	300.9		2,484	152.8	65
DryGASCON-v1	232.1	3	3,199	130.5	72
Xoodyak_XT-v1	222.1	4	2,282	140.6	81
Romulus-v2	215.9	5	2,086	141.7	84
Xoodyak_XT-v7	211.5		2,253	133.8	81
Xoodyak_XT-v8	205.1		4,337	91.3	57
PHOTON-Beetle-v1	200.7	6	3,602	125.4	80
Xoodyak_XT-v2	197.3		3,518	87.8	57
Xoodyak_GMU-v1	187.2		3,135	106.8	73
Romulus-v3	181.3		2,407	79.3	56
COMET_VT-v1	173.6	7	10,035	84.1	62
KNOT-v2	168.8	8	2,050	167.5	127
GIFT-COFB-v1	155.3	9	1,877	184.4	152
Elephant-v2	152.5	10	2,729	113.2	95
KNOT-v1	143.2		1,485	177.9	159
Romulus-v1	131.0		1,735	143.2	140
Romulus-v4	123.0		3,409	40.4	42
KNOT-v3	118.1		1,962	170.7	185
Spook-v2-v1	99.5	11	3,912	110.4	142
ESTATE-v1	96.1	12	3,880	114.1	152
TinyJAMBU-v1	93.6	13	856	196.8	269
KNOT-v4	91.8		2,412	171.3	239
SCHWAEMM-v2	85.7	14	5,773	85.7	128
Oribatida-v1	83.1	15	2,512	185.7	286
SCHWAEMM-v1	81.8		4,713	81.8	128
COMET_CI-v1	79.2		4,663	115.8	187
Elephant-v1	59.5		2,056	163.1	351
COMET_VT-v2	52.4		5,204	110.6	270
ISAP-v2	43.4	16	2,961	139.8	412
LOCUS-v1	39.5	17	3,121	125.8	408
ESTATE-v3	35.1		2,320	173.4	632
LOTUS-v1	32.5		2,642	103.5	408
WAGE-v1	21.7	18	1,774	159.6	940
COMET_CI-v2	20.9		2,629	132.9	816
Pyjamask-v2	20.2	19	8,692	90.6	573
Pyjamask-v1	11.3		8,599	109.7	1,241
Xoodyak_GMU-v2	9.4		5,871	77.0	1,050
Gimli-v1	4.1	20	2,044	101.3	3,162
Gimli-v2	2.1		2,074	97.3	5,922
Gimli-v3	1.1		2,115	100.5	11,442

Table 39: Intel Cyclone 10 LP Encryption AD Throughput for 1536 Byte Messages

Variant	Throughput AE AD 1536B [Mbits/s]	Candidate Ranking by Throughput	LEs	Freq. [MHz]	Cycles AD 1536B
Subterranean-v1	4,551.4	1	1,333	159.6	431
Xoodyak_XT-v1	1,780.5	2	2,282	140.6	970
Xoodyak_XT-v7	1,695.4		2,253	133.8	970
Xoodyak_XT-v8	1,512.8		4,337	91.3	742
Ascon_Graz-v2	1,490.5	3	2,666	146.7	1,209
Xoodyak_GMU-v1	1,466.2		3,135	106.8	895
Xoodyak_XT-v2	1,454.7		3,518	87.8	742
Ascon_Graz-v1	1,180.1		2,484	152.8	1,591
Ascon_VT-v1	1,100.0		2,432	176.6	1,973
Ascon_VT-v2	1,071.2		2,695	172.0	1,973
KNOT-v2	1,057.7	4	2,050	167.5	1,946
Romulus-v2	960.9	5	2,086	141.7	1,812
Romulus-v3	876.3		2,407	79.3	1,112
DryGASCON-v1	776.0	6	3,199	130.5	2,067
Elephant-v2	715.6	7	2,729	113.2	1,943
COMET_VT-v1	655.0	8	10,035	84.1	1,578
Romulus-v4	650.8		3,409	40.4	762
ISAP-v2	591.3	9	2,961	139.8	2,905
Spook-v2-v1	565.7	10	3,912	110.4	2,398
PHOTON-Beetle-v1	563.2	11	3,602	125.4	2,737
SCHWAEMM-v2	551.9	12	5,773	85.7	1,909
Romulus-v1	548.0		1,735	143.2	3,212
SCHWAEMM-v1	526.2		4,713	81.8	1,909
GIFT-COFB-v1	475.6	13	1,877	184.4	4,764
TinyJAMBU-v1	439.1	14	856	196.8	5,508
KNOT-v4	402.6		2,412	171.3	5,230
KNOT-v1	397.0		1,485	177.9	5,506
KNOT-v3	395.4		1,962	170.7	5,304
Oribatida-v1	333.5	15	2,512	185.7	6,841
ESTATE-v1	327.2	16	3,880	114.1	4,283
Elephant-v1	281.1		2,056	163.1	7,127
COMET_CI-v1	242.0		4,663	115.8	5,877
COMET_VT-v2	163.0		5,204	110.6	8,341
LOCUS-v1	138.9	17	3,121	125.8	11,124
LOTUS-v1	114.3		2,642	103.5	11,124
Pyjamask-v2	112.7	18	8,692	90.6	9,887
ESTATE-v3	107.6		2,320	173.4	19,803
ESTATE-v2	97.5		1,946	174.3	21,967
Xoodyak_GMU-v2	93.7		5,871	77.0	10,100
WAGE-v1	86.3	19	1,774	159.6	22,713
COMET_CI-v2	63.2		2,629	132.9	25,863
Pyjamask-v1	52.3		8,599	109.7	25,755
ESTATE-v4	36.4		1,572	200.1	67,557
Gimli-v1	16.0	20	2,044	101.3	77,829
Gimli-v2	8.2		2,074	97.3	145,945
Gimli-v3	4.4		2,115	100.5	282,177

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

Variant	**Throughput AE AD 64B [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles AD 64B**
Subterranean-v1	1,297.4	1	1,333	159.6	63
Ascon_Graz-v2	715.1	2	2,666	146.7	105
Ascon_VT-v1	679.9		2,432	176.6	133
Xoodyak_XT-v1	672.5	3	2,282	140.6	107
Ascon_VT-v2	662.1		2,695	172.0	133
Ascon_Graz-v1	657.4		2,484	152.8	119
Xoodyak_XT-v7	640.4		2,253	133.8	107
Xoodyak_XT-v8	607.4		4,337	91.3	77
Xoodyak_XT-v2	584.1		3,518	87.8	77
Xoodyak_GMU-v1	557.9		3,135	106.8	98
DryGASCON-v1	495.0	4	3,199	130.5	135
Romulus-v2	465.1	5	2,086	141.7	156
KNOT-v2	408.4	6	2,050	167.5	210
COMET_VT-v1	406.3	7	10,035	84.1	106
Romulus-v3	406.0		2,407	79.3	100
PHOTON-Beetle-v1	398.9	8	3,602	125.4	161
GIFT-COFB-v1	368.8	9	1,877	184.4	256
Elephant-v2	346.9	10	2,729	113.2	167
Spook-v2-v1	297.5	11	3,912	110.4	190
Romulus-v4	287.0		3,409	40.4	72
TinyJAMBU-v1	283.1	12	856	196.8	356
Romulus-v1	273.7		1,735	143.2	268
SCHWAEMM-v2	272.7	13	5,773	85.7	161
SCHWAEMM-v1	260.0		4,713	81.8	161
KNOT-v1	257.3		1,485	177.9	354
ESTATE-v1	248.5	14	3,880	114.1	235
KNOT-v3	227.5		1,962	170.7	384
ISAP-v2	217.6	15	2,961	139.8	329
KNOT-v4	196.7		2,412	171.3	446
Oribatida-v1	192.8	16	2,512	185.7	493
COMET_CI-v1	166.0		4,663	115.8	357
Elephant-v1	135.7		2,056	163.1	615
COMET_VT-v2	108.7		5,204	110.6	521
LOCUS-v1	101.2	17	3,121	125.8	636
ESTATE-v3	85.8		2,320	173.4	1,035
LOTUS-v1	83.3		2,642	103.5	636
ESTATE-v2	76.0		1,946	174.3	1,175
Pyjamask-v2	53.3	18	8,692	90.6	871
WAGE-v1	47.0	19	1,774	159.6	1,737
COMET_CI-v2	43.2		2,629	132.9	1,575
Xoodyak_GMU-v2	30.0		5,871	77.0	1,317
ESTATE-v4	29.1		1,572	200.1	3,525
Pyjamask-v1	27.8		8,599	109.7	2,019
Gimli-v1	9.4	20	2,044	101.3	5,517
Gimli-v2	4.8		2,074	97.3	10,337
Gimli-v3	2.6		2,115	100.5	19,977

Table 41: Intel Cyclone 10 LP Encryption AD Throughput for 16 Byte Messages

Variant	**Throughput AE AD 16B [Mbits/s]**	**Candidate Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles AD 16B**
Subterranean-v1	400.7	1	1,333	159.6	51
Ascon_VT-v1	309.7	2	2,432	176.6	73
Ascon_VT-v2	301.6		2,695	172.0	73
Ascon_Graz-v1	275.5		2,484	152.8	71
Ascon_Graz-v2	272.0		2,666	146.7	69
DryGASCON-v1	232.1	3	3,199	130.5	72
Xoodyak_XT-v1	224.9	4	2,282	140.6	80
GIFT-COFB-v1	216.5	5	1,877	184.4	109
Romulus-v2	215.9	6	2,086	141.7	84
Xoodyak_XT-v7	214.1		2,253	133.8	80
Xoodyak_XT-v8	208.8		4,337	91.3	56
PHOTON-Beetle-v1	208.5	7	3,602	125.4	77
Xoodyak_XT-v2	200.8		3,518	87.8	56
Xoodyak_GMU-v1	187.2		3,135	106.8	73
COMET_VT-v1	185.6	8	10,035	84.1	58
Romulus-v3	181.3		2,407	79.3	56
ESTATE-v1	141.7	9	3,880	114.1	103
KNOT-v2	139.2	10	2,050	167.5	154
TinyJAMBU-v1	134.0	11	856	196.8	188
Romulus-v1	131.0		1,735	143.2	140
Romulus-v4	123.0		3,409	40.4	42
KNOT-v1	122.4		1,485	177.9	186
Elephant-v2	121.7	12	2,729	113.2	119
Spook-v2-v1	99.5	13	3,912	110.4	142
KNOT-v3	97.5		1,962	170.7	224
SCHWAEMM-v2	89.2	14	5,773	85.7	123
SCHWAEMM-v1	85.1		4,713	81.8	123
COMET_CI-v1	83.7		4,663	115.8	177
Oribatida-v1	83.1	15	2,512	185.7	286
KNOT-v4	75.6		2,412	171.3	290
ISAP-v2	73.0	16	2,961	139.8	245
LOCUS-v1	54.8	17	3,121	125.8	294
COMET_VT-v2	53.2		5,204	110.6	266
ESTATE-v3	52.5		2,320	173.4	423
Elephant-v1	47.5		2,056	163.1	439
LOTUS-v1	45.1		2,642	103.5	294
ESTATE-v2	44.9		1,946	174.3	497
COMET_CI-v2	21.7		2,629	132.9	783
Pyjamask-v2	20.1	18	8,692	90.6	577
WAGE-v1	19.4	19	1,774	159.6	1,053
ESTATE-v4	17.8		1,572	200.1	1,437
Pyjamask-v1	11.3		8,599	109.7	1,245
Xoodyak_GMU-v2	9.4		5,871	77.0	1,050
Gimli-v1	4.1	20	2,044	101.3	3,159
Gimli-v2	2.1		2,074	97.3	5,915
Gimli-v3	1.1		2,115	100.5	11,427

Table 42: Intel Cyclone 10 LP Encryption AD+PT Throughput for 64 Byte Messages

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles AD+PT 64B**
Subterranean-v1	2,069.3	1	1,333	159.6	79
Ascon_Graz-v2	981.5	2	2,666	146.7	153
Xoodyak_XT-v1	940.7	3	2,282	140.6	153
Xoodyak_XT-v7	895.7		2,253	133.8	153
Ascon_Graz-v1	883.9		2,484	152.8	177
Ascon_VT-v2	855.0		2,695	172.0	206
Ascon_VT-v1	849.1		2,432	176.6	213
Xoodyak_XT-v8	842.7		4,337	91.3	111
Xoodyak_XT-v2	810.3		3,518	87.8	111
Xoodyak_GMU-v1	786.7		3,135	106.8	139
KNOT-v2	642.4	4	2,050	167.5	267
DryGASCON-v1	610.3	5	3,199	130.5	219
Romulus-v2	575.8	6	2,086	141.7	252
Romulus-v3	527.3		2,407	79.3	154
COMET_VT-v1	463.1	7	10,035	84.1	186
PHOTON-Beetle-v1	438.4	8	3,602	125.4	293
GIFT-COFB-v1	425.3	9	1,877	184.4	444
Spook-v2-v1	395.2	10	3,912	110.4	286
Romulus-v4	393.6		3,409	40.4	105
Elephant-v2	391.4	11	2,729	113.2	296
Romulus-v1	327.4		1,735	143.2	448
SCHWAEMM-v2	324.0	12	5,773	85.7	271
KNOT-v1	314.6		1,485	177.9	579
SCHWAEMM-v1	308.9		4,713	81.8	271
KNOT-v3	298.7		1,962	170.7	585
KNOT-v4	267.9		2,412	171.3	655
TinyJAMBU-v1	223.9	13	856	196.8	900
ISAP-v2	217.9	14	2,961	139.8	657
ESTATE-v1	197.3	15	3,880	114.1	592
COMET_CI-v1	186.1		4,663	115.8	637
Oribatida-v1	182.3	16	2,512	185.7	1,043
Elephant-v1	148.0		2,056	163.1	1,128
COMET_VT-v2	129.2		5,204	110.6	877
LOCUS-v1	83.2	17	3,121	125.8	1,548
Pyjamask-v2	72.5	18	8,692	90.6	1,280
LOTUS-v1	68.5		2,642	103.5	1,548
ESTATE-v3	66.5		2,320	173.4	2,672
COMET_CI-v2	49.3		2,629	132.9	2,763
Xoodyak_GMU-v2	42.8		5,871	77.0	1,842
Pyjamask-v1	36.6		8,599	109.7	3,068
Gimli-v1	12.0	19	2,044	101.3	8,673
Gimli-v2	6.1		2,074	97.3	16,261
Gimli-v3	3.3		2,115	100.5	31,437

Table 43: Intel Cyclone 10 LP Encryption AD+PT Throughput for 1536 Byte Messages

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles AD+PT 1536B**
Subterranean-v1	4,813.9	1	1,333	159.6	815
Ascon_Graz-v2	1,526.5	2	2,666	146.7	2,361
Xoodyak_XT-v1	1,502.5	3	2,282	140.6	2,299
Xoodyak_XT-v7	1,430.6		2,253	133.8	2,299
Xoodyak_XT-v8	1,326.1		4,337	91.3	1,693
Xoodyak_XT-v2	1,275.1		3,518	87.8	1,693
Xoodyak_GMU-v1	1,251.5		3,135	106.8	2,097
Ascon_Graz-v1	1,203.1		2,484	152.8	3,121
Ascon_VT-v2	1,141.8		2,695	172.0	3,702
Ascon_VT-v1	1,115.0		2,432	176.6	3,893
KNOT-v2	1,101.0	4	2,050	167.5	3,739
DryGASCON-v1	785.7	5	3,199	130.5	4,083
Romulus-v2	717.7	6	2,086	141.7	4,852
Romulus-v3	690.6		2,407	79.3	2,822
COMET_VT-v1	590.9	7	10,035	84.1	3,498
Spook-v2-v1	577.0	8	3,912	110.4	4,702
Romulus-v4	548.9		3,409	40.4	1,807
Elephant-v2	533.6	9	2,729	113.2	5,211
PHOTON-Beetle-v1	522.1	10	3,602	125.4	5,905
SCHWAEMM-v2	504.0	11	5,773	85.7	4,181
GIFT-COFB-v1	488.6	12	1,877	184.4	9,276
SCHWAEMM-v1	480.5		4,713	81.8	4,181
ISAP-v2	471.9	13	2,961	139.8	7,281
KNOT-v4	411.9		2,412	171.3	10,223
KNOT-v3	402.3		1,962	170.7	10,425
KNOT-v1	401.7		1,485	177.9	10,883
Romulus-v1	395.0		1,735	143.2	8,912
TinyJAMBU-v1	260.5	14	856	196.8	18,564
Oribatida-v1	228.2	15	2,512	185.7	19,995
COMET_CI-v1	225.8		4,663	115.8	12,597
ESTATE-v1	220.1	16	3,880	114.1	12,736
Elephant-v1	199.1		2,056	163.1	20,123
COMET_VT-v2	161.0		5,204	110.6	16,885
Pyjamask-v2	113.2	17	8,692	90.6	19,680
LOCUS-v1	93.6	18	3,121	125.8	33,012
LOTUS-v1	77.1		2,642	103.5	33,012
ESTATE-v3	72.3		2,320	173.4	58,976
Xoodyak_GMU-v2	71.3		5,871	77.0	26,548
COMET_CI-v2	60.1		2,629	132.9	54,375
Pyjamask-v1	52.9		8,599	109.7	50,908
Gimli-v1	16.2	19	2,044	101.3	153,573
Gimli-v2	8.3		2,074	97.3	288,121
Gimli-v3	4.4		2,115	100.5	557,217

Table 44: Intel Cyclone 10 LP Encryption AD+PT Throughput for 16 Byte Messages

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LEs**	**Freq. [MHz]**	**Cycles AD+PT 16B**
Subterranean-v1	743.1	1	1,333	159.6	55
Ascon_VT-v1	486.2	2	2,432	176.6	93
Ascon_Graz-v1	482.9		2,484	152.8	81
Ascon_VT-v2	478.6		2,695	172.0	92
Ascon_Graz-v2	463.5		2,666	146.7	81
Romulus-v2	431.8	3	2,086	141.7	84
Xoodyak_XT-v1	428.3	4	2,282	140.6	84
Xoodyak_XT-v7	407.9		2,253	133.8	84
Xoodyak_XT-v8	389.8		4,337	91.3	60
Xoodyak_XT-v2	374.8		3,518	87.8	60
Romulus-v3	362.5		2,407	79.3	56
Xoodyak_GMU-v1	359.7		3,135	106.8	76
DryGASCON-v1	359.3	5	3,199	130.5	93
GIFT-COFB-v1	302.6	6	1,877	184.4	156
PHOTON-Beetle-v1	291.9	7	3,602	125.4	110
KNOT-v2	276.6	8	2,050	167.5	155
COMET_VT-v1	276.1	9	10,035	84.1	78
Romulus-v1	261.9		1,735	143.2	140
Romulus-v4	246.0		3,409	40.4	42
Elephant-v2	243.4	10	2,729	113.2	119
KNOT-v1	187.4		1,485	177.9	243
KNOT-v3	164.9		1,962	170.7	265
TinyJAMBU-v1	155.5	11	856	196.8	324
ESTATE-v1	149.0	12	3,880	114.1	196
Spook-v2-v1	148.7	13	3,912	110.4	190
KNOT-v4	127.9		2,412	171.3	343
SCHWAEMM-v2	120.6	14	5,773	85.7	182
COMET_CI-v1	120.0		4,663	115.8	247
SCHWAEMM-v1	115.0		4,713	81.8	182
Oribatida-v1	111.8	15	2,512	185.7	425
Elephant-v1	95.1		2,056	163.1	439
ISAP-v2	81.2	16	2,961	139.8	441
COMET_VT-v2	79.8		5,204	110.6	355
LOCUS-v1	61.7	17	3,121	125.8	522
ESTATE-v3	53.1		2,320	173.4	836
LOTUS-v1	50.8		2,642	103.5	522
Pyjamask-v2	34.1	18	8,692	90.6	680
COMET_CI-v2	31.5		2,629	132.9	1,080
Xoodyak_GMU-v2	18.7		5,871	77.0	1,053
Pyjamask-v1	18.6		8,599	109.7	1,508
Gimli-v1	6.6	19	2,044	101.3	3,948
Gimli-v2	3.4		2,074	97.3	7,396
Gimli-v3	1.8		2,115	100.5	14,292

Table 45: Lattice ECP5 Encryption PT Throughput for 1536 Byte Messages

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles PT 1536B
Subterranean-v1	1,675.4	1	1,725	58.9	432
Xoodyak_XT-v2	865.3	2	4,302	70.7	1,004
Ascon_Graz-v2	858.4	3	7,246	83.9	1,201
Xoodyak_XT-v8	799.2		4,553	65.3	1,004
COMET_VT-v1	699.0	4	6,613	111.6	1,962
Xoodyak_XT-v1	690.6		2,986	79.0	1,406
Ascon_Graz-v1	641.1		6,507	82.7	1,585
Xoodyak_GMU-v1	616.6		3,474	63.8	1,272
Xoodyak_XT-v7	584.3		3,272	66.9	1,406
KNOT-v2	583.7	5	2,241	91.2	1,919
Xoodyak_XT-v3	541.0		5,569	38.3	870
DryGASCON-v1	537.4	6	3,854	90.4	2,067
Ascon_VT-v1	530.9		3,130	84.9	1,965
Ascon_VT-v2	514.0		3,256	74.2	1,774
Xoodyak_XT-v9	508.5		5,614	36.0	870
Xoodyak_XT-v4	408.6		6,839	26.7	803
Xoodyak_XT-v10	405.5		6,899	26.5	803
Spook-v2-v1	398.7	7	3,655	77.8	2,398
PHOTON-Beetle-v1	387.7	8	3,294	101.4	3,215
Romulus-v3	313.1	9	3,847	45.0	1,766
Elephant-v2	312.4	10	3,073	85.5	3,363
GIFT-COFB-v1	304.2	11	2,214	114.3	4,617
SCHWAEMM-v2	291.3	12	7,570	55.5	2,341
SCHWAEMM-v1	287.1		6,008	54.7	2,341
Xoodyak_XT-v11	277.0		9,447	16.6	736
Xoodyak_XT-v5	276.8		9,386	16.6	736
Romulus-v2	253.3		3,080	64.4	3,124
Romulus-v4	244.2		5,086	21.6	1,087
KNOT-v1	210.5		1,597	93.8	5,479
KNOT-v4	203.1		2,408	85.6	5,179
KNOT-v3	194.1		2,037	83.2	5,265
ISAP-v1	177.9	13	16,179	57.4	3,962
Romulus-v1	165.8		2,633	78.8	5,840
COMET_CI-v1	145.4		3,427	80.9	6,837
ESTATE-v1	144.9	14	3,085	100.4	8,512
COMET_VT-v2	129.9		3,154	92.2	8,725
Oribatida-v1	110.6	15	2,832	119.7	13,301
TinyJAMBU-v1	92.9	16	928	99.7	13,189
Elephant-v1	89.8		2,368	97.5	13,347
Pyjamask-v2	60.6	17	4,452	50.6	10,263
WAGE-v1	49.5	18	2,029	91.1	22,600
TinyJAMBU-v2	47.5		913	99.0	25,589
Xoodyak_GMU-v2	45.0		2,803	64.0	17,495
LOCUS-v1	44.3	19	3,161	79.6	22,068
COMET_CI-v2	39.9		1,974	94.3	29,031
ESTATE-v3	32.4		2,029	104.0	39,392
Pyjamask-v1	31.0		4,094	66.0	26,131
LOTUS-v1	31.0		2,820	55.6	22,068
Gimli-v1	12.3	20	1,767	78.0	78,117
Gimli-v2	6.2		1,767	73.5	146,617
Gimli-v3	3.4		1,772	78.5	283,617
TinyJAMBU-v3	3.0		881	97.7	397,589

Table 46: Lattice ECP5 Encryption PT Throughput for 64 Byte Messages

Variant	**Throughput [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles PT 64B**
Subterranean-v1	471.2	1	1,725	58.9	64
COMET_VT-v1	468.4	2	6,613	111.6	122
Ascon_Graz-v2	442.9	3	7,246	83.9	97
Xoodyak_XT-v2	416.1	4	4,302	70.7	87
Xoodyak_XT-v8	384.3		4,553	65.3	87
Ascon_Graz-v1	374.7		6,507	82.7	113
Ascon_VT-v1	347.8		3,130	84.9	125
DryGASCON-v1	342.9	5	3,854	90.4	135
Xoodyak_XT-v1	328.9		2,986	79.0	123
Ascon_VT-v2	322.0		3,256	74.2	118
Xoodyak_GMU-v1	294.4		3,474	63.8	111
PHOTON-Beetle-v1	290.2	6	3,294	101.4	179
Xoodyak_XT-v7	278.3		3,272	66.9	123
Xoodyak_XT-v3	261.5		5,569	38.3	75
KNOT-v2	255.0	7	2,241	91.2	183
Xoodyak_XT-v9	245.8		5,614	36.0	75
Spook-v2-v1	209.7	8	3,655	77.8	190
Romulus-v3	209.5	9	3,847	45.0	110
GIFT-COFB-v1	199.7	10	2,214	114.3	293
Xoodyak_XT-v4	198.1		6,839	26.7	69
Xoodyak_XT-v10	196.6		6,899	26.5	69
Elephant-v2	195.4	11	3,073	85.5	224
Romulus-v2	183.2		3,080	64.4	180
SCHWAEMM-v2	158.7	12	7,570	55.5	179
SCHWAEMM-v1	156.5		6,008	54.7	179
Romulus-v4	147.5		5,086	21.6	75
KNOT-v1	146.9		1,597	93.8	327
Xoodyak_XT-v11	134.8		9,447	16.6	63
Xoodyak_XT-v5	134.7		9,386	16.6	63
Romulus-v1	126.0		2,633	78.8	320
ESTATE-v1	123.6	13	3,085	100.4	416
KNOT-v3	123.4		2,037	83.2	345
KNOT-v4	111.0		2,408	85.6	395
COMET_CI-v1	104.3		3,427	80.9	397
COMET_VT-v2	88.0		3,154	92.2	537
Oribatida-v1	87.9	14	2,832	119.7	697
TinyJAMBU-v1	75.4	15	928	99.7	677
Elephant-v1	57.8		2,368	97.5	864
ISAP-v1	56.3	16	16,179	57.4	522
TinyJAMBU-v2	39.0		913	99.0	1,301
LOCUS-v1	37.3	17	3,161	79.6	1,092
Pyjamask-v2	29.5	18	4,452	50.6	879
WAGE-v1	28.7	19	2,029	91.1	1,624
ESTATE-v3	28.7		2,029	104.0	1,856
COMET_CI-v2	28.3		1,974	94.3	1,707
LOTUS-v1	26.1		2,820	55.6	1,092
Xoodyak_GMU-v2	20.9		2,803	64.0	1,572
Pyjamask-v1	16.7		4,094	66.0	2,027
Gimli-v1	7.2	20	1,767	78.0	5,529
Gimli-v2	3.6		1,767	73.5	10,365
TinyJAMBU-v3	2.5		881	97.7	20,021
Gimli-v3	2.0		1,772	78.5	20,037

Table 47: Lattice ECP5 Encryption PT Throughput for 16 Byte Messages

Variant	Through-put [Mbits/s]	Candi-date Ranking by Throughput	LUTs	Freq. [MHz]	Cycles PT 16B
COMET_VT-v1	230.4	1	6,613	111.6	62
Ascon_Graz-v2	176.1	2	7,246	83.9	61
Ascon_VT-v1	167.2		3,130	84.9	65
Ascon_Graz-v1	162.9		6,507	82.7	65
PHOTON-Beetle-v1	162.3	3	3,294	101.4	80
DryGASCON-v1	160.7	4	3,854	90.4	72
Xoodyak_XT-v2	158.8	5	4,302	70.7	57
Ascon_VT-v2	148.4		3,256	74.2	64
Xoodyak_XT-v8	146.6		4,553	65.3	57
Subterranean-v1	145.0	6	1,725	58.9	52
Xoodyak_XT-v1	124.9		2,986	79.0	81
Elephant-v2	115.2	7	3,073	85.5	95
Xoodyak_GMU-v1	111.9		3,474	63.8	73
Xoodyak_XT-v7	105.7		3,272	66.9	81
Romulus-v3	102.9	8	3,847	45.0	56
Xoodyak_XT-v3	100.0		5,569	38.3	49
Romulus-v2	98.1		3,080	64.4	84
GIFT-COFB-v1	96.3	9	2,214	114.3	152
Xoodyak_XT-v9	94.0		5,614	36.0	49
KNOT-v2	91.9	10	2,241	91.2	127
ESTATE-v1	84.5	11	3,085	100.4	152
Xoodyak_XT-v4	75.9		6,839	26.7	45
KNOT-v1	75.6		1,597	93.8	159
Xoodyak_XT-v10	75.4		6,899	26.5	45
Romulus-v1	72.0		2,633	78.8	140
Spook-v2-v1	70.1	12	3,655	77.8	142
Romulus-v4	65.8		5,086	21.6	42
KNOT-v3	57.5		2,037	83.2	185
SCHWAEMM-v2	55.5	13	7,570	55.5	128
COMET_CI-v1	55.4		3,427	80.9	187
SCHWAEMM-v1	54.7		6,008	54.7	128
Oribatida-v1	53.6	14	2,832	119.7	286
Xoodyak_XT-v11	51.8		9,447	16.6	41
Xoodyak_XT-v5	51.8		9,386	16.6	41
TinyJAMBU-v1	47.5	15	928	99.7	269
KNOT-v4	45.8		2,408	85.6	239
COMET_VT-v2	43.7		3,154	92.2	270
Elephant-v1	35.6		2,368	97.5	351
LOCUS-v1	25.0	16	3,161	79.6	408
TinyJAMBU-v2	24.9		913	99.0	509
ESTATE-v3	21.1		2,029	104.0	632
ISAP-v1	18.3	17	16,179	57.4	402
LOTUS-v1	17.4		2,820	55.6	408
COMET_CI-v2	14.8		1,974	94.3	816
WAGE-v1	12.4	18	2,029	91.1	940
Pyjamask-v2	11.3	19	4,452	50.6	573
Xoodyak_GMU-v2	7.8		2,803	64.0	1,050
Pyjamask-v1	6.8		4,094	66.0	1,241
Gimli-v1	3.2	20	1,767	78.0	3,162
TinyJAMBU-v3	1.6		881	97.7	7,709
Gimli-v2	1.6		1,767	73.5	5,922
Gimli-v3	0.9		1,772	78.5	11,442

Table 48: Lattice ECP5 Encryption AD Throughput for 1536 Byte Messages

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles AD 1536B
Subterranean-v1	1,679.3	1	1,725	58.9	431
Xoodyak_XT-v2	1,170.8	2	4,302	70.7	742
Xoodyak_XT-v8	1,081.4		4,553	65.3	742
Xoodyak_XT-v1	1,001.0		2,986	79.0	970
Xoodyak_GMU-v1	876.4		3,474	63.8	895
COMET_VT-v1	869.0	3	6,613	111.6	1,578
Ascon_Graz-v2	852.7	4	7,246	83.9	1,209
Xoodyak_XT-v7	847.0		3,272	66.9	970
Xoodyak_XT-v3	706.7		5,569	38.3	666
Xoodyak_XT-v9	664.2		5,614	36.0	666
Ascon_Graz-v1	638.7		6,507	82.7	1,591
KNOT-v2	575.6	5	2,241	91.2	1,946
Elephant-v2	540.7	6	3,073	85.5	1,943
DryGASCON-v1	537.4	7	3,854	90.4	2,067
Ascon_VT-v1	528.8		3,130	84.9	1,973
Xoodyak_XT-v4	522.4		6,839	26.7	628
Xoodyak_XT-v10	518.5		6,899	26.5	628
Romulus-v3	497.3	8	3,847	45.0	1,112
Ascon_VT-v2	462.1		3,256	74.2	1,973
PHOTON-Beetle-v1	455.4	9	3,294	101.4	2,737
Romulus-v2	436.7		3,080	64.4	1,812
Spook-v2-v1	398.7	10	3,655	77.8	2,398
SCHWAEMM-v2	357.2	11	7,570	55.5	1,909
SCHWAEMM-v1	352.1		6,008	54.7	1,909
Romulus-v4	348.3		5,086	21.6	762
Xoodyak_XT-v11	345.5		9,447	16.6	590
Xoodyak_XT-v5	345.3		9,386	16.6	590
Romulus-v1	301.4		2,633	78.8	3,212
ISAP-v1	298.1	12	16,179	57.4	2,364
GIFT-COFB-v1	294.8	13	2,214	114.3	4,764
ESTATE-v1	288.0	14	3,085	100.4	4,283
TinyJAMBU-v1	222.5	15	928	99.7	5,508
Oribatida-v1	215.0	16	2,832	119.7	6,841
KNOT-v1	209.4		1,597	93.8	5,506
KNOT-v4	201.1		2,408	85.6	5,230
KNOT-v3	192.6		2,037	83.2	5,304
COMET_CI-v1	169.2		3,427	80.9	5,877
Elephant-v1	168.1		2,368	97.5	7,127
COMET_VT-v2	135.9		3,154	92.2	8,341
TinyJAMBU-v2	118.9		913	99.0	10,228
LOCUS-v1	87.9	17	3,161	79.6	11,124
Xoodyak_GMU-v2	77.9		2,803	64.0	10,100
ESTATE-v3	64.5		2,029	104.0	19,803
Pyjamask-v2	62.9	18	4,452	50.6	9,887
LOTUS-v1	61.4		2,820	55.6	11,124
ESTATE-v2	50.6		1,691	90.5	21,967
WAGE-v1	49.3	19	2,029	91.1	22,713
COMET_CI-v2	44.8		1,974	94.3	25,863
Pyjamask-v1	31.5		4,094	66.0	25,755
ESTATE-v4	17.5		1,394	96.0	67,557
Gimli-v1	12.3	20	1,767	78.0	77,829
TinyJAMBU-v3	7.9		881	97.7	151,828
Gimli-v2	6.2		1,767	73.5	145,945
Gimli-v3	3.4		1,772	78.5	282,177

Table 49: Lattice ECP5 Encryption AD Throughput for 64 Byte Messages

Variant	Through put [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles AD 64B
COMET_VT-v1	539.0	1	6,613	111.6	106
Subterranean-v1	478.7	2	1,725	58.9	63
Xoodyak_XT-v2	470.1	3	4,302	70.7	77
Xoodyak_XT-v8	434.2		4,553	65.3	77
Ascon_Graz-v2	409.1	4	7,246	83.9	105
Xoodyak_XT-v1	378.1		2,986	79.0	107
Ascon_Graz-v1	355.8		6,507	82.7	119
DryGASCON-v1	342.9	5	3,854	90.4	135
Xoodyak_GMU-v1	333.5		3,474	63.8	98
Ascon_VT-v1	326.8		3,130	84.9	133
PHOTON-Beetle-v1	322.6	6	3,294	101.4	161
Xoodyak_XT-v7	319.9		3,272	66.9	107
Xoodyak_XT-v3	292.7		5,569	38.3	67
Ascon_VT-v2	285.6		3,256	74.2	133
Xoodyak_XT-v9	275.1		5,614	36.0	67
Elephant-v2	262.1	7	3,073	85.5	167
Romulus-v3	230.4	8	3,847	45.0	100
GIFT-COFB-v1	228.6	9	2,214	114.3	256
KNOT-v2	222.2	10	2,241	91.2	210
Xoodyak_XT-v4	220.5		6,839	26.7	62
Xoodyak_XT-v10	218.8		6,899	26.5	62
ESTATE-v1	218.7	11	3,085	100.4	235
Romulus-v2	211.4		3,080	64.4	156
Spook-v2-v1	209.7	12	3,655	77.8	190
SCHWAEMM-v2	176.5	13	7,570	55.5	161
SCHWAEMM-v1	174.0		6,008	54.7	161
Romulus-v4	153.6		5,086	21.6	72
Romulus-v1	150.5		2,633	78.8	268
Xoodyak_XT-v11	149.0		9,447	16.6	57
Xoodyak_XT-v5	148.9		9,386	16.6	57
TinyJAMBU-v1	143.4	14	928	99.7	356
KNOT-v1	135.7		1,597	93.8	354
Oribatida-v1	124.3	15	2,832	119.7	493
COMET_CI-v1	116.0		3,427	80.9	357
KNOT-v3	110.9		2,037	83.2	384
KNOT-v4	98.3		2,408	85.6	446
ISAP-v1	92.9	16	16,179	57.4	316
COMET_VT-v2	90.7		3,154	92.2	521
Elephant-v1	81.2		2,368	97.5	615
TinyJAMBU-v2	76.8		913	99.0	660
LOCUS-v1	64.1	17	3,161	79.6	636
ESTATE-v3	51.4		2,029	104.0	1,035
LOTUS-v1	44.8		2,820	55.6	636
ESTATE-v2	39.4		1,691	90.5	1,175
COMET_CI-v2	30.7		1,974	94.3	1,575
Pyjamask-v2	29.7	18	4,452	50.6	871
WAGE-v1	26.9	19	2,029	91.1	1,737
Xoodyak_GMU-v2	24.9		2,803	64.0	1,317
Pyjamask-v1	16.7		4,094	66.0	2,019
ESTATE-v4	13.9		1,394	96.0	3,525
Gimli-v1	7.2	20	1,767	78.0	5,517
TinyJAMBU-v3	5.1		881	97.7	9,780
Gimli-v2	3.6		1,767	73.5	10,337
Gimli-v3	2.0		1,772	78.5	19,977

Table 50: Lattice ECP5 Encryption AD Throughput for 16 Byte Messages

Variant	**Through-put [Mbits/s]**	**Candi-date Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles AD 16B**
COMET_VT-v1	246.3	1	6,613	111.6	58
PHOTON-Beetle-v1	168.6	2	3,294	101.4	77
Xoodyak_XT-v2	161.6	3	4,302	70.7	56
DryGASCON-v1	160.7	4	3,854	90.4	72
Ascon_Graz-v2	155.6	5	7,246	83.9	69
Xoodyak_XT-v8	149.3		4,553	65.3	56
Ascon_Graz-v1	149.1		6,507	82.7	71
Ascon_VT-v1	148.9		3,130	84.9	73
Subterranean-v1	147.8	6	1,725	58.9	51
GIFT-COFB-v1	134.2	7	2,214	114.3	109
Ascon_VT-v2	130.1		3,256	74.2	73
Xoodyak_XT-v1	126.4		2,986	79.0	80
ESTATE-v1	124.8	8	3,085	100.4	103
Xoodyak_GMU-v1	111.9		3,474	63.8	73
Xoodyak_XT-v7	107.0		3,272	66.9	80
Romulus-v3	102.9	9	3,847	45.0	56
Xoodyak_XT-v3	102.1		5,569	38.3	48
Romulus-v2	98.1		3,080	64.4	84
Xoodyak_XT-v9	96.0		5,614	36.0	48
Elephant-v2	92.0	10	3,073	85.5	119
Xoodyak_XT-v4	77.7		6,839	26.7	44
Xoodyak_XT-v10	77.1		6,899	26.5	44
KNOT-v2	75.8	11	2,241	91.2	154
Romulus-v1	72.0		2,633	78.8	140
Spook-v2-v1	70.1	12	3,655	77.8	142
TinyJAMBU-v1	67.9	13	928	99.7	188
Romulus-v4	65.8		5,086	21.6	42
KNOT-v1	64.6		1,597	93.8	186
COMET_CI-v1	58.5		3,427	80.9	177
SCHWAEMM-v2	57.8	14	7,570	55.5	123
SCHWAEMM-v1	56.9		6,008	54.7	123
Oribatida-v1	53.6	15	2,832	119.7	286
Xoodyak_XT-v11	53.1		9,447	16.6	40
Xoodyak_XT-v5	53.1		9,386	16.6	40
KNOT-v3	47.5		2,037	83.2	224
COMET_VT-v2	44.4		3,154	92.2	266
KNOT-v4	37.8		2,408	85.6	290
TinyJAMBU-v2	36.4		913	99.0	348
LOCUS-v1	34.7	16	3,161	79.6	294
ESTATE-v3	31.5		2,029	104.0	423
ISAP-v1	30.1	17	16,179	57.4	244
Elephant-v1	28.4		2,368	97.5	439
LOTUS-v1	24.2		2,820	55.6	294
ESTATE-v2	23.3		1,691	90.5	497
COMET_CI-v2	15.4		1,974	94.3	783
Pyjamask-v2	11.2	18	4,452	50.6	577
WAGE-v1	11.1	19	2,029	91.1	1,053
ESTATE-v4	8.5		1,394	96.0	1,437
Xoodyak_GMU-v2	7.8		2,803	64.0	1,050
Pyjamask-v1	6.8		4,094	66.0	1,245
Gimli-v1	3.2	20	1,767	78.0	3,159
TinyJAMBU-v3	2.4		881	97.7	5,148
Gimli-v2	1.6		1,767	73.5	5,915
Gimli-v3	0.9		1,772	78.5	11,427

Table 51: Lattice ECP5 Encryption AD+PT Throughput for 1536 Byte Messages

Variant	Through-put [Mbits/s]	Candi-date Ranking by Throughput	LUTs	Freq. [MHz]	Cycles AD+PT 1536B
Subterranean-v1	1,776.1	1	1,725	58.9	815
Xoodyak_XT-v2	1,026.3	2	4,302	70.7	1,693
Xoodyak_XT-v8	947.9		4,553	65.3	1,693
Ascon_Graz-v2	873.3	3	7,246	83.9	2,361
Xoodyak_XT-v1	844.7		2,986	79.0	2,299
COMET_VT-v1	784.1	4	6,613	111.6	3,498
Xoodyak_GMU-v1	748.1		3,474	63.8	2,097
Xoodyak_XT-v7	714.7		3,272	66.9	2,299
Ascon_Graz-v1	651.2		6,507	82.7	3,121
Xoodyak_XT-v3	631.3		5,569	38.3	1,491
KNOT-v2	599.1	5	2,241	91.2	3,739
Xoodyak_XT-v9	593.4		5,614	36.0	1,491
DryGASCON-v1	544.1	6	3,854	90.4	4,083
Ascon_VT-v1	536.0		3,130	84.9	3,893
Ascon_VT-v2	492.6		3,256	74.2	3,702
Xoodyak_XT-v4	472.1		6,839	26.7	1,390
Xoodyak_XT-v10	468.5		6,899	26.5	1,390
PHOTON-Beetle-v1	422.2	7	3,294	101.4	5,905
Spook-v2-v1	406.6	8	3,655	77.8	4,702
Elephant-v2	403.2	9	3,073	85.5	5,211
Romulus-v3	391.9	10	3,847	45.0	2,822
SCHWAEMM-v2	326.2	11	7,570	55.5	4,181
Romulus-v2	326.2		3,080	64.4	4,852
SCHWAEMM-v1	321.5		6,008	54.7	4,181
Xoodyak_XT-v11	316.3		9,447	16.6	1,289
Xoodyak_XT-v5	316.1		9,386	16.6	1,289
GIFT-COFB-v1	302.8	12	2,214	114.3	9,276
Romulus-v4	293.8		5,086	21.6	1,807
ISAP-v1	231.4	13	16,179	57.4	6,091
Romulus-v1	217.2		2,633	78.8	8,912
KNOT-v1	211.9		1,597	93.8	10,883
KNOT-v4	205.8		2,408	85.6	10,223
KNOT-v3	196.0		2,037	83.2	10,425
ESTATE-v1	193.7	14	3,085	100.4	12,736
COMET_CI-v1	157.8		3,427	80.9	12,597
Oribatida-v1	147.1	15	2,832	119.7	19,995
COMET_VT-v2	134.3		3,154	92.2	16,885
TinyJAMBU-v1	132.0	16	928	99.7	18,564
Elephant-v1	119.1		2,368	97.5	20,123
TinyJAMBU-v2	68.4		913	99.0	35,572
Pyjamask-v2	63.2	17	4,452	50.6	19,680
Xoodyak_GMU-v2	59.3		2,803	64.0	26,548
LOCUS-v1	59.3	18	3,161	79.6	33,012
ESTATE-v3	43.3		2,029	104.0	58,976
COMET_CI-v2	42.6		1,974	94.3	54,375
LOTUS-v1	41.4		2,820	55.6	33,012
Pyjamask-v1	31.8		4,094	66.0	50,908
Gimli-v1	12.5	19	1,767	78.0	153,573
Gimli-v2	6.3		1,767	73.5	288,121
TinyJAMBU-v3	4.4		881	97.7	545,812
Gimli-v3	3.5		1,772	78.5	557,217

Table 52: Lattice ECP5 Encryption AD+PT Throughput for 64 Byte Messages

Variant	**Throughput [Mbits/s]**	**Candidate Ranking by Throughput**	**LUTs**	**Freq. [MHz]**	**Cycles AD+PT 64B**
Subterranean-v1	763.5	1	1,725	58.9	79
Xoodyak_XT-v2	652.2	2	4,302	70.7	111
COMET_VT-v1	614.4	3	6,613	111.6	186
Xoodyak_XT-v8	602.4		4,553	65.3	111
Ascon_Graz-v2	561.5	4	7,246	83.9	153
Xoodyak_XT-v1	528.9		2,986	79.0	153
Ascon_Graz-v1	478.4		6,507	82.7	177
Xoodyak_GMU-v1	470.2		3,474	63.8	139
Xoodyak_XT-v7	447.5		3,272	66.9	153
DryGASCON-v1	422.7	5	3,854	90.4	219
Ascon_VT-v1	408.2		3,130	84.9	213
Xoodyak_XT-v3	404.3		5,569	38.3	97
Xoodyak_XT-v9	380.0		5,614	36.0	97
Ascon_VT-v2	368.8		3,256	74.2	206
PHOTON-Beetle-v1	354.5	6	3,294	101.4	293
KNOT-v2	349.6	7	2,241	91.2	267
Xoodyak_XT-v4	303.8		6,839	26.7	90
Xoodyak_XT-v10	301.5		6,899	26.5	90
Romulus-v3	299.2	8	3,847	45.0	154
Elephant-v2	295.8	9	3,073	85.5	296
Spook-v2-v1	278.6	10	3,655	77.8	286
GIFT-COFB-v1	263.6	11	2,214	114.3	444
Romulus-v2	261.7		3,080	64.4	252
Romulus-v4	210.7		5,086	21.6	105
SCHWAEMM-v2	209.7	12	7,570	55.5	271
SCHWAEMM-v1	206.7		6,008	54.7	271
Xoodyak_XT-v11	204.7		9,447	16.6	83
Xoodyak_XT-v5	204.6		9,386	16.6	83
Romulus-v1	180.1		2,633	78.8	448
ESTATE-v1	173.7	13	3,085	100.4	592
KNOT-v1	166.0		1,597	93.8	579
KNOT-v3	145.5		2,037	83.2	585
KNOT-v4	133.8		2,408	85.6	655
COMET_CI-v1	130.0		3,427	80.9	637
Oribatida-v1	117.5	14	2,832	119.7	1,043
TinyJAMBU-v1	113.5	15	928	99.7	900
COMET_VT-v2	107.7		3,154	92.2	877
ISAP-v1	97.4	16	16,179	57.4	603
Elephant-v1	88.5		2,368	97.5	1,128
TinyJAMBU-v2	59.1		913	99.0	1,716
LOCUS-v1	52.7	17	3,161	79.6	1,548
Pyjamask-v2	40.5	18	4,452	50.6	1,280
ESTATE-v3	39.8		2,029	104.0	2,672
LOTUS-v1	36.8		2,820	55.6	1,548
Xoodyak_GMU-v2	35.6		2,803	64.0	1,842
COMET_CI-v2	35.0		1,974	94.3	2,763
Pyjamask-v1	22.0		4,094	66.0	3,068
Gimli-v1	9.2	19	1,767	78.0	8,673
Gimli-v2	4.6		1,767	73.5	16,261
TinyJAMBU-v3	3.8		881	97.7	26,196
Gimli-v3	2.6		1,772	78.5	31,437

Table 53: Lattice ECP5 Encryption AD+PT Throughput for 16 Byte Messages

Variant	Throughput [Mbits/s]	Candidate Ranking by Throughput	LUTs	Freq. [MHz]	Cycles AD+PT 16B
COMET_VT-v1	366.3	1	6,613	111.6	78
Xoodyak_XT-v2	301.7	2	4,302	70.7	60
Xoodyak_XT-v8	278.6		4,553	65.3	60
Subterranean-v1	274.2	3	1,725	58.9	55
Ascon_Graz-v2	265.2	4	7,246	83.9	81
Ascon_Graz-v1	261.4		6,507	82.7	81
DryGASCON-v1	248.8	5	3,854	90.4	93
Xoodyak_XT-v1	240.8		2,986	79.0	84
PHOTON-Beetle-v1	236.1	6	3,294	101.4	110
Ascon_VT-v1	233.7		3,130	84.9	93
Xoodyak_GMU-v1	215.0		3,474	63.8	76
Ascon_VT-v2	206.5		3,256	74.2	92
Romulus-v3	205.7	7	3,847	45.0	56
Xoodyak_XT-v7	203.8		3,272	66.9	84
Romulus-v2	196.3		3,080	64.4	84
Xoodyak_XT-v3	188.6		5,569	38.3	52
GIFT-COFB-v1	187.6	8	2,214	114.3	156
Elephant-v2	183.9	9	3,073	85.5	119
Xoodyak_XT-v9	177.2		5,614	36.0	52
KNOT-v2	150.5	10	2,241	91.2	155
Romulus-v1	144.1		2,633	78.8	140
Xoodyak_XT-v4	142.4		6,839	26.7	48
Xoodyak_XT-v10	141.3		6,899	26.5	48
Romulus-v4	131.7		5,086	21.6	42
ESTATE-v1	131.1	11	3,085	100.4	196
Spook-v2-v1	104.8	12	3,655	77.8	190
KNOT-v1	98.9		1,597	93.8	243
Xoodyak_XT-v11	96.5		9,447	16.6	44
Xoodyak_XT-v5	96.5		9,386	16.6	44
COMET_CI-v1	83.8		3,427	80.9	247
KNOT-v3	80.3		2,037	83.2	265
TinyJAMBU-v1	78.8	13	928	99.7	324
SCHWAEMM-v2	78.1	14	7,570	55.5	182
SCHWAEMM-v1	76.9		6,008	54.7	182
Oribatida-v1	72.1	15	2,832	119.7	425
COMET_VT-v2	66.5		3,154	92.2	355
KNOT-v4	63.9		2,408	85.6	343
Elephant-v1	56.9		2,368	97.5	439
TinyJAMBU-v2	41.4		913	99.0	612
LOCUS-v1	39.0	16	3,161	79.6	522
ISAP-v1	35.7	17	16,179	57.4	411
ESTATE-v3	31.8		2,029	104.0	836
LOTUS-v1	27.3		2,820	55.6	522
COMET_CI-v2	22.4		1,974	94.3	1,080
Pyjamask-v2	19.0	18	4,452	50.6	680
Xoodyak_GMU-v2	15.6		2,803	64.0	1,053
Pyjamask-v1	11.2		4,094	66.0	1,508
Gimli-v1	5.1	19	1,767	78.0	3,948
TinyJAMBU-v3	2.7		881	97.7	9,252
Gimli-v2	2.5		1,767	73.5	7,396
Gimli-v3	1.4		1,772	78.5	14,292

Table 54: Cyclone-10-LP Encryption PT Throughput Rankings

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

Table 55: Cyclone-10-LP Encryption AD Throughput Rankings

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

Table 56: Cyclone-10-LP Encryption AD+PT Throughput Rankings

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

Table 57: ECP5 PT Throughput Rankings

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

Table 58: ECP5 AD Throughput Rankings

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

Table 59: ECP5 AD+PT Throughput Rankings

Rank	Long	1536 B	64 B	16 B
1	Subterranean-v1	Subterranean-v1	Subterranean-v1	COMET_VT-v1
2	Xoodyak_XT-v1	Xoodyak_XT-v2	Xoodyak_XT-v2	Xoodyak_XT-v2
3	Ascon_Graz-v2	Ascon_Graz-v2	COMET_VT-v1	Subterranean-v1
4	COMET_VT-v1	COMET_VT-v1	Ascon_Graz-v2	Ascon_Graz-v2
5	DryGASCON-v1	KNOT-v2	DryGASCON-v1	DryGASCON-v1
6	KNOT-v1	DryGASCON-v1	PHOTON-Beetle-v1	PHOTON-Beetle-v1
7	PHOTON-Beetle-v1	PHOTON-Beetle-v1	KNOT-v2	Romulus-v3
8	Spook-v2-v1	Spook-v2-v1	Romulus-v3	GIFT-COFB-v1
9	Elephant-v2	Elephant-v2	Elephant-v2	Elephant-v2
10	Romulus-v3	Romulus-v3	Spook-v2-v1	KNOT-v2
11	SCHWAEMM-v2	SCHWAEMM-v2	GIFT-COFB-v1	ESTATE-v1
12	GIFT-COFB-v1	GIFT-COFB-v1	SCHWAEMM-v2	Spook-v2-v1
13	ISAP-v1	ISAP-v1	ESTATE-v1	TinyJAMBU-v1
14	ESTATE-v1	ESTATE-v1	Oribatida-v1	SCHWAEMM-v2
15	Oribatida-v1	Oribatida-v1	TinyJAMBU-v1	Oribatida-v1
16	TinyJAMBU-v1	TinyJAMBU-v1	ISAP-v1	LOCUS-v1
17	Pyjamask-v2	Pyjamask-v2	LOCUS-v1	ISAP-v1
18	LOCUS-v1	LOCUS-v1	Pyjamask-v2	Pyjamask-v2
19	SpoC-v1	Gimli-v1	Gimli-v1	Gimli-v1
20	WAGE-v1			
21	Gimli-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 4.4: DryGASCON added to the list of algorithms that rank higher for short messages than for long messages
  Reason: Omission in the original version

1.0.2 (September 30, 2020)

Changed

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

Removed

- Section 3: "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 7 to 9, 16, 18, 19, 25, 36 to 44 and 54 to 56: 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 4.1: WAGE removed from the list of algorithms that did not pass all tests.
  Reason: Miscommunication regarding the version of reference software implementation to be used for generating test vectors