DATE 21
DESIGN, AUTOMATION & TEST IN EUROPE
01 – 05 February 2021 · virtual conference
The European Event for Electronic System Design & Test

Hardware Benchmarking of Round 2 Candidates in the NIST Lightweight Cryptography Standardization Process

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

CERG
Cryptographic Engineering Research Group
cryptography.gmu.edu

GEORGE MASON UNIVERSITY

GMU CERG LWC Benchmarking Team

Kamyar Mohajerani

Richard Haeussler

Rishub Nagpal

Farnoud Farahmand

Bakry Abdulgadir

Jens-Peter Kaps

NIST Standardization Process

- Performance of current NIST cryptographic standards not acceptable in constrained environments (e.g., sensor networks, healthcare, the Internet of Things, cyber physical systems)

Timeline of the NIST Lightweight Cryptography Standardization:

- Aug. 2018: Submission Requirements and Evaluation Criteria
- Feb. 2019: 57 candidates submitted
- Aug. 2019: 32 candidates qualified for Round 2
- Feb. 2021: Decision on Round 3 candidates expected

Hardware Benchmarking Goals

- Stimulate the development of hardware implementations that can be fairly compared with each other (e.g., common API & development package)
- Perform design space exploration of at least selected candidates
- Evaluate and rank candidates from the point of view of their performance in hardware

Benchmarking Platforms

- Widely used low-cost, low-power FPGA families
- Capable of holding side-channel-protected designs (possibly using up to 4 times more resources than unprotected designs)
- Supported by free versions of state-of-the-art industry tools

- Xilinx: Artix-7 : xc7a12tcsg325-3 (smallest)
- Intel: Cyclone 10 LP : 10CL016-YF484C6
- Lattice Semiconductor: ECP5 : LFE5U-25F-6BG381C

Optimization Target

- Maximum Throughput assuming
  - Up to 2500 LUTs, 5000 flip-flops of Artix-7 FPGA
  - No BRAMs & no DSP units
  - Resources comparable to those used by the lightweight implementation of the current standard AES-GCM

Benchmarking Metrics

1. Resource Utilization
   - Number of LUTs (LEs for Cyclone 10LP)
2. Throughput in Mbits/s
   - for the following sizes of inputs
     a. long [with Throughput = d · Block size/(Time(N+d blocks)-Time(N blocks))]
     b. 1536 bytes
     c. 64 bytes
     d. 16 bytes.
   - all throughputs calculated separately for
     - authenticated encryption: Plaintext, Associated Data (AD)
     - hashing

Summary of Hardware Design Submissions

32 submissions representing 25 out of 32 candidates (78%)

Candidate with 3 independent submissions:

Xoodyak

Candidates with 2 independent submissions:

Ascon, COMET, Gimli, Subterranean 2.0, TinyJAMBU

8 submissions from George Mason University

24 by groups from all over the world

Design Variants

Different variants correspond to

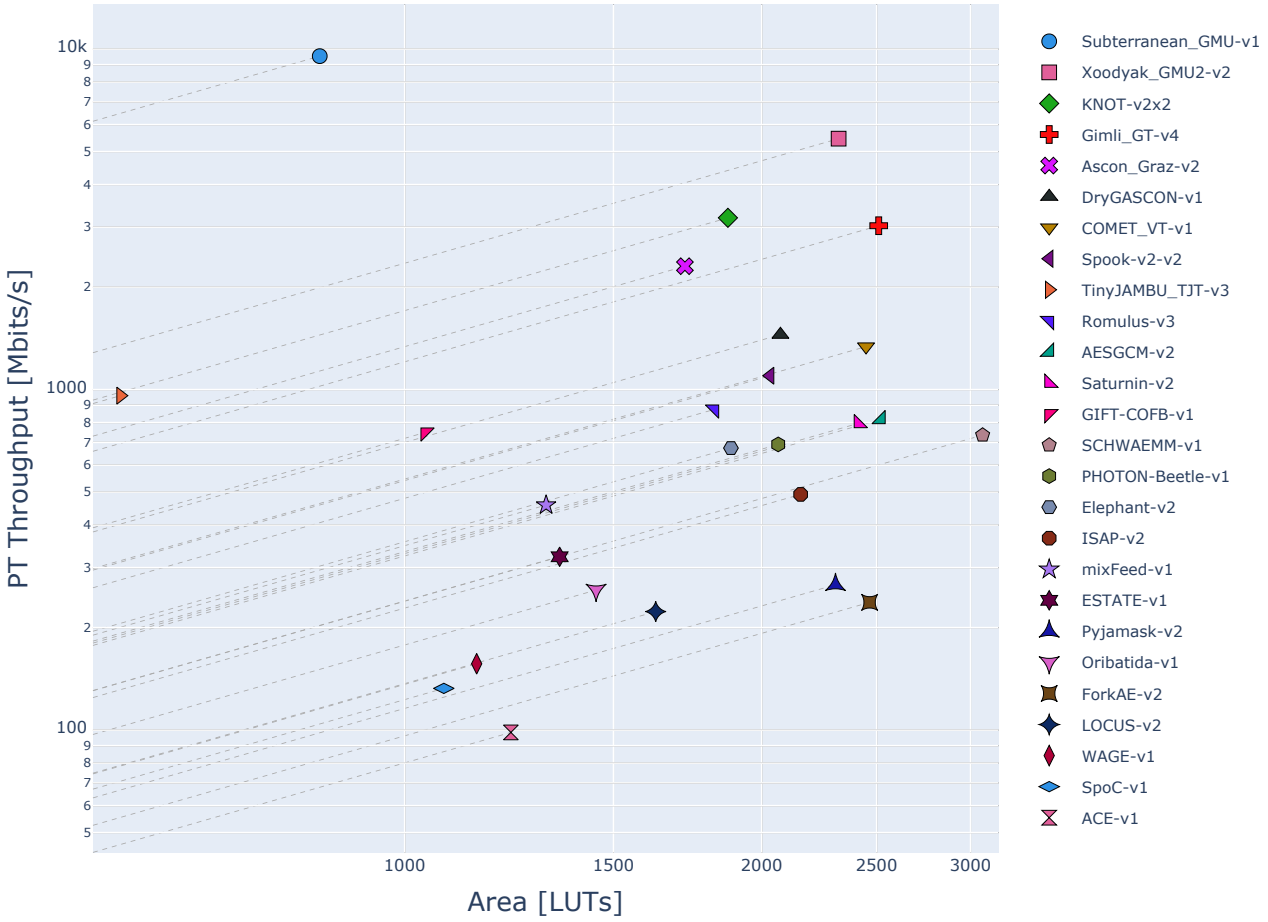
- different algorithms of the same family
- different parameter sets, such as sizes of keys, nonces, tags, etc.
- support for authenticated encryption vs. authenticated encryption+hashing
- different hardware architectures, e.g., basic iterative, folded, unrolled

92 variants

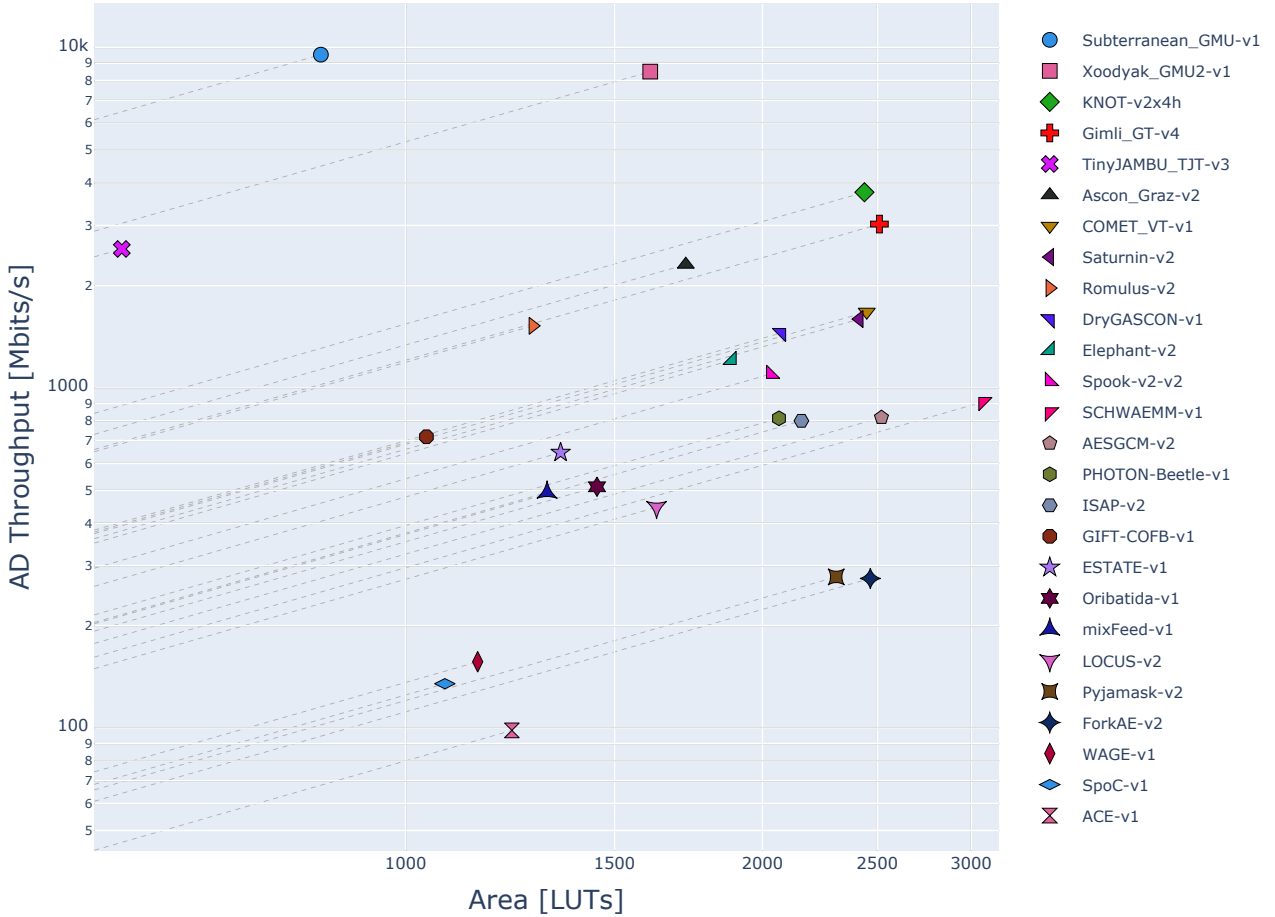
Minimum: 1, Maximum: 16, Average: 3.1

per hardware design submission

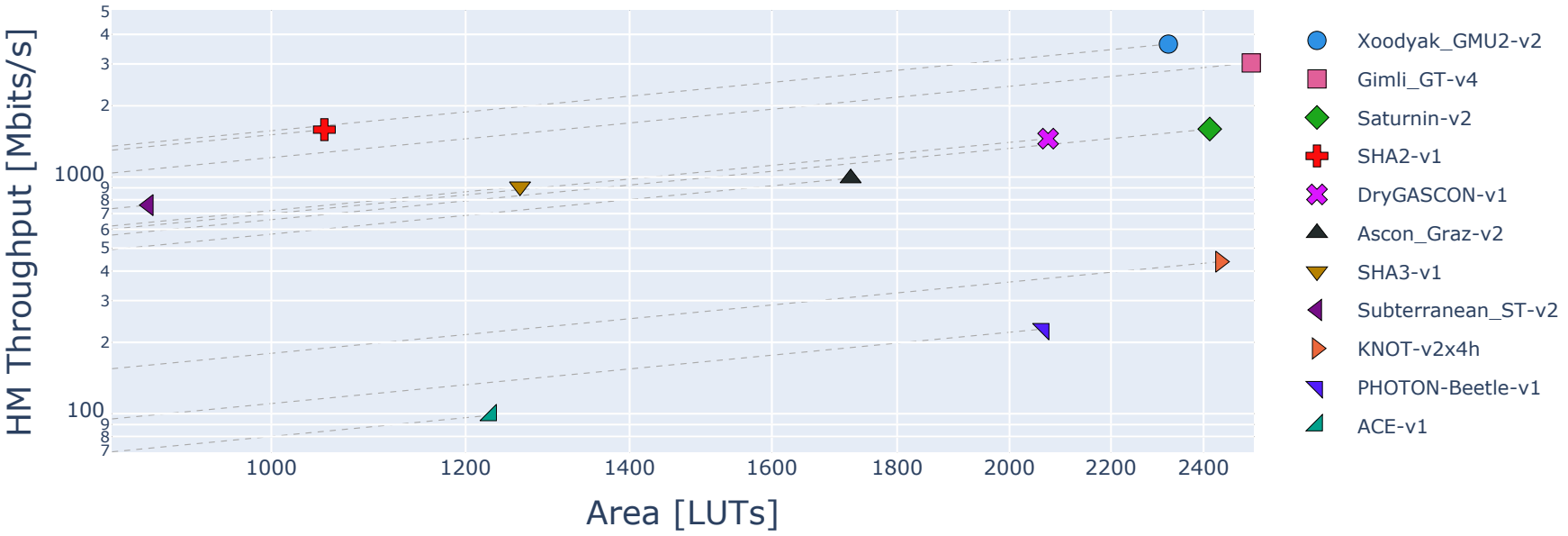
Throughput vs. Area for Long Plaintext: Artix-7



Throughput vs. Area for Long AD: Artix-7



Throughput vs. Area for Hashing: Artix-7



Dependence of Ranking on Input Size

Position	Long	1536 B	64 B	16 B
1	Subterranean	Subterranean	Subterranean	Subterranean
2	Xoodyak	Xoodyak	Xoodyak	Xoodyak
3	KNOT	KNOT	KNOT	Ascon
4	Gimli	Gimli	Ascon	COMET
5	Ascon	Ascon	DryGASCON	DryGASCON
6	DryGASCON	DryGASCON	Gimli	KNOT
7	COMET	COMET	COMET	TinyJAMBU
8	Spook v2	Spook v2	TinyJAMBU	Romulus
9	TinyJAMBU	TinyJAMBU	Romulus	Gimli
10	Romulus	Romulus	Spook v2	PHOTON-Beetle

Higher position
Lower position
for smaller messages

Conclusions

- For authenticated encryption of plaintexts 10 candidates outperform AES-GCM: Subterranean 2.0, Xoodyak, KNOT, Gimli, Ascon, DryGASCON, COMET, Spook v2, TinyJAMBU, and Romulus.
- For processing of associated data (ADs) all of them, as well as Saturnin and Elephant, outperform AES-GCM
- Out of them:
  - Xoodyak, Gimli, and Saturnin support hashing faster than SHA-2
  - DryGASCON and Ascon, perform hashing faster than the folded implementation of SHA-3
- All of the mentioned above 12 candidates have good chances of qualifying for Round 3

Concurrent & Future Work

- Evaluation in terms of Power consumption and Energy per bit
- ASIC Benchmarking
- Side-channel protected implementations of Round 3 candidates

Most recent results:

Cryptology ePrint Archive: Report 2020/1207

https://cryptography.gmu.edu/athena