Evaluation of the Finalists & Selection of Ascon

NIST Lightweight Cryptography Team
Presenter: Meltem Sönmez Turan

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

The Sixth Lightweight Cryptography Workshop – June 21, 2023

Overview of the Talk

I. NIST lightweight cryptography standardization process

II. Finalists

III. Evaluation of finalists

IV. Selection and next steps

Part I – NIST Lightweight Cryptography Standardization Process

Initial Phase
(July 2015 – August 2018)

Submission Call
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – February 2023)

Initial Phase
(July 2015 – August 2018)

Submission Call
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – February 2023)

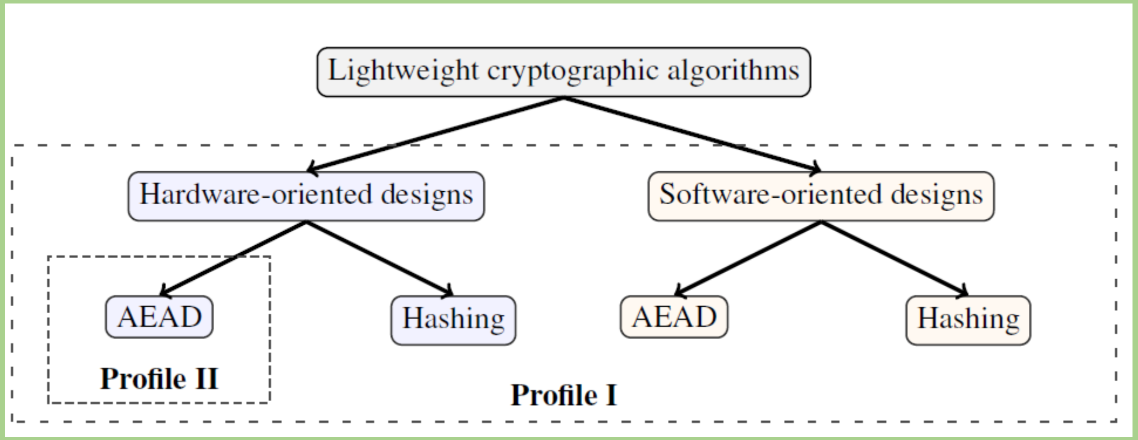
Workshops:

- First Lightweight Cryptography Workshop
  July 20 – 21, 2015
- Second Lightweight Cryptography Workshop
  October 17 – 18, 2016

to get feedback on target applications, industry need, requirements, etc.

Publications:

- NISTIR 8114 *Report on Lightweight Cryptography*
- (White paper, retired) *Profiles for the Lightweight Cryptography Standardization Process*



Initial Phase
(July 2015 – August 2018)

Submission Call
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – February 2023)

Process: Public competition-like process with multiple rounds like AES, SHA-3 and PQC standardization.

Scope: Authenticated Encryption and (optional) hashing for constrained software and hardware environments

---

In August 2018, NIST published '*Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process*'.

Submission deadline: February 2019

Initial Phase
(July 2015 – August 2018)

Submission Call
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – February 2023)

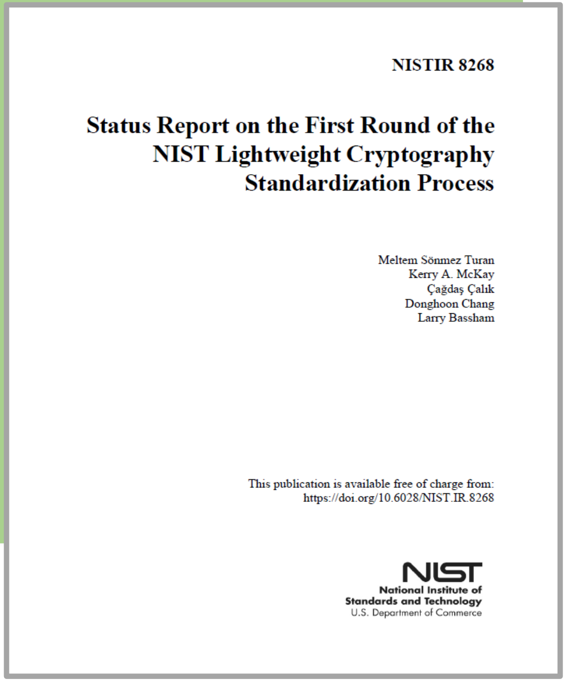
Around 4 months

56 First-round candidates

Evaluation of the candidates were done based on their security

- e.g., distinguishing attacks, practical tag forgeries, domain separation issues, new designs with no third-party analysis etc.

NIST IR 8268 explains how 32 candidates (out of 56) were selected to move forward to the second round.



NISTIR 8268

Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalık
Donghoon Chang
Larry Bassham

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8268

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Initial Phase
(July 2015 – August 2018)

Submission Call
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – February 2023)

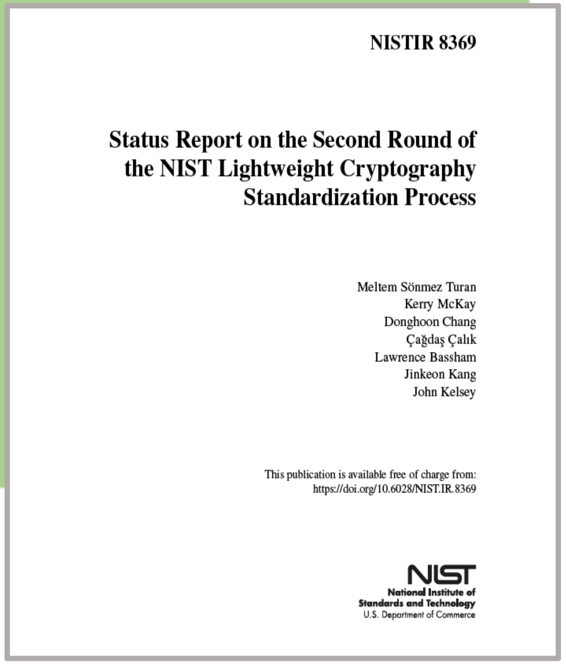
Around 20 months

32 Second-round candidates

Workshops:

- Third Lightweight Cryptography Workshop
  November 4 – 6, 2019
- Fourth Lightweight Cryptography Workshop 2016
  October 19 – 21, 2020

NIST IR 8369 explains how 10 finalists were selected to move forward to the final round.


NISTIR 8369

Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Çağdaş Çalık
Lawrence Bassham
Jinkeon Kang
John Kelsey

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8369

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Initial Phase
(July 2015 – August 2018)

Submission Call
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

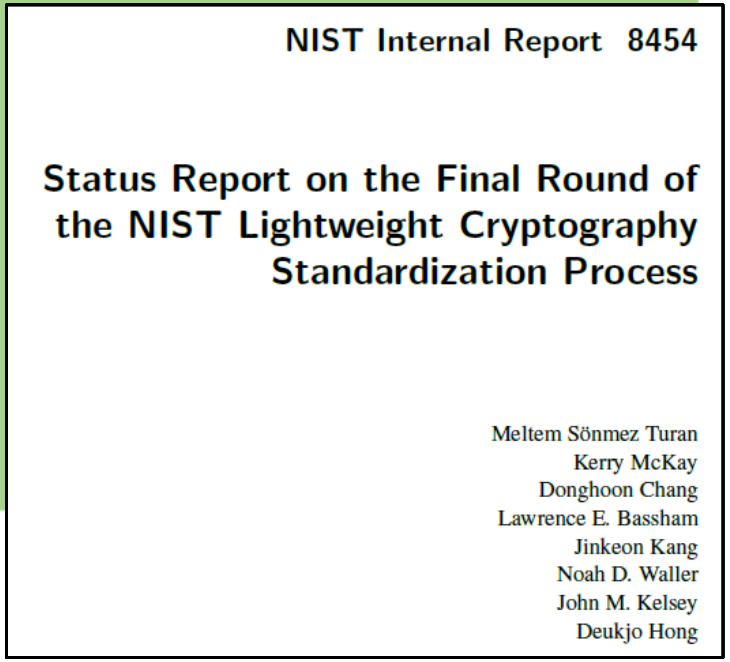
Final Round
(March 2021 – February 2023)

Around 24 months

10 finalists:

Ascon	Photon-Beetle
Elephant	Romulus
GIFT-COFB	Sparkle
Grain-128AEAD	TinyJambu
ISAP	Xoodyak

NIST IR 8454 explains the selection of Ascon.


NIST Internal Report 8454

Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Lawrence E. Bassham
Jinkeon Kang
Noah D. Waller
John M. Kelsey
Deukjo Hong

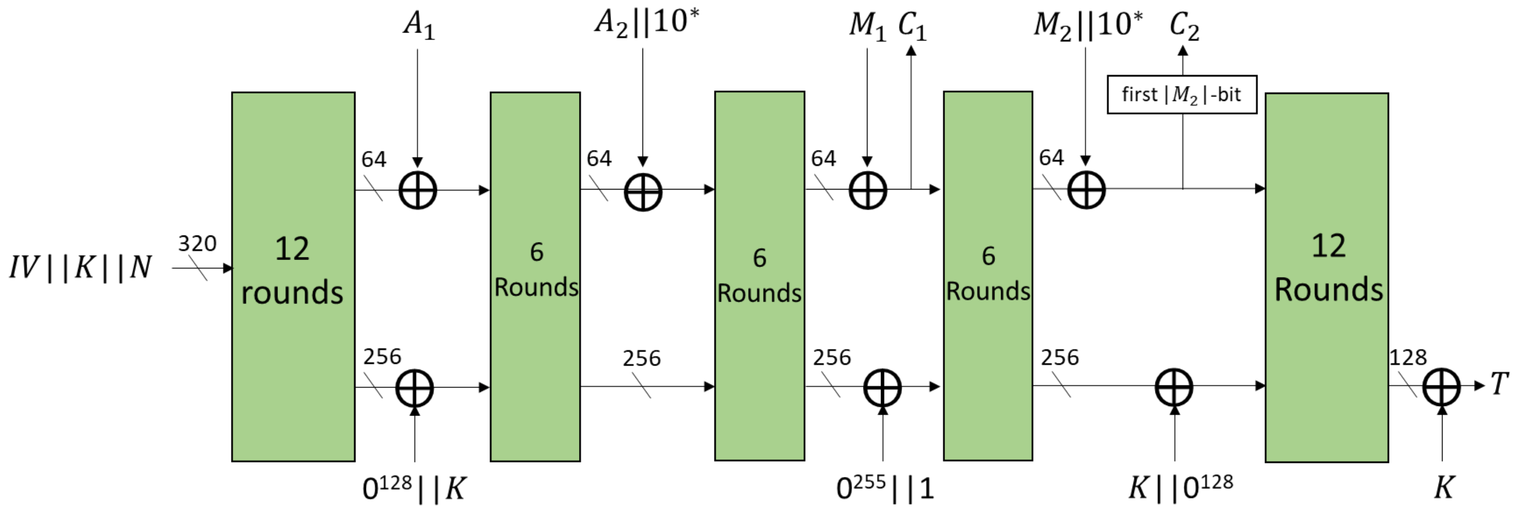
Part II – Finalists

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

ASCON

- Permutation-based (320-bit) AEAD and hashing scheme (fixed or variable output length)
- MonkeyDuplex mode with keyed initialization and finalization
- No design tweak, new variant added in the final round
- Included in the final portfolio of CAESAR for lightweight authenticated encryption

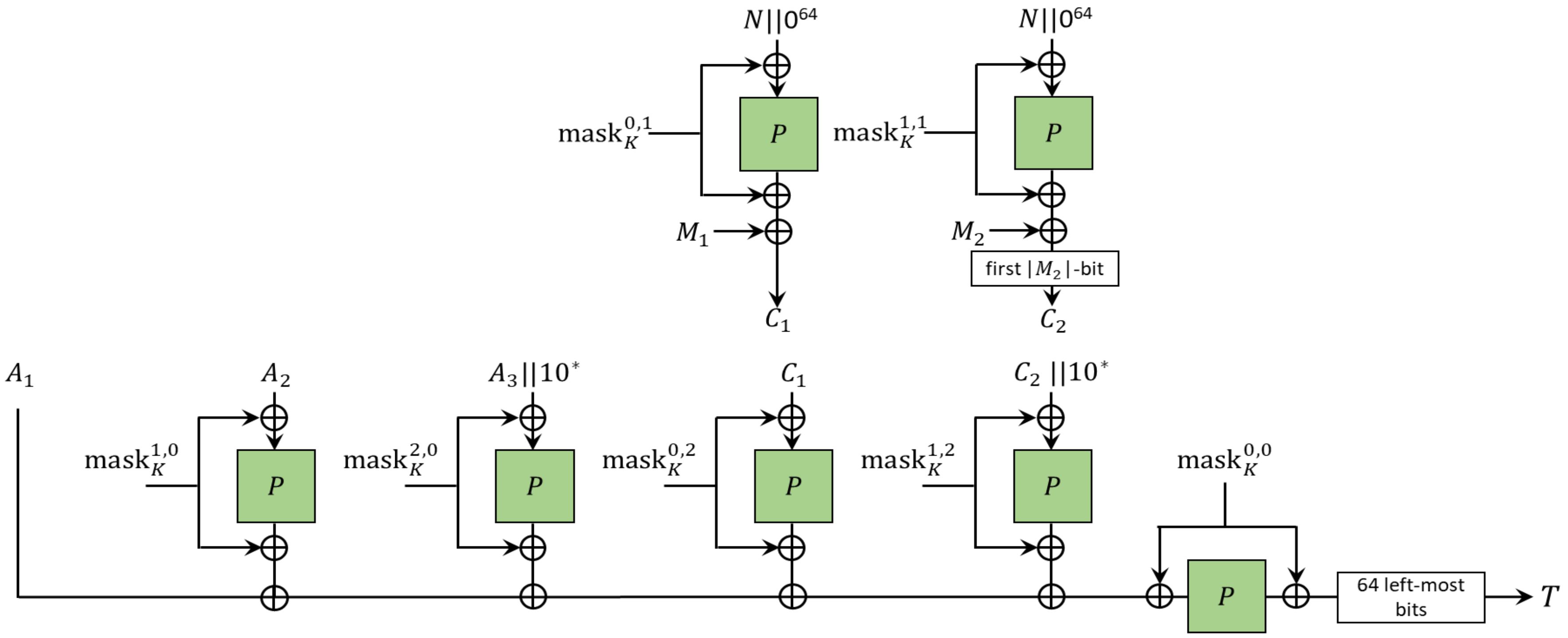
	Variant	Parameter sizes
AEAD	**Ascon-128**	128-bit key/nonce/tag
	Ascon-128a	128-bit key/nonce/tag
	Ascon-80-pq	160-bit key, 128-bit nonce/tag
Hash	**Ascon-hash**	256-bit digest
	Ascon-hasha	256-bit digest
XOF	Ascon-XOF	Arbitrary length digest
	Ascon-XOFa	Arbitrary length digest



ELEPHANT

- Permutation-based (Spongent and Keccak[200]) AEAD scheme
- Nonce-based Encrypt-then-MAC mode
- Only finalist with a parallel mode
- Design tweak: Mode slightly modified to achieve authenticity under nonce-reuse.

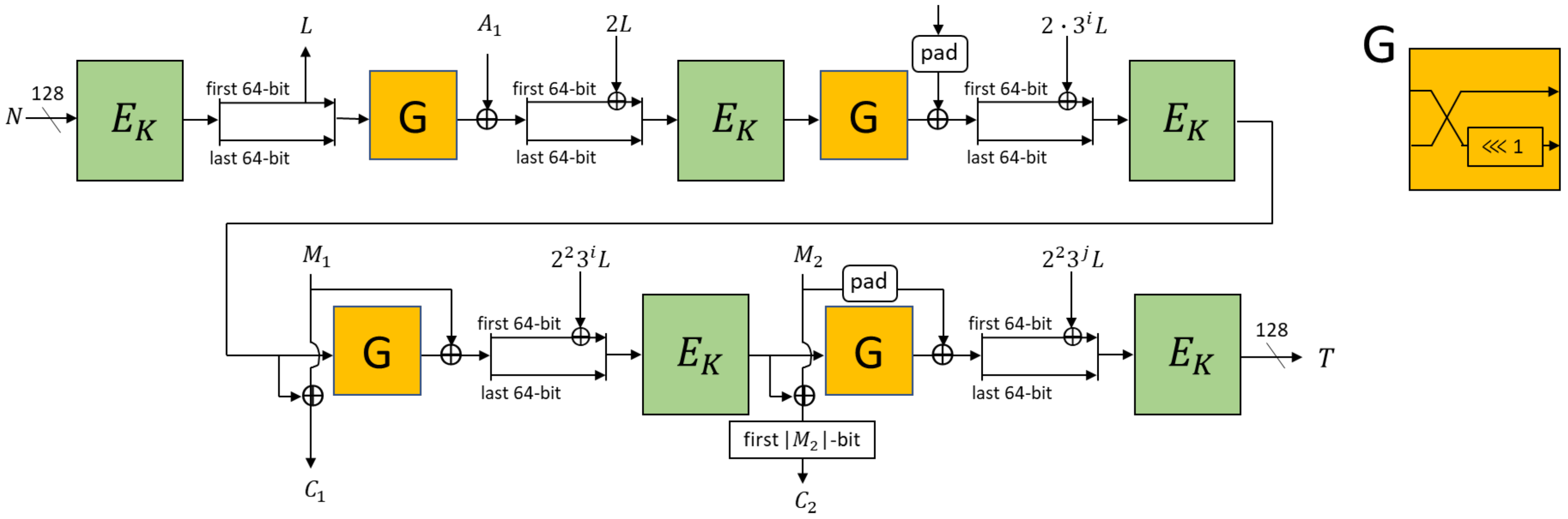
Variant	Parameter sizes
Dumbo	128-bit key, 96-bit nonce, 64-bit tag
Jumbo	128-bit key, 96-bit nonce, 64-bit tag
Delirium	128-bit key, 96-bit nonce, 128-bit tag



GIFT-COFB

- Block-cipher (GIFT-128) based AEAD scheme
- Combined Feedback (COFB) mode
- No design tweak

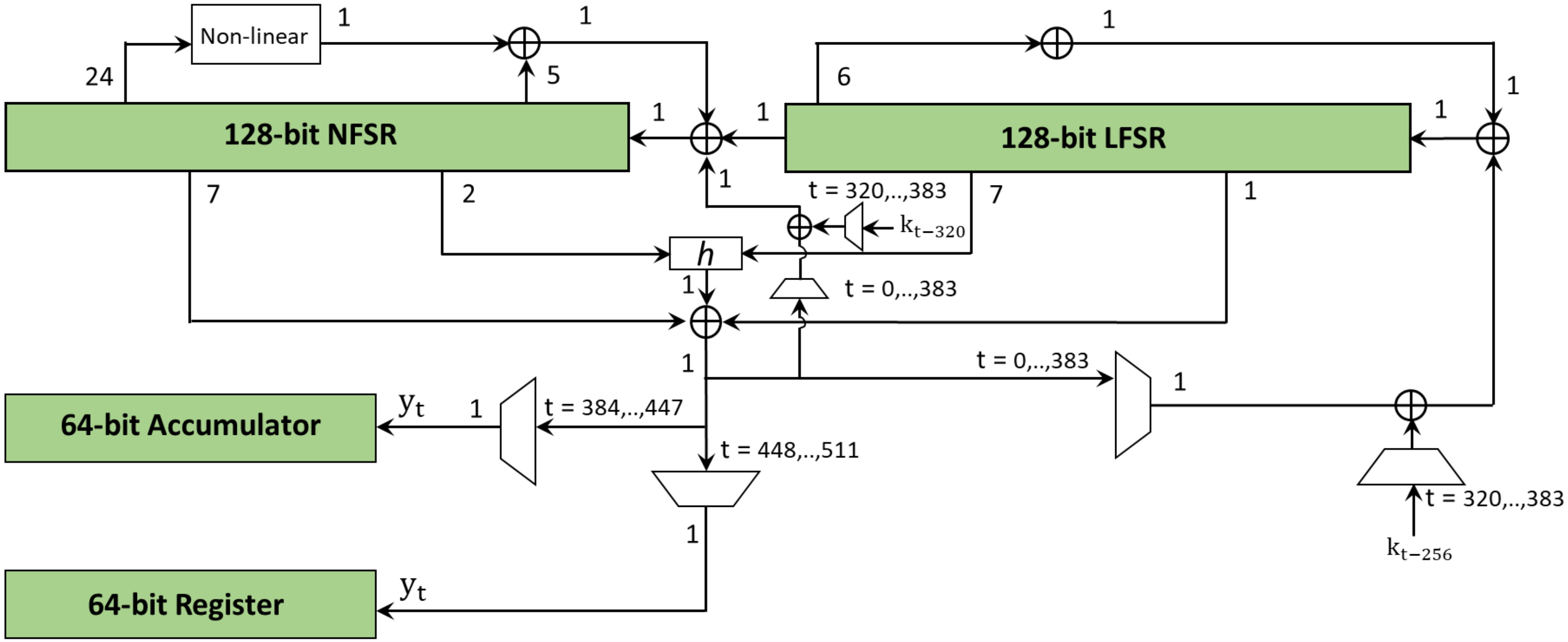
Variant	Parameter sizes
Gift-COFB	128-bit key/nonce/tag



Grain-128AEAD

- Feedback shift register based AEAD scheme
- Design tweak on the initialization part
- (Earlier versions) Part of eSTREAM portfolio, included in ISO/IEC 29167-13:2005

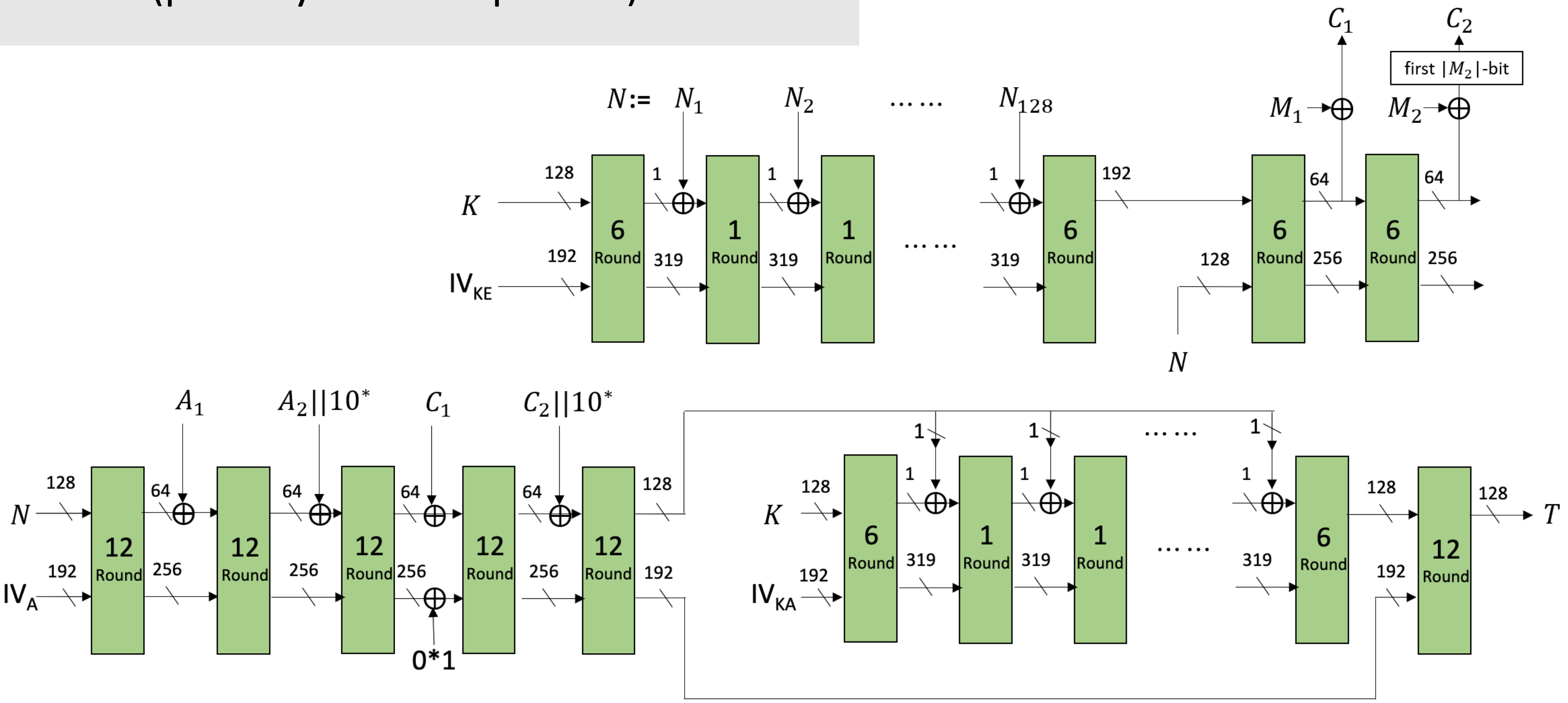
Variant	Parameter sizes
Grain-128AEAD	128-bit key, 96-bit nonce, 64-bit tag



ISAP

- Permutation-based (Ascon and Keccak permutations) AEAD scheme
- Can be paired with Ascon Hash
- Nonce-based Encrypt-then-MAC mode
- Algorithm-level security against implementation attacks
- No design tweak (primary variant updated)

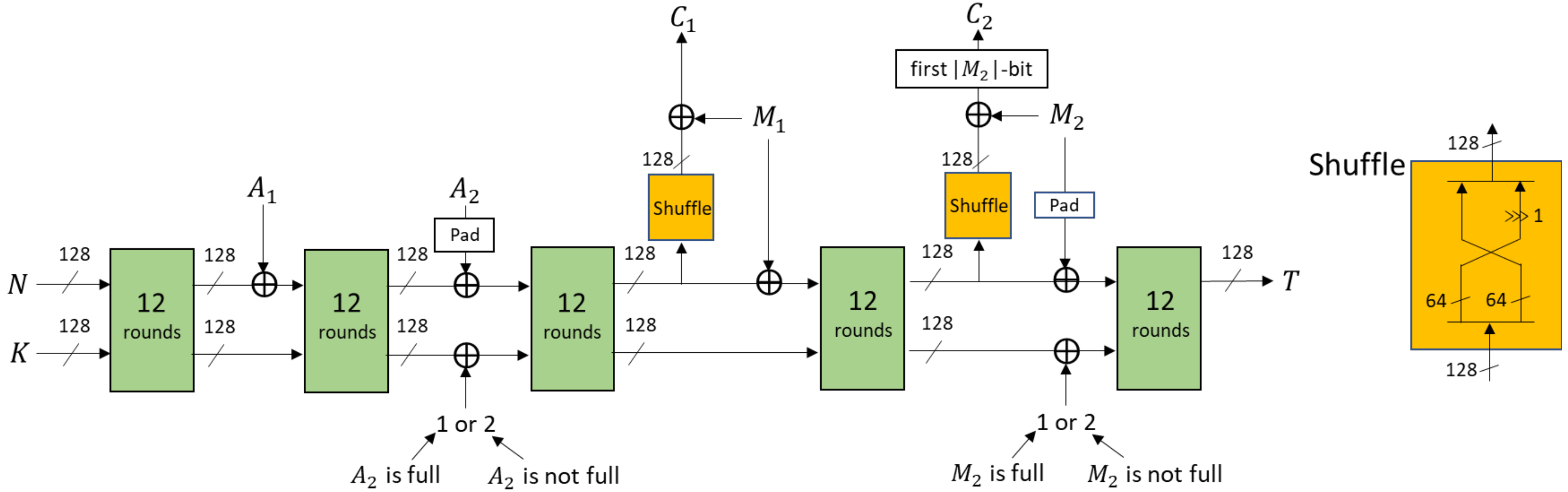
Variant	Parameter sizes
ISAP-A-128a	128-bit key/nonce/tag
ISAP-K-128a	128-bit key/nonce/tag
ISAP-A-128	128-bit key/nonce/tag
ISAP-K-128	128-bit key/nonce/tag



PHOTON-Beetle

- Family of permutation-based (256-bit Photon permutation) AEAD & hashing scheme
- Sponge-like mode with a combined feedback.
- No design tweak

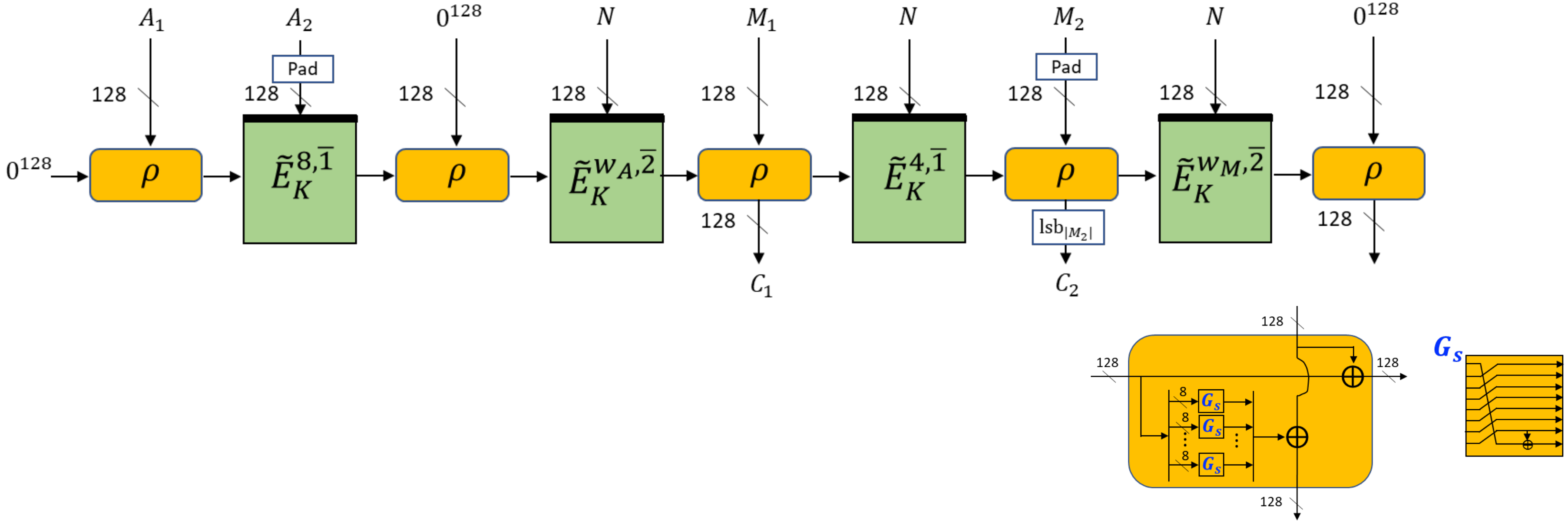
	Variant	Parameter sizes
AEAD	**Photon-Beetle-AEAD[128]**	128-bit key/nonce/tag
	Photon-Beetle-AEAD[32]	128-bit key/nonce/tag
Hash	**Photon-Beetle-Hash[32]**	256-bit digest



ROMULUS

- Family of tweakable-block-cipher (Skinny) based AEAD & hashing
- Romulus-N: rate-1 TBC-based combined feedback, Romulus-M: MAC-then-Encrypt
- Nonce-misuse and nonce-respecting variants
- Design tweak to reduce the number of rounds from 56 to 40, removal of non-primary variants, addition of new variants.

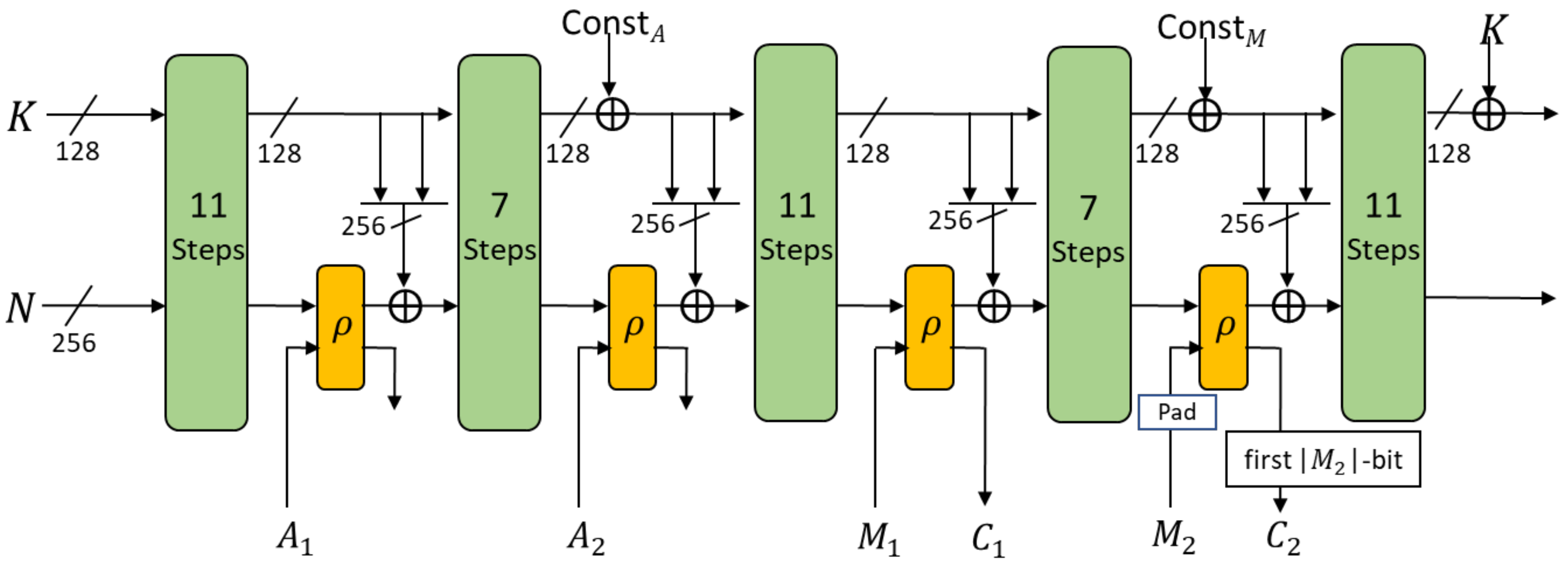
	Variant	Parameter sizes
AEAD	**Romulus-N**	128-bit key/nonce/tag
	Romulus-M	128-bit key/nonce/tag
	Romulus-T	128-bit key/nonce/tag
Hash	**Romulus-H**	256-bit digest

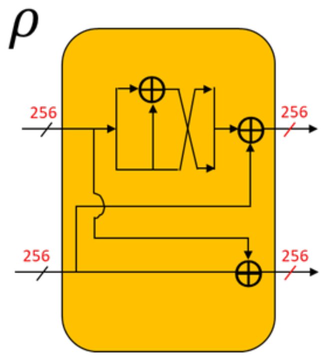


SPARKLE

- Family of permutation-based AEAD (SCHWAEMM) and hashing (ESCH)
- ARX based design
- Sponge construction with combined feedback
- Tweak to change the primary variant

	Variant	Parameter sizes
AEAD	**SCHWAEMM256-128**	128-bit key/tag, 256-bit nonce
	SCHWAEMM128-128	128-bit key/nonce/tag
	SCHWAEMM192-192	192-bit key/nonce/tag
	SCHWAEMM256-256	256-bit key/nonce/tag
Hash	**ESCH256**	256-bit digest
	ESCH384	384-bit digest
XOF	XOESCH256	Arbitrary length digest
	XOESCH384	Arbitrary length digest

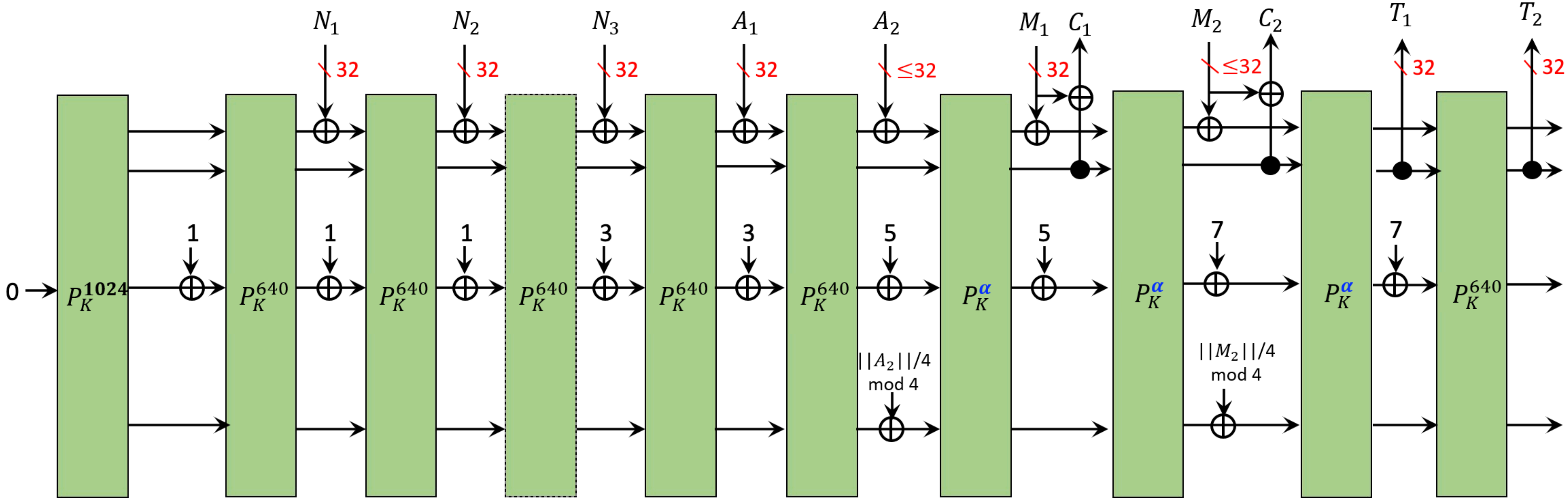




TINYJAMBU

- Keyed-permutation based AEAD scheme
- Uses 128-bit nonlinear feedback shift register
- Inspired by JAMBU (CAESAR candidate)
- Design tweak: increase in number of rounds to improve security margin.

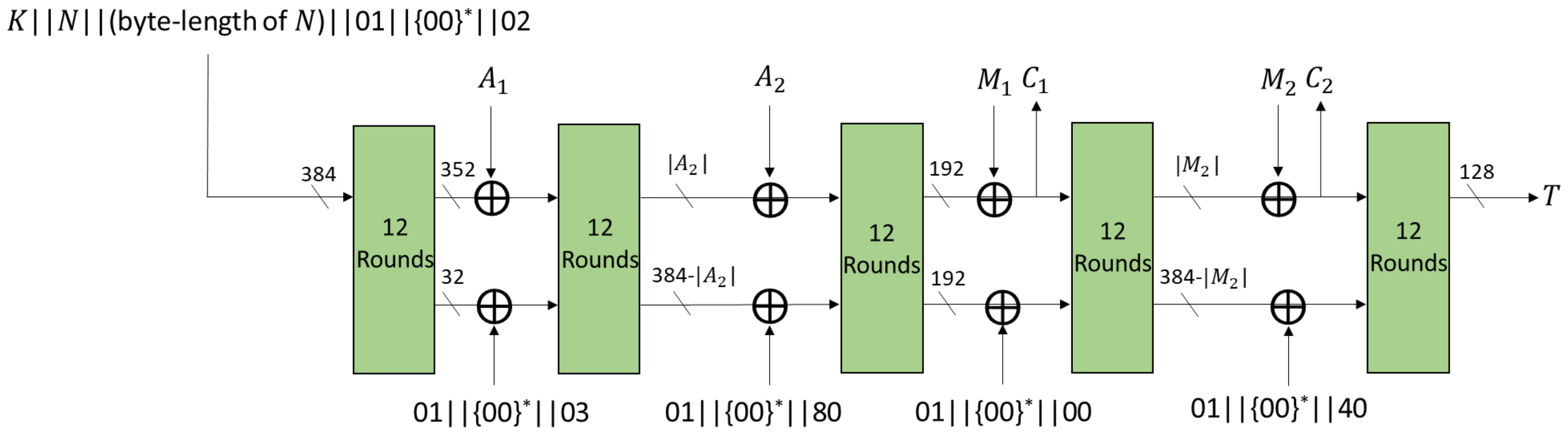
Variant	Parameter sizes
TinyJambu-128	128-bit key, 96-bit nonce, 64-bit tag
TinyJambu-192	192-bit key, 96-bit nonce, 64-bit tag
TinyJambu-256	256-bit key, 96-bit nonce, 64-bit tag



XOODYAK

- Family of permutation based AEAD & hashing scheme
- Based on 384-bit Xoodoo permutation
- Uses Cyclist mode
- Design tweak: simplified initialization to improve performance for short messages

	Variant	Parameter sizes
AEAD	Xoodyak	128-bit key/nonce/tag
Hash	Xoodyak	256-bit digest
XOF	Xoodyak	Arbitrary length digest



Underlying Components and Functionalities

AEAD-only

Permutation
- Elephant
- ISAP

Block Cipher
- GIFT-COFB
- TinyJAMBU

Stream cipher
- Grain-128AEAD

AEAD and Hashing

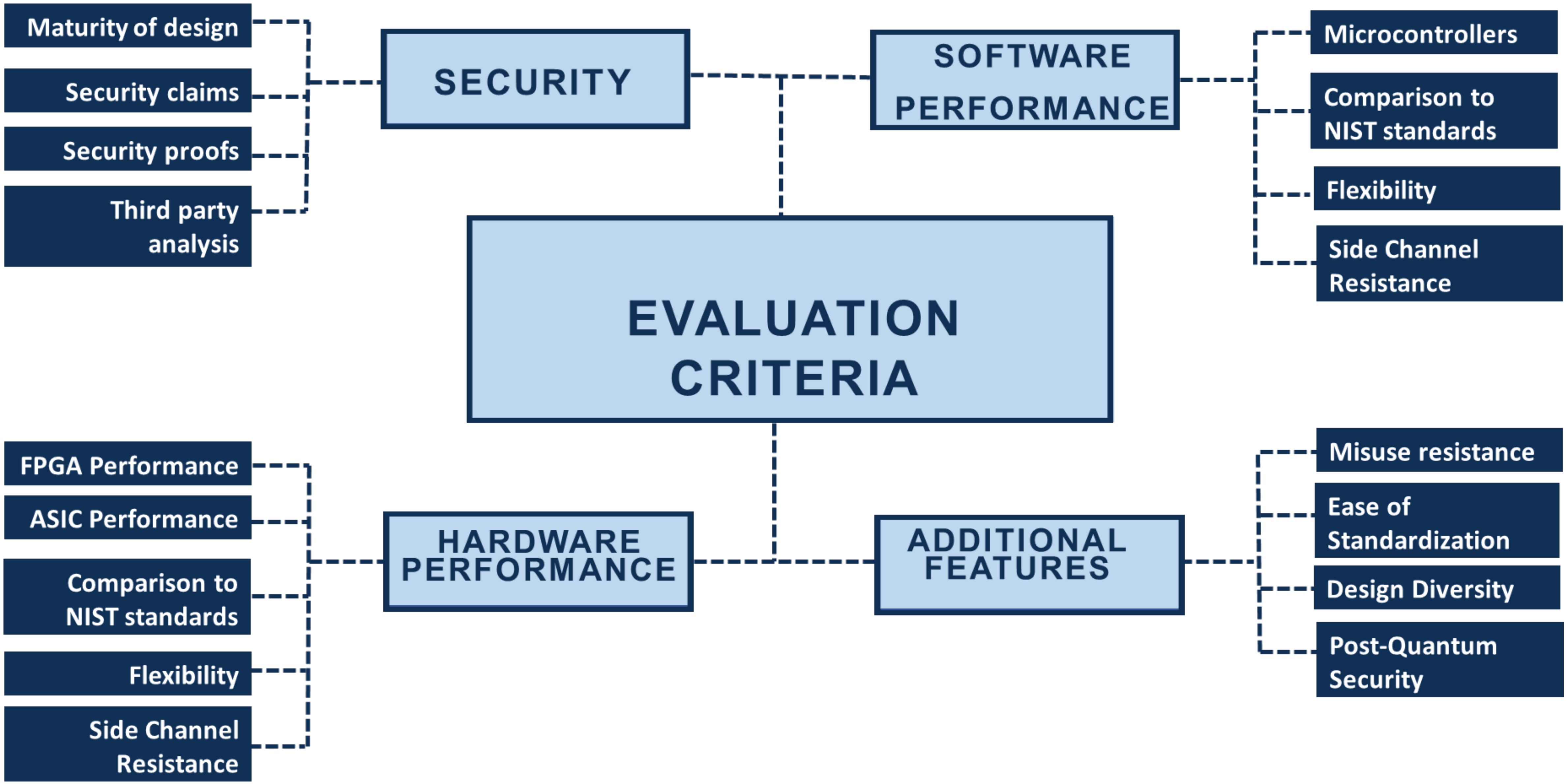
Permutation
- ASCON
- PHOTON-Beetle
- SPARKLE
- Xoodyak

Tweakable block cipher
- Romulus

Variants of the Finalists

Finalist	# Variants	Key size (bits)	Nonce size (bits)	Tag size (bits)	Digest size (bits)
Ascon	3 AEAD 2 hash	128 - 160 --	128 --	128 --	-- 256
Elephant	3 AEAD	128	96	64-128	--
GIFT-COFB	1 AEAD	128	128	128	--
Grain-128aead	1 AEAD	128	96	64	--
ISAP	4 AEAD	128	128	128	--
PHOTON-Beetle	2 AEAD 1 hash	128 --	128 --	128 --	-- 256
Romulus	3 AEAD 1 hash	128 --	128 --	128 --	-- 256
Sparkle	4 AEAD 2 hash	128-256 --	128-256 --	128-256 --	-- 256-384
TinyJambu	3 AEAD	128-256	96	64	
Xoodyak	1 AEAD 1 hash	128 --	128 --	128 --	-- 256

Part III – Evaluation and Selection


EVALUATION CRITERIA
SECURITY
Maturity of design
Security claims
Security proofs
Third party analysis
SOFTWARE PERFORMANCE
Microcontrollers
Comparison to NIST standards
Flexibility
Side Channel Resistance
HARDWARE PERFORMANCE
FPGA Performance
ASIC Performance
Comparison to NIST standards
Flexibility
Side Channel Resistance
ADDITIONAL FEATURES
Misuse resistance
Ease of Standardization
Design Diversity
Post-Quantum Security

Security Requirements

The submission call included the security requirements:

- Key size is at least 128-bit.
- The limits on the input sizes (e.g., message, AD) is at least 2^{50}-1 bytes.
- Any nonce-respecting attack on the AEAD with 128-bit key requires at least 2^{112} time complexity on a classical computer in the single-key setting.
  (For 256 bit key, time complexity of at least 2^{224}, if applicable.)
- Any attack on the hash function variants requires at least 2^{112} time complexity on a classical computer (if applicable).

Security Margins and Claims and Maturity

- All finalists have met the security requirements and provided sufficient security margins.
- None of the security claims made by the submitters have been invalidated.
- Maturity of the design is one of the important security evaluation factors.
  - Is the finalist based on well-established design principles?
  - Did the finalist receive enough third-party analysis?
  - Are there design tweaks that invalidate the earlier security analysis?
  - Are there any additional concerns (e.g., nonce misuse, related-key, RUP security, post quantum)?

Security Evaluations of the Finalists

Ascon: Received large number of third-party analysis. High security margin. Best key-recovery attack on 7 (out of 12) rounds of initialization. Distinguishers on full permutation.

Elephant: High security margin. Best distinguisher* on 160-bit Spongent permutation covers 40 (out of 80) rounds. Some results on Even-Mansour construction in the quantum setting.

GIFT-COFB: Large number of third-party analysis on GIFT. Best key-recovery attack on GIFT-128 covers 27 (out of 40) rounds. High security margin. Some level of nonce-misuse resilience.

Grain-128AEAD: Large number of third-party analysis on *earlier* versions. Tweaked in response to the state-recovery observation. Best key-recovery attack* covers 192 (out of 512) rounds of initialization. High security margin.

ISAP: Large number of third-party analysis on Ascon permutation. Best forgery attack covers 4 (out of 12) rounds. High security margin.

*Requires time complexity beyond the time limit made by the submitters.

Security Evaluations of the Finalists

Photon-Beetle: No analysis on round-reduced Photon-Beetle-AEAD. Distinguishing attack on the permutation covers 10 (out of 12) rounds.

Romulus: High security margin. Number of rounds reduced from 56 to 40. Best key-recovery attacks* on Skinny with 32 (out of 40) rounds in the related-key setting. Nonce misuse resistance. For hash variant, preimage attack* on 23 (out of 40) rounds.

Sparkle: High security margin. Best key-recovery attack* covers 4.5 (out of 11) steps of 384-bit permutation without whitening. No known results on the hash variants. Distinguishers* on permutation up to 6 steps.

TinyJambu: Tweak to increase the number of rounds. Weak-key distinguishing attack covers 476 (out of 1024) rounds. Forgery attacks on full-round TinyJambu-192 and TinyJambu-256 in the related-key setting.

Xoodyak: Best key recovery attack covers 6 (out of 12) rounds. High security margin.

*Requires time complexity beyond the time limit made by the submitters.

Software Benchmarking

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Software Benchmarking

Microcontroller benchmarking by NIST LWC Team

Devices:
- 8-bit AVR
- 32-bit ARM Cortex M0+, M4, M3
- MIPS32 M4K
- Tensilica L106

Metrics:
- Code size
- Execution time

Microcontroller benchmarking by Renner et al.

Devices:
- 8-bit AVR
- 32-bit ARM Cortex M3, M7
- Tensilica Xtensa LX6
- RISC-V

Metrics:
- Speed
- Code Size
- RAM usage

Microcontroller benchmarking by Weatherly

Devices:
- AVR
- ARM Cortex-M3
- Tensilica Xtensa LX6

Metrics:
- Speed

eBACS (ECRYPT Benchmarking of Cryptographic Systems) by Lange and Bernstein

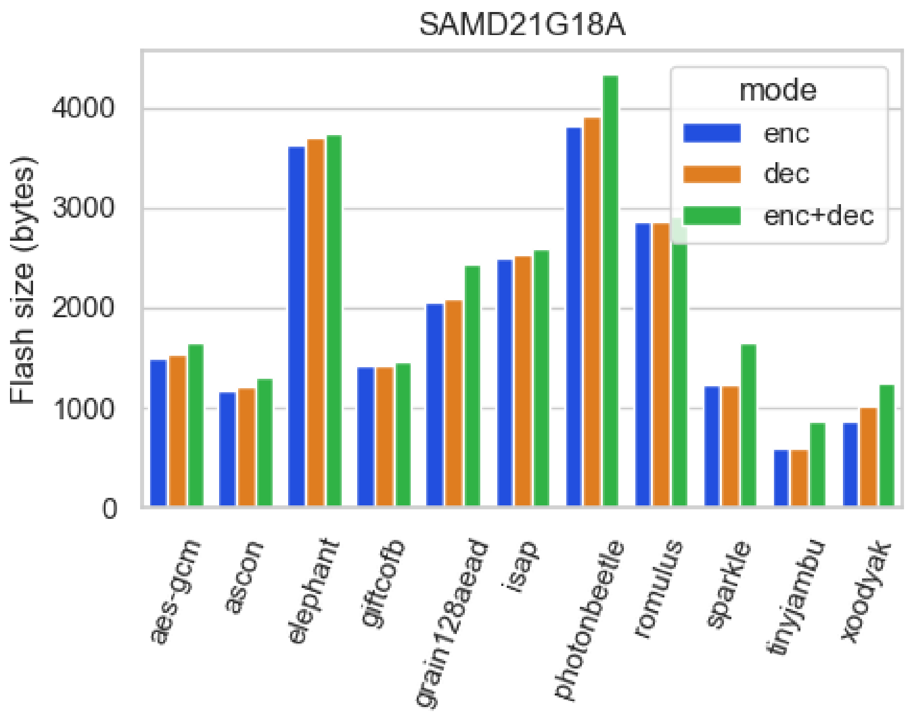
Devices:
- Many systems covering ARM, AMD, Intel, PPC, RISC V, and MIPS architectures

Metrics:
- Speed

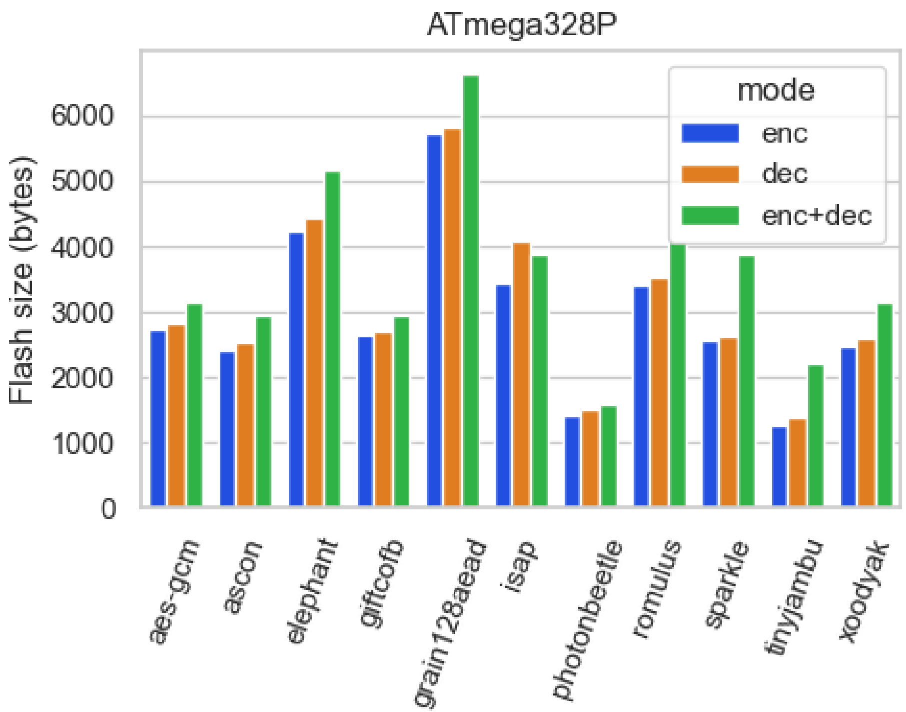
Available Implementations

Finalist	#AEAD	#Hash	#Combined	Total
Ascon	120	110	52	282
Elephant	6	-	-	6
GIFT-COFB	11	-	-	11
Grain-128AEAD	6	-	-	6
ISAP	37	1	4	42
PHOTON-Beetle	20	10	16	46
Romulus	32	11	27	70
Sparkle	25	13	3	41
TinyJambu	9	-	-	9
Xoodyak	9	8	1	18
Total	**275**	**153**	**103**	**531**

Size comparisons

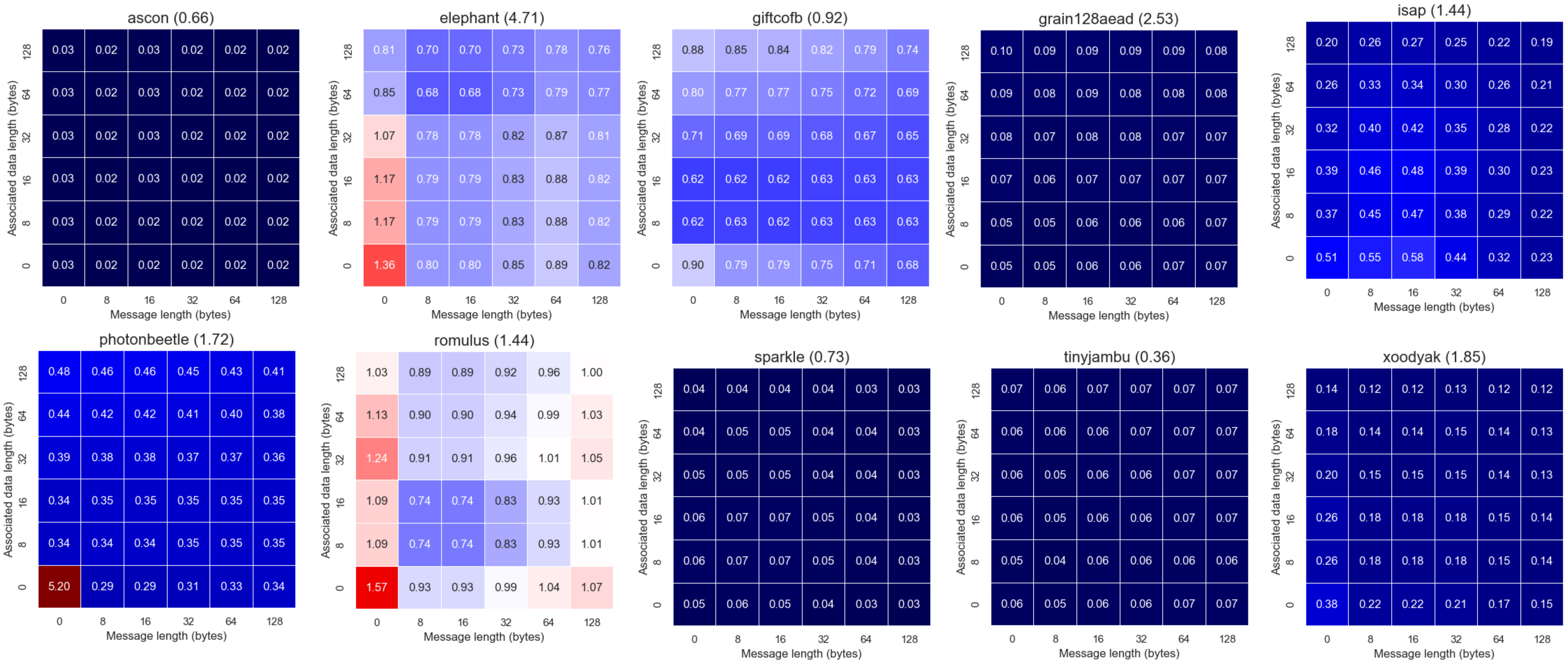


32-bit ARM Cortex-M0+



8-bit AVR

Execution time comparison to AES



Execution time ratio of smallest primary AEAD implementations to AES-GCM on nRF52840

Summary of Results

A group of candidates emerged as having compact and fast implementations across software platforms and studies (listed alphabetically)

AEAD	Hashing	AEAD + hashing
Ascon	Ascon	Ascon
GIFT-COFB	SPARKLE	SPARKLE
SPARKLE	Xoodyak	Xoodyak
TinyJAMBU		
Xoodyak		

Hardware Benchmarking

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Hardware Benchmarking (Round 2)

Initiative	*Platforms*	*Metrics*
GMU CERG group [270]	Xilinx Artix-7 Intel Cyclone 10 LP Lattice Semiconductor ECP5	Resource utilization (LUT or LE, flip-flops) Maximum clock frequency (MHz) Throughput (Mbits/s) Energy per bit (nJ/bit)
Khairallah et al. [274]	TSMC 65nm FDSOI 28nm	Area (μm^2 and GE) Clock period (ns) Power (mW) Energy (mJ)
Aagaard and Zidarič [276]	ST Micro 65nm TSMC 65nm ST Micro 90nm TSMC 90nm ARM/IBM 130nm	Throughput (bits per cycle) Area (GE) Energy (nJ) Area$\times$Energy (GE$\times$nJ) Clock Speed (GHz)

Top performers across hardware technologies and studies (listed alphabetically)

Area	**Energy**	**Throughput**
Ascon	Ascon	Ascon
GIFT-COFB	GIFT-COFB	GIFT-COFB
Romulus	TinyJAMBU	TinyJAMBU
TinyJAMBU	Xoodyak	Xoodyak

Anticipated effects of final round tweaks:

- Romulus and Xoodyak: tweaked to increase performance.
  Decrease energy, increase throughput.
- TinyJambu tweaked to increase security
  Increase energy, decrease throughput

Protected Implementations

Protected Implementations

In January 2022, GMU organized effort to evaluate protected hardware and software implementations and published three calls:

- Call for Protected Hardware Implementations
- Call for Protected Software Implementations
- Call for Side-Channel Security Evaluation Labs

Benchmarked implementations with 1st, 2nd, and 3rd order masking.

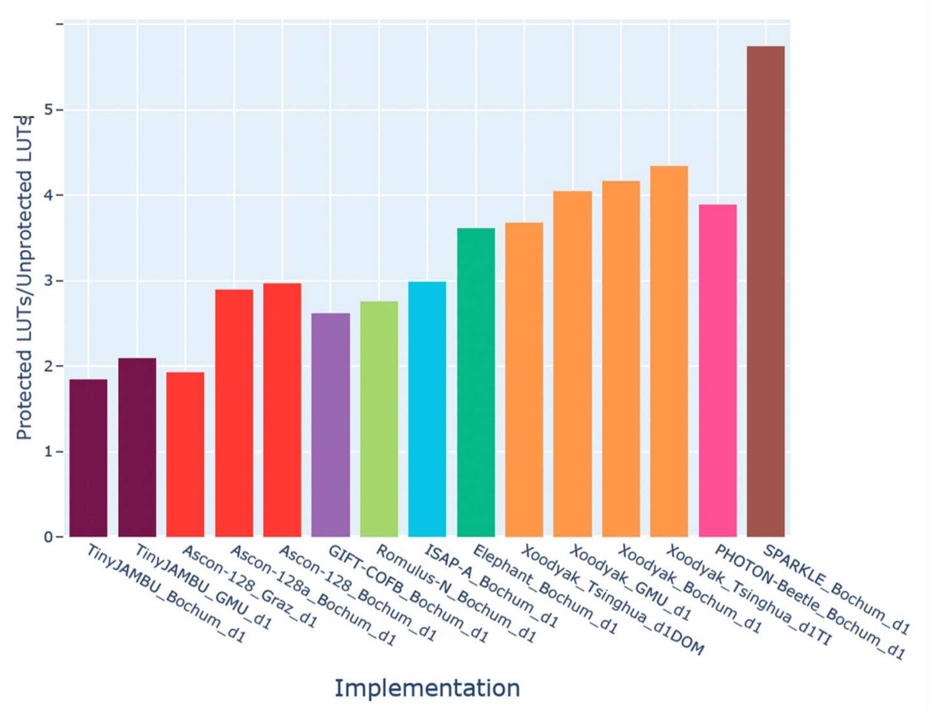


Figure 15: 1st order protected area over unprotected base area

TinyJAMBU, Ascon, and GIFT-COFB had lowest first-order protected area over base area.

Part IV – Selection and Next Steps

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Selection Process

Fair evaluation of finalists is challenging

- Assigning different weights for different criteria (security, performance in software and hardware, design maturity, amount of third-party analysis, IP issues, etc.)
- Different security claims, different functionality, attacks with different complexities etc.
- Limited resources (not all algorithms got the same attention from the crypto community) for security analysis and benchmarking.

Decision relied on publicly available analysis and benchmarking results.

Selection of Ascon

In February 2023, NIST announced the Ascon family as the winner.

- High security margin, large number of third-party analysis
- No design tweaks
- Primary choice for the for lightweight applications in the final CAESAR portfolio
- Mode-level protection mechanism for security against leakage.
- Support for additional functionalities XOF, dedicated MAC, in addition to Hash
- Performs better than the NIST standards in hardware and software benchmarks
- Implementation and design flexibility
- Lower additional cost for protected implementations

Check for updates

NIST Internal Report
NIST IR 8454

Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Lawrence E. Bassham
Jinkeon Kang
Noah D. Waller
John M. Kelsey
Deukjo Hong

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8454

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NEXT STEPS

- Getting feedback on standardization details
- Publication of draft standards (later in 2023)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

CONTACT US

lightweight-crypto@nist.gov

PUBLIC FORUM lwc-forum@list.nist.gov

GITHUB https://github.com/usnistgov/Lightweight-Cryptography-Benchmarking

WEBSITE https://csrc.nist.gov/Projects/lightweight-cryptography