Heavyweight Protection via Lightweight Cryptography

Meltem Sönmez Turan

NIST Lightweight Cryptography Team

Real World Cryptography 2022 – April 13, 2022

advanced encryption standard

- 1. Smid, Development of the Advanced Encryption Standard, 2021
- 2. Leech et al., *The Economic Impacts of the Advanced Encryption Standard*, 2018
- 3. Mouha, NISTIR 8319 Review of the Advanced Encryption Standard, 2021

Why do the crypto community continue designing new symmetric-key primitives?

New applications

Format preserving encryption, searchable encryption, order-preserving encryption, white-box cryptography, full-disk encryption, ciphers suitable for protocols like multi-party computation, zero-knowledge proofs, etc.

New features

Nonce-misuse resistance, related-key security, combined functionality, inherent side channel resistance, post-quantum security, RUP security, key commitment, *suitable for constrained environments* etc.

Lightweight Cryptography



CONSTRAINED DEVICES

e.g., RFID tags, sensors, IoT devices



NEW APPLICATIONS

e.g., home automation, healthcare, smart city



PRIVATE INFORMATION

e.g., location, health data

LACK OF CRYPTOGRAPHY STANDARDS

NIST crypto standards are optimized for general-purpose computers

Weight of an algorithm



Weight of an algorithm is a property of its implementation depending on different metrics of the target platform.

Hardware applications

Area, latency, power consumption, throughput etc.

Software applications

Code size, latency, throughput, RAM/ROM etc.

Anti-counterfeiting

- Most RAIN RFID chips have small amount of user memory (typically < 64 bits, some special chips have <2k bits).
- Hardware-oriented primitives with small area

Healthcare

- Measuring blood pressure, blood sugar, pulse etc.
- Hardware-oriented primitives by small energy requirements

Vehicle communication

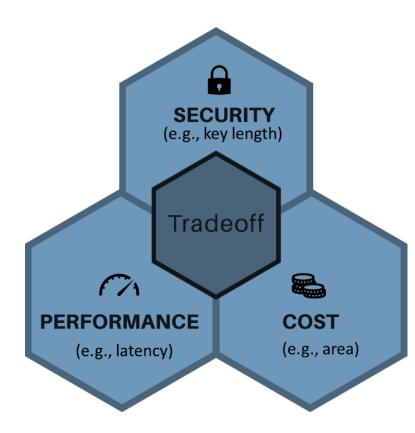
- In-vehicle, vehicle-to-vehicle and road-to-vehicle communication, driving assistance systems
- Low latency, high throughput

Smart Home

- Electrical home appliances with low-end CPUs
- Software-oriented primitives that consume less CPU time and smaller ROM requirements

Designing Lightweight Primitives





- Engineering challenge
 - "Too much crypto"
- Earlier designs
 - Shorter keys, smaller block sizes, smaller security margins by design.
- Newer designs
 - Many iterations of simple rounds, simple operations (e.g., 4-bit s-boxes, bit permutations), simpler key schedules (e.g., sponge construction)

NIST Lightweight Cryptography Standardization Process



Public competition-like process with multiple rounds like AES, SHA3 and PQC standardization.



Develop new guidelines, recommendations and standards optimized for constrained devices



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



In August 2018, NIST published the '<u>Submission Requirements and</u> <u>Evaluation Criteria for the Lightweight Cryptography Standardization</u> <u>Process</u>'.

Submission deadline: February 2019

Requirements



Security requirements

- Confidentiality + integrity
- At least 128-bit keys
- Plaintext up to 2⁵⁰ bytes
- etc.



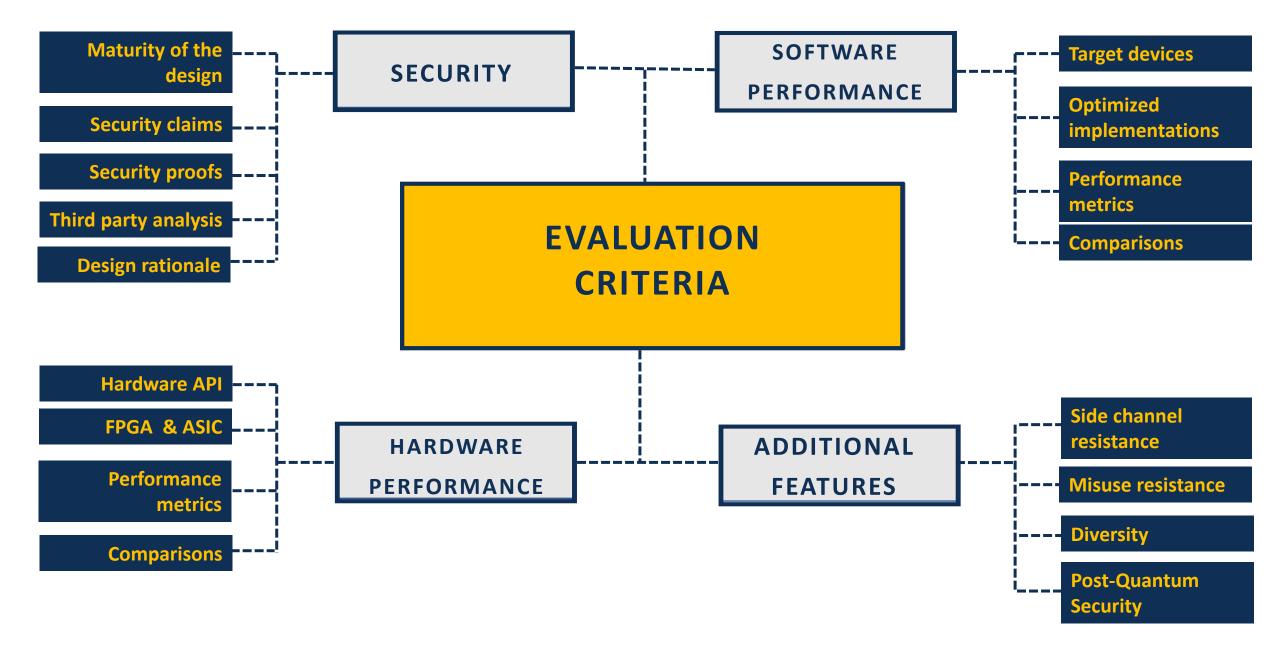
Design requirements

- Perform better than NIST standards
- Optimized for short messages
- etc.



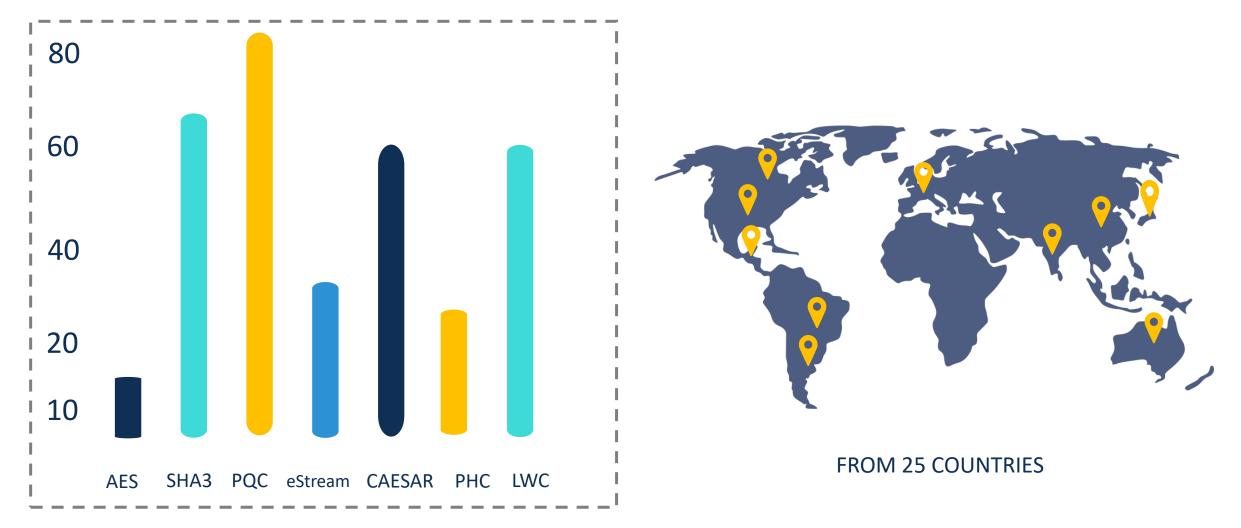
Implementation requirements

- Reference and optimized implementation compatible with API
- etc.



SUBMISSIONS





NUMBER OF SUBMISSIONS

Round 1

Around 4 months

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.

32 Candidates (out of 56) are 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



Candidates providing AEAD-only functionality

Permutation	Elephant, ISAP, Oribatida, SPIX, SpoC, Spook ³ , WAGE						
Block Cipher	COMET, GIFT-COFB, HyENA, mixFeed, Pyjamask, SAEAES, SUNDAE-GIFT, TinyJAMBU ¹						
Tweakable Block Cipher	ESTATE, ForkAE, LOTUS-AEAD and LOCUS-AEAD, Ro- mulus, Spook						
Stream Cipher	Grain-128AEAD						
Candidates providing AEAD and hashing functionalities							
Permutation	ACE, ASCON, DryGASCON, Gimli, KNOT, ORANGE, PHOTON-Beetle, SPARKLE, Subterranean 2.0, Xoodyak						
Block Cipher	SATURNIN ²						
Tweakable Block Cipher	SKINNY-AEAD and SKINNY-HASH						

Round 2

Around 20 months (from Aug. 2019 to March 2021)

Two workshops

- Nov. 2019 Third LWC Workshop
- Oct. 2020 Fourth LWC Workshop (virtual)

August 2020, status updates (optional)

Evaluation of the candidates were done based on their security and performance.

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



Software Benchmarking

Microcontroller benchmarking by NIST LWC Team

Devices:

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

Metrics:

- Code size
- Speed

Microcontroller benchmarking by Renner et al.

Devices:

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

Metrics:

- Size
- RAM usage

Microcontroller benchmarking by Weatherly

Devices:

- AVR
- ARM Cortex-M3
- Tensilica Xtensa LX6

Metrics:

• Speed

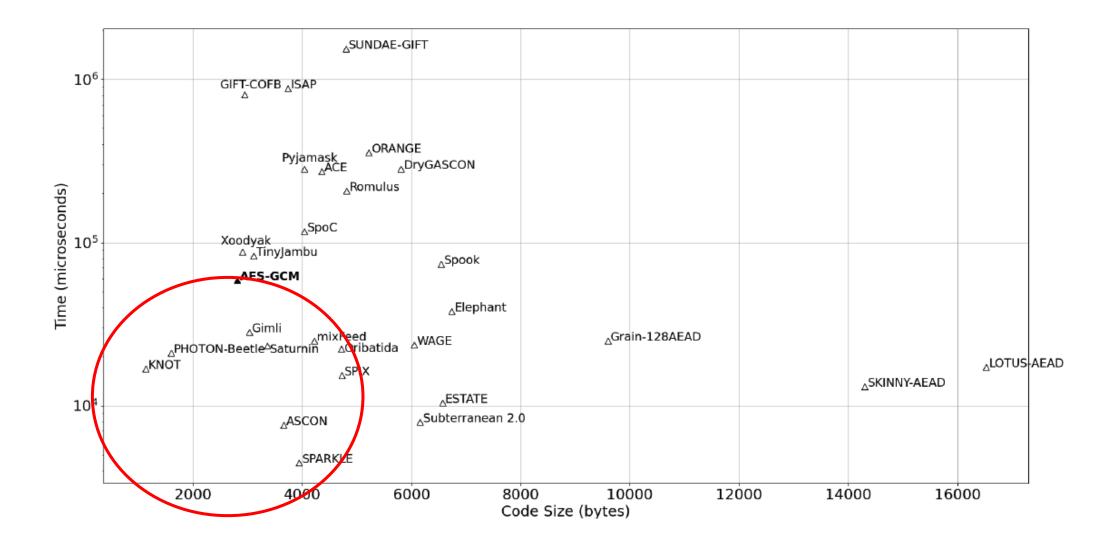
eBACS (ECRYPT Benchmarking of Cryptographic Systems) by Lange and Bernstein

Devices:

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

Metrics:

• Speed



Code size vs. speed results of the smallest primary AEAD variants - 16-byte message and 16-byte AD on ATmega328P

Software Benchmarking

Relative timings for each candidate are shown by a matrix of values, where

- rows = message lengths (0 bytes 128 bytes),
- columns = AD lengths (0 bytes 128 bytes).

 $Metric = \frac{Execution time of the candidate}{Execution time of AES-GCM}$

Result:

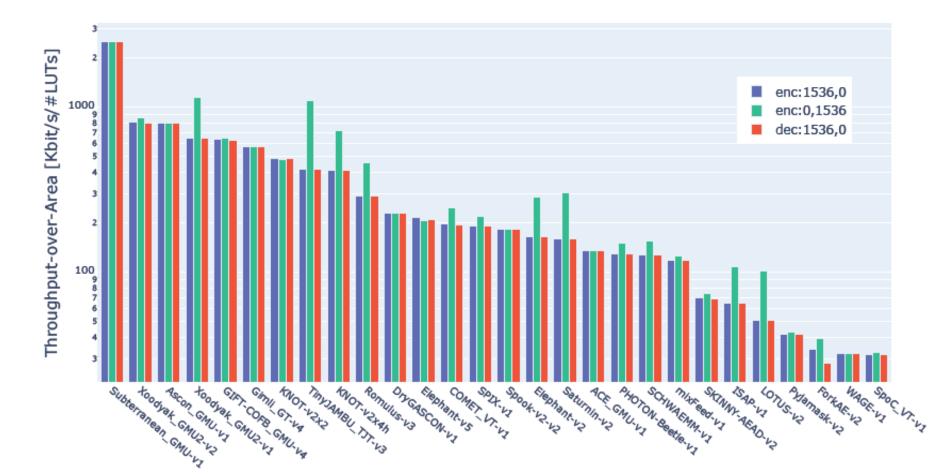
Ascon, Estate, Gimli, Knot, Lotus-AEAD, mixFeed, Orange, Photon-Beetle, Pyjamask, Romulus, Saturnin, Skinny-AEAD, Sparkle, Spoc, Spook, Subterranean, SUNDAE-GIFT, TinyJambu, Xoodyak perform better than AES-GCM on ATmega328P.

			ACE			ASC	ON			_		COM	IET				DryGA	SCON		
		128 - 2.94 2.71	2.82 2.73	2.59 2.42	0.58	0.53 0.56	0.54	0.52	0.49	- ·	-	-		-	- 9.24	9.05	9.04	8.88	8.65	8.36
		64 - 3.19 2.80	2.97 2.81	2.60 2.39	0.60	0.53 0.57	0.54	0.51	0.48	- ·		-		-	- 8.76	8.56	8.55	8.40	8.20	7.98
		32 - 3.52 2.88	3.12 2.89	2.62 2.37	0.62	0.52 0.57	0.54	0.51	0.47	- ·	-	-		-	- 8.18	8.02	8.00	7.94	7.82	7.72
		16 - 3.84 2.96	3.25 2.94	2.62 2.35	0.65	0.52 0.58	0.54	0.50	0.47	- ·	-	-		-	- 7.59	7.58	7.56	7.56	7.56	7.55
			2.96 2.72		0.56			0.47		- ·	-	-		-	- 7.60	7.59				7.56
		0-3.88 2.71	3.09 2.75	2.46 2.24	0.56	0.42 0.51	0.48	0.46	0.44	I 1.	-	-		-	6.43	6.88	6.86	7.03	7.24	7.36
			Elephant			F	ATE					Fork	AE				GIFT-0			
		128 - 1.70 1.83		2.08 2.09	- 0.29	0.32 532		0.36			-	-		-		0.38	0.38	0.37		0.34
		64 - 1.57 1.80		2.16 2.14	- 0.28	0.37 0.33	0.35		0.41	· ·	-	-		-	- 0.39	0.38	0.37	0.36	0.35	0.33
			2.11 2.26	2.42 2.31	- 0.27	1.33 0.33	0.36		0.42		-	-		-	- 0.39	0.37	0.36	0.36	0.34	0.33
			2.16 2.32		0.76	0.34 0.34	0.37	0.40	0.43		-	-		-	- 0.38				0.33	
		8 - 1.89 2.17	2.16 2.32	2.48 2.34	0.26	0.34 0.34	0.37		0.43						- 0.39	0.36	0.36	0.35	0.34	0.32
			ASC	ON				-	0.44	1 1,] 10.58	0.47		,	0.50	0.55
1			7 10 0				1	-	1.31			HyEl	NA] [21]	2.70	2.79		2.26	2.04
-	0.58	0.53	0.56	0.54	0.52	0.49			1.31						4.53	3.79				2.30
									1.27						6.31	4.83			3.25	
-	0.60	0.53	0.57	0.54	0.51	0.48			1.23						- 8.09	5.73	5.71	4.64		2.59
									1.18].					- 8.09	5.74	5.72	4.65		2.59
-	0.62	0.52	0.57	0.54	0.51	0.47		23	1.21						- 12.0	7.47	7.45	5.64	4.01	2.80
											,	-				,	0.04			
-	0.65	0.52	0.58	0.54	0.50	0.47		0	0.96	- 0.4	7 0.49	0.49	0.47 0.4	5 0.42	0.55	0.58	0RA 0.58	0.52	0.51	0.49
									1.01	- 0.5			0.50 0.4			0.61		0.52	0.50	
-	0.56	0.45	0.51	0.49	0.47	0.45			1.04	- 0.5	0.57	0.58	0.53 0.4	7 0.42	- 0.55	0.63	0.63	0.51	0.49	0.46
)9	1.06	- 0.5	3 0.61	0.61	0.55 0.4	8 0.42	- 0.73	0.77	0.77	0.59	0.55	0.50
_	0.56	0.42	0.51	0.48	0.46	0.44		94	1.03	- 0.5	3 0.61	0.61	0.54 0.4	7 0.42	- 0.73	0.77	0.77	0.59	0.54	0.50
								2	1.07	- 0.23	2 0.52	0.53	0.47 0.4	0.38	- 0.55	0.68	0.68	0.49	0.47	0.45
											'	Pyjarr	nask		. —		Rom	ulus		
		128 - 1.03 1.07	1.07 1.11	1.16 1.22	- 0.92	0.90 0.90	0.89	0.87	0.85	- 0.8	0.77		0.75 0.3	1 0.67	- 0.65	0.58	0.58	0.60	0.64	0.69
		64 - 1.10 1.15	5 1.15 1.19	1.24 1.30	0.86	0.85 0.85	0.84	0.83	0.82	- 0.8	0.81	0.81	0.77 0.3	0.66	- 0.73	0.61	0.61	0.64	0.68	0.72
		32 - 1.19 1.23	3 1.23 1.27	1.31 1.35	- 0.78	0.79 0.78	0.79	0.79	0.79	- 0.9	5 0.85	0.85	0.80 0.3	2 0.66	- 0.83	0.62	0.62	0.67	0.71	0.75
		16 - 1.26 1.30	1.30 1.33	1.36 1.38	0.70	0.73 0.73	0.75	0.76	0.77	- 1.04	0.88	0.89	0.81 0.3	0.65	- 0.75	0.53	0.53	0.60	0.67	0.73
		8 - 1.26 1.30	1.30 1.33	1.36 1.38	- 0.71	0.73 0.73	0.75	0.76	0.77	- 1.04	0.88	0.89	0.81 0.3	0.65	- 0.75	0.53	0.53	0.60	0.67	0.73
		0-0.96 1.14	1.14 1.22			0.65 0.65	0.69		0.75	- 1.2	0.94	0.95	0.83 0.1	3 0.65	- 1.12					0.78
			1.14 1.22	1.29 1.34	0.55	0.05 0.05	0.05	0.73	0.75		_					0.68	0.68	0.73	0.76	
			SAEAES	1.29 1.34	- 0.55	Satu		0.73	0.75		-	, SKINNY-	AEAD			0.68	0.68 SPAR		0.76	
		128		1.29 1.34		Satu	Irnin	0.73	_	- 0.91	3 0.96		AEAD 0.95 0.9	93 0.91	- 0.23	0.68	SPAR	RKLE	0.76	0.21
		128 64		1.29 1.34 		Satu	Irnin 0.70	0.70	_	- 0.93	3 0.96	0.97			- 0.23	0.25	SPAR	KLE 0.23		
				1.29 1.34 	- 0.69 - 0.83 - 1.00	Satu 0.69 0.69 0.81 0.81 0.93 0.93	0.70 0.80 0.90	0.70 0.78 0.84	0.71 0.76 0.80	- 0.9:	3 0.96 ? 0.90 3 0.83	0.97 0.91 0.84	0.95 0.9 0.89 0.4 0.84 0.4	38 0.87 34 0.84	- 0.26	0.25 0.29 0.33	SPAR 0.26 0.29 0.33	KLE 0.23 0.25 0.27	0.22 0.23 0.24	0.21 0.21
		64 32 16		1.29 1.34 	- 0.69 - 0.83 - 1.00 - 1.01	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92	0.70 0.80 0.90 0.88	0.70 0.78 0.84 0.83	0.71 0.76 0.80 0.79	- 0.9) - 0.8) - 0.7)	3 0.96 2 0.90 3 0.83 5 0.77	0.97 0.91 0.84 0.78	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.1	38 0.87 34 0.84 31 0.82	- 0.26 - 0.29 - 0.39	0.25 0.29 0.33 0.40	SPAR 0.26 0.29 0.33 0.40	0.23 0.25 0.27 0.31	0.22 0.23 0.24 0.27	0.21 0.21 0.23
		64 32 16 8		1.29 1.34 	- 0.69 - 0.83 - 1.00 - 1.01 - 1.01	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92	0.70 0.80 0.90 0.88 0.88	0.70 0.78 0.84 0.83 0.83	0.71 0.76 0.80 0.79 0.79	- 0.9) - 0.8) - 0.7! - 0.74	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77	0.97 0.91 0.84 0.78 0.78	0.95 0.9 0.89 0.4 0.84 0.4 0.80 0.4 0.79 0.4	88 0.87 84 0.84 81 0.82 81 0.82	- 0.26 - 0.29 - 0.39 - 0.38	0.25 0.29 0.33 0.40 0.40	SPAR 0.26 0.29 0.33 0.40 0.40	<pre>KLE 0.23 0.25 0.27 0.31 0.31</pre>	0.22 0.23 0.24 0.27 0.27	0.21 0.21 0.23 0.23
		64 32 16	SAEAES 	1.29 1.34 	- 0.69 - 0.83 - 1.00 - 1.01 - 1.01	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92	0.70 0.80 0.90 0.88 0.88	0.70 0.78 0.84 0.83	0.71 0.76 0.80 0.79 0.79	- 0.9) - 0.8) - 0.7)	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77	0.97 0.91 0.84 0.78 0.78	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.1	88 0.87 84 0.84 81 0.82 81 0.82	- 0.26 - 0.29 - 0.39 - 0.38	0.25 0.29 0.33 0.40 0.40	SPAR 0.26 0.29 0.33 0.40	<pre>KLE 0.23 0.25 0.27 0.31 0.31</pre>	0.22 0.23 0.24 0.27 0.27	0.21 0.21 0.23 0.23
		64 32 16 8 0	SAEAES SPIX		- 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92 0.92 0.92 1.20 1.20	0.70 0.80 0.90 0.88 0.88 1.07 oC	0.70 0.78 0.84 0.83 0.83 0.94	0.71 0.76 0.80 0.79 0.79 0.85	- 0.93 - 0.83 - 0.74 - 0.74 - 0.74	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68	0.97 0.91 0.84 0.78 0.78 0.78 0.69	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.1 0.79 0.1 0.73 0.7	88 0.87 84 0.84 81 0.82 81 0.82 81 0.82 77 0.80	- 0.26 - 0.29 - 0.39 - 0.38 - 0.38	0.25 0.29 0.33 0.40 0.40 0.35 Su	SPAR 0.26 0.29 0.33 0.40 0.40 0.35	KLE 0.23 0.25 0.27 0.31 0.31 0.26 nean	0.22 0.23 0.24 0.27 0.27 0.23 2.0	0.21 0.21 0.23 0.23 0.20
		64 32 16 8 0 128 - 1.20 1.10	SAEAES 		- 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92 0.92 0.92 1.20 1.20 Sp 0.95 1.00	0.70 0.80 0.90 0.88 0.88 1.07 oC 0.98	0.70 0.78 0.84 0.83 0.83 0.94	0.71 0.76 0.80 0.79 0.79 0.85	- 0.9 - 0.8 - 0.7 - 0.7 - 0.5 - 0.5	 3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.56 	0.97 0.91 0.84 0.78 0.78 0.69 Spot	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.1 0.79 0.1 0.73 0. 0k 0.50 0.4	 38 0.87 34 0.84 31 0.82 31 0.82 77 0.80 47 0.44 	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30	0.25 0.29 0.33 0.40 0.40 0.35 Su 0.52	SPAR 0.26 0.29 0.33 0.40 0.40 0.35 bterrat	KLE 0.23 0.25 0.27 0.31 0.31 0.26 nean 0.52	0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48	0.21 0.21 0.23 0.23 0.20
		64 32 16 8 0 128 - 1.20 1.10 64 - 1.42 1.23	SAEAES 	 	- 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53 - 1.02 - 0.95	Satu 0.69 0.69 0.81 0.81 0.93 0.92 0.92 0.92 1.20 1.20 Sp 0.95 0.95 1.00 0.86 0.93	0.70 0.80 0.90 0.88 0.88 1.07 0C 0.98 0.92	0.70 0.78 0.84 0.83 0.83 0.94 0.96 0.91	0.71 0.76 0.80 0.79 0.79 0.85 0.94 0.89	- 0.9 - 0.8 - 0.7 - 0.7 - 0.5 - 0.5 - 0.5	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.56 9 0.61	0.97 0.91 0.84 0.78 0.78 0.69 Spot 0.56 0.61	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.4 0.79 0.4 0.79 0.4 0.73 0.7 0.8 0.50 0.4	 0.87 0.84 0.84 0.82 0.82 0.80 0.44 0.44 	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30 - 0.57 - 0.57	0.25 0.29 0.33 0.40 0.40 0.35 Su 0.52 0.61	SPAR 0.26 0.29 0.33 0.40 0.40 0.35 bterrat 0.54 0.64	KLE 0.23 0.25 0.27 0.31 0.31 0.26 nean 0.52 0.59	0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48 0.52	0.21 0.23 0.23 0.20 0.44 0.46
		64 32 16 8 128 - 1.20 1.10 64 - 1.42 1.23 32 - 1.70 1.36	SAEAES 		- 0.69 - 0.83 - 100 - 101 - 101 - 153 - 102 - 0.95 - 0.86	Satu 0.69 0.69 0.81 0.81 0.93 0.92 0.92 0.92 1.20 1.20 0.95 1.00 0.86 0.93	0.70 0.80 0.90 0.88 0.88 1.07 0.98 0.98 0.92 0.86	0.70 0.78 0.83 0.83 0.94 0.96 0.91 0.86	0.71 0.76 0.80 0.79 0.79 0.85 0.94 0.89 0.86	- 0.9: - 0.8: - 0.7: - 0.7: - 0.7: - 0.5: - 0.5: - 0.5: - 0.6:	 0.96 0.90 0.83 0.77 0.77 0.68 0.56 0.61 0.67 	0.97 0.91 0.84 0.78 0.69 Spot 0.56 0.61 0.67	0.95 0.9 0.89 0.1 0.84 0.1 0.84 0.1 0.80 0.3 0.79 0.1 0.73 0.1 0.50 0.4 0.52 0.4 0.54 0.4	 0.87 0.84 0.84 0.82 0.84 0.44 0.44 0.44 	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.86	0.25 0.29 0.33 0.40 0.40 0.35 Sul 0.52 0.61 0.69	SPAR 0.26 0.29 0.33 0.40 0.40 0.35 0.54 0.54 0.64 0.73	KLE 0.23 0.25 0.27 0.31 0.31 0.26 0.52 0.52 0.59 0.65	0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48 0.52 0.56	0.21 0.21 0.23 0.23 0.20 0.44 0.44
		64 32 16 8 0 128 - 1.20 1.10 64 - 1.42 1.22 32 - 1.70 1.36 16 - 1.99 1.48	SAEAES 	1.001 0.92 1.101 0.92 1.11 0.94 1.14 0.95	- 0.69 - 0.83 - 1.00 - 1.01 - 1.53 - 1.02 - 0.95 - 0.86 - 0.77	Sat. 0.69 0.69 0.81 0.81 0.93 0.92 0.92 0.92 1.20 1.20 0.95 1.00 0.86 0.93 0.97 0.96	Irnin 0.70 0.80 0.90 0.88 0.88 1.07 0.88 0.92 0.98 0.92 0.86 0.81	0.70 0.78 0.83 0.83 0.94 0.94 0.96 0.91 0.86 0.83	0.71 0.76 0.80 0.79 0.85 0.85 0.84 0.86 0.84	- 0.9: - 0.8: - 0.7: -	 0.96 0.90 0.83 0.77 0.77 0.68 0.56 0.61 0.82 	0.97 0.91 0.84 0.78 0.78 0.69 5pot 0.56 0.61 0.67 0.82	0.95 0.9 0.89 0.4 0.84 0.4 0.80 0.4 0.79 0.1 0.73 0.7 0.50 0.4 0.52 0.4 0.52 0.4 0.63 0.9	 0.87 0.84 0.82 0.44 0.44 0.44 0.44 0.44 0.44 0.44 0.44 	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30 - 0.57 - 0.57 - 0.70 - 0.86 - 1.03	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76	SPAR 0.26 0.29 0.33 0.40 0.40 0.35 0.54 0.54 0.64 0.73 0.81	RKLE 0.23 0.25 0.27 0.31 0.31 0.26 0.52 0.52 0.52 0.52 0.52 0.52 0.52 0.52	0.22 0.23 0.24 0.27 0.27 0.27 0.23 2.0 0.48 0.52 0.56 0.58	0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48
		64 32 16 8 128 - 1.20 1.10 64 - 1.42 1.23 32 - 1.70 1.36	SAEAES 		- 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58	Satu 0.69 0.69 0.81 0.81 0.93 0.92 0.92 0.92 1.20 1.20 0.95 1.00 0.86 0.93	Irnin 0.70 0.80 0.88 0.88 1.07 0.98 0.98 0.92 0.86 0.81 0.71	0.70 0.78 0.84 0.83 0.94 0.94 0.91 0.86 0.83 0.76	0.71 0.76 0.80 0.79 0.79 0.85 0.85 0.84 0.80	- 0.9: - 0.8: - 0.7: - 0.7: - 0.7: - 0.5: - 0.5: - 0.5: - 0.6:	 0.96 0.90 0.83 0.77 0.77 0.68 0.56 0.61 0.67 0.82 0.82 	0.97 0.91 0.84 0.78 0.78 0.69 .50 0.56 0.61 0.67 0.82 0.82	0.95 0.9 0.89 0.1 0.84 0.1 0.84 0.1 0.80 0.3 0.79 0.1 0.73 0.1 0.50 0.4 0.52 0.4 0.54 0.4	38 0.87 34 0.84 31 0.82 31 0.82 77 0.80 47 0.44 48 0.44 49 0.44 54 0.47	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.86	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76 0.72	SPAR 0.26 0.29 0.33 0.40 0.40 0.35 0.54 0.54 0.54 0.73 0.81	RKLE 0.23 0.25 0.27 0.31 0.31 0.26 0.27 0.31 0.26 0.52 0.52 0.52 0.52 0.52 0.52 0.52 0.53 0.70	0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48 0.52 0.56 0.58 0.56	0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47
		64 32 16 8 0 128 - 1.20 1.10 64 - 1.42 1.23 32 - 1.70 1.34 16 - 1.99 1.44 8 - 1.85 1.38 0 - 2.35 1.55	SAEAES SAEAES	101 0.92 106 0.93 111 0.94 1.14 0.95 1.08 0.92 1.12 0.92	- 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58	Satt 0.69 0.69 0.81 0.93 0.92 0.92 1.20 1.20 0.81 0.93 0.92 0.92 0.93 0.92 0.94 0.93 0.95 1.00 0.86 0.93 0.75 0.86 0.67 0.80 0.53 0.77	Irnin 0.70 0.80 0.90 0.88 0.88 1.07 0.98 0.92 0.86 0.81 0.71 0.74	0.70 0.78 0.84 0.83 0.94 0.96 0.96 0.96 0.86 0.83 0.76 0.79	0.71 0.76 0.80 0.79 0.79 0.85 0.85 0.84 0.80	- 0.9: - 0.8: - 0.7' - 0.7' - 0.7' - 0.7' - 0.5' - 0.5' - 0.6' - 0.8! - 0.8!	 0.96 0.90 0.83 0.77 0.77 0.68 0.56 0.61 0.67 0.82 0.82 	0.97 0.91 0.84 0.78 0.78 0.69 5po 0.56 0.61 0.67 0.82 0.82 0.82	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.1 0.79 0.1 0.73 0.3 0.50 0.4 0.52 0.4 0.52 0.4 0.63 0.3 0.63 0.3	38 0.87 34 0.84 31 0.82 31 0.82 77 0.80 47 0.44 48 0.44 49 0.44 54 0.47	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30 - 0.30 - 0.30 - 0.30 - 0.57 - 0.70 - 0.86 - 1.03 - 0.96	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76 0.72	SPAR 0.26 0.29 0.33 0.40 0.40 0.40 0.54 0.54 0.73 0.81 0.77 0.94	RKLE 0.23 0.25 0.27 0.31 0.26 0.52 0.52 0.52 0.52 0.52 0.52 0.70 0.65 0.70 0.67 0.77	0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48 0.52 0.56 0.58 0.56	0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47
		64 - - 32 - - 16 - - 8 - - 0 - - 128 - - 128 1.20 1.10 64 1.42 1.22 32 1.70 1.36 1.99 1.46 8 8 1.85 1.36 0 2.35 1.55	SAEAES SAEAES SAEAES SAEAES SAEAES SUX SUX SUX SUX SUX SUX SAEAES	1.01 0.92 1.06 0.93 1.11 0.94 1.14 0.95 1.08 0.92 1.12 0.92	- 0.69 - 0.83 - 100 - 101 - 153 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58 - 0.59	Satu 0.69 0.69 0.81 0.81 0.92 0.92 0.92 0.92 1.20 1.20 0.95 1.00 0.66 0.93 0.75 0.66 0.67 0.80 0.53 0.70	Irnin 0.70 0.80 0.90 0.88 0.88 1.07 0.98 0.92 0.86 0.92 0.86 0.91 0.71 0.74	0.70 0.78 0.84 0.83 0.94 0.94 0.96 0.91 0.86 0.83 0.76 0.79	0.71 0.76 0.80 0.79 0.85 0.94 0.84 0.84 0.84 0.84	- 0.9: - 0.8: - 0.7: - 0.5: - 0.5: - 0.5: - 0.5: - 0.6: - 0.8: - 0.8: - 0.8: - 0.8: - 0.8:	3 0.96 2 0.90 3 0.83 5 0.77 4 0.76 7 3 6 0.61 5 0.67 3 0.68 9 0.61 5 0.67 3 0.82 9 0.61 5 0.77	0.97 0.91 0.84 0.78 0.78 0.78 0.69 5pot 0.56 0.61 0.67 0.82 0.82 0.82 0.79	0.95 0.9 0.89 0.1 0.84 0.1 0.79 0.1 0.73 0.1 0.73 0.1 0.50 0.4 0.52 0.4 0.52 0.4 0.63 0.9 0.63 0.9 0.57 0.4 3E	4 0.87 34 0.84 31 0.82 31 0.82 77 0.80 47 0.44 48 0.44 49 0.44 54 0.47 54 0.47 54 0.47	- 0.26 - 0.29 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.86 - 1.03 - 0.96 - 1.36	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76 0.72 0.88	SPAR 0.26 0.29 0.33 0.40 0.35 0.54 0.64 0.73 0.64 0.77 0.94 Xooo	RKLE 0.23 0.25 0.27 0.31 0.31 0.26 0.70 0.65 0.70 0.67 0.77 dyak	0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48 0.52 0.56 0.58 0.56 0.61	0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49
		64	SAEAES 	1.01 0.92 1.01 0.92 1.06 0.93 1.11 0.94 1.14 0.95 1.08 0.92 1.12 0.92 T 0.47 0.49	- 0.69 - 0.83 - 1.00 - 1.01 - 1.53 - 0.55 - 0.58 - 0.59 - 0.51	Satu 0.69 0.81 0.93 0.93 0.92 0.92 1.20 1.20 0.95 1.00 0.86 0.93 0.75 0.86 0.67 0.80 0.51 1.00 0.85 1.30 0.75 1.67 0.53 0.70 0.53 0.70	Imin 0.70 0.80 0.88 0.88 1.07 0.98 0.92 0.86 0.81 0.71 0.74 0.74 0.36	0.70 0.78 0.84 0.83 0.94 0.94 0.94 0.94 0.86 0.83 0.76 0.79 0.39	0.71 0.76 0.80 0.79 0.79 0.85 0.85 0.84 0.84 0.84 0.81	- 0.9: - 0.8: - 0.7: - 0.7: - 0.5: - 0.5: - 0.6: - 0.8: - 0.5: - 0.8: - 0.8:	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.56 9 0.61 5 0.67 3 0.82 3 0.82 5 0.79 9 1.66	0.97 0.91 0.84 0.78 0.78 0.78 0.69 0.61 0.61 0.67 0.82 0.82 0.82 0.79 VAC	0.95 0.9 0.89 0.1 0.84 0.1 0.80 0.1 0.79 0.1 0.73 0.3 0.6 0.50 0.4 0.52 0.4 0.52 0.4 0.63 0.3 0.63 0.3 0.57 0.4 3E 1.67 1.5	38 0.87 34 0.84 31 0.82 31 0.82 31 0.82 37 0.80 37 0.44 48 0.44 49 0.44 54 0.47 54 0.43 54 0.43 54 0.43	- 0.57 - 0.57 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.66 - 1.03 - 0.96 - 1.36 - 1.36	0.25 0.29 0.33 0.40 0.35 Sui 0.52 0.61 0.76 0.76 0.72 0.88	SPAR 0.26 0.29 0.33 0.40 0.35 0.54 0.73 0.81 0.77 0.94 Xooo 0.33	RKLE 0.23 0.25 0.27 0.31 0.31 0.32 0.52 0.52 0.59 0.65 0.70 0.65 0.70 0.67 0.77 dyak 0.34	0.22 0.23 0.24 0.27 0.27 0.23 0.57 0.52 0.56 0.58 0.56 0.58 0.58	0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49
		64 - - 32 - - 16 - - 8 - - 0 - - 128 - - 128 1.20 1.10 64 1.42 1.22 32 1.70 1.36 1.99 1.46 8 8 1.85 1.36 0 2.35 1.55	SAEAES SAEAES	1.01 0.92 1.06 0.93 1.11 0.95 1.14 0.95 1.12 0.92 1.12 0.92 T 0.47 0.49 0.52	- 0.69 - 0.83 - 1.00 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58 - 0.58 - 0.59 - 0.58 - 0.59 - 0.58 - 0.59 - 0.59 - 0.58 - 0.59 - 0.58 - 0.59 - 0.59 - 0.58 - 0.59 - 0.58 - 0.55 -	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92 1.20 1.20 0.95 1.00 0.86 0.93 0.75 0.86 0.67 0.86 0.54 0.67 0.53 0.70 0.31 0.34	Irnin 0.70 0.80 0.90 0.88 0.88 1.07 0.98 0.92 0.86 0.81 0.71 0.74 0.74 0.74 0.36 0.39	0.70 0.78 0.84 0.83 0.94 0.96 0.91 0.86 0.83 0.76 0.79 0.39 0.43	0.71 0.76 0.80 0.79 0.79 0.85 0.85 0.84 0.84 0.84 0.81 0.43 0.43	- 0.8; - 0.7; - 0.7; - 0.7; - 0.5; - 0.5; - 0.6; - 0.8; - 0.7; - 0.5; - 0.7; - 0.5; -	3 0.96 2 0.90 3 0.83 5 0.77 3 0.63 4 0.77 3 0.68 9 0.61 5 0.67 3 0.82 3 0.82 5 0.79 - 1.66 - 1.74	0.97 0.91 0.84 0.78 0.78 0.69 5 5 0.61 0.67 0.82 0.82 0.82 0.79 0.82 0.79 0.82 0.79	0.95 0.4 0.89 0.4 0.84 0.1 0.79 0.1 0.73 0.7 0.50 0.4 0.52 0.4 0.52 0.4 0.53 0.5 0.63 0.5 0.57 0.4 5E 1.67 1.5	38 0.87 34 0.84 31 0.82 31 0.82 31 0.82 37 0.44 48 0.44 49 0.44 54 0.47 54 0.47 54 0.47 54 0.47 54 0.47 54 0.47 54 0.47 54 0.47 54 0.43 56 1.47 50 1.46	- 0.26 - 0.29 - 0.39 - 0.38 - 0.38 - 0.30 - 0.51 - 0.66 - 1.03 - 0.96 - 1.36 - 1.36 - 0.37 - 0.51	0.25 0.29 0.33 0.40 0.40 0.35 Sul 0.52 0.61 0.69 0.76 0.72 0.88 0.32 0.32	SPAR 0.26 0.29 0.33 0.40 0.35 0.54 0.64 0.73 0.81 0.77 0.94 Xooo 0.33 0.42	RKLE 0.23 0.25 0.31 0.31 0.26 0.52 0.59 0.655 0.70 0.67 0.77 dyak 0.34 0.34	0.22 0.23 0.24 0.27 0.27 0.23 0.56 0.56 0.56 0.56 0.61	0.21 0.21 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49 0.33 0.37
		64	SAEAES SAEAES SAEAES SAEAES SAEAES SAEAES SUIVAL SPIUX SP	101 0.92 106 0.93 111 0.94 114 0.95 112 0.92 120 0.93 111 0.94 114 0.95 112 0.92 0.53 0.54	- 0.69 - 0.83 - 100 - 101 - 101 - 101 - 101 - 101 - 102 - 0.95 - 0.86 - 0.97 - 0.58 - 0.59 - 0.59 - 0.31 - 0.32 - 0.33	Satu 0.69 0.69 0.81 0.81 0.93 0.93 0.92 0.92 1.20 1.20 0.95 1.00 0.86 0.93 0.75 0.86 0.67 0.86 0.54 0.67 0.53 0.70 0.31 0.34	min 0.70 0.80 0.80 0.88 0.88 1.07 0.98 0.92 0.86 0.81 0.71 0.71 0.74 ambu 0.36 0.39 0.42	0.70 0.78 0.84 0.83 0.94 0.91 0.96 0.91 0.86 0.83 0.76 0.79 0.39 0.43 0.45	0.71 0.76 0.80 0.79 0.85 0.85 0.85 0.84 0.80 0.81 0.81 0.43 0.43 0.43	- 0.8; - 0.7; - 0.5; - 0.5; - 0.5; - 0.6; - 0.8; - 0.7; - 0.5; -	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.77 3 0.68 4 0.77 5 0.61 5 0.67 3 0.82 5 0.77 7 1.66 9 1.74 3 1.82	0.97 0.91 0.84 0.78 0.78 0.56 0.69 , 500 0.56 0.61 0.67 0.82 0.82 0.79 VAA 1.73 1.84 1.96	0.95 0.1 0.89 0.1 0.89 0.1 0.89 0.1 0.80 0.1 0.81 0.1 0.73 0.1 0.73 0.1 0.73 0.1 0.73 0.1 0.63 0.2 0.63 0.3 0.57 0.4 5E 1.67 1.71 1.61 1.81 1.41	38 0.87 34 0.84 31 0.82 31 0.82 31 0.82 31 0.82 31 0.82 31 0.82 31 0.82 31 0.82 31 0.82 31 0.82 32 0.84 33 0.82 34 0.44 35 0.44 36 0.47 36 1.47 36 1.47 36 1.46 37 0.46 38 0.47	- 0.36 - 0.39 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.86 - 1.03 - 0.96 - 1.35 - 0.97 - 0.96 - 1.35 - 0.57 - 0.96	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.72 0.88 0.32 0.32 0.42 0.46	SPAR 0.26 0.29 0.33 0.40 0.40 0.40 0.40 0.40 0.40 0.64 0.73 0.81 0.77 0.94 Xooc 0.33 0.42 0.46	RLE 0.23 0.25 0.27 0.31 0.31 0.26 0.70 0.52 0.59 0.65 0.70 0.67 0.77 dyak 0.34 0.34 0.46	0.22 0.23 0.24 0.27 0.27 0.23 0.57 0.58 0.56 0.56 0.56 0.56 0.56 0.56 0.58 0.56 0.58 0.56 0.58 0.56 0.58	0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.48 0.47 0.33 0.33
		64	SAEAES - - <t< td=""><td>101 0.92 106 0.93 111 0.94 114 0.95 108 0.92 112 0.92 T 0.47 0.49 0.50 0.52 0.55 0.56</td><td>- 0.69 - 0.83 - 100 - 101 - 101 - 101 - 101 - 133 - 0.55 - 0.66 - 0.77 - 0.58 - 0.59 - 0.55 - 0.55 -</td><td>Satu 0.69 0.69 0.81 0.81 0.93 0.92 0.92 0.92 1.20 1.20 0.85 0.60 0.86 0.93 0.75 0.66 0.54 0.67 0.53 0.70 Tiny1 0.34 0.31 0.34 0.31 0.34 0.31 0.34</td><td>rmin 0.70 0.80 0.88 0.88 1.07 0.74 0.36 0.31 0.71 0.74 0.36 0.39 0.32 0.34 0.34 0.34 0.34 0.34 0.34 0.35</td><td>0.70 0.78 0.84 0.83 0.94 0.94 0.94 0.91 0.86 0.91 0.86 0.76 0.79 0.39 0.43 0.43 0.43</td><td>0.71 0.76 0.80 0.79 0.85 0.84 0.89 0.86 0.84 0.80 0.81 0.43 0.46 0.43 0.46</td><td>- 0.5: - 0.5: - 0.5: - 0.5: - 0.5: - 0.6: - 0.8: - 0.9: - 0.5: - 0.8: - 0.9: - 0.9: - 0.9: - 0.9: - 0.8: - 0.9: - 0.9: -</td><td>3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.56 5 0.61 5 0.61 5 0.62 6 0.82 5 0.79 7 1.66</td><td>0.97 0.91 0.84 0.78 0.78 0.69 0.56 0.61 0.67 0.82 0.82 0.79 WAC 1.73 1.84 1.96 2.06</td><td>0.95 0.4 0.89 0.4 0.84 0.1 0.79 0.1 0.73 0.7 0.50 0.4 0.52 0.4 0.52 0.4 0.53 0.5 0.63 0.5 0.57 0.4 5E 1.67 1.5</td><td></td><td>- 0.36 - 0.39 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.86 - 1.03 - 0.96 - 1.35 - 0.51 - 0.96 - 1.35 - 0.51 - 0.57 - 0.96 - 0.51 - 0.51 - 0.96 - 0.51 - 0.95 - 0.95 -</td><td>0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76 0.72 0.88 0.32 0.42 0.42 0.46 0.57</td><td>SPAR 0.26 0.29 0.33 0.40 0.40 0.40 0.40 0.40 0.40 0.64 0.73 0.81 0.77 0.94 Xooc 0.33 0.42 0.46</td><td>RLE 0.23 0.25 0.27 0.31 0.31 0.26 0.59 0.65 0.70 0.677 0.477 0.477 0.474 0.434 0.54</td><td>0.22 0.23 0.24 0.27 0.23 0.23 0.56 0.56 0.56 0.56 0.56 0.56 0.56 0.56</td><td>0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.48 0.47 0.33 0.33 0.33 0.33</td></t<>	101 0.92 106 0.93 111 0.94 114 0.95 108 0.92 112 0.92 T 0.47 0.49 0.50 0.52 0.55 0.56	- 0.69 - 0.83 - 100 - 101 - 101 - 101 - 101 - 133 - 0.55 - 0.66 - 0.77 - 0.58 - 0.59 - 0.55 -	Satu 0.69 0.69 0.81 0.81 0.93 0.92 0.92 0.92 1.20 1.20 0.85 0.60 0.86 0.93 0.75 0.66 0.54 0.67 0.53 0.70 Tiny1 0.34 0.31 0.34 0.31 0.34 0.31 0.34	rmin 0.70 0.80 0.88 0.88 1.07 0.74 0.36 0.31 0.71 0.74 0.36 0.39 0.32 0.34 0.34 0.34 0.34 0.34 0.34 0.35	0.70 0.78 0.84 0.83 0.94 0.94 0.94 0.91 0.86 0.91 0.86 0.76 0.79 0.39 0.43 0.43 0.43	0.71 0.76 0.80 0.79 0.85 0.84 0.89 0.86 0.84 0.80 0.81 0.43 0.46 0.43 0.46	- 0.5: - 0.5: - 0.5: - 0.5: - 0.5: - 0.6: - 0.8: - 0.9: - 0.5: - 0.8: - 0.9: - 0.9: - 0.9: - 0.9: - 0.8: - 0.9: -	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.56 5 0.61 5 0.61 5 0.62 6 0.82 5 0.79 7 1.66	0.97 0.91 0.84 0.78 0.78 0.69 0.56 0.61 0.67 0.82 0.82 0.79 WAC 1.73 1.84 1.96 2.06	0.95 0.4 0.89 0.4 0.84 0.1 0.79 0.1 0.73 0.7 0.50 0.4 0.52 0.4 0.52 0.4 0.53 0.5 0.63 0.5 0.57 0.4 5E 1.67 1.5		- 0.36 - 0.39 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.86 - 1.03 - 0.96 - 1.35 - 0.51 - 0.96 - 1.35 - 0.51 - 0.57 - 0.96 - 0.51 - 0.51 - 0.96 - 0.51 - 0.95 -	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76 0.72 0.88 0.32 0.42 0.42 0.46 0.57	SPAR 0.26 0.29 0.33 0.40 0.40 0.40 0.40 0.40 0.40 0.64 0.73 0.81 0.77 0.94 Xooc 0.33 0.42 0.46	RLE 0.23 0.25 0.27 0.31 0.31 0.26 0.59 0.65 0.70 0.677 0.477 0.477 0.474 0.434 0.54	0.22 0.23 0.24 0.27 0.23 0.23 0.56 0.56 0.56 0.56 0.56 0.56 0.56 0.56	0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.48 0.47 0.33 0.33 0.33 0.33
			SAEAES - - <tr tr=""> - -</tr>	- 0.69 - 0.83 - 100 - 101 - 101 - 153 - 0.55 - 0.66 - 0.77 - 0.58 - 0.59 - 0.59 - 0.59 - 0.31 - 0.33 - 0.33 - 0.33 - 0.33 - 0.28	Satu 0.69 0.69 0.81 0.81 0.92 0.92 0.92 0.92 1.20 50 0.81 0.81 0.93 0.92 0.92 0.92 0.93 0.70 0.86 0.83 0.75 0.86 0.54 0.67 0.53 0.70 Tinyl 0.31 0.31 0.36 0.32 0.40	rmin 0.70 0.80 0.88 0.88 1.07 0.98 0.92 0.86 0.92 0.86 0.91 0.71 0.74 0.36 0.39 0.42 0.43 0.41	0.70 0.78 0.84 0.83 0.94 0.94 0.94 0.94 0.94 0.94 0.94 0.45 0.45	0.71 0.76 0.80 0.79 0.85 0.94 0.84 0.80 0.81 0.81 0.43 0.43 0.45 0.49	- 0.93 - 0.83 - 0.74 - 0.74 - 0.74 - 0.55 - 0.64 - 0.81 - 0.91 -	3 0.96 2 0.90 3 0.83 5 0.77 4 0.73 5 0.77 3 0.68 4 0.56 5 0.61 5 0.61 5 0.62 3 0.82 5 0.79 6 0.82 7 1.66 7 1.89 1 1.72	0.97 0.91 0.84 0.78 0.78 0.69 0.56 0.61 0.67 0.82 0.82 0.82 0.79 VAA 1.96 2.06 1.89	0.95 0.1 0.89 0.1 0.84 0.1 0.85 0.1 0.80 0.1 0.77 0.1 0.73 0.7 0.74 0.7 0.75 0.4 0.50 0.4 0.51 0.4 0.63 0.3 0.54 0.4 0.55 0.4 0.63 0.3 0.57 0.4 56 1.67 1.71 1.6 1.85 1.6 1.85 1.6		- 0.29 - 0.39 - 0.39 - 0.38 - 0.30 - 0.57 - 0.70 - 0.66 - 1.03 - 0.96 - 1.36 - 0.37 - 0.51 - 0.52 - 0.55 -	0.25 0.29 0.33 0.40 0.40 0.35 Sull 0.52 0.61 0.69 0.76 0.72 0.88 0.32 0.42 0.42 0.46 0.57 0.57	SPAR 0.26 0.29 0.33 0.40 0.40 0.40 0.35 0.40 0.73 0.81 0.77 0.94 Xooc 0.33 0.42 0.33	RKLE 0.23 0.25 0.27 0.31 0.31 0.26 0.27 0.31 0.26 0.27 0.31 0.26 0.77 0.65 0.77 dyak 0.34 0.43 0.44 0.54	0.22 0.23 0.24 0.27 0.23 2.0 0.48 0.52 0.56 0.56 0.56 0.56 0.56 0.56 0.56 0.56	0.21 0.23 0.23 0.24 0.44 0.46 0.47 0.48 0.47 0.48 0.47 0.48 0.47 0.33 0.33 0.33 0.33
		64	SAEAES - - <tr tr=""> - -</tr>	- 0.69 - 0.83 - 100 - 101 - 101 - 1.53 - 0.55 - 0.86 - 0.77 - 0.58 - 0.59 - 0.59 - 0.31 - 0.32 - 0.33 - 0.33 - 0.28 - 0.28 - 0.28		rrnin 0.70 0.80 0.90 0.88 1.07 0.98 0.92 0.86 0.81 0.71 0.74 0.36 0.39 0.42 0.43 0.41 0.46	0.70 0.78 0.84 0.83 0.94 0.94 0.94 0.94 0.94 0.94 0.94 0.45 0.43 0.45 0.49	0.71 0.76 0.80 0.79 0.79 0.85 0.84 0.84 0.86 0.84 0.84 0.84 0.81 0.45 0.43 0.46 0.49 0.50 0.42	- 0.8 - 0.7 - 0.5 - 0.5	3 0.96 2 0.90 3 0.83 5 0.77 4 0.77 3 0.68 4 0.77 5 0.77 4 0.77 5 0.61 5 0.61 6 0.61 7 1.66 7 1.89 1 1.72 3 1.78	0.97 0.91 0.84 0.78 0.78 0.99 Spor 0.56 0.61 0.67 0.82 0.82 0.82 0.79 0.82 0.82 1.73 1.84 1.96 2.06 1.89 2.00	0.95 0.1 0.89 0.1 0.84 0.1 0.84 0.1 0.80 0.1 0.80 0.1 0.77 0.1 0.73 0.1 0.74 0.1 0.75 0.4 0.63 0.2 0.63 0.2 0.63 0.2 0.57 0.4 56 1.67 1.71 1.61 1.85 1.4 1.85 1.4 1.85 1.4 1.72 1.2	0.87 0.87 0.88 0.87 0.81 0.82 0.83 0.82 0.83 0.82 0.83 0.82 0.87 0.84 0.87 0.44 88 0.44 99 0.44 99 0.43 99 0.43 90 0.43 91 0.43 92 1.46 92 1.46 1.45 1.45 1.45 1.45	- 0.27 - 0.29 - 0.39 - 0.38 - 0.30 - 0.66 - 1.36 - 1.36 - 0.57 - 0.66 - 1.36 - 0.51 - 0.61 - 0.81 - 0.81 - 0.81	0.25 0.29 0.33 0.40 0.40 0.35 50 0.40 0.52 0.61 0.69 0.76 0.72 0.88 0.32 0.42 0.42 0.46 0.57 0.57	SPAR 0.26 0.29 0.33 0.40 0.40 0.35 0.54 0.73 0.81 0.77 0.94 X000 0.33 0.42 0.46 0.57 0.57	RKLE 0.23 0.25 0.27 0.31 0.31 0.31 0.26 0.27 0.31 0.32 0.31 0.32 0.52 0.59 0.65 0.70 0.65 0.70 0.67 0.77 dyak 0.34 0.43 0.54 0.54	0.22 0.23 0.24 0.27 0.23 2.0 0.48 0.52 0.56 0.56 0.56 0.56 0.56 0.56 0.58 0.56 0.38 0.32 0.38 0.40 0.45 0.45 0.51	0.21 0.23 0.23 0.24 0.44 0.46 0.47 0.48 0.47 0.48 0.47 0.33 0.33 0.33 0.37 0.38 0.41 0.41

Hardware Benchmarking

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

Hardware Benchmarking



Throughput-over-Area for Authenticated Encryption and Decryption of 1536-byte messages at 75MHz by GMU

ACE	Gimli	Oribatida	SPIX
ASCON	Grain-128aead	Photon-Beetle	SpoC
COMET	HyENA	Pyjamask	Spook
DryGascon	ISAP	Romulus	Subterranean
Elephant	KNOT	SAEAES	Sundae-GIFT
ESTATE	LOTUS&LOCUS	Saturnin	TinyJambu
ForkAE	mixFeed	Skinny- AEAD&Hash	Wage
GIFT-COFB	ORANGE	Sparkle	Xoodyak

Round 3

Ongoing (March 2021 --)

Finalists had the opportunity to update submission packages and propose tweaks to submissions.

Evaluation also includes side channel resistance.

ASCON	Elephant	GIFT-COFB	Grain-128aead	ISAP
Photon-Beetle	Romulus	Sparkle	TinyJambu	Xoodyak

Resistance to side-channel attacks



CERG from *George Mason University* proposes a general framework for evaluating side-channel resistance of LWC candidates using resources, experience, and general practices of the cryptographic engineering community developed over the last two decades.

Three calls

- for Side-Channel Security Validation Labs
- for Protected Hardware Implementations, targeting low-cost modern FPGAs
- for Protected Software Implementations, targeting low-cost modern embedded processors.

Lightweight Cryptography Workshop 2022 May 9-11, 2022 (Virtual Event)

#NISTLWC

0000

2015-2018

First workshop Second workshop NISTIR 8114 2020 - 2021

Fourth workshop Round 3 NISTIR 8369

2019

Submissions due Round 1 NISTIR 8268 Round 2 Third workshop 2022

Fifth workshop

Next steps



Evaluation of the finalists



Fifth Lightweight Cryptography Workshop



Selection of the winner(s) and status report publication



Standardization

Thanks!

CONTACT NIST TEAM 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