On the Final Round of the NIST Lightweight Cryptography Standardization

Meltem Sönmez Turan NIST Lightweight Cryptography Team

Security and Implementation of Lightweight Cryptography (SILC) October 16, 2021 – Zagreb, Croatia





Background Evaluation of the Second-round Candidates Final Round Next Steps

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





Background



CONSTRAINED DEVICES

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



e.g., home automation, healthcare,

smart city



LACK OF CRYPTOGRAPHY
STANDARDS

NIST crypto standards are optimized for general-purpose computers

Early Feedback from Academia & Industry

- Two Lightweight Cryptography Workshops at NIST in July 2015 and October 2016.
- In March 2017, NISTIR 8114 Report on Lightweight Cryptography is published.

Profiles for Lightweight Cryptography (white paper)

- Profile | Authenticated Encryption with associated data (AEAD) and hashing for constrained software and hardware environments
- Profile II AEAD for constrained hardware environments





Example Applications



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-tovehicle 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



RESEARCH DEVELOPMENTS

e.g., permutation-based designs, simpler key schedules, inherent side channel resistance



GOAL Develop new guidelines, recommendations and standards optimized for constrained devices

PROCESS

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



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



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

Submission deadline: February 2019



AEAD

- Confidentiality of the plaintexts (under adaptive chosen-plaintext attacks) + Integrity of the ciphertexts (under adaptive forgery attempts)
- At least 128-bit key
- At least 2¹¹² computation for attacks (nonce is assumed to be unique under the same key)
- Family of (at most 10) algorithms
 - One primary member with key ≥ 128 bits, nonce
 ≥ 96 bits and tag ≥ 64 bits
 - Limits on the input sizes for the primary member at least 2⁵⁰-1 bytes

Hash

- Computationally infeasible to find a collision or a (second) preimage. Resistance to length extension attacks. (Attacks requiring at least 2¹¹² computations)
- Digest size at least 256 bits
- Family of (at most 10) algorithms
 - One **primary member** has a hash size of 256 bits.
 - Limits on the input sizes for the primary member at least 2⁵⁰-1 bytes
- Common design components with the AEAD

Design and Implementation Requirements



- Perform significantly better in constrained environments (HW and SW platforms) compared to NIST standards.
- Efficient for short messages
- Implementations that lend themselves to countermeasures against side channel attacks, and fault attacks

56 Round 1 Candidates



FROM 25 COUNTRIES





First Round of the Standardization Process

- Approximately 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 <u>Status Report on the First Round</u> of the NIST Lightweight Cryptography <u>Standardization Process</u> (October 2019)

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



The Second Round

0

Second-Round Candidates









Classification based on Modes*



Sequential

Classical Sponge with Public Permutation ACE, ASCON, DryGASCON, Gimli, KNOT, Spix, Spook,

Subterranean 2.0, WAGE, Xoodyak

Modified Sponge with Public Permutation ORANGE, Oribatida, PHOTON-Beetle, SPARKLE, SpoC

(T)BC-based Feedback with Rate 1 COMET, GIFT-COFB, HyENA, mixFeed, Romulus

Classical Sponge with Secret Permutation SAEAES, TinyJAMBU Enc-then-Mac ISAP, Saturnin

Mac-then-Enc

ESTATE, SUNDAE-GIFT

Stream Cipher Based Grain-128AEAD

Parallel

ForkAE

LOTUS-AEAD & LOCUS-AEAD

OCB3-based SKINNY-AEAD

OCB3-based

Pyjamask

Enc-then-Mac Elephant

* Primary variant only

Common Building Blocks







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

Results – Software Benchmarking



NIST

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

Results – 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 = <u>Execution time of AES-GCM</u>

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			-			CON	1ET					[DryGA	SCON		
_	128 - 2.94	2.71 2	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	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	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	3.25 2.	94 Z.	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
	8 - 3.42	2.07 2	2.90 2.	72 2.	47 2.20		0.56	0.45	0.51	0.49	0.47	0.45	1								6.43	6.88	6.86	7.03	7.24	7.36
		,					_					-			,				,		,	,			-	
	128 - 1.70	1.83	Elepha	nt 93 2.	08 2.09		0.29	0.32	5	0.33	0.36	0.39				Fork	AE		-		0.39	0.38	GIFT-	0.37	0.36	0.34
	64 - 1.57	1.80	1.80 1.	95 2.	16 2.14		0.28	0.37	0.33	0.35	0.38	0.41				-					0.39	0.38	0.37	0.36	0.35	0.33
	32 - 1.89	2.11 2	2.11 2.	26 2.	42 2.31		0.27	.33	0.33	0.36	0.39	0.42			-	-	-	-	-	-	0.39	0.37	0.36	0.36	0.34	0.33
	16 - 1.90	2.17 2	2.16 2.	32 2.	48 2.34		0.7	0.34	0.34	0.37	0.40	0.43	-			-	-	-	-	-	0.38	0.36	0.36	0.35	0.33	0.32
	8 - 1.89	2.17 2	2.16 2.	32 2.	48 2.34		0.26	0.34	0.34	0.37	0.40	0.43	-			-	-		-	-	0.39	0.36	0.36	0.35	0.34	0.32
			AC	<u> </u>	NI.						1	0.44	-		-	-	-	-	-	-	0.58	0.47	0.46	0.42	0.38	0.35
			AS	00									_		·	HyE	NA						IS	ΔP		
0.58	0.53	3 (0.56	C	.54	0.5	52	0.4	19		35	1.31	-		•	-	-	-	-	-	3.11	2.79	2.79	2.62	2.36	2.04
											31	1.27	1			-	-	-			4.53	3.79	3.78	3.38	2.85	2.30
0.60	0.53	3 (0.57	C	.54	0.5	51	0.4	18		28	1.25	1			-				-	6.31	4.83	4.82	4.10	3.25	2.48
											.0	1.23]								8.09	5.74	5.72	4.65	3.53	2.59
0.62	0.52	2 (0.57	0	.54	0.5	51	0.4	17		:3	1.21									12.0	7.47	7.45	5.64	4.01	2.80
																mivE	hood	,			L_,		OPA	NGE		
0.65	0.52	2 (0.58	C).54	0.5	50	0.4	17		0	0.96	0.	47 C).49	0.49	0.47	0.45	0.42	-	0.55	0.58	0.58	0.52	0.51	0.49
											94	1.01	- o.	50 C).53	0.53	0.50	0.46	0.42	-	0.55	0.61	0.61	0.52	0.50	0.47
0.56	0.45	5 (0.51	C	.49	0.4	17	0.4	45)7	1.04	- 0.	54 C).57	0.58	0.53	0.47	0.42	-	0.55	0.63	0.63	0.51	0.49	0.46
											9	1.06	- 0.	58 0	0.61	0.61	0.55	0.48	0.42	-	0.73	0.77	0.77	0.59	0.55	0.50
0.56	0.42	2 (0.51	C	.48	0.4	16	0.4	44)4	1.03	- 0.	58 C	0.61	0.61	0.54	0.47	0.42	-	0.73	0.77	0.77	0.59	0.54	0.50
'	· ·	-	·	-	-					1	2	1.07	- 0.	22 0).52	0.53	0.47	0.42	0.38	1	0.55	0.68	0.68	0.49	0.47	0.45
																De site es							-			
	100 103	1.07	107 1		16 1 22	1	0.92	0.90	0.90	0.89	0.97	0.05	0	0 0	77	Pyjan	nask	0.71	0.67		0.65	0.50	Rom	ulus	0.64	0.69
	128 - 1.03 64 - 1.10	1.07 :	1.07 1. 1.15 1.	11 1. 19 1.	16 1.22 24 1.30		0.92	0.90	0.90	0.89 0.84	0.87	0.85	- 0.	30 C).77).81	0.77 0.81	0.75 0.77	0.71	0.67	-	0.65	0.58	0.58	0.60 0.64	0.64	0.69
	128 - 1.03 64 - 1.10 32 - 1.19	1.07 : 1.15 : 1.23 :	1.07 1. 1.15 1. 1.23 1.	11 1. 19 1. 27 1.	16 1.22 24 1.30 31 1.35		0.92	0.90 0.85 0.79	0.90 0.85 0.78	0.89 0.84 0.79	0.87 0.83 0.79	0.85 0.82 0.79	- 0. - 0.	30 0 37 0 96 0	0.77 0.81 0.85	0.77 0.81 0.85	0.75 0.77 0.77 0.80	0.71 0.72 0.72	0.67 0.66 0.66		0.65	0.58 0.61 0.62	0.58 0.61 0.62	0.60 0.64 0.67	0.64 0.68 0.71	0.69 0.72 0.75
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26	1.07 : 1.15 : 1.23 : 1.30 :	1.07 1. 1.15 1. 1.23 1. 1.30 1.	11 1. 19 1. 27 1. 33 1.	16 1.22 24 1.30 31 1.35 36 1.38		0.92 0.86 0.78 0.70	0.90 0.85 0.79 0.73	0.90 0.85 0.78 0.73	0.89 0.84 0.79 0.75	0.87 0.83 0.79 0.76	0.85 0.82 0.79 0.77	- 0. - 0. - 0.	80 0 87 0 96 0	0.77 0.81 0.85 0.88	0.77 0.81 0.85 0.89	0.75 0.77 0.80 0.81	0.71 0.72 0.72 0.72	0.67 0.66 0.66 0.65	-	0.65	0.58 0.61 0.62 0.53	Rom 0.58 0.61 0.62 0.53	0.60 0.64 0.67 0.60	0.64 0.68 0.71 0.67	0.69 0.72 0.75 0.73
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26	1.07 : 1.15 : 1.23 : 1.30 :	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1.	11 1. 19 1. 27 1. 33 1. 33 1.	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38		0.92 0.86 0.78 0.70 0.71	0.90 0.85 0.79 0.73 0.73	0.90 0.85 0.78 0.73 0.73	0.89 0.84 0.79 0.75 0.75	0.87 0.83 0.79 0.76 0.76	0.85 0.82 0.79 0.77 0.77	- 0. - 0. - 0. - 1.	80 0 87 0 96 0 04 0).77).81).85).88	0.77 0.81 0.85 0.89 0.89	0.75 0.77 0.80 0.81 0.81	0.71 0.72 0.72 0.72 0.72	0.67 0.66 0.66 0.65 0.65	-	0.65 0.73 0.83 0.75 0.75	0.58 0.61 0.62 0.53	Rom 0.58 0.61 0.62 0.53 0.53	0.60 0.64 0.67 0.60 0.60	0.64 0.68 0.71 0.67 0.67	0.69 0.72 0.75 0.73 0.73
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 :	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.14 1.	11 1. 19 1. 27 1. 33 1. 33 1. 22 1.	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38 29 1.34		0.92 0.86 0.78 0.70 0.71 0.55	0.90 0.85 0.79 0.73 0.73 0.65	0.90 0.85 0.78 0.73 0.73 0.65	0.89 0.84 0.79 0.75 0.75 0.69	0.87 0.83 0.79 0.76 0.76 0.73	0.85 0.82 0.79 0.77 0.77 0.75	- 0. - 0. - 0. - 1. 1. - 1.	B0 0 B7 0 D6 0 D4 0 D4 0 22 0).77).81).85).88).88	0.77 0.81 0.85 0.89 0.89 0.95	0.75 0.77 0.80 0.81 0.81 0.83	0.71 0.72 0.72 0.72 0.72 0.73	0.67 0.66 0.65 0.65 0.65	-	0.65 0.73 0.83 0.75 0.75 1.12	0.58 0.61 0.62 0.53 0.53 0.68	Rom 0.58 0.61 0.62 0.53 0.53 0.68	0.60 0.64 0.67 0.60 0.60 0.73	0.64 0.68 0.71 0.67 0.67 0.76	0.69 0.72 0.75 0.73 0.73 0.78
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 :	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.14 1. SAEAE	11 1. 19 1. 27 1. 33 1. 33 1. 22 1. 5	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38 29 1.34		0.92 0.86 0.78 0.70 0.71 0.55	0.90 0.85 0.79 0.73 0.73 0.65	0.90 0.85 0.78 0.73 0.73 0.65 Satu	0.89 0.84 0.79 0.75 0.75 0.69	0.87 0.83 0.79 0.76 0.76 0.73	0.85 0.82 0.79 0.77 0.77	- 0. - 0. - 1. - 1. - 1.	80 0 87 0 96 0 04 0 22 0).77).81).85).88).88).94	0.77 0.81 0.85 0.89 0.89 0.95	0.75 0.77 0.80 0.81 0.81 0.83	0.71 0.72 0.72 0.72 0.72 0.73	0.67 0.66 0.65 0.65 0.65	-	0.65 0.73 0.83 0.75 0.75 1.12	0.58 0.61 0.62 0.53 0.53 0.68	Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF	0.60 0.64 0.67 0.60 0.60 0.73	0.64 0.68 0.71 0.67 0.67 0.76	0.69 0.72 0.75 0.73 0.73 0.78
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 :	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.14 1. SAEAE	11 1. 19 1. 27 1. 33 1. 33 1. 22 1. 5 -	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38 29 1.34		0.92 0.86 0.78 0.70 0.71 0.55	0.90 0.85 0.73 0.73 0.65	0.90 0.85 0.73 0.73 0.65 Satu 0.69	0.89 0.84 0.79 0.75 0.75 0.69 rnin 0.70	0.87 0.83 0.79 0.76 0.76 0.73	0.85 0.82 0.79 0.77 0.77 0.75	- 0. - 0. - 1. - 1. - 1. - 1.	30 0 37 0 96 0 04 0 22 0 98 0	0.77 0.81 0.85 0.88 0.88 0.94 5 0.96	0.77 0.81 0.85 0.89 0.95 <inny 0.97</inny 	0.75 0.77 0.80 0.81 0.81 0.83 -AEAD 0.95	0.71 0.72 0.72 0.72 0.72 0.73 0.73	0.67 0.66 0.65 0.65 0.65	-	0.65 0.73 0.83 0.75 0.75 1.12	0.58 0.61 0.53 0.53 0.68 0.25	Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF 0.26	0.60 0.64 0.67 0.60 0.73 0.73 KLE 0.23	0.64 0.68 0.71 0.67 0.76 0.76	0.69 0.72 0.75 0.73 0.73 0.78
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 :	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.14 1. SAEAE	11 1. 19 1. 27 1. 33 1. 33 1. 22 1. 5 -	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38 29 1.34 - - - - - - - - - -		- 0.92 0.86 0.78 0.70 0.71 0.55 0.69 0.83	0.90 0.85 0.79 0.73 0.65 0.65	0.90 0.85 0.78 0.73 0.73 0.65 Satu 0.69 0.81	0.89 0.84 0.79 0.75 0.75 0.69 rnin 0.70 0.80	0.87 0.83 0.79 0.76 0.76 0.73 0.73	0.85 0.82 0.79 0.77 0.77 0.75	- 0. - 0. - 1. - 1. - 1. - 1. - 0. - 0.	80 0 87 0 96 0 04 0).77).81).85).88).88).94 SH SH SH SH SH SH SH SH SH SH SH SH SH	0.77 0.81 0.85 0.89 0.89 0.95 (INNY 0.97 0.91	0.75 0.77 0.80 0.81 0.81 0.83 -AEAD 0.95 0.89	0.71 0.72 0.72 0.72 0.73 0.73 0.93 0.88	0.67 0.66 0.65 0.65 0.65 0.65	-	0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26	0.58 0.61 0.53 0.53 0.68 0.25 0.29	Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF 0.26 0.29	0.60 0.64 0.67 0.60 0.73	0.64 0.68 0.71 0.67 0.76 0.22 0.22	0.69 0.72 0.75 0.73 0.73 0.78 0.21 0.21
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 64 32 16	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 : - - - -	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.14 1. SAEAE - - -	111 1. 199 1. 277 1. 333 1. 333 1. 222 1. 5 - - -	16 1.22 24 1.30 31 1.35 36 1.38 39 1.34 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -		0.92 0.86 0.78 0.70 0.71 0.55 0.69 0.83 1.00	0.90 0.85 0.79 0.73 0.73 0.65 0.69 0.81 0.93 0.92	0.90 0.85 0.78 0.73 0.73 0.65 5atu 0.69 0.81 0.93 0.92	0.89 0.84 0.79 0.75 0.75 0.69 rnin 0.70 0.80 0.90 0.88	0.87 0.83 0.79 0.76 0.76 0.73 0.73 0.70 0.78 0.84 0.83	0.85 0.82 0.79 0.77 0.77 0.75 0.71 0.76 0.80 0.79	- 0. - 0. - 1. - 1. - 1. - 1. - 0. - 0. - 0.	80 0 87 0 96 0 04 0).77).81).85).88).88).88).88).88).94 ,.94).90).83).77	0.77 0.81 0.85 0.89 0.89 0.95 (INNY 0.97 0.91 0.84 0.78	0.75 0.77 0.80 0.81 0.81 0.83 -AEAD 0.95 0.89 0.84 0.80	0.71 0.72 0.72 0.72 0.73 0.73 0.93 0.88 0.84 0.81	0.67 0.66 0.65 0.65 0.65 0.65 0.91 0.87 0.87		0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29	0.58 0.61 0.53 0.53 0.68 0.25 0.25 0.29 0.33	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.68 SPAF 0.26 0.29 0.33 0.40	0.60 0.64 0.67 0.60 0.60 0.73 , KLE 0.23 0.25 0.27 0.31	0.64 0.68 0.71 0.67 0.76 0.76 0.22 0.23 0.24 0.27	0.69 0.72 0.75 0.73 0.73 0.78 0.21 0.21 0.21 0.23
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 128 126 132 16 8	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 : - - - - - -	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.30 1. 1.30 1.	11 1. 19 1.: 27 1.: 33 1.: 33 1.: 5 - - - - -	16 1.22 24 1.30 31 1.35 36 1.38 29 1.34 - -		0.92 0.86 0.78 0.70 0.71 0.55 0.69 0.83 1.00 1.01	0.90 0.85 0.79 0.73 0.73 0.65 0.81 0.93 0.92	0.90 0.85 0.78 0.73 0.73 0.65 5atu 0.69 0.81 0.93 0.92	0.89 0.84 0.79 0.75 0.75 0.69	0.87 0.83 0.79 0.76 0.76 0.76 0.73 0.84 0.83 0.83	0.85 0.82 0.79 0.77 0.75 0.75 0.71 0.76 0.80 0.79	- 0. - 0. - 1. - 1. - 1. - 1. - 0. - 0. - 0. - 0. - 0. - 0.	80 0 87 0 96 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 95 0 96 0 97 0 97 0).77).81).85).88).94).94).96).96).90).83).77	Pyjan 0.77 0.81 0.85 0.89 0.95 (NNY 0.97 0.91 0.84 0.78	0.75 0.77 0.80 0.81 0.81 0.83 -AEAD 0.95 0.89 0.84 0.80 0.79	0.71 0.72 0.72 0.72 0.72 0.72 0.73 0.93 0.88 0.88 0.84 0.81	0.67 0.66 0.65 0.65 0.65 0.65 0.87 0.87 0.84 0.82		0.65 0.73 0.83 0.75 1.12 0.23 0.26 0.29 0.39	0.58 0.61 0.62 0.53 0.53 0.53 0.25 0.29 0.33 0.40 0.40	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.26 0.29 0.33 0.40 0.40	0.60 0.64 0.67 0.60 0.60 0.73 0.23 0.25 0.27 0.31	0.64 0.68 0.71 0.67 0.67 0.26 0.22 0.23 0.24 0.27 0.27	0.69 0.72 0.75 0.73 0.73 0.73 0.78 0.21 0.21 0.21 0.23
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 128 16 8 16 8 0 - 0.96	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 : - - - - - - - - - -	1.07 1 1.15 1 1.23 1 1.30 1 1.30 1 1.14 1 SAEAE - - - - - - - - -	11 1. 19 1. 17 1. 33 1. 33 1. 5 5 - - - - - - - -	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38 29 1.34 - -		- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53	0.90 0.85 0.79 0.73 0.73 0.65 0.81 0.93 0.92 0.92 1.20	0.90 0.85 0.78 0.73 0.65 0.65 0.81 0.93 0.92 0.92 1.20	0.89 0.84 0.79 0.75 0.75 0.69 0.70 0.80 0.90 0.88 0.88 0.88 1.07	0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.83 0.83	0.85 0.82 0.79 0.77 0.77 0.75 0.75 0.76 0.80 0.79 0.85	- 0. - 0. - 1. - 1. - 1. - 1. - 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0	80 0 87 0 96 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 05 0 07 0 05 0).77).81).85).88).94).94).94).96).90).83).77).77	Pyjan 0.77 0.81 0.85 0.89 0.95 (INNY 0.95 (INNY 0.95 0.91 0.84 0.78 0.78 0.78	0.75 0.77 0.80 0.81 0.81 0.81 0.83 0.83 0.83 0.95 0.89 0.89 0.89 0.79 0.73	0.71 0.72 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.77	0.67 0.66 0.65 0.65 0.65 0.65 0.85 0.81 0.87 0.84 0.82 0.82 0.82		 0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30 	0.58 0.61 0.53 0.53 0.68 0.25 0.29 0.33 0.40 0.40 0.40	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.26 0.29 0.33 0.40 0.40 0.35	UUS 0.60 0.64 0.67 0.60 0.60 0.73 0.23 0.25 0.27 0.31 0.26	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.23	0.69 0.72 0.75 0.73 0.73 0.78 0.21 0.21 0.21 0.23 0.23 0.23 0.20
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 64 32 16 8 8 0	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 : - - - - - - -	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.14 1. SAEAE - - - - - - - - - - - - -	11 1. 19 1. 27 1. 33 1. 33 1. 5 5 - - - - - - -	16 1.22 24 1.30 31 1.35 36 1.38 36 1.38 37 1.34 38 1.38 39 1.34 - -		- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.01	0.90 0.85 0.79 0.73 0.73 0.65 0.81 0.93 0.92 0.92 1.20	0.90 0.85 0.78 0.73 0.73 0.65 5atu 0.69 0.81 0.93 0.92 1.20 5p	0.89 0.84 0.79 0.75 0.75 0.69 rmin 0.70 0.80 0.88 0.88 1.07	0.87 0.83 0.79 0.76 0.76 0.76 0.76 0.78 0.84 0.84 0.83 0.94	0.85 0.82 0.79 0.77 0.75 0.75 0.76 0.80 0.79 0.79 0.79	- 0. - 0. - 1. - 1. - 1. - 1. - 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0.	80 0 96 0 96 0 94 0 94 0 94 0 94 0 92 0 98 0 92 0 93 0 93 0 94 0 95 0 96 0 97 0 98 0 90 0).77).81).85).88).94).94).94).94).94).94).94).95).90).83).77).68	0.77 0.81 0.85 0.89 0.95 0.95 0.95 0.95 0.97 0.97 0.97 0.97 0.97 0.97 0.97 0.97	0.75 0.77 0.80 0.81 0.81 0.83 -AEAC 0.95 0.89 0.84 0.80 0.73 0.73	0.71 0.72 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.77	0.67 0.66 0.65 0.65 0.65 0.91 0.91 0.87 0.82 0.82 0.82		 0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.30 	0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.53 0.25 0.29 0.33 0.40 0.40 0.35	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.53 0.53 0.26 0.29 0.33 0.40 0.40 0.35 0.40	ulus 0.60 0.64 0.67 0.60 0.60 0.73 0.23 0.25 0.27 0.31 0.26 pean 1	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.23	0.69 0.72 0.73 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 64 32 16 8 0 - 0.98 8 16 8 128 128	1.107 : 1.15 : 1.23 : 1.30 : 1.30 : 1.14 : - - - - - - - - - - - - -	1.07 1 1.15 1 1.23 1 1.30 1 1.30 1 1.30 1 1.14 1	11 1. 19 1. 27 1. 33 1. 33 1. 33 1. 5 5 - - - - - - - - - - - - -	16 1.22 1.30 1.35 3.36 1.38 3.36 1.38 3.37 1.38 3.36 1.38 3.37 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.37 1.34 3.36 1.38 3.37 1.34 3.38 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39 1.34 3.39		- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.53 - 1.02	0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.92 0.92 1.20	0.90 0.85 0.73 0.73 0.65 0.81 0.93 0.92 1.20 5p 1.00	0.89 0.84 0.79 0.75 0.75 0.75 0.75 0.75 0.80 0.80 0.88 0.88 1.07 0.02	0.87 0.83 0.79 0.76 0.76 0.76 0.73 0.84 0.83 0.83 0.83 0.94	0.85 0.82 0.79 0.77 0.77 0.75 0.75 0.76 0.80 0.79 0.85	- 0. - 0. - 1. - 1. - 1. - 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0	80 0 37 0 37 0 38 0 30 0	0.77 0.81 0.85 0.88 0.94 0.94 0.94 0.94 0.94 0.94 0.94 0.95 0.77 0.68	0.77 0.81 0.85 0.89 0.95 (INNY 0.97 0.91 0.78 0.78 0.78 0.78 0.78 0.69 5pc 0.56	0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.83 0.89 0.84 0.80 0.79 0.73 0.73	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.77	0.67 0.66 0.65 0.65 0.65 0.87 0.87 0.87 0.84 0.82 0.82 0.82 0.82		0.65 0.73 0.83 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30	0.58 0.61 0.53 0.53 0.53 0.25 0.29 0.33 0.40 0.40 0.35 5.52	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.68 0.29 0.33 0.40 0.40 0.35 0.40 0.35	UUS 0.60 0.64 0.67 0.60 0.60 0.73 0.23 0.25 0.27 0.31 0.26 nean 0.52	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.23 2.0 0.48	0.69 0.72 0.75 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 64 32 16 8 - 0 0 128 - 1.20 64 - 1.20 64 - 1.20 120 - 1.20 1	1.107 : 1.115 : 1.23 : 1.30 : 1.30 : 1.30 : 1.14 : - - - - - - - - - - - - -	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.30 1. 1.30 1. 1.30 1.	111 1. 19 1. 27 1. 33 1. 22 1. 5 5 - - - - - - - - - - - - -	16 1.222 1.301 1.353 3.31 1.353 3.36 1.383 3.36 1.383 3.36 1.383 3.36 1.383 3.36 1.383 3.36 1.383 3.36 1.383 3.37 1.343 3.38 1.343 3.39 1.343 <td></td> <td>- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53 - 1.02 - 0.95</td> <td>0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 0.92 1.20</td> <td>0.90 0.85 0.73 0.73 0.65 0.81 0.93 0.92 0.92 0.92 1.20 5p 1.00 0.93</td> <td>0.89 0.84 0.79 0.75 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.05 0.05 0.92</td> <td>0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.83 0.83 0.94</td> <td>0.85 0.82 0.79 0.77 0.77 0.75 0.75 0.80 0.79 0.85 0.94 0.94 0.94</td> <td>- 0. - 0. - 1. - 1. - 1. - 1. - 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0</td> <td>80 0 337 0 34 0 34 0 34 0 34 0 34 0 35 0</td> <td>0.77 0.81 0.88 0.88 0.94 0.94 0.90 0.90 0.77 0.68 0.77 0.56 0.61</td> <td>0.77 0.81 0.85 0.89 0.89 0.95 (INNY 0.91 0.91 0.91 0.78 0.78 0.78 0.78 0.78 0.56 0.61</td> <td>0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.89 0.89 0.89 0.89 0.89 0.89 0.89 0.89</td> <td>0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.77 0.47 0.47</td> <td>0.67 0.66 0.65 0.65 0.65 0.81 0.81 0.82 0.82 0.80 0.82</td> <td></td> <td> 0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30 0.57 0.57 0.70 </td> <td>0.58 0.61 0.53 0.53 0.25 0.25 0.29 0.33 0.40 0.40 0.40 0.35 Sut 0.52 0.61</td> <td>Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.68 9 0.26 0.29 0.33 0.40 0.40 0.40 0.40 0.40 0.40 0.40</td> <td>0.60 0.64 0.67 0.60 0.60 0.73 0.25 0.27 0.31 0.31 0.31 0.26 nean 0.52 0.59</td> <td>0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.27 0.23 0.24 0.27 0.23</td> <td>0.69 0.72 0.75 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.22 0.23 0.23 0.20</td>		- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.53 - 1.02 - 0.95	0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 0.92 1.20	0.90 0.85 0.73 0.73 0.65 0.81 0.93 0.92 0.92 0.92 1.20 5p 1.00 0.93	0.89 0.84 0.79 0.75 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.05 0.05 0.92	0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.83 0.83 0.94	0.85 0.82 0.79 0.77 0.77 0.75 0.75 0.80 0.79 0.85 0.94 0.94 0.94	- 0. - 0. - 1. - 1. - 1. - 1. - 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0	80 0 337 0 34 0 34 0 34 0 34 0 34 0 35 0	0.77 0.81 0.88 0.88 0.94 0.94 0.90 0.90 0.77 0.68 0.77 0.56 0.61	0.77 0.81 0.85 0.89 0.89 0.95 (INNY 0.91 0.91 0.91 0.78 0.78 0.78 0.78 0.78 0.56 0.61	0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.89 0.89 0.89 0.89 0.89 0.89 0.89 0.89	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.77 0.47 0.47	0.67 0.66 0.65 0.65 0.65 0.81 0.81 0.82 0.82 0.80 0.82		 0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30 0.57 0.57 0.70 	0.58 0.61 0.53 0.53 0.25 0.25 0.29 0.33 0.40 0.40 0.40 0.35 Sut 0.52 0.61	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.68 9 0.26 0.29 0.33 0.40 0.40 0.40 0.40 0.40 0.40 0.40	0.60 0.64 0.67 0.60 0.60 0.73 0.25 0.27 0.31 0.31 0.31 0.26 nean 0.52 0.59	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.27 0.23 0.24 0.27 0.23	0.69 0.72 0.75 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.22 0.23 0.23 0.20
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 64 32 16 8 0 128 - 1.20 64 - 1.22 0 128 - 1.20 64 - 1.22 1.20 64 - 1.22 1.20 64 - 1.22 1.20 64 - 1.22 1.20 64 - 2.22 1.20 64 - 2.22 1.20 7.22 7.22 7.22 7.22 7.22 7.22 7.22 7	1.107 : 1.115 : 1.23 : 1.30 : 1.30 : 1.14 : - - - - - - - - - - - - -	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1. 1.30 1.	111 1. 19 1. 27 1. 33 1. 33 1. 5 5 - - - - - - - - - - - - -	16 1.22 1.30 1.35 3.31 1.35 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.36 1.38 3.37 2.38 3.38 2.38 3.39 2.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39 3.38 3.39		- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.01 - 1.02 - 0.95 - 0.86	0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.93 0.92 0.92 0.92 0.92 0.95 0.86	0.90 0.85 0.78 0.73 0.65 0.81 0.93 0.92 0.92 0.92 1.20 5p 1.00 0.93	0.89 0.84 0.79 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.20 0.98 0.92 0.98	0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.83 0.83 0.94	0.85 0.82 0.77 0.77 0.77 0.75 0.76 0.80 0.79 0.85 0.94 0.85	- 0. - 0. - 0. - 1. - 1. - 1. - 1. - 1. - 1. - 1. - 1	80 0 37 0 37 0 387 0 387 0 400 400 400 400 400 400 400 4	0.77 0.81 0.88 0.88 0.94 0.96 0.90 0.77 0.77 0.68 0.56 0.61 0.67	Pyjan 0.77 0.81 0.85 0.89 0.95 0.95 0.91 0.91 0.78 0.78 0.78 0.78 0.69 0.56 0.61 0.67	0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.83 0.89 0.84 0.80 0.79 0.73 0.73 0.50 0.52 0.52	0.71 0.72 0.72 0.72 0.72 0.73 0.73 0.83 0.84 0.81 0.81 0.81 0.77 0.47 0.47	0.67 0.66 0.65 0.65 0.65 0.87 0.87 0.87 0.82 0.82 0.82 0.82 0.80		 0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.57 0.57 0.70 0.86 	0.58 0.61 0.62 0.53 0.68 0.25 0.29 0.33 0.40 0.40 0.35 Sut 0.52 0.51 0.52	Rom 0.58 0.61 0.62 0.53 0.63 0.53 0.68 SPAF 0.29 0.33 0.40 0.35 Otherral 0.54 0.54 0.54	0.60 0.64 0.67 0.60 0.73 0.73 0.25 0.27 0.31 0.26 0.31 0.26 0.52 0.52	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.23 0.24 0.27 0.27 0.23 0.23 0.24 0.52 0.56	0.69 0.72 0.75 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 64 32 16 8 0 128 - 1.20 64 - 1.42 32 - 1.70 16 - 1.99	1.07 : 1.15 : 1.23 : 1.30 : 1.10 : 1.10 : 1.12 : 1.10 : 1.23 : 1.13 : 1.23 : 1.14 : 1.23 : 1.14 : 1.23 : 1.24 : 1.25 : 1.26 :	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.30 1.	111 1. 19 1. 27 1. 33 1. 33 1. 5 - - - - - - - - - - - - -	16 1.22 1.30 1.35 36 1.38 36 1.38 36 1.38 37 1.35 38 1.38 39 1.38 30 1.38 31 1.35 33 1.38 36 1.38 36 1.38 36 1.38 36 1.38 36 1.38 36 1.38 36 1.38 37 - 38 - 39 - 30 - 31 0.92 31 0.94 31 0.94 31 0.94 31 0.94		- 0.92 - 0.86 - 0.78 - 0.70 - 0.71 - 0.55 - 0.69 - 1.01 - 1.01 - 1.02 - 0.95 - 0.86 - 0.95 - 0.86 - 0.77	0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 1.20 0.92 1.20 0.95 0.86 0.75 0.67	0.90 0.85 0.73 0.73 0.65 Satu 0.93 0.92 0.92 1.20 5p 1.00 0.93 0.86 0.80	0.89 0.84 0.79 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.88 0.88 0.88 0.88 0.88 0.88 0.90 0.88 0.90 0.88 0.90 0.88	0.87 0.83 0.79 0.76 0.76 0.73 0.84 0.83 0.84 0.83 0.94 0.96 0.91 0.86 0.83	0.85 0.82 0.79 0.77 0.75 0.75 0.80 0.80 0.79 0.80 0.89 0.84 0.84	- 0. 0. - 0. 0. - 1. 1. - 1. 1. - 1. 1. - 1. 1. - 1. 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0	80 0 337 0 96 0 024 0 024 0 024 0 033 0 0333 0 0333 0 0333 0 0333 0 03558 0 03559 0 0566 0).77).81).85).88).94).94).94).94).94).94).94).94	Pyjan 0.77 0.81 0.85 0.89 0.95 (INNY 0.95 0.91 0.84 0.78 0.78 0.78 0.78 0.69 5pc 0.61 0.67 0.82	0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.95 0.89 0.84 0.80 0.73 0.73 0.73 0.50 0.52 0.54 0.63	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.77 0.48 0.49 0.54	0.67 0.66 0.65 0.65 0.65 0.81 0.87 0.84 0.82 0.82 0.82 0.82 0.84 0.44 0.44		 0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.38 0.30 0.57 0.70 0.86 1.03 	0.58 0.61 0.62 0.53 0.68 0.25 0.29 0.33 0.40 0.35 0.40 0.35 Sut 0.52 0.61 0.69 0.76	Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF 0.26 0.29 0.33 0.40 0.35 0.40 0.35 0.40 0.35 0.54 0.73 0.81	0.60 0.64 0.67 0.60 0.73 0.25 0.27 0.31 0.26 0.27 0.31 0.26 0.52 0.59 0.65 0.70	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.23 0.23 0.24 0.25 0.56 0.58	0.69 0.72 0.75 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.23 0.20 0.44 0.44 0.46 0.47 0.48
	1228 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 128 16 8 16 128 - 1.20 16 128 - 1.20 16 128 - 1.20 16 - 1.42 32 - 1.10 16 - 1.42 32 - 1.10 16 - 1.42 32 - 1.10 16 - 1.20 17 - 1.10 18 - 1.20 18 1.20 19 - 1.20 19 - 1.20 10 - 1.20 1	1.07 : 1.15 : 1.23 : 1.30 : 1.30 : 1.30 : 1.30 : 1.30 : 1.14 :	L107 L L15 L L23 L L30 L L30 L L30 L L30 L L34 L SAEAE - - - - - - - - - - - - -	111 1. 119 1. 27 1. 33 1. 33 1. 22 1. 5 - - - - - - - - - - - - -	16 1.22 130 1.35 331 1.35 336 1.38 336 1.38 336 1.38 337 1.35 338 1.38 339 1.34 330 1.38 331 1.35 336 1.38 336 1.38 336 1.38 336 1.38 336 1.38 336 1.38 337 1.34 337 1.34 337 1.34 337 1.34 337 1.34 337 1.34 337 1.34 337 1.34 337 1.34 338 1.34 339 1.34 339 1.34 339 1.34 331 1.34 331 1.34 331 1.34		- 0.92 - 0.86 - 0.78 - 0.70 - 0.55 - 0.69 - 0.83 - 1.00 - 1.01 - 1.53 - 1.02 - 0.95 - 0.86 - 0.77 - 0.86 - 0.77 - 0.55	0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 0.92 1.20 0.95 0.86 0.75 0.67	0.90 0.85 0.73 0.73 0.65 0.81 0.93 0.92 0.92 1.20 0.92 1.20 0.93 0.86 0.86 0.80	0.89 0.84 0.79 0.75 0.75 0.69 rrnin 0.70 0.80 0.88 0.88 1.07 0.98 0.98 0.92 0.86 0.81 0.71	0.87 0.83 0.79 0.76 0.76 0.76 0.78 0.84 0.83 0.83 0.94 0.94 0.96 0.91 0.86 0.83 0.76	0.85 0.82 0.79 0.77 0.75 0.75 0.80 0.80 0.79 0.85 0.84 0.84 0.84	- 0. 0. - 0. 0. - 1. 1. - 1. 1. - 1. 1. - 1. 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0	800 0 837 0 996 0 996 0 997 0 998 0 992 0 993 0 994 0 995 0 997 0 998 0 997 0 998 0 997 0 998 0 997 0 998 0 998 0 998 0 998 0 998 0 998 0 998 0 998 0 998 0 998 0 998 0).77).81).85).88).94).94).94).94).94).94).95).97).83).77).68).97).68).61).66).61).62).82	0.77 0.81 0.85 0.89 0.95 0.95 (INNY 0.97 0.91 0.84 0.78 0.78 0.78 0.78 0.56 0.61 0.67 0.82 0.82	0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.83 0.84 0.80 0.79 0.73 0.73 0.50 0.52 0.52 0.54 0.63 0.63	0.71 0.72 0.72 0.72 0.72 0.73 0.88 0.84 0.81 0.81 0.81 0.77 0.48 0.49 0.54	0.67 0.66 0.65 0.65 0.65 0.65 0.87 0.87 0.82 0.82 0.82 0.82 0.82 0.82 0.82 0.84 0.44 0.44 0.44		0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.38 0.30 0.38 0.30 0.57 0.57 0.86 1.03 0.96	0.58 0.61 0.53 0.53 0.25 0.29 0.33 0.40 0.35 0.40 0.35 0.52 0.61 0.69 0.76	Rom 0.58 0.61 0.62 0.53 0.63 SPAF 0.26 0.29 0.33 0.40 0.40 0.35 Oterra 0.54 0.54 0.64 0.73 0.81 0.77	0.60 0.64 0.67 0.60 0.73 0.25 0.27 0.31 0.26 0.52 0.52 0.59 0.65 0.70	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.23 0.23 0.23 0.24 0.25 0.56 0.58	0.69 0.72 0.75 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 64 32 16 8 16 8 128 - 1.20 64 - 1.20 16 8 128 128 128 16 8 128 16 8 128 16 8 128 16 8 128 16 10	1.107 : 1.15 : 1.23 : 1.30 : 1.30 : 1.30 : 1.30 : 1.30 : 1.31 : 1.31 : 1.32 : 1.32 : 1.32 : 1.33 : 1.33 : 1.34 : 1.35 : 1.55 : 1.55 : 1.15 : 1.10	L07 L L15 L L13 L L30 L L3	111 1. 119 1. 27 1. 33 1. 33 2. 22 1. 5 - - - - - - - - - - - - -	16 1.22 130 1.35 131 1.35 136 1.38 137 1.38 138 1.38 139 1.38 139 1.38 139 1.38 139 1.38 139 1.38 139 1.38 139 1.38 130 1.38 130 1.38 130 1.38 130 1.38 130 1.38 131 1.38 131 1.38 131 1.39 131 1.39 131 1.39 131 1.39 131 1.39 131 1.39 131 1.39 131 1.39 132 1.39		 0.92 0.86 0.78 0.70 0.71 0.55 0.69 0.83 1.00 1.01 1.01 1.01 1.02 0.95 0.86 0.77 0.58 0.59 0.58 0.59 	0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 1.20 0.92 1.20 0.95 0.86 0.75 0.67 0.54	0.90 0.85 0.73 0.73 0.65 0.81 0.93 0.93 0.92 1.20 5p 1.00 0.93 0.86 0.80 0.86 0.80	0.89 0.84 0.79 0.75 0.75 0.69 7min 0.80 0.80 0.80 0.88 1.07 0.98 0.98 0.92 0.86 0.81 0.71 0.74	0.87 0.83 0.79 0.76 0.76 0.73 0.78 0.84 0.83 0.84 0.83 0.94 0.94 0.94 0.91 0.86 0.91 0.86 0.83 0.76 0.79	0.85 0.82 0.77 0.77 0.77 0.75 0.80 0.80 0.80 0.84 0.84 0.81	- 0. 0. - 0. 0. - 1. 1. - 1. 1. - 1. 1. - 1. 1. - 0. - 0. - 0. - 0. - 0. - 0. - 0. - 0	80 0 87 0 996 0 996 0 997 0 998 0 998 0 998 0 997 0 998 0 998 0 998 0 997 0 998 <t< td=""><td>),77),81),88),88),94 (5)),96),96),90),83),77),83),77),83),77),66),61),67),82),82),79</td><td>0.77 0.81 0.85 0.89 0.95 (INNY 0.97 0.91 0.84 0.78 0.78 0.78 0.56 0.69 5pc 0.56 0.61 0.67 0.82 0.82</td><td>0.75 0.77 0.80 0.81 0.83 0.83 0.83 0.83 0.83 0.89 0.84 0.80 0.79 0.73 0.50 0.52 0.52 0.52 0.54 0.63 0.63</td><td>0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.77 0.48 0.49 0.54 0.54 0.54</td><td>0.67 0.66 0.65 0.65 0.65 0.91 0.87 0.82 0.82 0.82 0.82 0.82 0.82 0.82 0.82</td><td></td><td>0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.23 0.29 0.39 0.38 0.30 0.57 0.70 0.86 1.03 0.96 1.36</td><td>0.58 0.61 0.53 0.53 0.29 0.33 0.40 0.35 0.40 0.35 0.40 0.52 0.61 0.52 0.61 0.69 0.76 0.72</td><td>Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF 0.26 0.29 0.33 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.40 0.53 0.53 0.68 0.77 0.94 0.77 0.94</td><td>0.60 0.64 0.67 0.60 0.73 0.23 0.25 0.27 0.31 0.26 0.52 0.59 0.65 0.70 0.67</td><td>0.64 0.68 0.71 0.67 0.22 0.23 0.24 0.23 0.24 0.27 0.23 0.24 0.23 0.24 0.52 0.56 0.56 0.51</td><td>0.69 0.72 0.75 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49</td></t<>),77),81),88),88),94 (5)),96),96),90),83),77),83),77),83),77),66),61),67),82),82),79	0.77 0.81 0.85 0.89 0.95 (INNY 0.97 0.91 0.84 0.78 0.78 0.78 0.56 0.69 5pc 0.56 0.61 0.67 0.82 0.82	0.75 0.77 0.80 0.81 0.83 0.83 0.83 0.83 0.83 0.89 0.84 0.80 0.79 0.73 0.50 0.52 0.52 0.52 0.54 0.63 0.63	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.77 0.48 0.49 0.54 0.54 0.54	0.67 0.66 0.65 0.65 0.65 0.91 0.87 0.82 0.82 0.82 0.82 0.82 0.82 0.82 0.82		0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.23 0.29 0.39 0.38 0.30 0.57 0.70 0.86 1.03 0.96 1.36	0.58 0.61 0.53 0.53 0.29 0.33 0.40 0.35 0.40 0.35 0.40 0.52 0.61 0.52 0.61 0.69 0.76 0.72	Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF 0.26 0.29 0.33 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.40 0.53 0.53 0.68 0.77 0.94 0.77 0.94	0.60 0.64 0.67 0.60 0.73 0.23 0.25 0.27 0.31 0.26 0.52 0.59 0.65 0.70 0.67	0.64 0.68 0.71 0.67 0.22 0.23 0.24 0.23 0.24 0.27 0.23 0.24 0.23 0.24 0.52 0.56 0.56 0.51	0.69 0.72 0.75 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49
	1228 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 32 16 8 16 8 16 8 128 - 1.20 64 - 1.42 32 - 1.70 16 - 1.42 32 - 1.42 17 - 1.42 18 - 1.42 19 - 1.42 1	1.107 : 1.15 : 1.130 : 1.130 : 1.130 : 1.14 : - - - - - - - - - - - - -	1.07 1. 1.15 1. 1.23 1. 1.30 1. 1.3	11 1. 19 1. 27 1. 33 1. 22 2.	1.22 1.30 24 1.30 311 1.35 323 1.38 329 1.34 329 1.34 32 1.34 32 1.34 32 1.34 33 1.38 34 1.38 35 1.38 36 1.38 37 - 38 - 39 - 311 0.94 308 0.92 311 0.94 39 - 30 - 31 0.92 32 - 33 - 34 0.95 30 -		 0.92 0.86 0.78 0.70 0.71 0.55 0.69 0.83 1.00 1.01 1.01 1.01 1.02 0.95 0.86 0.77 0.58 0.59 	0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.93 0.92 0.92 1.20 0.95 0.86 0.75 0.67 0.54 0.53	0.90 0.85 0.78 0.73 0.65 0.81 0.93 0.92 0.92 1.00 0.93 0.86 0.80 0.86 0.80 0.67 0.70	0.89 0.84 0.79 0.75 0.69 0.80 0.90 0.88 0.88 1.07 0.90 0.88 0.92 0.86 0.92 0.86 0.92 0.86 0.81 0.71 0.74	0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.84 0.83 0.94 0.94 0.96 0.91 0.86 0.83 0.76 0.79	0.85 0.82 0.79 0.77 0.77 0.75 0.76 0.80 0.79 0.85 0.89 0.85 0.84 0.84 0.80 0.81		80 0 87 0 96 0 94 0 94 0 94 0 94 0 94 0 95 0 98 0 933 0 933 0 933 0 95 0 96 0 97 0 98 0 98 0 98 0 98 0 98 0 98 0 98 0 98 0 98 0 98 0 98 0),77),81),88),88),94 (5)),90),88),90),88),90),88),90),88),77),77),68 (6)),61),65 (7)),82),82),82	Pyjan 0.77 0.81 0.85 0.89 0.95 0.95 0.95 0.95 0.97 0.97 0.97 0.84 0.78 0.78 0.78 0.78 0.78 0.78 0.69 0.61 0.65 0.61 0.62 0.82 0.82 0.82	0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.83 0.89 0.84 0.80 0.79 0.73 0.73 0.52 0.54 0.63 0.63 0.57 0.57 0.57 0.57	0.71 0.72 0.72 0.72 0.72 0.73 0.88 0.84 0.81 0.81 0.81 0.81 0.81 0.47 0.44 0.49 0.54 0.54	0.67 0.66 0.65 0.65 0.65 0.87 0.84 0.82 0.82 0.82 0.82 0.82 0.44 0.44 0.44 0.44 0.44		0.65 0.73 0.83 0.75 0.75 1.12 0.26 0.29 0.39 0.39 0.38 0.30 0.57 0.70 0.86 1.03 0.96 1.03	0.58 0.61 0.53 0.53 0.25 0.29 0.33 0.40 0.35 0.40 0.35 0.52 0.61 0.69 0.76 0.72 0.88	Rom 0.58 0.61 0.62 0.53 0.53 0.68 SPAF 0.26 0.29 0.33 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.40 0.54 0.54 0.54 0.54 0.54 0.53 0.54 0	0.60 0.64 0.67 0.60 0.73 0.23 0.25 0.27 0.31 0.25 0.27 0.31 0.26 0.52 0.59 0.65 0.70 0.65 0.77 0.77	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.23 0.23 0.23 0.56 0.56 0.56 0.56	0.69 0.72 0.75 0.73 0.73 0.73 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 128 16 8 16 8 129 128 128 128 128 128 128 128 129 128 129 129 129 129 129 129 129 129 129 129 129 129 128 129 128 128 129 128 128 129 128 129 128 129 128 129 128 129 128 129 128 128 129 128 128 129 128 129 128 129 128 128 128 128 129 129 129 129 129 129 129 129 129 129 129 129 129 129 129 129	1.107 : 1.15 : 1.130 : 1.130 : 1.130 : 1.14 : - - - - - - - - - - - - -	1.07 1 1.15 1 1.23 1 1.30 1 1.44 1 1.44 1 1.44 1 1.467 1 1.40	11 1. 19 1. 27 1. 33 1. 22 1. 5 - - - - - - - - - - - - -	1.222 1.30 24 1.30 313 1.35 36 1.38 36 1.38 37 - - </td <td></td> <td>- 0.92 0.86 0.78 0.70 0.71 0.55 - 0.69 0.83 - 1.00 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58 - 0.59 - 0.58 - 0.59 - 0.58 - 0.59 - 0.55 - 0.59 - 0.55 - 0.59 - 0.55 - 0.55 -</td> <td>0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.92 0.92 1.20 0.95 0.86 0.75 0.67 0.54 0.53 0.31 0.31</td> <td>0.90 0.85 0.78 0.73 0.65 5atu 0.93 0.92 0.92 1.20 5p 1.00 0.93 0.86 0.80 0.67 0.70 Tiny]3</td> <td>0.89 0.84 0.79 0.75 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.90 0.88 0.90 0.88 0.90 0.88 0.92 0.86 0.92 0.86 0.81 0.71 0.71 0.74</td> <td>0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.94 0.96 0.91 0.86 0.91 0.86 0.91 0.86 0.91 0.83 0.76 0.79</td> <td>0.85 0.82 0.79 0.77 0.77 0.75 0.80 0.80 0.79 0.85 0.86 0.84 0.84 0.84 0.84 0.81</td> <td></td> <td>80 0 96 0 96 0 94 0 94 0 92 0 98 0 998 0</td> <td>0.77 0.81 0.88 0.94 0.96 0.90 0.83 0.77 0.68 0.61 0.67 0.82 0.82 0.82 0.79 0.82</td> <td>Pyjan 0.77 0.81 0.85 0.89 0.95 0.82 0.79 0.73 0.73 0.73 0.82 0.73 0.73 0.73 0.75</td> <td>0.75 0.77 0.80 0.81 0.83 0.83 0.83 0.83 0.95 0.84 0.80 0.79 0.73 0.84 0.80 0.73 0.50 0.52 0.52 0.54 0.63 0.63 0.57 GE 1.67</td> <td>0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.81 0.47 0.47 0.44 0.49 0.54 0.54 0.54 0.54 0.54</td> <td>0.67 0.66 0.65 0.65 0.65 0.87 0.81 0.82 0.82 0.82 0.82 0.82 0.82 0.82 0.82</td> <td></td> <td>0.65 0.73 0.83 0.75 0.75 1.12 0.29 0.39 0.39 0.38 0.30 0.57 0.70 0.86 1.03 0.96 1.36</td> <td>0.58 0.61 0.62 0.53 0.53 0.25 0.25 0.29 0.33 0.40 0.40 0.35 0.52 0.61 0.69 0.76 0.72 0.88 0.52 0.32 0.42</td> <td>Rom 0.58 0.61 0.62 0.53 0.53 0.68 0.29 0.33 0.40 0.40 0.33 0.40 0.40 0.35 0.54 0.64 0.77 0.94 X.000 0.33</td> <td>Ulus 0.60 0.64 0.67 0.60 0.73 0.23 0.25 0.27 0.31 0.26 0.52 0.59 0.65 0.70 0.67 0.77 1yak 0.34 0.34</td> <td>0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.23 0.24 0.23 0.56 0.56 0.58 0.56 0.56</td> <td>0.69 0.72 0.75 0.73 0.73 0.73 0.78 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.20 0.20 0.20 0.20 0.20</td>		- 0.92 0.86 0.78 0.70 0.71 0.55 - 0.69 0.83 - 1.00 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58 - 0.59 - 0.58 - 0.59 - 0.58 - 0.59 - 0.55 - 0.59 - 0.55 - 0.59 - 0.55 -	0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.92 0.92 1.20 0.95 0.86 0.75 0.67 0.54 0.53 0.31 0.31	0.90 0.85 0.78 0.73 0.65 5atu 0.93 0.92 0.92 1.20 5p 1.00 0.93 0.86 0.80 0.67 0.70 Tiny]3	0.89 0.84 0.79 0.75 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.90 0.88 0.90 0.88 0.90 0.88 0.92 0.86 0.92 0.86 0.81 0.71 0.71 0.74	0.87 0.83 0.79 0.76 0.76 0.73 0.70 0.78 0.84 0.83 0.94 0.96 0.91 0.86 0.91 0.86 0.91 0.86 0.91 0.83 0.76 0.79	0.85 0.82 0.79 0.77 0.77 0.75 0.80 0.80 0.79 0.85 0.86 0.84 0.84 0.84 0.84 0.81		80 0 96 0 96 0 94 0 94 0 92 0 98 0 998 0	0.77 0.81 0.88 0.94 0.96 0.90 0.83 0.77 0.68 0.61 0.67 0.82 0.82 0.82 0.79 0.82	Pyjan 0.77 0.81 0.85 0.89 0.95 0.82 0.79 0.73 0.73 0.73 0.82 0.73 0.73 0.73 0.75	0.75 0.77 0.80 0.81 0.83 0.83 0.83 0.83 0.95 0.84 0.80 0.79 0.73 0.84 0.80 0.73 0.50 0.52 0.52 0.54 0.63 0.63 0.57 GE 1.67	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.81 0.47 0.47 0.44 0.49 0.54 0.54 0.54 0.54 0.54	0.67 0.66 0.65 0.65 0.65 0.87 0.81 0.82 0.82 0.82 0.82 0.82 0.82 0.82 0.82		0.65 0.73 0.83 0.75 0.75 1.12 0.29 0.39 0.39 0.38 0.30 0.57 0.70 0.86 1.03 0.96 1.36	0.58 0.61 0.62 0.53 0.53 0.25 0.25 0.29 0.33 0.40 0.40 0.35 0.52 0.61 0.69 0.76 0.72 0.88 0.52 0.32 0.42	Rom 0.58 0.61 0.62 0.53 0.53 0.68 0.29 0.33 0.40 0.40 0.33 0.40 0.40 0.35 0.54 0.64 0.77 0.94 X.000 0.33	Ulus 0.60 0.64 0.67 0.60 0.73 0.23 0.25 0.27 0.31 0.26 0.52 0.59 0.65 0.70 0.67 0.77 1yak 0.34 0.34	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.23 0.24 0.23 0.56 0.56 0.58 0.56 0.56	0.69 0.72 0.75 0.73 0.73 0.73 0.78 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.20 0.20 0.20 0.20 0.20
	$\begin{array}{c} 128 \\ 64 \\ -1.10 \\ 32 \\ -1.19 \\ 16 \\ -1.26 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ $	1.07 : 1 1.15 : 1 1.23 : 1 1.30 : 1 1.30 : 1 1.30 : 1 1.30 : 1 1.30 : 1 1.30 : 1 1.14 : 1 - - - - - - - - - - - - -	107 1. 115 1. 123 1. 130 1.	11 1. 1. 19 1. 27 1. 33 1. 22 1. 5 - - - - - - - - - - - - -	1 1.22 1 1.33 1 1.33 1 1.33 1 1.33 1 1.33 1 1.33 1 1.33 1 1.33 1 1.34 1 1.34 1 0.94 1 0.94 1 0.94 1 0.94 1 0.94 1 0.94 1 0.94 1 0.94 1 0.95 1 0.94 1 0.95 1 0.95 1 0.95 1 0.95 1 0.95 1 0.95		 0.92 0.86 0.78 0.70 0.71 0.55 0.69 0.83 1.00 1.01 1.53 1.02 0.86 0.77 0.58 0.59 0.31 0.32 0.33 	0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.93 0.92 0.92 1.20 0.92 0.92 0.92 0.92 0.92 0.92 0.92 0	0.90 0.85 0.78 0.73 0.65 5atu 0.93 0.92 0.92 1.20 0.92 1.20 0.93 0.86 0.80 0.67 0.70 TinyJa 0.34 0.36	0.89 0.84 0.79 0.75 0.75 0.69 0.80 0.80 0.88 0.88 1.07 0.88 0.92 0.88 0.92 0.86 0.92 0.86 0.92 0.86 0.92 0.81 0.71 0.74 4 0.74 4 0.74	0.87 0.83 0.79 0.76 0.76 0.78 0.84 0.83 0.83 0.94 0.95 0.91 0.86 0.91 0.86 0.91 0.86 0.91 0.83 0.76 0.91 0.83 0.76	0.85 0.82 0.79 0.77 0.75 0.75 0.80 0.79 0.80 0.79 0.85 0.84 0.84 0.84 0.84 0.81 0.81	- 0 0 - 0 0 - 1 1 - 1 1 - 1 1 - 1 1 - 1 1 - 1 1 - 0 0 - 0 -	80 0 96 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 95 0 95 0 95 0 95 0 95 0 95 0 96 0 98 0 98 0 98 0 99 1 99 1 99 1	0.77 0.81 0.88 0.88 0.94 5 0.94 0.95 0.94 0.95 0.9	Pyjan 0.77 0.81 0.89 0.89 0.95 (INNY 0.95 0.91 0.91 0.78 0.78 0.78 0.78 0.78 0.78 0.69 Spo 0.61 0.67 0.82 0.82 0.82 0.79 WA 1.73 1.84 1.96	0.75 0.77 0.80 0.81 0.83 0.83 0.83 0.83 0.83 0.83 0.83 0.83	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.81 0.81 0.81 0.81 0.81	0.67 0.66 0.65 0.65 0.91 0.81 0.82 0.82 0.82 0.82 0.82 0.82 0.44 0.44 0.44 0.44 0.44 0.44 0.44 1.47 1.46 1.46		0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30 0.37 0.57 0.57 0.57 0.51 1.36	0.58 0.61 0.62 0.53 0.53 0.29 0.29 0.33 0.40 0.40 0.40 0.40 0.40 0.40 0.52 0.61 0.72 0.61 0.72 0.88 0.72 0.88	Rom 0.58 0.61 0.62 0.53 0.68 SPAF 0.26 0.29 0.33 0.40 0.40 0.40 0.35 0.40 0.40 0.35 0.40 0.40 0.35 0.41 0.77 0.94 Xooc 0.33 0.42 0.46	Ulus 0.60 0.64 0.67 0.60 0.73 0.23 0.25 0.27 0.31 0.26 0.31 0.26 0.52 0.59 0.65 0.70 0.67 0.77 1yak 0.34 0.34 0.34	0.64 0.68 0.71 0.67 0.22 0.23 0.24 0.27 0.27 0.23 0.24 0.52 0.56 0.56 0.56 0.56 0.51 0.32 0.38 0.340	0.69 0.72 0.75 0.73 0.73 0.78 0.78 0.21 0.21 0.23 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.48 0.47 0.48 0.47
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 1.26 8 - 1.26 0 - 0.96 128 16 32 16 8 0 128 - 1.20 8 16 22 - 1.20 64 - 1.22 2 - 1.70 16 - 1.22 1.70 16 - 1.29 8 - 1.20 0 - 2.35 0 - 2	1.107 :: 1.115 :: 1.23 :: 1.30 :: 3.30 :: 3	107 1. 115 1. 123 1. 130 1.	11 1. 19 1. 27 1. 33 1. 22 1. 5 - - - - - - - - - - - - -	1.22 1.33 1.33 1.33 1.33 1.33 1.33 1.33 1.33 1.33 1.34 1.35 1.34 1.34 1.34 1.34 1.34 1.34 1.35 1.34 1.34 1.35 1.34 1.35 1.34 1.35 1.36 1.34 1.35 1.34 1.35 1.34 1.35 1.36 1.36 1.37 1.38 1.38 1.39 1.39 1.30 1.31 1.31 1.31 1.31 1.32 1.32 1.32 1.31 1.32		 0.92 0.86 0.71 0.55 0.69 0.71 0.55 0.69 0.83 1.00 1.01 1.53 0.86 0.77 0.58 0.59 0.86 0.77 0.58 0.59 0.31 0.32 0.33 0.33 	0.90 0.85 0.79 0.73 0.65 0.69 0.81 0.93 0.92 0.92 1.20 0.92 0.92 0.92 0.92 0.95 0.86 0.75 0.64 0.75 0.54 0.53 0.31 0.31	0.90 0.85 0.78 0.73 0.65 Satu 0.69 0.81 0.93 0.92 1.20 0.92 1.20 0.92 1.20 0.92 1.20 0.92 1.00 0.92 0.92 1.00 0.92 0.92 0.92 0.92 1.00 0.93 0.92 0.92 0.92 1.00 0.93 0.92 0.92 0.92 0.92 1.00 0.93 0.93 0.92 0.92 0.92 0.92 0.92 0.92 0.93 0.93 0.92 0.92 0.92 0.92 0.93 0.93 0.92 0.92 0.92 0.93 0.93 0.92 0.92 0.93 0.93 0.92 0.92 0.92 0.93 0.92 0.92 0.92 0.93 0.93 0.92 0.92 0.92 0.92 0.93 0.93 0.92 0.92 0.93 0.93 0.92 0.92 0.92 0.93 0.93 0.93 0.92 0.92 0.93 0.93 0.93 0.92 0.92 0.93 0.93 0.93 0.93 0.93 0.93 0.93 0.93	0.89 0.84 0.79 0.75 0.69 0.80 0.80 0.80 0.88 0.88 1.07 0.88 0.90 0.88 0.90 0.88 0.90 0.88 0.92 0.86 0.92 0.86 0.81 0.71 0.74 0.74 0.36 0.36	0.87 0.83 0.79 0.76 0.76 0.73 0.78 0.84 0.83 0.94 0.94 0.94 0.95 0.94 0.95 0.95 0.79 0.39 0.39 0.39 0.39	0.85 0.82 0.79 0.77 0.75 0.75 0.80 0.79 0.79 0.79 0.85 0.80 0.84 0.84 0.84 0.84 0.81 0.81	- 0. 0 - 0. 0 - 1. 1 - 1. 1	80 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 94 0 95 0 95 0 95 0 95 0 95 0 95 0 95 0 95 0 95 0 95 0 96 0 97 1 99 1 99 1 99 1 99 1 10 1	0.777 0.81 0.88 0.88 0.94	Pyjan 0.77 0.81 0.89 0.89 0.95 (INNY 0.97 0.91 0.97 0.91 0.97 0.91 0.84 0.78 0.78 0.78 0.69 0.69 0.61 0.62 0.82 0.82 0.82 0.82 1.73 1.84 1.96 2.06	nask 0.75 0.77 0.80 0.81 0.83 0.83 0.83 0.83 0.83 0.84 0.80 0.79 0.73 0.84 0.80 0.79 0.73 0.57 0.52 0.54 0.63 0.63 0.57 GE 1.67 1.74 1.81	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.81 0.81 0.81 0.47 0.44 0.54 0.54 0.54 0.54 0.54 0.54 0.54	0.67 0.66 0.65 0.65 0.87 0.87 0.82 0.82 0.82 0.82 0.82 0.82 0.82 0.82		0.65 0.73 0.83 0.75 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30 0.38 0.30 0.38 0.30 0.38 0.30 0.38 0.30 0.33 0.30 0.33 0.30 0.33 0.30 0.35 0.30 0.35 0.30 0.35 0.30 0.35 0.30 0.35 0.30 0.35 0.35	0.58 0.61 0.53 0.53 0.25 0.29 0.33 0.40 0.33 0.40 0.35 0.40 0.35 0.52 0.61 0.72 0.88 0.72 0.88	Rom 0.58 0.61 0.62 0.53 0.68 SPAF 0.26 0.29 0.33 0.40 0.33 0.40 0.35 0.40 0.35 0.40 0.40 0.35 0.40 0.40 0.35 0.40 0.54 0.57	Ulus 0.60 0.64 0.67 0.60 0.73 0.23 0.23 0.23 0.23 0.25 0.27 0.31 0.26 0.31 0.26 0.52 0.52 0.70 0.65 0.70 0.67 0.77 Jyak 0.34 0.34 0.34	0.64 0.68 0.71 0.67 0.22 0.23 0.24 0.27 0.27 0.23 0.24 0.52 0.56 0.56 0.56 0.56 0.56 0.56 0.56 0.56	0.69 0.72 0.75 0.73 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49 0.33 0.37 0.38 0.41
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 2.2 22 - - 16 - - 32 - - 16 - - 22 - - 16 - - 22 - - 16 - - 128 1.20 - 64 - - 128 1.20 - 64 - - 128 1.20 - 16 1.99 8 1.85 0 - - - 128 0.41 - - 128 0.41 - - 12 0.47 - - 12 0.47 - - 12 0.47 - -	1.107 :: 1.123 :: 1.300 :: 1.130 :: 1.130 :: 1.144 :: - - - - - - - - - - - - -	107 1. 113 1. 113 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 5SREAE	11 1. 19 1. 27 1. 33 1. 2 2. 5 - - - - - - - - - - - - -	10 1.22 1.3 1.35 3.6 1.38 3.6 1.38 3.6 1.38 2.9 1.34 2.9 1.34 2.9 1.34 3.9 1.38 3.9 1.34		- 0.92 0.86 0.78 0.70 0.71 0.55 0.83 - 0.09 - 0.101 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58 - 0.59 - 0.59 - 0.59 - 0.31 - 0.32 - 0.33 - 0.32 - 0.33 - 0.32	0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 0.92 1.20 0.92 0.92 0.92 0.92 0.93 0.95 0.86 0.75 0.67 0.54 0.53 0.54 0.53 0.54 0.53	0.90 0.85 0.73 0.73 0.65 Satu 0.93 0.92 0.92 1.20 1.20 0.92 1.20 0.92 0.92 0.92 0.92 0.92 0.92 0.92 0	0.89 0.84 0.79 0.75 0.69 0.75 0.80 0.80 0.80 0.88 0.88 1.07 0.88 0.90 0.88 0.90 0.88 0.90 0.88 0.90 0.88 0.92 0.86 0.92 0.86 0.81 0.71 0.71 0.72 0.93 0.92 0.84 0.73 0.75 0.75 0.90 0.88 0.90 0.90	0.87 0.83 0.79 0.76 0.76 0.78 0.84 0.83 0.84 0.83 0.94 0.94 0.94 0.94 0.94 0.94 0.91 0.86 0.91 0.83 0.94 0.91 0.83 0.94 0.91 0.83 0.91 0.91 0.91 0.91 0.91 0.91 0.91 0.91	0.85 0.77 0.77 0.77 0.75 0.76 0.80 0.79 0.88 0.88 0.88 0.84 0.85 0.84 0.85	- 0. 0. - 0. 0. - 1. 1. - 1. 1. - 1. 1. - 1. 1. - 1. 1. - 0. 0. - 0. 0. 0. - 0. 0. 0. - 0. 0. 0. - 0. 0. 0. 0. - 0. 0. 0. 0. - 0. 0. 0. 0. - 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.	80 0 37 0 37 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 052 0 058 0 058 0 056 0 088 0 088 0 099 1 1223 1 1223 1	0.77 0.81 0.85 0.88 0.94	Pyjan 0.77 0.81 0.83 0.89 0.95 VINNY 0.97 0.91 0.84 0.78 0.78 0.78 0.78 0.76 0.78 0.79 0.82 0.79 0.82 0.79 0.71 1.73	nask 0.75 0.77 0.80 0.81 0.81 0.83 0.83 0.83 0.83 0.84 0.89 0.84 0.89 0.84 0.89 0.84 0.89 0.84 0.89 0.73 0.73 0.65 0.52 0.52 0.52 0.52 0.52 0.52 0.52 0.5	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.77 0.48 0.47 0.47 0.44 0.54 0.54 0.54 0.54 0.54 0.54 1.56	0.67 0.66 0.65 0.65 0.87 0.81 0.87 0.84 0.82 0.82 0.82 0.82 0.82 0.44 0.44 0.44 0.44 0.44 1.45 1.46 1.45 1.40		0.65 0.73 0.83 0.75 0.75 0.75 0.75 0.26 0.29 0.39 0.38 0.30 0.38 0.30 0.38 0.30 0.38 0.30 0.38 0.30 0.30	0.58 0.61 0.53 0.53 0.29 0.33 0.40 0.33 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.35 0.40 0.52 0.52 0.52 0.52 0.52 0.52 0.52 0.5	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.26 0.23 0.40 0.33 0.40 0.35 obterra 0.54 0.54 0.77 0.94 Xooc 0.33 0.42 0.46 0.57	ulus 0.60 0.64 0.67 0.60 0.73 0.25 0.27 0.31 0.25 0.31 0.25 0.31 0.26 0.52 0.52 0.52 0.70 0.65 0.70 0.67 0.77 typek 0.34 0.34 0.34	0.64 0.68 0.71 0.67 0.22 0.23 0.24 0.27 0.27 0.23 0.27 0.23 0.52 0.56 0.56 0.56 0.56 0.56 0.56 0.56 0.56	0.69 0.72 0.75 0.73 0.73 0.21 0.21 0.21 0.21 0.23 0.23 0.20 0.44 0.46 0.47 0.48 0.47 0.49 0.33 0.33 0.33 0.33
	128 - 1.03 64 - 1.10 32 - 1.19 16 - 2.26 32 - - 16 - - 32 - - 16 - - 16 - - 16 - - 16 - - 16 1.20 - 64 - - 128 1.20 - 64 1.42 - 128 1.85 - 0 - - 128 0.41 - 64 0.43 - 32 0.47 - 16 0.50 -	1.107 : : 1.123 : : 1.300 : : 1.130 : : 1.130 : : 1.140 : : 1.140 : : 1.123 : : 1.146 : : 1.148 : :	107 1. 113 1. 123 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 130 1. 5SREAE 5SPLX 5SPLX 114 1. 129 1. 144 1. 129 1. 144 1. 129 1. 144 1. 157 1. 148 1. 157 1. 148 1. 157 1. 148 1. 157 1.	11 1 1 11 1 127 1 133 1 134 1 1	10 1.22 1.3 1.35 3.3 1.35 3.3 1.35 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.3 1.38 3.4 1.38 3.5 1.38 3.5 1.56 3.5 1.56 3.5 1.56		- 0.92 0.86 0.78 0.70 0.55 0.69 0.83 - 1.00 - 1.01 - 1.53 - 0.95 - 0.86 - 0.77 - 0.58 - 0.95 - 0.86 - 0.77 - 0.58 - 0.95 - 0.83 - 0.95 - 0.86 - 0.73 - 0.95 - 0.86 - 0.73 - 0.95 - 0.83 - 0.95 - 0.95 - 0.86 - 0.73 - 0.55 - 0.69 - 0.55 - 0.69 - 0.55 - 0.69 - 0.55 - 0.55 - 0.55 - 0.55 - 0.85 - 0.95 - 0.86 - 0.95 - 0.86 - 0.77 - 0.55 - 0.86 - 0.77 - 0.55 - 0.86 - 0.77 - 0.55 - 0.31 - 0.32 - 0.33 - 0.28 - 0.33 - 0.32 - 0.35 - 0.35 - 0.32 - 0.33 - 0.28 - 0.35 - 0.32 - 0.33 - 0.28 - 0.35 - 0.32 - 0.33 - 0.28 - 0.35 - 0.32 - 0.35 - 0.35 - 0.32 - 0.35 -	0.90 0.85 0.79 0.73 0.65 0.81 0.93 0.92 0.92 0.92 0.92 0.95 0.86 0.75 0.86 0.75 0.86 0.75 0.54 0.54 0.53 0.54 0.53 0.54 0.53	0.90 0.85 0.73 0.73 0.65 0.81 0.93 0.92 0.92 1.20 0.93 0.86 0.80 0.67 0.70 TinyJa 0.36 0.36 0.36 0.38	0.89 0.84 0.79 0.75 0.69 0.80 0.80 0.88 0.88 1.07 0.98 0.92 0.88 0.92 0.88 0.92 0.88 0.92 0.88 0.92 0.88 0.92 0.84 0.92 0.92 0.93 0.92 0.93 0.92 0.93 0.92 0.93 0.92 0.93 0.92 0.93 0.92 0.93 0.92 0.93 0.94 0.94 0.90 0.90 0.90 0.90 0.90 0.90	0.87 0.83 0.79 0.76 0.76 0.78 0.84 0.83 0.84 0.83 0.94 0.94 0.94 0.91 0.86 0.91 0.86 0.91 0.86 0.91 0.83 0.76 0.79 0.43 0.79 0.43 0.44 0.45 0.44	0.85 0.82 0.77 0.77 0.77 0.75 0.80 0.80 0.80 0.80 0.89 0.85 0.84 0.89 0.84 0.84 0.84 0.81 0.81 0.81 0.81	- 0 0 - 0 0 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	80 0 37 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 04 0 054 0 058 0 056 0 0588 0 0888 0 080 1 099 1 123 1 121 1 1258 1	0.77 0.81 0.85 0.88 0.94 54 0.96 0.90 0.83 0.77 0.68 0.61 0.61 0.61 0.62 0.83 0.85 0.75 0.85 0.75 0.85 0.75 0.	Pyjan 0.77 0.81 0.83 0.89 0.95 (INNY 0.97 0.91 0.84 0.78 0.78 0.78 0.78 0.78 0.69 500 0.61 0.67 0.82 0.82 0.82 0.82 1.73 1.84 1.96 2.06 1.89 2.00	nask 0.75 0.77 0.80 0.81 0.83 0.83 0.89 0.84 0.89 0.89 0.89 0.89 0.89 0.89 0.89 0.89	0.71 0.72 0.72 0.72 0.73 0.93 0.88 0.84 0.81 0.81 0.81 0.81 0.81 0.81 0.81 0.81	0.67 0.66 0.65 0.65 0.65 0.87 0.87 0.84 0.82 0.82 0.82 0.82 0.82 0.82 0.84 0.44 0.44 0.44 0.44 0.447 0.447 1.445 1.46 1.45 1.40 1.38		0.65 0.73 0.75 1.12 0.23 0.26 0.29 0.39 0.38 0.30 0.57 0.70 0.38 1.03 0.36 1.03 0.36 1.03 0.36 1.03 0.57 0.51 0.37 0.51 0.51 0.51 0.51 0.51 0.51 0.32 0.37 0.55 0.39 0.38 0.55 0.39 0.39 0.38 0.30 0.55 0.39 0.39 0.39 0.39 0.39 0.39 0.39 0.39	0.58 0.61 0.53 0.53 0.29 0.33 0.40 0.35 Sut 0.52 0.61 0.69 0.76 0.72 0.88 0.72 0.88 0.72 0.42 0.42 0.42 0.57 0.57 0.74	Rom 0.58 0.61 0.62 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.53 0.26 0.29 0.33 0.40 0.33 0.54 0.64 0.77 0.94 Xoood 0.33 0.42 0.46 0.57 0.57 0.74	ulus 0.60 0.64 0.67 0.60 0.73 0.25 0.27 0.31 0.25 0.31 0.25 0.31 0.26 0.77 0.85 0.70 0.65 0.70 0.67 0.77 dyak 0.34 0.34 0.34 0.34 0.34	0.64 0.68 0.71 0.67 0.76 0.22 0.23 0.24 0.27 0.27 0.23 0.24 0.52 0.56 0.58 0.56 0.58 0.56 0.58 0.56 0.51	0.69 0.72 0.73 0.73 0.73 0.21 0.21 0.21 0.23 0.23 0.23 0.23 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 0.33 0.33

Hardware Benchmarking



Initiative	Platforms	Metrics				
		Resource utilization (LUT or LE, flip-flops)				
GMU CERG group	Xilinx Artix-7 Intel Cyclone 10 I P	Maximum clock frequency (MHz)				
Give entre group	Lattice Semiconductor ECP5	Throughput (Mbits/s)				
		Energy per bit (nJ/bit)				
		Area (μm^2 and GE)				
Khairallah et al	TSMC 65nm	Clock period (ns) Power (mW)				
Khananan et al.	FDSOI 28nm					
		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)				

Results – Hardware Benchmarking



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

Additional Features



- Nonce is assumed to be unique. Misuse resistance is a plus.
- Post quantum security is not included in the call.
 - Most symmetric-key algorithms are believed to be secure against quantum threats. Best generic attack: Grover's algorithm (quadratic speedup over exhaustive search)
 - Ascon, Gimli, Saturnin address the issue in their specification
 - Six candidates with large key sizes: DryGascon, Knot, SAEAES, Sparkle, Spook, TinyJambu.
- Complexity of recovering the key from the internal state is not mentioned in the call.
 - Keyed initialization and finalization makes it hard to recover the key.
- Status updates and the tweak plans were also considered.
 - e.g., Increasing/decreasing number of rounds, new functionality, internal changes
- Diversity of the finalists + current NIST standards

Challenges of Evaluation



- Large number of candidates:
 - 32 family of algorithms (89 AEAD, 19 hash variants). Evaluation mostly done on *primary variants*.
- Limited resources:
 - Mostly relies on third-party analysis.
 - Not all algorithms get the same attention.
- The industry need is not clear.
 - too specific vs. too broad
- Assigning weights for different criteria:
 - Different security claims (nonce misuse, RUP security, side channel resistance, etc.), different functionality (AEAD, hash, XOF etc.), attacks with different complexities

Evaluation strategy





Selecting the Finalist

27

• Evaluation of the second-round candidates took around 20 months (from Aug. 2019 to March 2021).

Two workshops

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

In March 2021, NIST announced 10 finalists:

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

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





Finalist	Building Block	Mode	#variants	Key size	Nonce size	Tag size
Ascon	Permutation	Monkey dublex	3 aead 4 hash	128-160	128	128
Elephant	Permutation	Enc-then-MAC	3 aead	128	96	64-128
Gift-COFB	Block cipher	Combined feedback	1 aead	128	128	128
Grain-128aead	Stream cipher	-	1 aead	128	96	64
ISAP	Permutation	Enc-then-MAC	4 aead	128	128	128
Photon-beetle	Permutation	Combined feedback	2 aead 1 hash	128	128	128
Romulus	Tweakable BC	Mac-then-Enc	3 aead 1 hash	128	128	128
Sparkle	Permutation	Duplex	4 aead 2 hash	128-256	128-256	128
TinyJambu	Keyed Permutation	Duplex	3 aead	128-256	96	64
Xoodyak	Permutation	Cyclist	1 aead 1 hash	128	128	128







Evaluation of the finalists



Fifth Lightweight Cryptography Workshop(~May 9-11, 2022)



Selection of the winner(s) and publication of the report



Standardization

Timeline





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

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

