Published in ASecuritySite: When Bob Met Alice

Prof Bill Buchanan OBE Follow
Feb 7 · 5 min read · ✦ · ▶ Listen

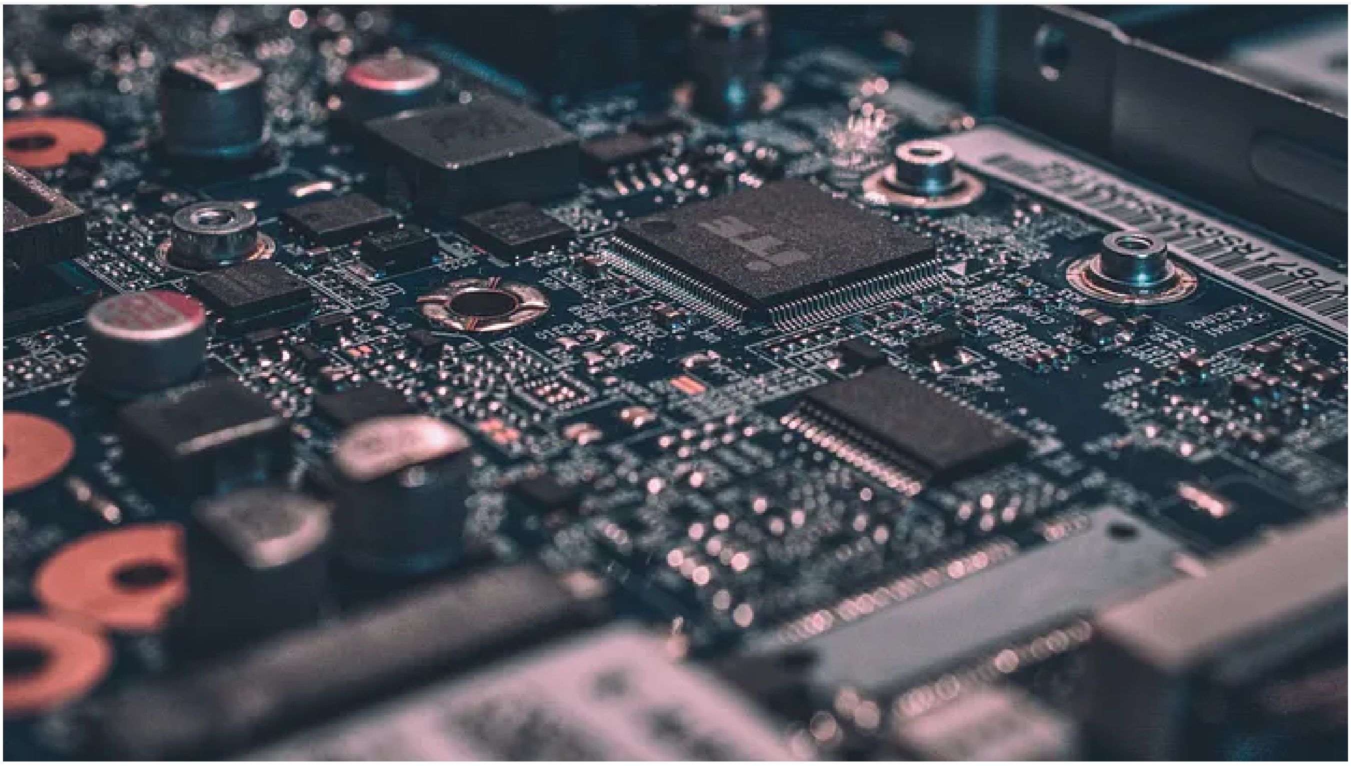
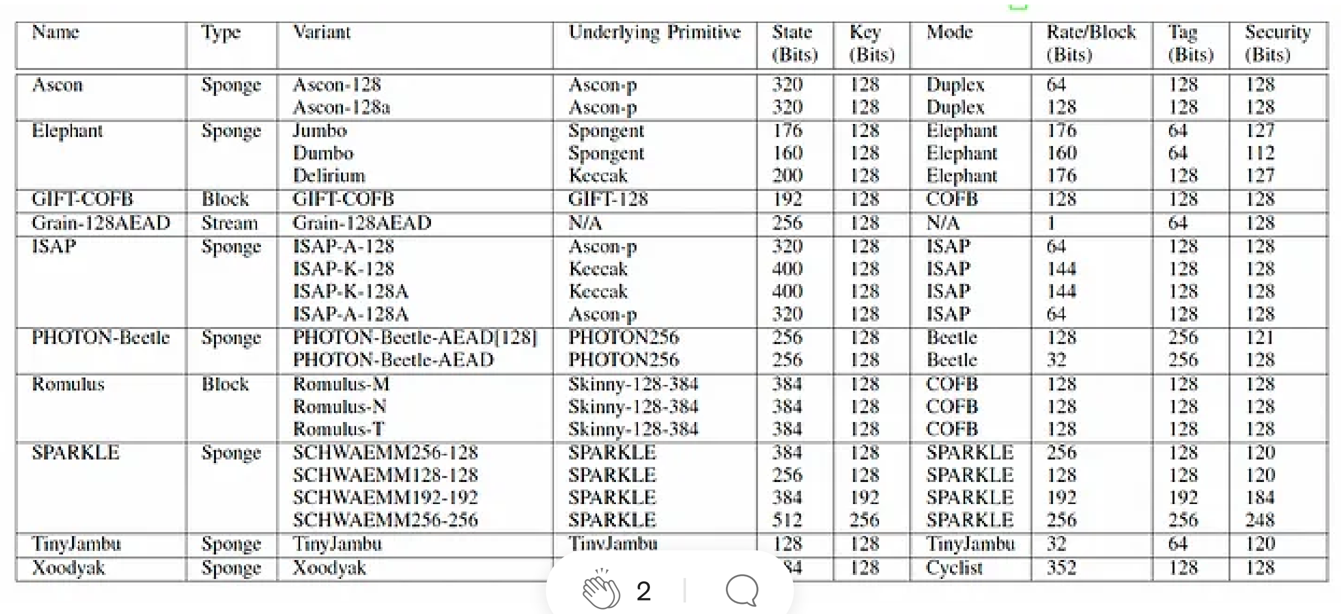


Photo by Alexandre Debiève on Unsplash

ASCON is a Light-weight Champion

Snce 2016, NIST has been assessing light-weight encryption methods, and, in 2022, NIST published the final 10: ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, and Xoodyak (Table 1). A particular focus is on the security of the methods, along with their performance on low-cost FPGAs/embedded processes and their robustness against side-channel attacks.



Name	Type	Variant	Underlying Primitive	State (Bits)	Key (Bits)	Mode	Rate/Block (Bits)	Tag (Bits)	Security (Bits)
Ascon	Sponge	Ascon-128	Ascon-p	320	128	Duplex	64	128	128
		Ascon-128a	Ascon-p	320	128	Duplex	128	128	128
Elephant	Sponge	Jumbo	Spongent	176	128	Elephant	176	64	127
		Dumbo	Spongent	160	128	Elephant	160	64	112
		Delirium	Keccak	200	128	Elephant	176	128	127
GIFT-COFB	Block	GIFT-COFB	GIFT-128	192	128	COFB	128	128	128
Grain-128AEAD	Stream	Grain-128AEAD	N/A	256	128	N/A	1	64	128
ISAP	Sponge	ISAP-A-128	Ascon-p	320	128	ISAP	64	128	128
		ISAP-K-128	Keccak	400	128	ISAP	144	128	128
		ISAP-K-128A	Keccak	400	128	ISAP	144	128	128
		ISAP-A-128A	Ascon-p	320	128	ISAP	64	128	128
PHOTON-Beetle	Sponge	PHOTON-Beetle-AEAD[128]	PHOTON256	256	128	Beetle	128	256	121
		PHOTON-Beetle-AEAD	PHOTON256	256	128	Beetle	32	256	128
Romulus	Block	Romulus-M	Skinny-128-384	384	128	COFB	128	128	128
		Romulus-N	Skinny-128-384	384	128	COFB	128	128	128
		Romulus-T	Skinny-128-384	384	128	COFB	128	128	128
SPARKLE	Sponge	SCHWAEMM256-128	SPARKLE	384	128	SPARKLE	256	128	120
		SCHWAEMM128-128	SPARKLE	256	128	SPARKLE	128	128	120
		SCHWAEMM192-192	SPARKLE	384	192	SPARKLE	192	192	184
		SCHWAEMM256-256	SPARKLE	512	256	SPARKLE	256	256	248
TinyJambu	Sponge	TinyJambu	TinyJambu	128	128	TinyJambu	32	64	120
Xoodyak	Sponge	Xoodyak	[illegible]	[illegible]84	128	Cyclist	352	128	128

Table 1: Specifications of the NIST LWC finalist algorithms [3]

ASCON

Today, NIST has finally announced a winner for its Lightweight champion: ASCON [here]. Generally, it does well in most tests and is a good all-rounder. ASCON [4] was designed by Christoph Dobraunig, Maria Eichlseder, Florian Mendel and Martin Schläffer from Graz University of Technology, Infineon Technologies, and Radboud University. It is both a lightweight hashing and encryption method.

ASCON uses a single lightweight permutation with Sponge-based modes of operation and an SPN (substitution–permutation network) permutation. Overall it has an easy method of implementing within hardware (2.6 gate equivalents) and software. A 5-bit S-box (as used in Keccak's S-box core) is used to enable a light-weight approach and it has no known side-channel attacks. It can also achieve high throughputs such as throughputs of between 4.9 and 7.3 Gbps. It stores its current state with 320 bits. The code is here:

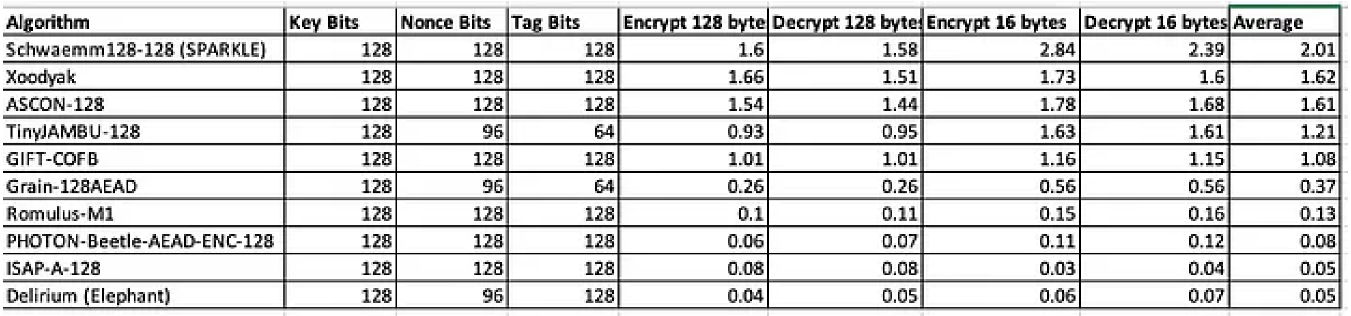
https://asecuritysite.com/light/lw_ascon

Evaluations

The current set of benchmarks includes running on an Arduino Uno R3 (AVR ARmega 328P — Figure 1), Arduino Nano Every (AVR ARmega 4809), Arduino MKR Zero (ARM Cortex M10+) and Arduino Nano 33 BLE (ARM Cortex M4F). These are just 8-bit processors and fit into an Arduino board. Along with their processing limitations, they are also limited in their memory footprint (to run code and also store it). The lightweight cryptography method must thus overcome these limitations and still, be secure and provide a good performance level. Running AES in block modes on these devices is often not possible, as there are insufficient resources. Overall we use a benchmark for encryption — with AEAD (Authenticated Encryption with Additional Data) and for hashing. With AEAD we add extra information — such as the session ID — into the encryption process. This type of method can bind the encryption to a specific stream.

ARM Cortex M3

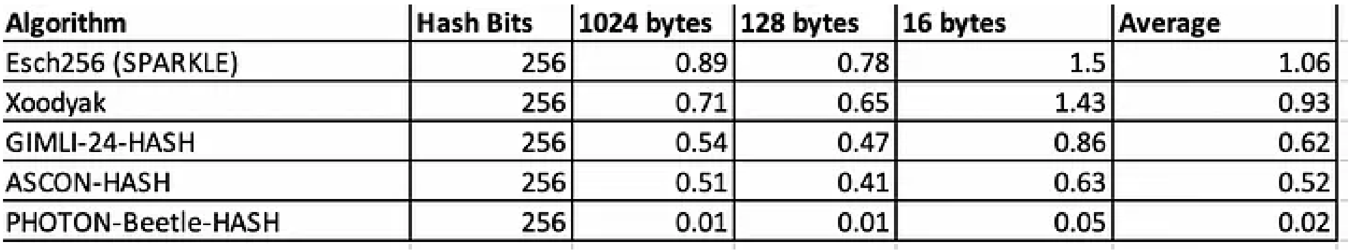
In Table 2 [1], we see a sample run using an Arduino Due with an ARM Cortex M3 running at 84MHz. The tests are taken in comparison with the ChaCha20 stream cipher and defined for AEAD, and where the higher the value, the better the performance. We can see that Sparkle, Xoodyak, and **ASCON** are the fastest of all. Sparkle has a 100% improvement, and Xoodyak gives a 60% increase in speed over ChaCha20. Elephant, ISAP and PHOTON-Beetle have the worst performance for encryption (with around 1/20th of the speed of ChaCha20).



Algorithm	Key Bits	Nonce Bits	Tag Bits	Encrypt 128 byte	Decrypt 128 byte	Encrypt 16 bytes	Decrypt 16 bytes	Average
Schwaemm128-128 (SPARKLE)	128	128	128	1.6	1.58	2.84	2.39	2.01
Xoodyak	128	128	128	1.66	1.51	1.73	1.6	1.62
ASCON-128	128	128	128	1.54	1.44	1.78	1.68	1.61
TinyJAMBU-128	128	96	64	0.93	0.95	1.63	1.61	1.21
GIFT-COFB	128	128	128	1.01	1.01	1.16	1.15	1.08
Grain-128AEAD	128	96	64	0.26	0.26	0.56	0.56	0.37
Romulus-M1	128	128	128	0.1	0.11	0.15	0.16	0.13
PHOTON-Beetle-AEAD-ENC-128	128	128	128	0.06	0.07	0.11	0.12	0.08
ISAP-A-128	128	128	128	0.08	0.08	0.03	0.04	0.05
Delirium (Elephant)	128	96	128	0.04	0.05	0.06	0.07	0.05

Table 2: Arduino Due with an ARM Cortex M3 running at 84MHz for encryption against ChaCha20 [1]

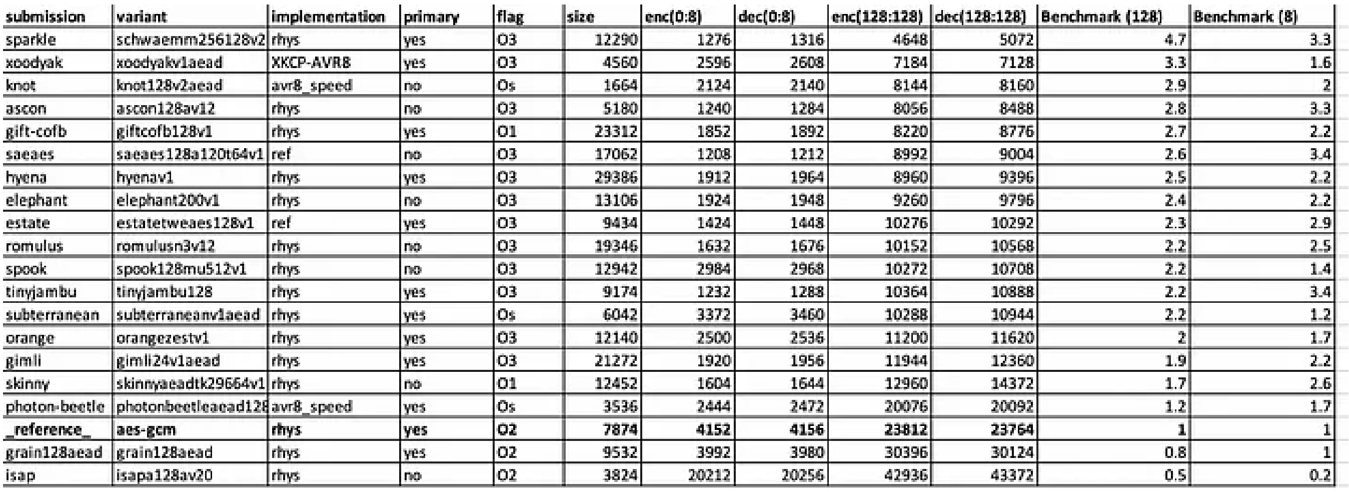
Not all of the finalists can do hash functions. Table 3 outlines these, of which ASCON is not quite as fast, but isn’t too far behind SPARKE and Xoodyak.



Algorithm	Hash Bits	1024 bytes	128 bytes	16 bytes	Average
Esch256 (SPARKLE)	256	0.89	0.78	1.5	1.06
Xoodyak	256	0.71	0.65	1.43	0.93
GIMLI-24-HASH	256	0.54	0.47	0.86	0.62
ASCON-HASH	256	0.51	0.41	0.63	0.52
PHOTON-Beetle-HASH	256	0.01	0.01	0.05	0.02

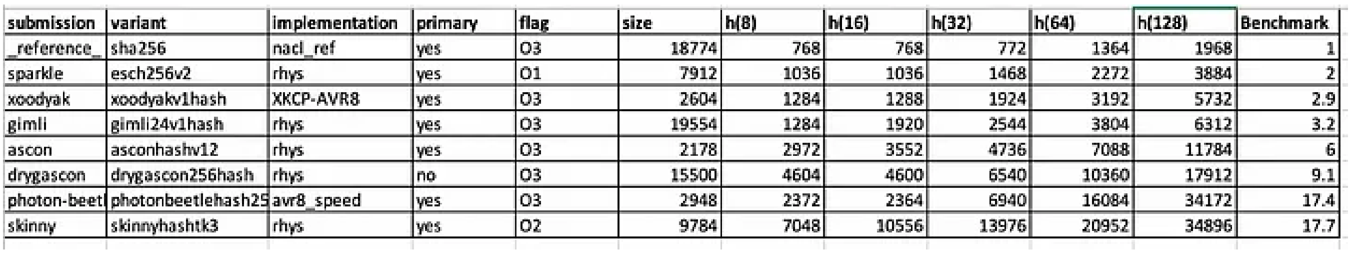
Table 3: Arduino Due with an ARM Cortex M3 running at 84MHz for hashing against BLAKE2s [1]

Again, we see Sparkle and Xoodyak in the lead, with Sparkle actually faster in the test than BLAKE2s, and Xoodyak just a little bit slower. **ASCON** has a weaker performance, and PHOTON-Beetle is relatively slow. For all the tests, the ranking for authenticated encryption is (and where the higher the rank, the better):



submission	variant	implementation	primary	flag	size	enc(0:8)	dec(0:8)	enc(128:128)	dec(128:128)	Benchmark (128)	Benchmark (8)
sparkle	schwaemm256128v2	rhys	yes	O3	12290	1276	1316	4648	5072	4.7	3.3
xoodyak	xoodyakv1aead	XKCP-AVR8	yes	O3	4560	2596	2608	7184	7128	3.3	1.6
knot	knot128v2aead	avr8_speed	no	Os	1664	2124	2140	8144	8160	2.9	2
ascon	ascon128av12	rhys	no	O3	5180	1240	1284	8056	8488	2.8	3.3
gift-cofb	giftcofb128v1	rhys	yes	O1	23312	1852	1892	8220	8776	2.7	2.2
saeaes	saeaes128a120t64v1	ref	no	O3	17062	1208	1212	8992	9004	2.6	3.4
hyena	hyenav1	rhys	yes	O3	29386	1912	1964	8960	9396	2.5	2.2
elephant	elephant200v1	rhys	no	O3	13106	1924	1948	9260	9796	2.4	2.2
estate	estatetweaes128v1	ref	yes	O3	9434	1424	1448	10276	10292	2.3	2.9
romulus	romulusn3v12	rhys	no	O3	19346	1632	1676	10152	10568	2.2	2.5
spook	spook128mu512v1	rhys	no	O3	12942	2984	2968	10272	10708	2.2	1.4
tinyjambu	tinyjambu128	rhys	yes	O3	9174	1232	1288	10364	10888	2.2	3.4
subterranean	subterraneanv1aead	rhys	yes	Os	6042	3372	3460	10288	10944	2.2	1.2
orange	orangezestv1	rhys	yes	O3	12140	2500	2536	11200	11620	2	1.7
gimli	gimli24v1aead	rhys	yes	O3	21272	1920	1956	11944	12360	1.9	2.2
skinny	skinnyaeadtk29664v1	rhys	no	O1	12452	1604	1644	12960	14372	1.7	2.6
photon-beetle	photonbeetleaead128	avr8_speed	yes	Os	3536	2444	2472	20076	20092	1.2	1.7
reference	**aes-gcm**	**rhys**	**yes**	**O2**	**7874**	**4152**	**4156**	**23812**	**23764**	**1**	**1**
grain128aead	grain128aead	rhys	yes	O2	9532	3992	3980	30396	30124	0.8	1
isap	isapa128av20	rhys	no	O2	3824	20212	20256	42936	43372	0.5	0.2

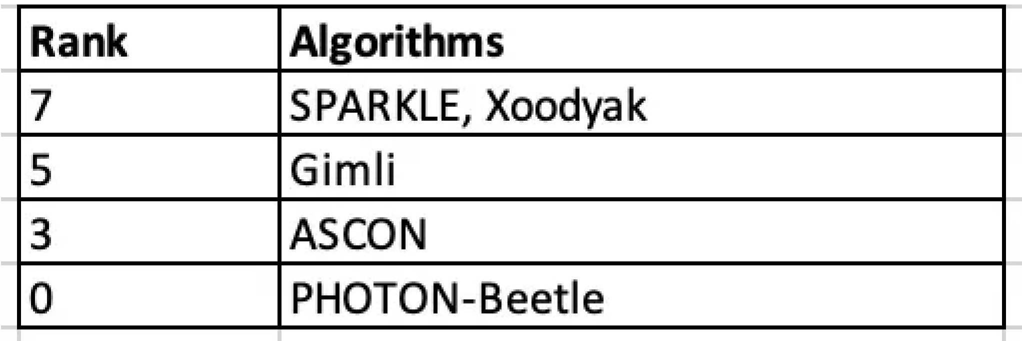
and for hashing Sparkle and Xoodyak are ranked the same:



submission	variant	implementation	primary	flag	size	h(8)	h(16)	h(32)	h(64)	h(128)	Benchmark
reference	sha256	nacl_ref	yes	O3	18774	768	768	772	1364	1968	1
sparkle	esch256v2	rhys	yes	O1	7912	1036	1036	1468	2272	3884	2
xoodyak	xoodyakv1hash	XKCP-AVR8	yes	O3	2604	1284	1288	1924	3192	5732	2.9
gimli	gimli24v1hash	rhys	yes	O3	19554	1284	1920	2544	3804	6312	3.2
ascon	asconhashv12	rhys	yes	O3	2178	2972	3552	4736	7088	11784	6
drygascon	drygascon256hash	rhys	no	O3	15500	4604	4600	6540	10360	17912	9.1
photon-beetl	photonbeetlehash25	avr8_speed	yes	O3	2948	2372	2364	6940	16084	34172	17.4
skinny	skinnyhashtk3	rhys	yes	O2	9784	7048	10556	13976	20952	34896	17.7

Uno Nano performance

For AEAD on Uno Nano Every [2], the benchmark is against AES GCM. We can see in Table 4, that Sparkle is 4.7 times faster than AES GCM for 128-bit data sizes, and Xoodyak comes in second with a 3.3 times improvement over AES GCM. When it comes to 8-bit data sizes, TinyJambu is actually the fastest, but where Sparkle and Xoodyak still perform well. PHOTON-Beetle, Grain128 and ISAP do not do well and only slightly improve on AES GCM. In fact, Grain128 and ISAP are actually slower than AES GCM. ASCON



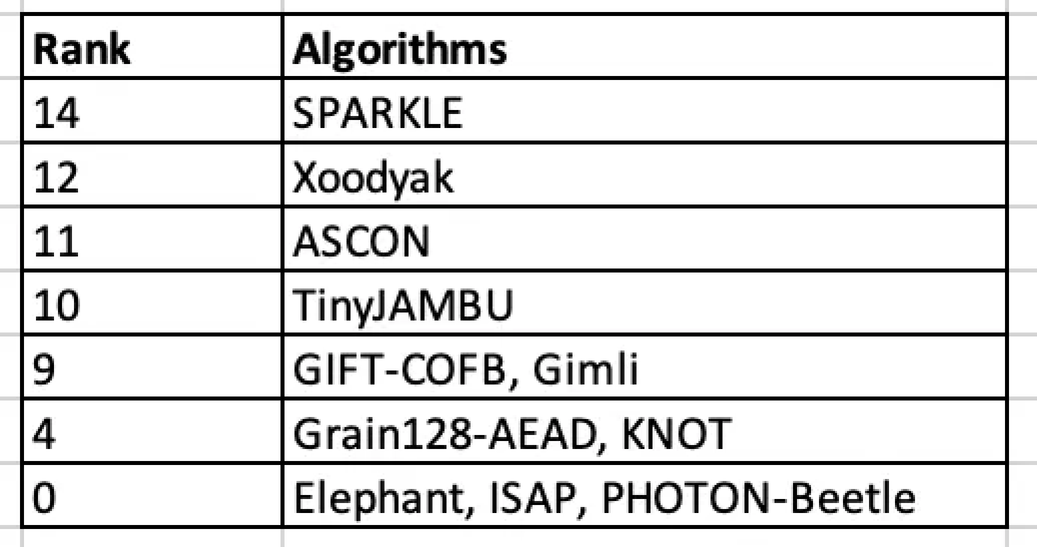
Rank	Algorithms
7	SPARKLE, Xoodyak
5	Gimli
3	ASCON
0	PHOTON-Beetle

Table 4: Uno Nano for AEAD against AES GCM and showing cycles [2] (showing fastest of the method)

And so for AEAD (performance), ASCON does well:

```
1. Sparkle.
2. Xoodyak.
3. ASCON.
4. GIFT-COFB.
5. Elephant.
6. Romulus.
7. Tiny Jambu.
8. PHOTON-Beetle.
9. Grain128.
10. ISAP.
```

For hashing on an Uno Nano Every [2], Table 5 shows a similar performance level as the ARM Cortex M3 assessment. In this case, the benchmark hash is SHA-256, and we can see that it takes Sparkle twice as many cycles for a 128-bit hash and 2.9 times for Xoodyak. PHOTON-Beetle is way behind with a 128-bit hash and which is 17.4 times slower than SHA-256. That said, though, PHOTON-Beetle could be more focused on reducing power consumption rather than speed. GIMLI and SKINNY are included to show a comparison with well-designed methods in lightweight hashing. It can be seen that every method beats SKINNY, but only Sparkle and Xoodyak beat GIMLI.



Rank	Algorithms
14	SPARKLE
12	Xoodyak
11	ASCON
10	TinyJAMBU
9	GIFT-COFB, Gimli
4	Grain128-AEAD, KNOT
0	Elephant, ISAP, PHOTON-Beetle

Table 5: Uno Nano for hashing against SHA-256 and showing cycles [2] (showing fastest of the method for hashing)

And so for hashing (performance):

```
1. Sparkle.
2. Xoodyak.
3. ASCON.
4. PHOTON-Beetle.
```

Conclusions

While Sparkle and Xoodyak looked to be best for hashing and AEAD, it is ASCON that moves forward. Why? Well, it's a good all-rounder, and perhaps has fewer security risks than Sparkle and Xoodyak. ASCON has been around since 2014 and has proven to be secure against attacks.

Reference

[1] https://rweather.github.io/lightweight-crypto/performance.html

[2] https://github.com/usnistgov/Lightweight-Cryptography-Benchmarking/blob/main/benchmarks/results_nano_every_hash_all.csv

[3] Madushan, H., Salam, I., & Alawatugoda, J. (2022). A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses. Electronics, 11(24), 4199.

[4] Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2016). Ascon v1. 2. Submission to the CAESAR Competition.

Cryptography Cybersecurity