Google

Need for Low-latency Ciphers: A Comparative Study of NIST LWC Finalists

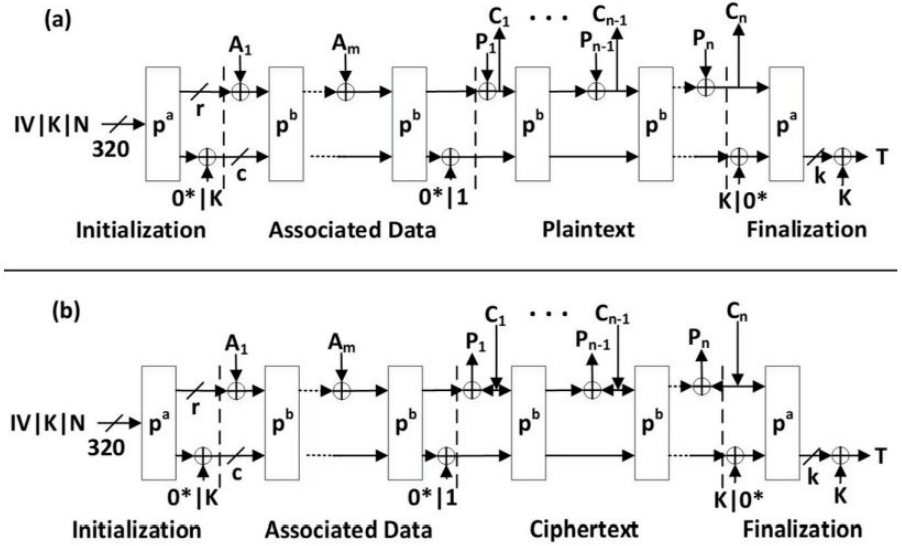
Tolga Yalcin, Samaneh Ghandali
{tyalcin, samaneh}@google.com

Overview

- Fair evaluation of NIST LWC finalists for low-latency applications, e.g. memory encryption
- Include known ciphers in the comparison
  - AES-128
  - PRINCE v2
  - KECCAK in duplex mode
- Evaluation methodology:
  - Use of open-source tools for synthesis (**yosys**) and timing analysis (**openSTA**)
  - Use of open-source generic library (**Nangate 45nm**)
  - No back-annotation (no SDF)
  - All ciphers evaluated in unrolled fashion using for single-cycle operation
  - All RTL codes written from scratch for fair comparison
  - Performance figures not absolute - relative comparison

ASCON

- ASCON is a sponge-based cipher, which has a sponge state of 320 bits and two permutations *pa* and *pb*
- Ascon authenticated encryption or decryption consists of four phases:
  - initialization
  - Associated Data (AD)
  - Plaintext or Ciphertext
  - finalization
- Permutation *pa* applies to initialization and finalization, and *pb* applies to AD and Plaintext or Ciphertext.
- Ascon-128 includes a 128-bit Key, a 128-bit Npub, a 128-bit Tag, a 64-bit data block, and 12 and 6 rounds of *pa* and *pb*, respectively



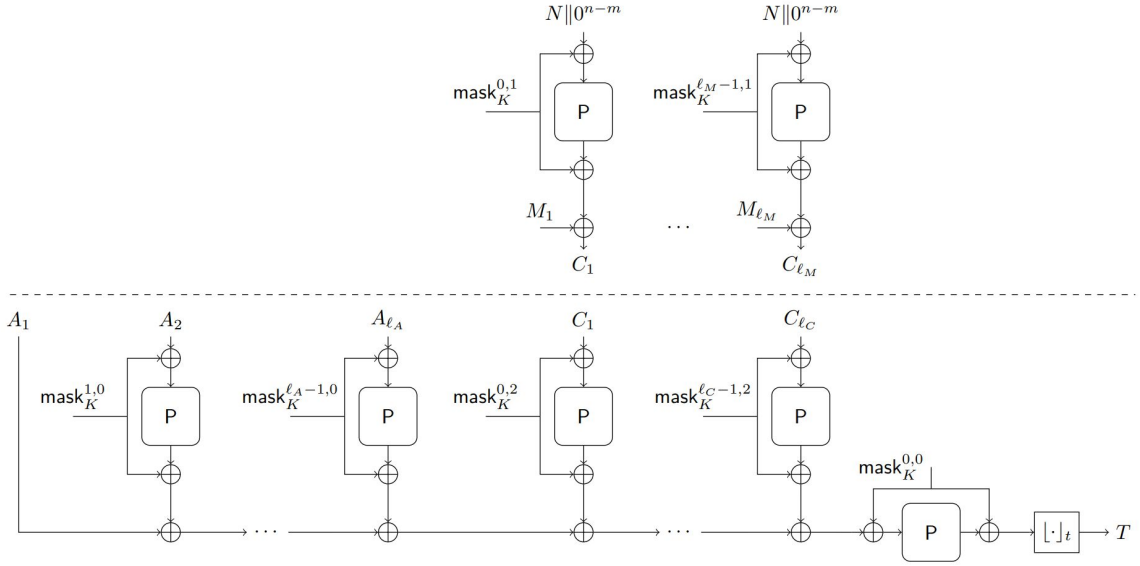
Ascon authenticated (a) encryption and (b) decryption

Fastest instance is Ascon-128a: Can encrypt 128 bits of data every 8 rounds
Unrolled 8 rounds:

- Area: 24.437 KGE
- Delay: 2.97 ns, Max Freq: 336.7 MHz
- Throughput: 43.098 Gbps
- Tput/Area = 1.763 Gbps/KGE

Elephant

- Elephant is a nonce-based encrypt-then-MAC construction
- Encryption is performed using counter mode
- Message authentication is performed using a variant of the protected counter sum MAC function

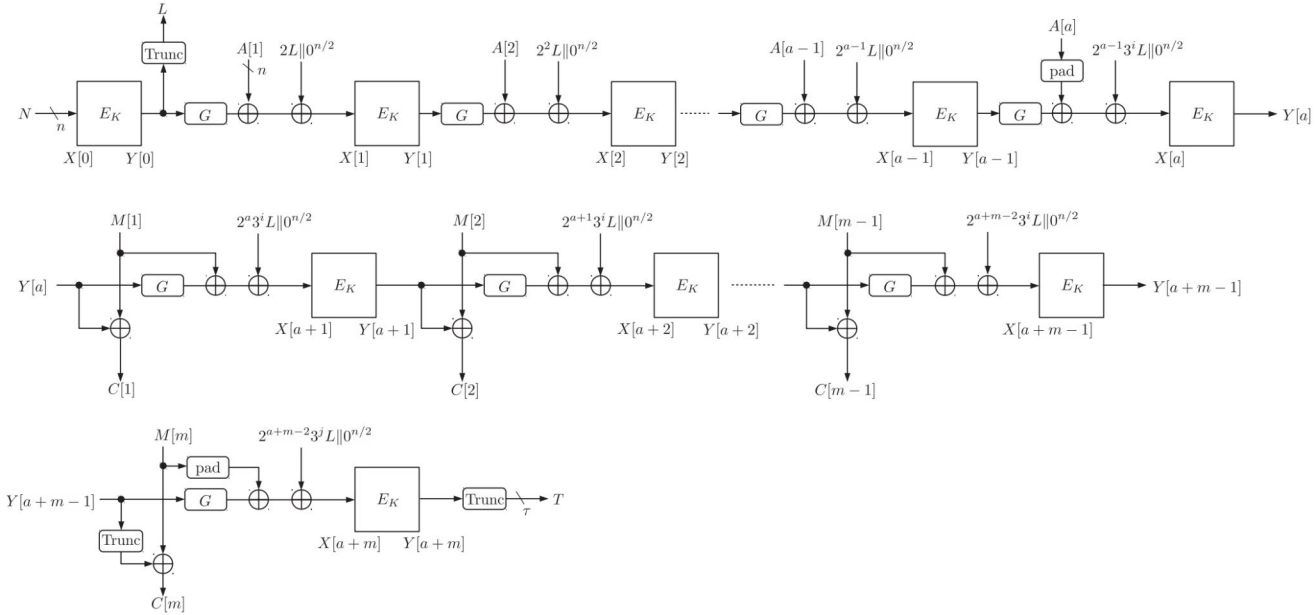


Fastest instance is Delirium: Can encrypt 200 bits of data every 18 Keccak rounds
Unrolled 18 rounds:

- Area: 28.350 KGE
- Delay: 8.16 ns , Max Freq: 122.55 MHz
- Throughput: 24.510 Gbps
- Tput/Area = 864.54 Mbps/KGE

GIFT-COFB

- GIFT-COFB authenticated instantiates the COFB (COmbined FeedBack) block cipher based AEAD mode with the GIFT block cipher



Single instance: Can encrypt 128 bits of data every 40 GIFT rounds

Unrolled 40 rounds:

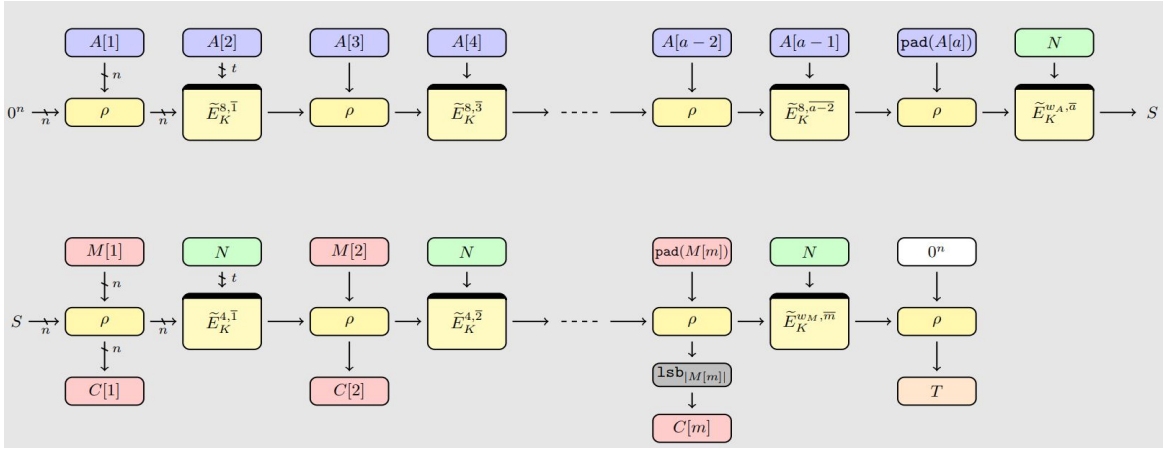
- Area: 28.709 KGE
- Delay: 12.53 ns , Max Freq: 79.81 MHz
- Throughput: 10.215 Gbps
- Tput/Area = 355.82 Mbps/KGE

Romulus

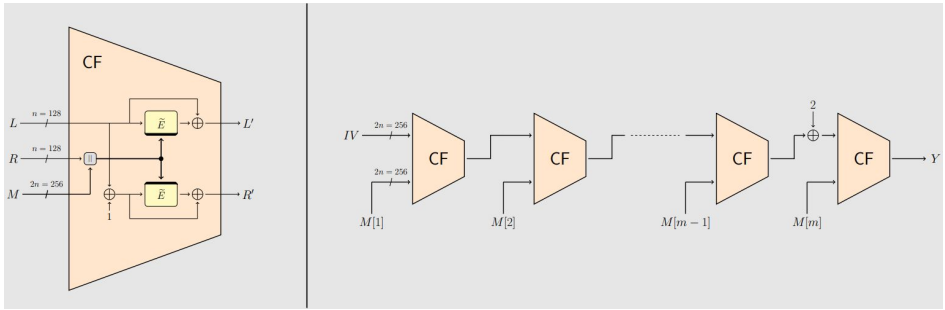
- Romulus is three authenticated encryption schemes with associated data (AEAD) and a hash function, all based on a tweakable block cipher (TBC) Skinny.

Single instance is Romulus-N: Can encrypt 128 bits of data every 40 Skinny rounds
Unrolled 40 rounds:

- Area: 43.392 KGE
- Delay: 22.97 ns
  Max Freq: 43.535 MHz
- Throughput: 5.572 Gbps
- Tput/Area = 128.42 Mbps/KGE



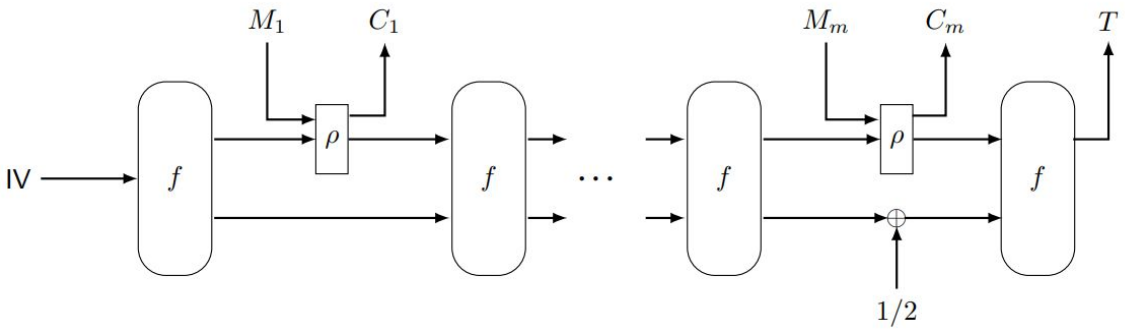
Romulus-N: nonce-based AE (NAE) scheam



Romulus-T:
leakage-resilient AE
Romulus-T and a hash function Romulus-H

PHOTON-Beetle

- PHOTON-Beetle is an authenticated encryption and hash family, that uses a sponge-based mode Beetle with the P256 being the underlying permutation
- PHOTON-Beetle-AEAD: a family of authenticated encryptions
- PHOTON-Beetle-Hash: a family of hash functions



PHOTON-Beetle-AEAD.ENC with a AD blocks and m message blocks

Fastest instance is Beetle-AEAD[128]: Can encrypt 128 bits of data every 12 PHOTON rounds

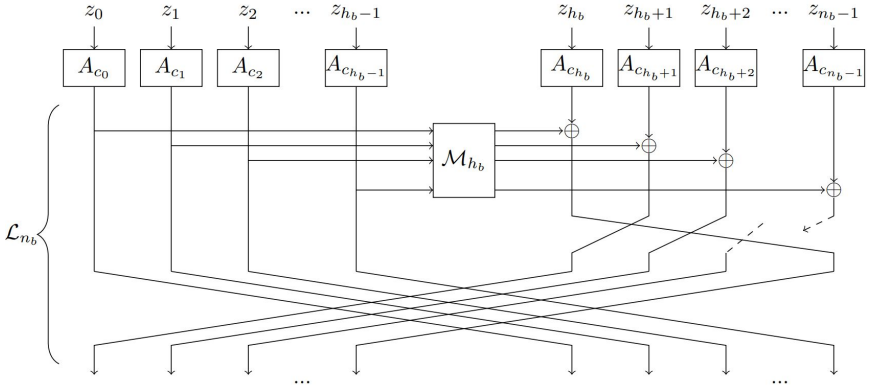
Unrolled 12 rounds:

- Area: 343.55 (96.512*) KGE
- Delay: 12.87 (36.43*) ns , Max Freq: 77.700 (27.450*) MHz
- Throughput: 9.945 (3.513*) Gbps
- Tput/Area = 28.949 (36.406) Mbps/KGE

*: MixColumnsSerial implementation

SPARKLE

- Sparkle family of permutations together with the AEAD instances Schwaemm and the hash functions Esch.
- Esch: Efficient, Sponge-based, and Cheap Hashing
- Schwaemm: Sponge-based Cipher for Hardened but Weightless Authenticated Encryption on Many Microcontrollers

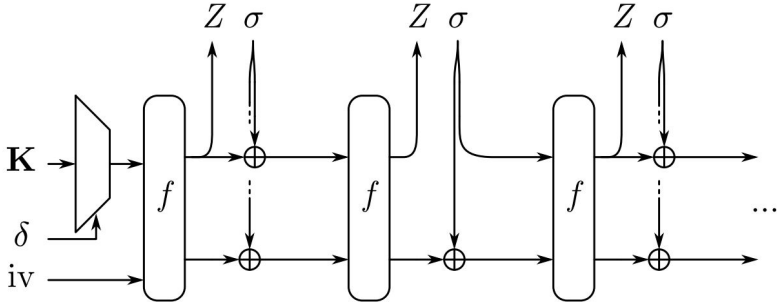


Fastest instance is Schwaemm256-128: Can encrypt 256 bits of data every 7 Sparkle rounds
Unrolled 7 rounds:

- Area: 128.51 KGE
- Delay: 59.75 ns , Max Freq: 16.736 MHz
- Throughput: 4.2845 Gbps
- Tput/Area = 33.339 Mbps/KGE

Xoodyak

- It is based on the duplex construction, and on its full-state variant when it is fed with a secret key



Single instance: Can encrypt 256 bits of data every 12 Xoodo rounds
Unrolled 12 rounds:

- Area: 34.148 KGE
- Delay: 4.78 ns , Max Freq: 209.21 MHz
- Throughput: 40.167 Gbps
- Tput/Area = 1176.3 Mbps/KGE

AES and PRINCE

Both AES-128 and PRINCE_v2 evaluated in XEX mode

- Tweak generation is not included in the evaluation

AES-128: Can encrypt 128 bits of data every 10 rounds
Unrolled 10 rounds:

- Area: 83.581 KGE
- Delay: 14.34 ns , Max Freq: 69.735 MHz
- Throughput: 8.9261 Gbps
- Tput/Area = 106.80 Mbps/KGE

PRINCE_v2: Can encrypt 64 bits of data every 12* rounds
Unrolled 12 rounds:

- Area: 7.9813 KGE
- Delay: 3.89 ns , Max Freq: 257.07 MHz
- Throughput: 16.452 Gbps
- Tput/Area = 2061.4 Mbps/KGE

KECCAK

KECCAK-400/800/1600 evaluated in duplex mode with fixed capacity c = 256

KECCAK-400: Can encrypt 144 bits of data every 20 rounds
Unrolled 20 rounds:

- Area: 60.128 KGE
- Delay: 8.90 ns , Max Freq: 112.36 MHz
- Throughput: 16.180 Gbps
- Tput/Area = 269.09 Mbps/KGE

KECCAK-800: Can encrypt 544 bits of data every 22 rounds
Unrolled 22 rounds:

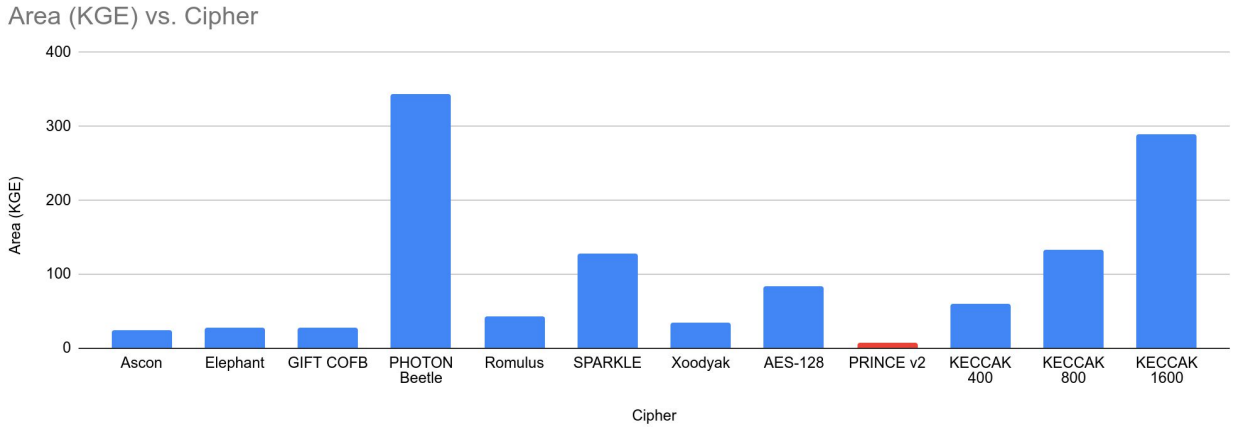
- Area: 132.74 KGE
- Delay: 9.72 ns , Max Freq: 102.88 MHz
- Throughput: 55.967 Gbps
- Tput/Area = 421.64 Mbps/KGE

KECCAK-1600: Can encrypt 1344 bits of data every 24 rounds
Unrolled 24 rounds:

- Area: 289.92 KGE
- Delay: 10.65 ns , Max Freq: 93.897 MHz
- Throughput: 126.20 Gbps
- Tput/Area = 435.28 Mbps/KGE

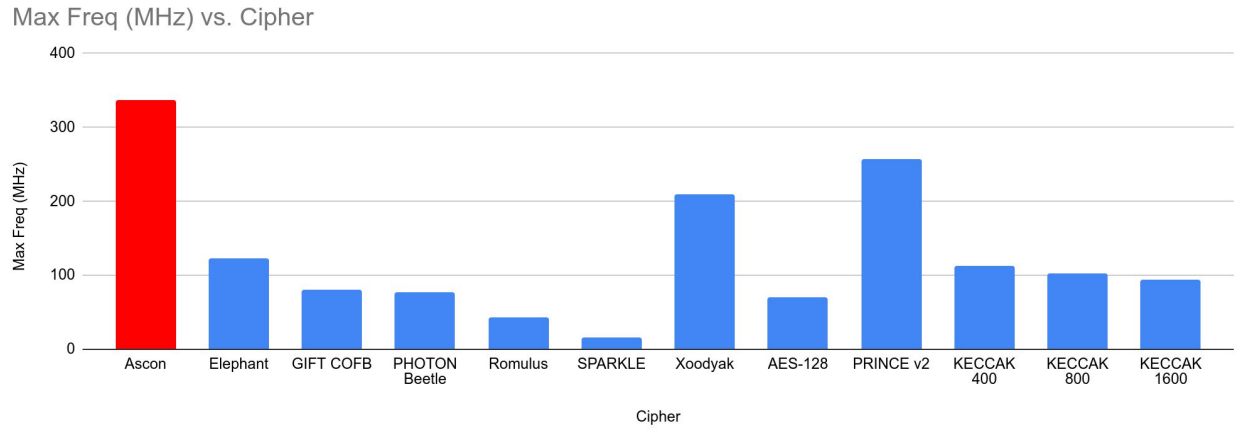
Analysis

Compactness												
	Ascon	Elephant	GIFT COFB	PHOTON Beetle	Romulus	SPARKLE	Xoodyak	AES-128	**PRINCE v2**	KECCAK 400	KECCAK 800	KECCAK 1600
Area (KGE)	24.437	28.350	28.709	343.55	43.392	128.51	34.148	83.581	**7.9813**	60.128	132.74	289.92



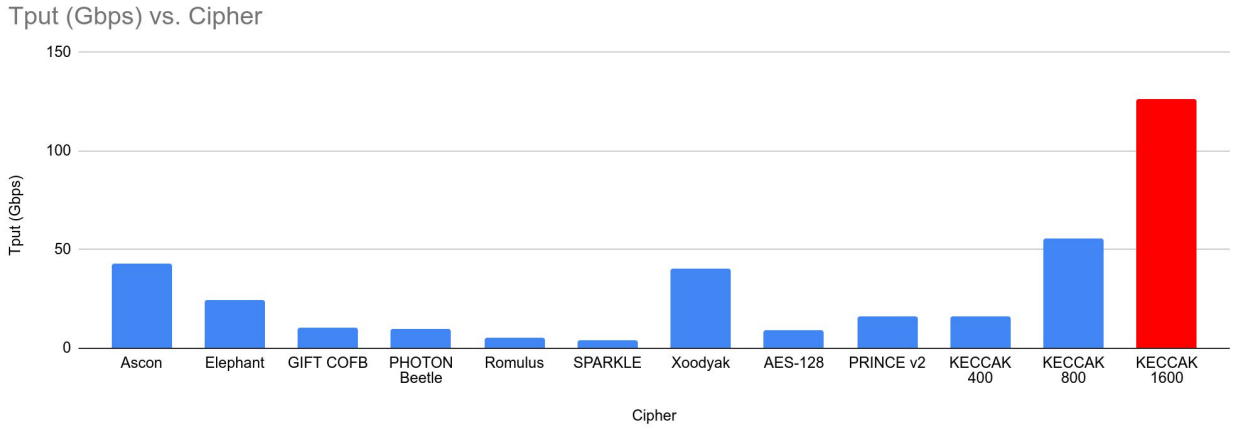
Analysis

High Frequency												
	Ascon	Elephant	GIFT COFB	PHOTON Beetle	Romulus	SPARKLE	Xoodyak	AES-128	PRINCE v2	KECCAK 400	KECCAK 800	KECCAK 1600
Max Freq (MHz)	**336.7**	122.55	79.81	77.700	43.535	16.736	209.21	69.735	257.07	112.36	102.88	93.897



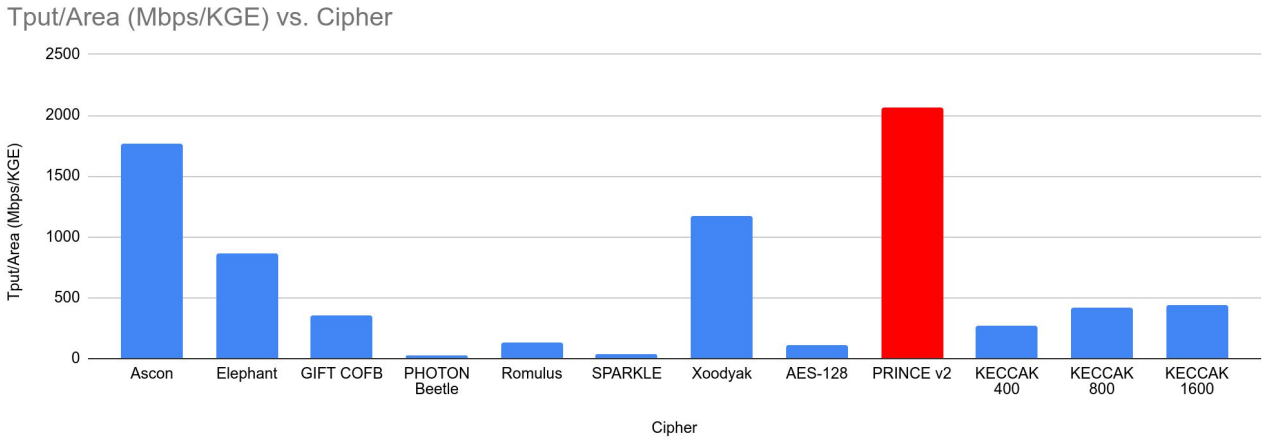
Analysis

High Throughput												
	Ascon	Elephant	GIFT COFB	PHOTON Beetle	Romulus	SPARKLE	Xoodyak	AES-128	PRINCE v2	KECCAK 400	KECCAK 800	**KECCAK 1600**
Tput (Gbps)	43.098	24.510	10.215	9.945	5.572	4.2845	40.167	8.9261	16.452	16.180	55.967	**126.20**



Analysis

Throughput per Area												
	Ascon	Elephant	GIFT COFB	PHOTON Beetle	Romulus	SPARKLE	Xoodyak	AES-128	**PRINCE v2**	KECCAK 400	KECCAK 800	KECCAK 1600
Tput/Area (Mbps/KGE)	1763	864.54	355.82	28.949	128.42	33.339	1176	106.80	**2061**	269.09	421.64	435.28



Conclusion

- Memory encryption not a design target in LWC competition - none of the finalists offer high throughput in a compact area
- ASCON is the best option in terms of max frequency - x3 area of PRINCE
  - Initialization requires additional cycles
- PRINCE can be used for memory encryption efficiently - Not a NIST standard
  - Any NIST plans to add an optional mode for memory encryption?
- Very high throughputs possible by using variants of KECCAK in duplex mode - Not a NIST standard
  - Any NIST plans to support KECCAK in duplex mode?

THANK YOU