Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look

Behnaz Rezvani
William Diehl

Bradley Dept. of Electrical and Computer Eng.
Virginia Tech
Blacksburg, Virginia

November 5, 2019

SAL
SIGNATURES ANALYSIS LAB

VIRGINIA TECH

Outline

- Introduction
- Rationale of selecting Ciphers
- FPGA Implementations
  - SpoC
  - Spook
  - GIFT-COFB
  - CAESAR LW API
- Results
- Conclusions

Introduction

- Devices in IoT are vulnerable to theft of privacy information and are subject to potentially more destructive attacks

- Conventional methods of security provisions:
  - Encryption/Decryption → Confidentiality
  - MAC → Authentication
  - Hash → Data integrity

- AEAD combines confidentiality, data integrity, and authentication into a single algorithm
  - Savings in cost and performance
  - Good for lightweight applications
  - But, more complex security analysis

Round 1 Candidates

- Functionality:
  - AEAD (34)
  - AEAD + Hash (22)
- Block cipher or permutation-based (51) vs. stream cipher and others (5)
  - Permutation-based (26)
- Permutation structures: SPN (37), Feistel (10), 3D state (4), Misty (1), LS-design (1)
- Non-linearity:
  - S-box: 4-to-2-bit (1) 3-bit (1), 4-bit (22), 5-bit (5), 8-bit (12), 9-bit (1)
  - AND (9)
  - ARX* (6)

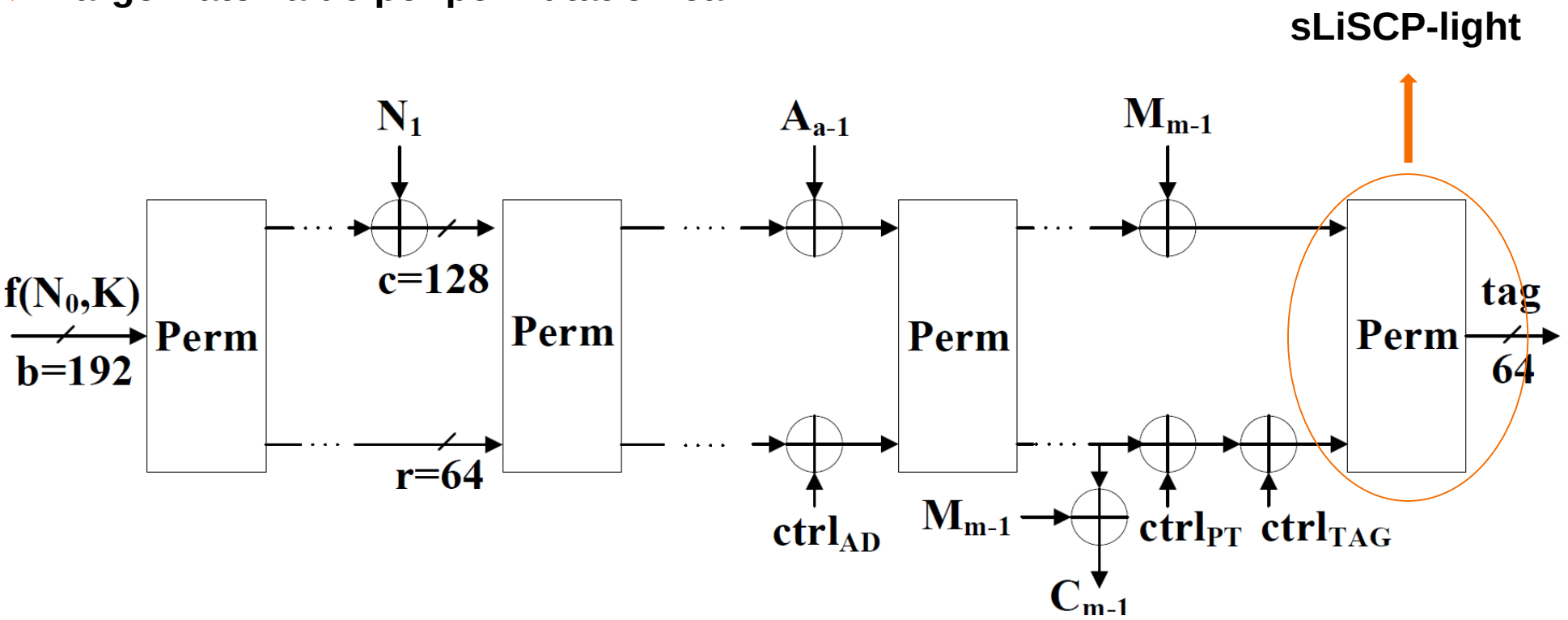
*ARX: Addition, Rotation, XOR

Rationale of Selection

- Different structures:
  - Block-based: GIFT-COFB
  - Sponge-based: SpoC, Spook
- Different permutation designs:
  - sLiSCP-light permutation: SpoC
  - LS-design: Spook
  - SPN: GIFT-COFB
- Different types of confusion:
  - S-box: Spook, GIFT-COFB
  - AND: SpoC
- Tweakable Block Cipher:
  - Spook

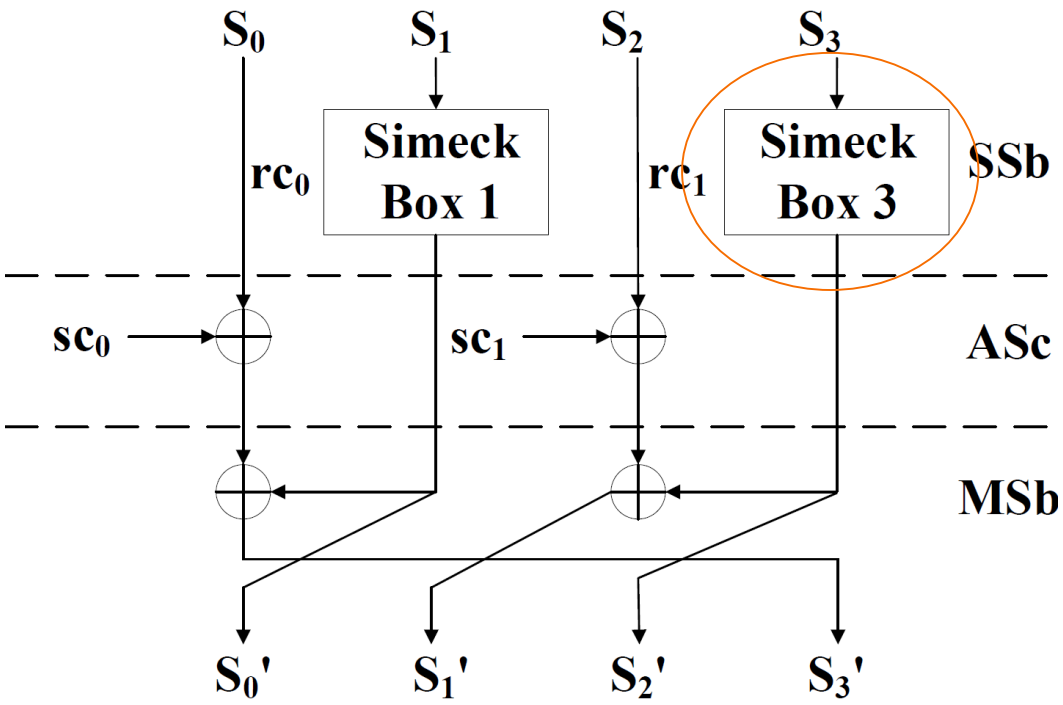
SpoC Construction

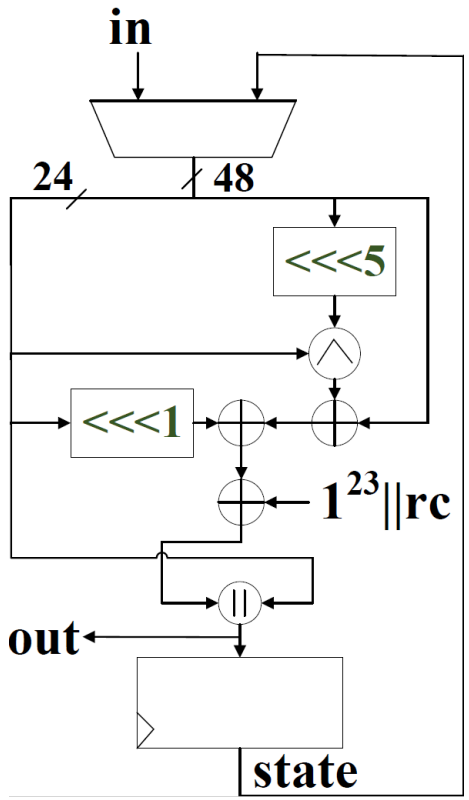
- SpoC mode of operation:
  - Sponge with a masked capacity
  - Higher security
  - Larger rate value per permutation call



SpoC: sLiSCP-light[192]

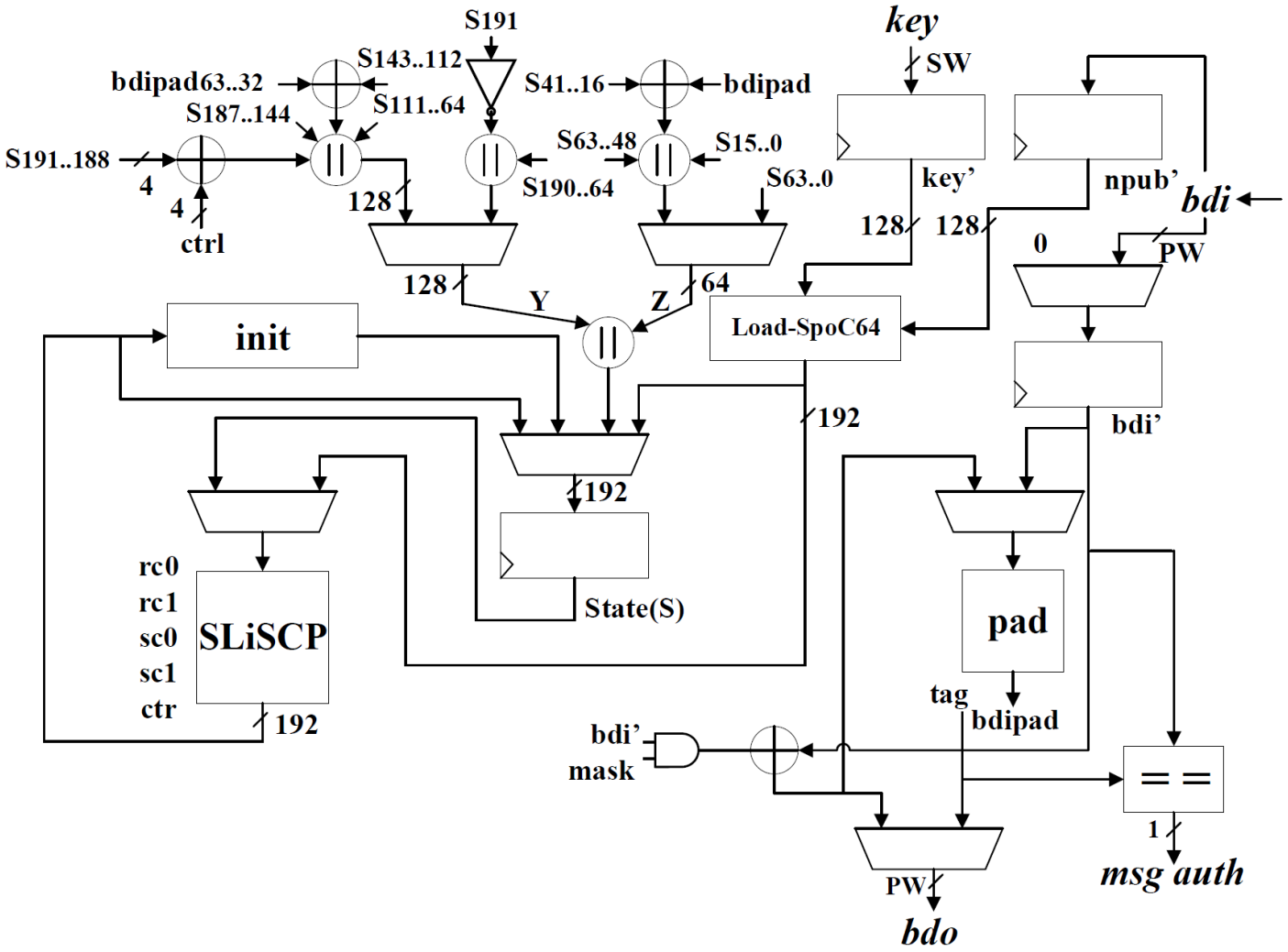
- Combination of a type II generalized Feistel structure (GFS) and Simeck box
- 3 transformations in each step (18 steps)
  - SubstituteSubblocks (SSb) (6 rounds)
  - AddStep constants (ASc)
  - MixSubblocks (MSb)





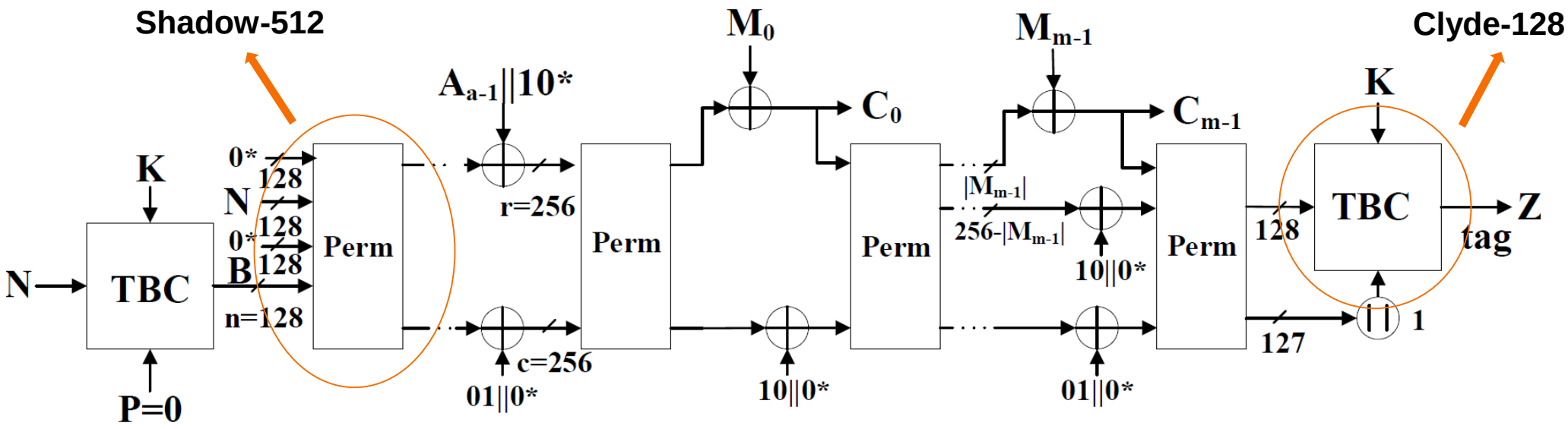
SpoC Implementation

- 1 round of the SSb: 1 clock cycle
  - 108 clock cycles per permutation
- Initialization and Tag gen.: 219 CC
- Every block of AD: 109 CC
- Every block of M: 111 CC
- Requires 10* padding
- Truncate the output (|CT|=|PT|)



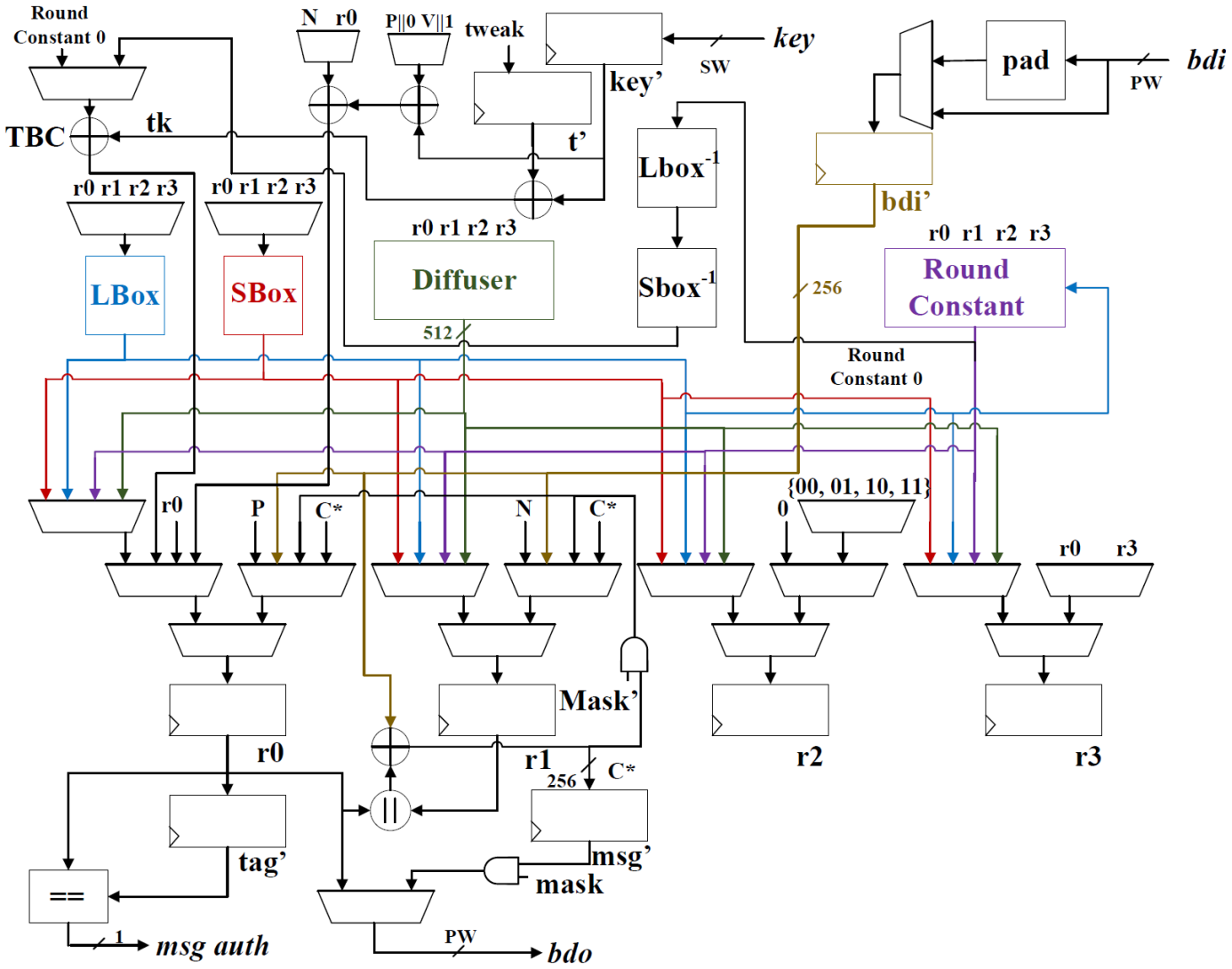
Spook Construction

- Primary member achieves Ciphertext Integrity and Misuse with Leakage in encryption and decryption (CIML2), which is an extension of ciphertext integrity in the presence of nonce misuse and side-channel leakages
- Single one pass (S1P) mode of operation
- Clyde-128: A tweakable LS-design (L-box, S-box)
- Shadow-512: A multiple LS-design (L-box, S-box, diffusion layer)



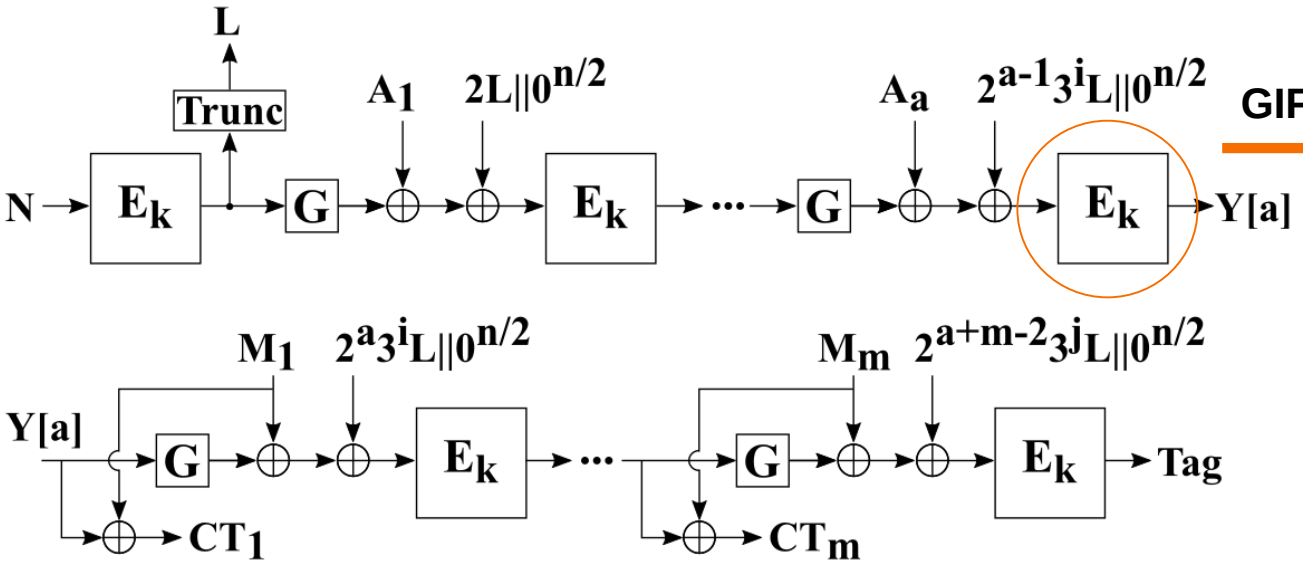
Spook Implementation

- 1 round of TBC: 1 clock cycle
  - 12 clock cycles per TBC
  - 144 clock cycles per permutation
- Initialization and Tag gen.: 169 CC
- Every block of AD: 145 CC
- Every block of M: 145 CC
- L-box and S-box are shared
- Requires 10* padding
- Truncate the output (|CT|=|PT|)

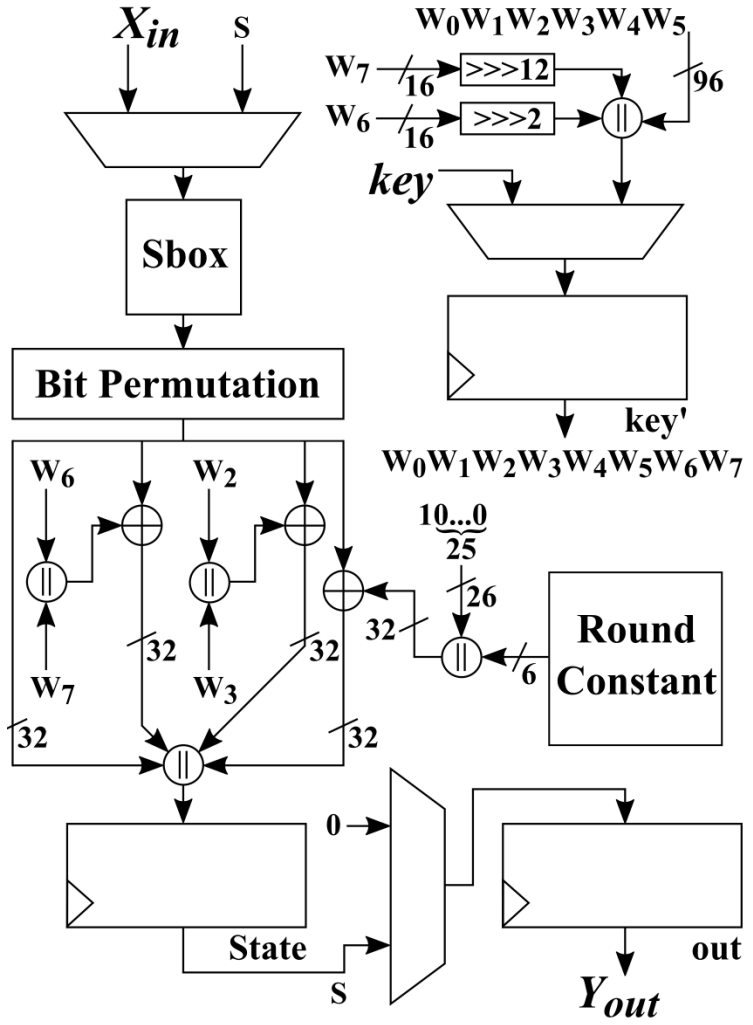


GIFT-COFB Construction

- Combined-feedback mode of operation
  - Single pass
  - Inverse free
- Underlying cipher: GIFT-128

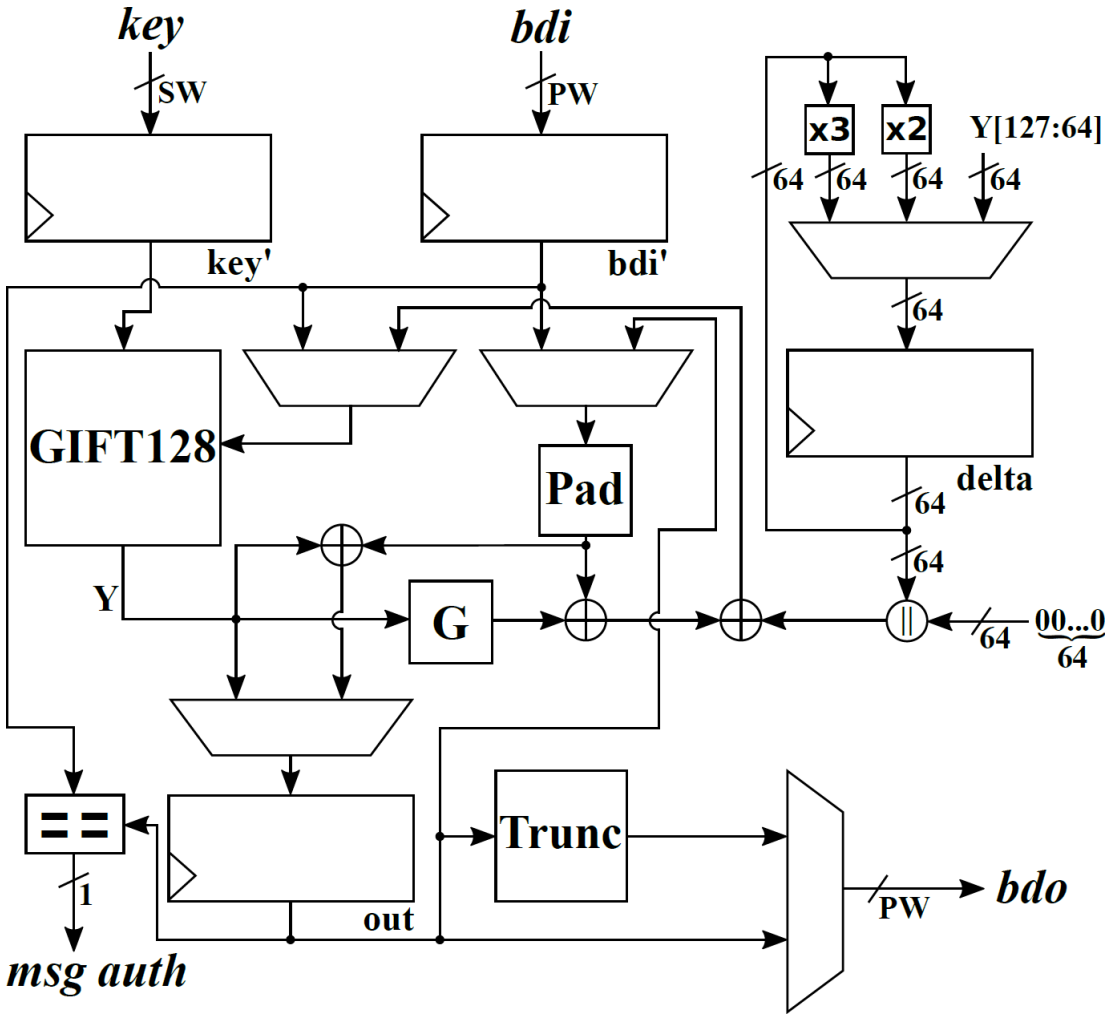


GIFT-128



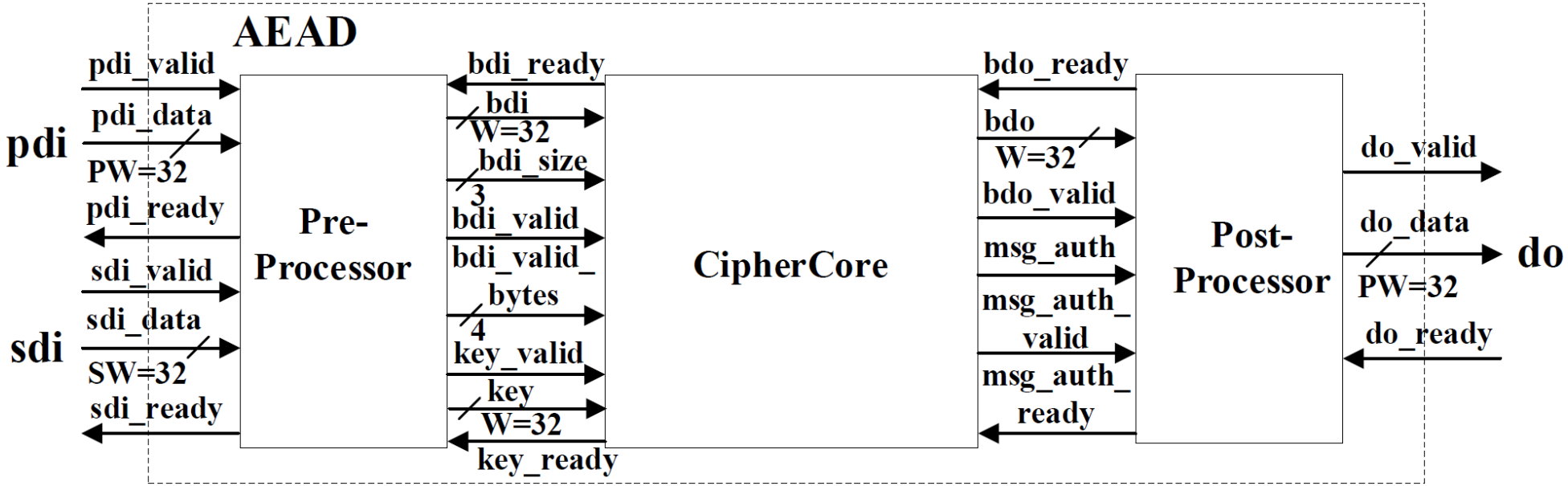
GIFT-COFB Implementation

- 1 round: 1 clock cycle
  - 40 clock cycles per GIFT cipher
- Initialization and Tag gen.: 112 CC
- Every block of AD: 50 CC
- Every block of M: 53 CC
- Requires 10* padding
- Truncate the output (|CT|=|PT|)



CAESAR LW API

- CAESAR LW developer's package:
  - Input processor (Pre-Processor)
  - Output processor (Post-Processor)
  - Designer's cipher (CipherCore)



Implementation Setup

• Methodology	→	RTL
• FPGA platform	→	Artix-7
• Interface	→	CAESAR hardware API (LW developer's package)
• Operation tool	→	Xilinx Vivado 2018.3
• Optimization tool	→	Minerva automated hardware optimization tool
• Goal of optimization	→	Throughput to area (TPA) ratio
• Test vector generator	→	aeadtvgen in the developer's package
• Verification hardware	→	FOBOS

- All ciphers are implemented in basic iterative (round-based) architecture.

Benchmarking Results

- **Latency: # of clock cycles to process one block of PT from start to end**
- **Throughput:**

  (Max Freq) x (Bits/Block)/(Cycles/Block)

- **SpoC has the highest frequency and smallest area.**
- **GIFT-COFB has the highest TP and TPA and the smallest latency.**
- **Spook has largest area but higher TP than SpoC.**

Cipher	SpoC	Spook	GIFT-COFB
Max Freq (MHz)	**265**	141	172
#Bits/Block	64	256	128
#Cycles/Block	111	145	53
Latency	330	314	**165**
Throughput (TP) (Mbps)	152.8	248.9	**415.4**
LUTs	**1344**	7082	2695
TPA (Mbps/LUT)	0.114	0.035	**0.154**

Comparison

Cipher	Type	FPGA	Freq (MHz)	Area (LUTs)	TP (Mbps)	TPA (Mbps/LUT)	Ref
CAESAR							
Ascon-128	Sponge	Spartan-6	**216.0**	**684**	60.1	**0.088**	Yalla et al.: Evaluation of the CAESAR Hardware API for Lightweight Implementations. 2017
Ascon-small	Sponge	Spartan-6	146.1	1640	**114.0**	0.070	Diehl et al.: Face-off between the caesar lightweight finalists: Acorn vs. ascon. 2018
CLOC-AES	Block	Spartan-6	101.9	1604	68.7	0.043	Farahmand et al.: Improved lightweight implementations of caesar authenticated ciphers. 2018
SILC-AES	Block	Spartan-6	115.1	872	15.1	0.017	Farahmand et al.: Improved lightweight implementations of caesar authenticated ciphers. 2018
NIST LWC (AEAD)							
SpoC	Sponge	Artix-7	265.0	1344	152.8	0.114	TW
Spook	Sponge	Artix-7	141.0	7082	248.9	0.035	TW
Spook	Sponge	Artix-7	181.8	3771	**3878.4**	**1.028**	Spook Team: Spook (unprotected) implementation of encryption. email of Jul. 30, 2019.
GIFT-COFB	Block	Artix-7	172.0	2695	415.4	0.154	TW
ESTATE	Block	Virtex-7	**580.1**	1413	928.3	0.657	Chakraborti, A., Datta, N., Jha, A., Lopez, C.M., Nandi, M., Sasaki, Y.: ESTATE (Mar 2019).
SAEAES	Block	Virtex-7	145.9	**348**	263.3	0.757	Naito, Y., Matsui, M., Sakai, Y., Suzuki, D., Sakiyama, K., Sugawara, T.: SAEAES (Feb 2019).
Oribatida	Sponge	Virtex-7	554.2	940	514	0.547	Bhattacharjee, A., List, E., Lpez, C.M., Nandi, M.: The Oribatida Family of Lightweight Authenticated Encryption Schemes (Mar 2019).

Power and Energy/Bit

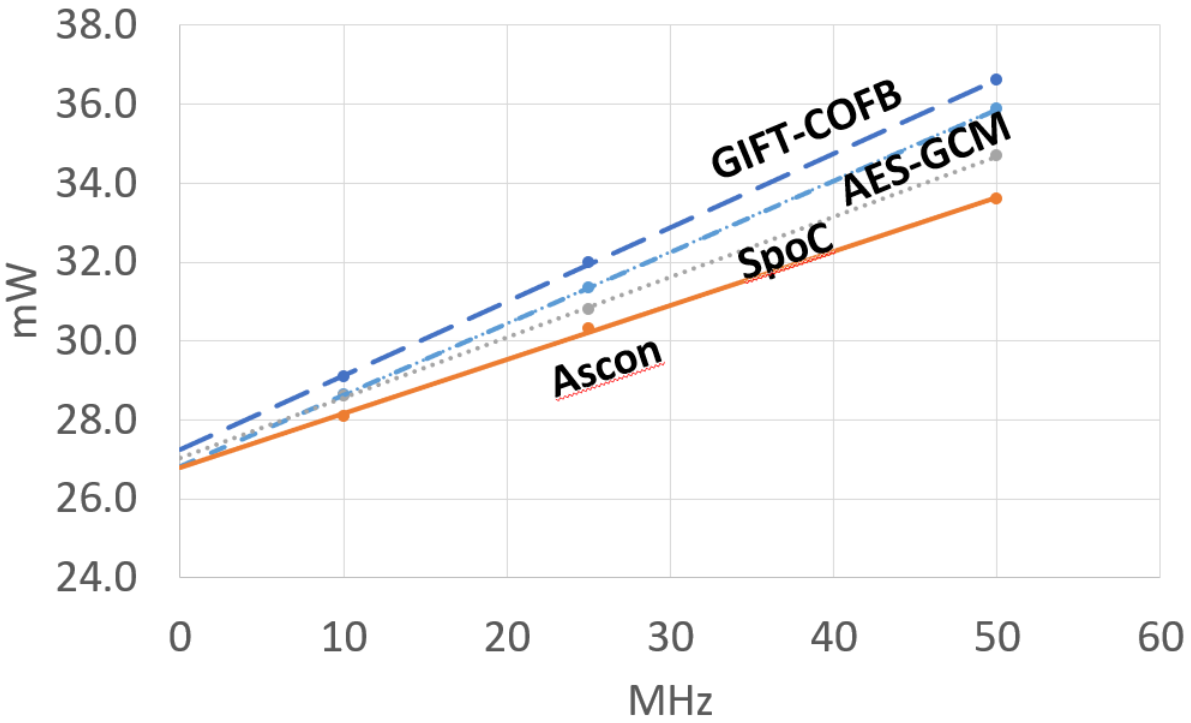
- **Power measured @ 10, 25, 50 MHz using FOBOS on Artix-7**
- **E/bit (nJ/bit) = P (mW)/TP(Mbps)**
- **Ascon has the lowest power at 50 MHz.**
- **GIFT-COFB has the lowest E/bit at 50 MHz.**
- **Spook has the highest power.**

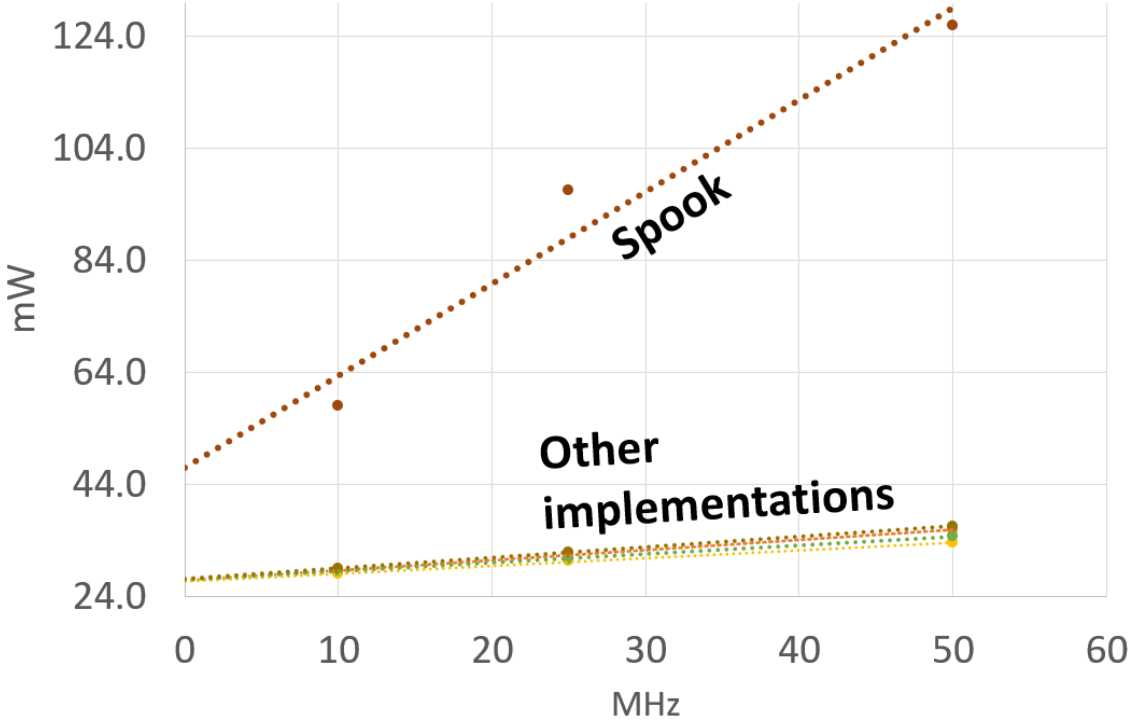
Cipher	Freq (MHz)	P_{mean} (mW)	TP (Mbps)	E/bit (nJ/bit)
AES-GCM	10	28.6	6.2	4.59
	25	31.4	15.6	2.01
	50	35.9	31.2	1.15
ASCON	10	28.1	7.8	3.60
	25	30.3	19.5	1.55
	50	**33.6**	39.0	0.86
SpoC	10	28.6	5.8	4.96
	25	30.8	14.4	2.14
	50	34.7	28.8	1.20
Spook	10	58.8	17.7	3.33
	25	96.5	44.1	2.19
	50	125.9	88.3	1.43
GIFT-COFB	10	29.1	24.2	1.20
	25	32.0	60.4	0.53
	50	36.6	120.8	**0.30**

Abdulgadir A., Diehl W., Kaps J.P.: An Open-Source Platform for Evaluation of Hardware Implementations of Lightweight Authenticated Ciphers. Submitted in ReConFig 2019.

Power Consumption vs. Freq

- P_{static} is estimated with linear interpolation.
- Static powers of all ciphers (except Spook) are 27.0mW±1%.
- The static power of Spook is much higher, likely due to its larger area.





Abdulgadir A., Diehl W., Kaps J.P.: An Open-Source Platform for Evaluation of Hardware Implementations of Lightweight Authenticated Ciphers. Submitted in ReConFig 2019.

Conclusions

- We provided the first look at 3rd-party FPGA implementations of selected NIST LWC standardization process Round 1 candidates.
- SpoC has the highest maximum frequency of 265 MHz (1.9 greater than Spook), and has the lowest area, in terms of LUTs, with1344 LUTs (19% of the LUTs of Spook).
- GIFT-COFB has the highest throughput (TP) at 415.4 Mbps (2.7 greater than SpoC), the highest throughput-to-area (TPA) ratio at 0.154 Mbps/LUT (4.4 more than Spook), and the lowest energy/bit at 50 MHz.
- Spook has the highest area due to its security features that it guarantees, but can be implemented in leveled implementations to get smaller area and higher TP.

Thank you!