A Quantitative Security Analysis of S-boxes in the NIST Lightweight Cryptography Finalists

Mahnoor Naseer[1], Sundas Tariq[2], Naveed Riaz[3*], Naveed Ahmed[3], Shah Fahd[4], Mureed Hussain[5], Sajid Ali Khan[6]

[1]Crypto Group, ICTEAM Institute, UCLouvain, Louvain-la-Neuve, Belgium.
[2]3MI Labs and COSIC, KU Leuven, Leuven, Belgium.
[3]SEECS, National University of Sciences and Technology, Islamabad, Pakistan.
[4]MCS, National University of Sciences and Technology, Islamabad, Pakistan.
[5]National Center for Cyber Security (NCCS), Air University, Islamabad, Pakistan.
[6]Department of Software Engineering, Foundation University, Islamabad, Pakistan.

*Corresponding author(s). E-mail(s): naveed.riaz@seecs.edu.pk;

Abstract

Lightweight cryptography was primarily inspired by the design criteria of symmetric cryptography. It plays a vital role in ensuring the security, privacy, and reliability of microelectronic devices without compromising the overall functionality and efficiency. However, the increasingly platform specific design requirements prompted the development of a standard lightweight algorithm. In 2017, NIST put forward security requirements for a standard lightweight scheme — security strength of at least 112 bits against known cryptanalysis attacks, mitigation against side channel and fault injection attacks, and implementation efficiency. After three rounds of review, ASCON was crowned as the winner of the competition. Evaluating the individual components used in any cryptographic algorithm is an important step in the verification of security claims. A fundamental component used to ensure Shannon's property of confusion in cryptographic primitives is an S-box. Hence, the quality of an S-box is a significant contributing factor in the security strength of a cipher. In this paper, we evaluate the S-boxes of **6** NIST LWC competition finalists based on well-known cryptographic properties, and comment on how the results reflect upon NIST security requirements. Our findings have revealed that these S-boxes do not comply with the basic notions of avalanche, making it vulnerable to high-order sophisticated cryptanalysis.

Keywords: NIST, Lightweight Cryptography, Substitution layer, Cryptanalysis, S-box

1 Introduction

Application specific computing has become an emerging trend in modern information technology due to the wide usability of smart devices. The highly evolving yet resource constrained environment enumerates to countless security concerns. It is difficult to use traditional cryptographic primitives on these platforms while striking an optimal trade-off between compact implementation and security strength [1]. In order to effectively resolve this issue, NIST laid the foundation for lightweight cryptography standardization in 2017 [2].

Lightweight cryptography aims to provide security for Internet of Things (IoT) devices, namely sensors, RFID tags, medical implants, smart cards, etc. Design choices such as small block and key size, simple round structure and key schedule, and nominal implementation make lightweight ciphers the right choice to ensure a sufficient level of security using less power, computing, and memory resources. As a result of NIST's call, a total of 57 proposals were submitted by research teams across the globe.

After two rounds of the rigorous evaluation process, as described in NIST IR 8369 [3], 10 candidates were shortlisted as finalists of the competition (see Table 1 [4]). In the third and final round, candidates were evaluated on the basis of claims made in terms of security strength against known attacks (112 bits or more); performance in both hardware and software environments; resilience against side channel and fault injection attacks; and intellectual property rights [5].
In February 2023, NIST declared the ASCON family as the new lightweight cryptography standard [6]. The most important evaluation criteria for cryptographic algorithms is measuring their security strength against known attacks such as differential and linear cryptanalysis (and their variants), as well as implementation based attacks. Designers and cryptanalysts across the globe tried their level best to suffice this requirement. As a result, the competition finalists received a noticeable amount of third-party security analysis [7–44], a few highlighted in Table 2:-

Table 1: Classification of NIST LWC Finalists based on Presence/Absence of S-box

With S-box	Without S-box
ASCON, ISAP, GIFT-COFB,	Grain-128-AEAD, Sparkle,
Photon-Beetle, Elephant, Romulus	Xoodyak, TinyJAMBU

Shannon's property confusion in any symmetric cipher is mainly dependent on the non-linear component used. The most commonly used component to achieve non-linearity in symmetric cryptography is a substitution box (S-box). Analysing the cryptographic profile of an S-box plays a vital role in determining the overall strength of a cryptosystem. The literature reports nearly 24 cryptographic properties [58–73] that can be used as a tool to estimate the quality of an S box. Some of the attacks mentioned earlier exploit specific S-box properties in order to devise practical attack characteristics for a particular cipher. This paper aims to provide a complete picture of the cryptographic properties of S-boxes, their relevance to known attacks, and related security limits [1]. Our primary goal is to help researchers better understand and evaluate the security profile of S-boxes in a principle manner.

Section 2 of this paper elaborates the specifications of six finalists of NIST LWC. Section 3 discusses the fundamental properties of S boxes and classifies them according to the relevant attack category. Secondly, the upper and lower bounds of these properties are highlighted along with their behavior under affine equivalence. In Section 4, the results of the S-box analysis are discussed in detail. In Section 5, we generate a new 4−bit S-box with optimal cryptographic properties using the PEIGEN S-box generation tool [75], and draw a comparison of the properties of this S-box with the LWC finalists having 4−bit S-boxes. Section 6 discusses and highlights the scope and limitations of this paper. Finally, we conclude our findings in Section 7.

2 Overview of Finalists

This section provides a brief introduction to each of the 6 finalists from NIST lightweight standardization that make use of S-box as one of the design components.

2.1 ASCON

It is a cryptographic cipher suite presented by Maria *et al.* [76]. ASCON comprises of three authenticated encryption and associated data (AEAD) variants: 128, 128 (a and pq), and two hashing algorithms: Hash and Hash-a. Its main functionality comes from the use of a 320 bit permutation, which is combined with different constants and number of rounds, depending upon the variant. In addition, to achieve non-linearity in the encryption algorithm a 5×5 affine equivalent S-box of χ mapping from Keccak permutation is used. The ASCON family has been selected by NIST for lightweight standardization because of its security strength and flexibility to be used in multiple applications while bearing a minimum implementation cost [6].

[1] Current paper is an extended version of our previous paper [74]

Table 2: Summary of Third-Party Security Analysis on NIST LWC Finalists

Cipher	Attack Type	Rounds	Complexity	Reference
ASCON	Differential-Linear	4	Time = 2^{15}, 2^{18}	[7]
		5	Time = $2^{33.1}$, 2^{36}	[9]
	Impossible Differential	4, 5	Data = 2^{2}, 2^{109}	[45]
	Truncated Differential	4, 5	Data = 2^{2}, 2^{109}	
	Cube Attack	5	Time = 2^{35}	[9]
		6	Time = 2^{66}	
	Key Recovery	Init (7/12)	Time = 2^{97}, 2^{101}, $2^{123.92}$	[8]
	(Nonce Misuse)	8, 9		[46]
	Forgery Attack	Final (4 – 6)	Time = 2^{9}, 2^{17} & 2^{33}	[8]
	Round Reduction + Cube	Init (5)	Time = 2^{24}	[10]
	CPA using Multi-bit Selection Function	Full	2-bit selection function = 7200 traces 3-bit selection function = 8200 traces	[47]
	Differential Fault Attack	Full	Fault queries = 2^{10}	[48]
	Collision Attack	2	Time = 2^{98}	[49]
	Free-start Collison Attack	3	Time = 2^{10}	[50]
GIFT-128 / COFB	MILP-Based Linear Attack	20	65-bit key recovery	[18]
	Differential Key Recovery Attack	23	Time = 2^{120}, Data = 2^{86}	[51]
	Integral Distinguisher using Division Property	11	–	[20]
	Differential Attack	26	Time = $2^{123.245}$	[21]
Photon-Beetle	Key Recovery Irregularity	Full	Data = 2^{50} bytes	[28]
	Differential Fault Attack	Full	Time = 2^{16}, Fault queries = $2^{37.15}$	[52]
	Committing Attack	Initial State	No queries	[53]
	Pre-image Attack	3.5	Time = 2^{112}, Data = 2^{65}	[54]
Elephant	Interpolation Attack	8	Time = 2^{70}	[33]
	Fault Analysis (Dumbo)	Full	85 – 250 ciphertexts	[34]
	Blind SCA on LFSR	Full	< 2 days (practical)	[35]
Romulus	Impossible Differential	22	Time = $2^{373.48}$, Data = $2^{92.22}$	[38]
	Matching / Authenticity Attack	Full	–	[39]
	Meet-in-the-Middle (MITM)	23	Time = 2^{376} , Data = 2^{104}	[40]
	Impossible Boomerang	27	Time = 2^{337}, Data = $2^{131.3}$	[55]
		28	Time = $2^{382.8}$, Data = $2^{130.26}$	
	Differential MITM	25	Time = 2^{366}, Data = $2^{122.3}$	[56]
	Impossible Differential MITM	21	Time = $2^{344.33}$, Data = $2^{122.89}$	[57]
		22	Time = $2^{378.22}$, Data = $2^{121.50}$	
		23	Time = $2^{378.22}$, Data = $2^{121.50}$	
		27	Time = $2^{361.06}$, Data = $2^{124.99}$	
		28	Time = $2^{378.22}$, Data = $2^{129.50}$	

2.2 ISAP

ISAP was proposed by S. Mangard *et al.* [77], it is a nonce based AEAD cryptographic scheme designed to resist against implementation based attacks at an optimized implementation cost. ISAP uses 400 bit Keccak and 320 bit ASCON permutations in its design alongside 5×5 bit ASCON S-box as a non-linear component.

2.3 GIFT-COFB

Proposed by A. Chakraborti. *et al.*[78]. GIFT-COFB is an encryption scheme that uses combined feedback mode with GIFT-128. GIFT-COFB employs 40 rounds of encryption where the input is: an arbitrary length associated data, an input message of variable length, a nonce of 128 bits, and a 128 bit encryption key. Whereas the output is a 128 bit tag and ciphertext of same length as the input message. A 4×4 bit S-box is used as the confusion component.

2.4 Photon-Beetle

Photon-Beetle is an AEAD based hashing and encryption scheme presented by J. Guo *et al.* [79]. The encryption routine comprises of 12 rounds consisting of 4 separate stages i.e. XOR constant, substitute cells, shift rows and serial mix columns. Photon-Beetle (AEAD) uses the 4×4 bit S-box of Present block cipher in order to achieve non-linearity in its design.

2.5 Elephant

C. Dobarunig *et al.* [80], proposed Elephant as a permutation based AEAD algorithm. It has 3 variants based on Spongent and Keccak permutations: Delirium, Jumbo and Dumbo. These encryption variants take 128 bit key and 96 bit nonce, however the block sizes are 160, 176, 200. A 4×4 S-box as the non-linear part. In the 80 rounds of encryption there are 160 differentially active S-boxes.

2.6 Romulus

T. Iwata. *et al.* [81], proposed Romulus as a nonce based AEAD encryption and hashing scheme that uses Skinny block cipher as underlying encryption algorithm. It operates in 4 modes of encryption and hashing: nonce misuse based Romulus-M, nonce based Romulus-N, leakage resistant based Romulus-T and hashing based Romulus-H. The encryption algorithm takes 128 bits of key and nonce, and runs 40 rounds of encryption. Skinny-128 tweakable block cipher [82] uses 8×8 S-box to achieve non-linearity in its design.

Table 3: Classification of S-box properties as per relevance to existing cryptanalysis techniques

S#	Criteria	Properties
1	Generic	Balancedness; Permutation; Order of Permutation; Fixed Points (FP); Opposite Fixed Points (OFP); Bit Independence Criteria (BIC); Strict Avalanche Criteria (SAC); Auto Correlation Table (ACT) [83]; Absolute Indicator (AI) [84]; Sum of Square Indicators (SSI) [84]
2	Linear Cryptanalysis	Nonlinearity (NL) [62, 63]; Linear Approximation Table (LAT) [64, 85]; Linear Approximation Probability (LAP); Linear Branch Number (LBN); Linear Structures (LS) [65, 66]; Correlation Immunity (CI) [86]
3	Differential Cryptanalysis	Differential Distribution Table (DDT) [64]; Differential Uniformity (DU) [62, 63]; Differential Branch Number (DBN); Propagation Characteristics (PC) [87]; Undisturbed Bits [68]
4	Boomerang Cryptanalysis	Boomerang Connectivity Table (BCT); Boomerang Uniformity (BU) [67]
5	Differential–Linear Cryptanalysis	Linear Structures (LS) [65, 66]; Differential Linear Connectivity Table (DLCT) [69]; Differential Linear Uniformity (DLU) [70]
6	Algebraic Cryptanalysis	Algebraic Degree (AD) [71]; Interpolation Polynomial (IP)
7	Side-Channel Analysis	DPA-SNR [72]; Transparency Order (TO) [73]

Table 4: Theoretical Bounds on the Cryptographic Properties of S-boxes

S#	Properties	Bounds	For 4×4	For 5×5	For 8×8	Ideal Value
1	OP	$1 \leq \mathsf{OP} \leq 2^n$	$1 \leq \mathsf{OP} \leq 16$	$1 \leq \mathsf{OP} \leq 32$	$1 \leq \mathsf{OP} \leq 256$	Close to UB
2	FP	$0 \leq \mathsf{FP} \leq 2^n$	$0 \leq \mathsf{FP} \leq 16$	$0 \leq \mathsf{FP} \leq 32$	$0 \leq \mathsf{FP} \leq 256$	Close to LB
3	OFP	$0 \leq \mathsf{OFP} \leq 2^n$	$0 \leq \mathsf{OFP} \leq 16$	$0 \leq \mathsf{OFP} \leq 32$	$0 \leq \mathsf{OFP} \leq 256$	Close to LB
4	BIC	$0 \leq \mathsf{BIC} \leq 1$	$0 \leq \mathsf{BIC} \leq 1$	$0 \leq \mathsf{BIC} \leq 1$	$0 \leq \mathsf{BIC} \leq 1$	0
5	SAC	$0 \leq \mathsf{SAC} \leq 1$	$0 \leq \mathsf{SAC} \leq 1$	$0 \leq \mathsf{SAC} \leq 1$	$0 \leq \mathsf{SAC} \leq 1$	0.5
6	$\overline{\wedge}_S$	$\sqrt{\frac{2^{2n}}{2^n-1}} \leq \overline{\wedge}_S \leq 2^n$	$0 < \overline{\wedge}_S \leq 16$	$0 < \overline{\wedge}_S \leq 32$	$0 < \overline{\wedge}_S \leq 256$	Close to LB
7	$\overline{\overline{\wedge}}_S$	$2^{2n} \leq \overline{\overline{\wedge}}_S \leq 2^{3n+m}$	$256 \leq \overline{\overline{\wedge}}_S \leq 65536$	$1024 \leq \overline{\overline{\wedge}}_S \leq 1048576$	$65536 \leq \overline{\overline{\wedge}}_S \leq 4294967296$	Close to LB
8	LAT	$0 \leq \mathsf{LAT} \leq 2^n - 1$	$0 \leq \mathsf{LAT} \leq 15$	$0 \leq \mathsf{LAT} \leq 31$	$0 \leq \mathsf{LAT} \leq 255$	-
9	ξ	$0 \leq \xi \leq \frac{1}{2}$	$0 \leq \xi \leq \frac{1}{2}$	$0 \leq \xi \leq \frac{1}{2}$	$0 \leq \xi \leq \frac{1}{2}$	Close to LB
10	NL	For n even: $0 \leq \mathsf{NL} < 2^{n-1} - 2^{\frac{n}{2}-1}$ For n odd: $0 \leq \mathsf{NL} < 2^{n-1} - 2^{\frac{n-1}{2}}$	$0 \leq \mathsf{NL} < 6$	$0 \leq \mathsf{NL} < 12$	$0 \leq \mathsf{NL} < 120$	Close to UB
11	$\mathsf{BN_L}$	$2 \leq \mathsf{BN_L} \leq n-1$	$2 \leq \mathsf{BN_L} \leq 3$	$2 \leq \mathsf{BN_L} \leq 4$	$2 \leq \mathsf{BN_L} \leq 7$	Close to UB
12	LS	$0 \leq \mathsf{LS} \leq 2^{n+m}$	$0 \leq \mathsf{LS} \leq 256$	$0 \leq \mathsf{LS} \leq 1024$	$0 \leq \mathsf{LS} \leq 65536$	Close to LB
13	CI	$0 \leq \mathsf{CI} \leq n$	$0 \leq \mathsf{CI} \leq 4$	$0 \leq \mathsf{CI} \leq 5$	$0 \leq \mathsf{CI} \leq 8$	Close to LB
14	DDT	$0 \leq \mathsf{DDT} \leq 2^n - 1$	$0 \leq \mathsf{DDT} \leq 15$	$0 \leq \mathsf{DDT} \leq 31$	$0 \leq \mathsf{DDT} \leq 255$	-
15	DU	$2 \leq \mathsf{DU} \leq 2^n$	$2 \leq \mathsf{DU} \leq 16$	$2 \leq \mathsf{DU} \leq 32$	$2 \leq \mathsf{DU} \leq 256$	Close to LB
16	$\mathsf{BN_D}$	$2 \leq \mathsf{BN_D} \leq \lceil \frac{2n}{3} \rceil$	$2 \leq \mathsf{BN_D} \leq 3$	$2 \leq \mathsf{BN_D} \leq 4$	$2 \leq \mathsf{BN_D} \leq 6$	Close to UB
17	PC	$0 \leq \mathsf{PC} \leq n$	$0 \leq \mathsf{PC} \leq 4$	$0 \leq \mathsf{PC} \leq 5$	$0 \leq \mathsf{PC} \leq 8$	Close to UB
18	UDB	$\mathsf{UDB} = 0$	$\mathsf{UDB} = 0$	$\mathsf{UDB} = 0$	$\mathsf{UDB} = 0$	0
19	βU	$2 \leq \beta\mathsf{U} \leq 2^n$	$2 \leq \beta\mathsf{U} \leq 16$	$2 \leq \beta\mathsf{U} \leq 32$	$2 \leq \beta\mathsf{U} \leq 256$	Close to LB
20	DLU	$2^{\frac{n}{2}-1} < \mathsf{DLU} \leq 2^{n-1}$	$2 < \mathsf{DLU} \leq 8$	$4 < \mathsf{DLU} \leq 16$	$8 < \mathsf{DLU} \leq 128$	Close to LB
21	AD	$1 \leq \mathsf{AD} \leq n-1$	$1 \leq \mathsf{AD} \leq 3$	$1 \leq \mathsf{AD} \leq 4$	$1 \leq \mathsf{AD} \leq 7$	Close to UB
22	$\mathsf{DPA_{SNR}}$	For balanced S-box: $1 \leq \mathsf{DPA_{SNR}} \leq 2^{\frac{n}{2}}$	$0 \leq \mathsf{DPA_{SNR}} \leq 4$	$0 \leq \mathsf{DPA_{SNR}} < 6$	$0 \leq \mathsf{DPA_{SNR}} \leq 16$	Close to LB
23	TO	$0 \leq \mathsf{TO} \leq m$	$0 \leq \mathsf{TO} \leq 4$	$0 \leq \mathsf{TO} \leq 5$	$0 \leq \mathsf{TO} \leq 8$	Close to LB

3 Cryptographic Properties of S-boxes and their Classification

The strength of cryptographic primitives is best analysed with the help of well-known cryptanalysis techniques. Shannon's theory of confusion and diffusion plays the foundational role in the design and analysis of iterative ciphers. The aspect of confusion is introduced in symmetric ciphers using highly non-linear components such as S-boxes. Designers and cryptanalysts treat these ciphers as a white box, analysing all the underlying mathematical components in order to understand and rule out any potential attack vectors, by imposing design practices based on standard characteristics and theoretically well-defined bounds. Owing to the importance of S-boxes in the design of cryptographic algorithms, an extensive research has been done over the years to explain the most refined design and analysis criteria that could be employed in order to secure them against potential attack vectors. These properties can be classified in a number of ways depending whether upon the types of representation in boolean algebra or the statistical and implementation based attacks that could be launched through exploitation of relevant metrics or via studying the inter-dependencies that link one property to another.

This section briefly covers an introduction to around twenty-four cryptographic properties of S-boxes that hold significance in the current literature. Each of the properties is related to one or more crytanalysis techniques, that could exploit the non-linear part of a block cipher, see Table 3. In addition, Table 4 presents the upper and lower bounds (UB & LB) on these properties with respect to the dimension of S-box being used [71–73, 88–92]. We also talk about the behaviour of these properties under affine equivalence, see Table 5. The properties along with their respective bounds and equivalence characteristics aid designers and cryptanalysts in the selection of good S-boxes.

Table 5: S-box Properties under Affine Equivalence

Property	**Affine Variant**	**Affine Invariant**
Bijectivity		✓
Balancedness		✓
Permutation	✓	
OP	✓	
FP	✓	
OFP	✓	
BIC	✓	
SAC	✓	
ACT		✓
$\overline{\wedge}$		✓
$\overline{\overline{\wedge}}$		✓
NL		✓
LAT		✓
BN_L	✓	
LS	✓	
CI	✓	
DDT		✓
DU		✓
BN_D	✓	
PC		✓
UDB		✓
BCT		✓
βU		✓
DLCT		✓
DLU		✓
AD		✓
IP		✓
DPA-SNR	✓	
TO	✓	

3.1 Diffusion Characteristics

Properties such as balancedness, bijectivity, order of permutation, fixed and opposite fixed points, strict avalanche and bit independence criteria, absolute and sum of square indicator are general pre-requisites that should adhere to defined bounds for any S-box in order to avoid correlations between the input and output bits and serve as a pre-requisite to ensure security against various statistical cryptanalysis attacks.

Table 6: Results of S-box Analysis – 8×8 and 5×5 bit case

S#	Properties	Romulus 8×8 **Skinny-128**	**ASCON/ISAP** 5×5
1	Bijectivity	✓	✓
2	Balancedness	✓	✓
3	Permutation	✓	✓
4	OP	140	26
5	FP	1	0
6	OFP	0	0
7	BIC	1.000000	1.000000
8	SAC	1.000000	1.000000
9	$\overline{\lambda}_S$	256	32
10	$\overline{\overline{\lambda}}_S$	4194304	8192
11	ξ	0.25000	0.25000
12	NL	64	8
13	BN_L	2	3
14	LS	601	91
15	CI	0	0
16	DU	64	8
17	BN_D	2	3
18	PC	0	0
19	UDB	258	35
20	βU	256	16
21	DLU	128	16
22	AD	6	2
23	DPA-SNR	6.312455	3.015113
24	TO	7.174510	4.258065

Balancedness

A vectorial boolean mapping $S : F_2^n \to F_2^m$ is balanced if it has an equal number of 1's and 0's in its coordinate and component functions. Mathematically;

$$P(0) = P(1) = \frac{1}{2} = 50\% \tag{1}$$

An imbalanced boolean mapping stays at a risk of achieving high linear approximation probabilities [93]. Balancedness is invariant when under affine equivalence, which means that the number of 0's ad 1's is preserved in S if an affine transformation is applied to it [94–96].

Permutation

A boolean mapping $S : F_2^n \to F_2^m$ is permutation when the entire input space is utilized in such a way that one input maps only at one output. To fulfill this property it is necessary for S to be a bijective mapping i.e. $n = m$. Permutation property of S is variant under affine transformation [62, 63, 97, 98].

Order of Permutation (OP)

The minimum number of compositions applied to get an identity mapping on the coordinate and component functions of a boolean mapping S is called the order of permutation. OP is not an invariant property under affine equivalence [62, 63, 97, 98].

Table 7: Results of S-box Analysis – 4×4 bit case

S#	Properties	New Sbox 4×4	Elephant 4×4	GIFT-COFB 4×4 GIFT	Photon-Beetle 4×4 Present
1	Bijectivity	✓	✓	✓	✓
2	Balancedness	✓	✓	✓	✓
3	Permutation	✓	✓	✓	✓
4	OP	7	13	9	7
5	FP	3	0	0	0
6	OFP	1	1	1	1
7	BIC	0.577350	1.000000	1.000000	1.000000
8	SAC	0.7500	1.000000	1.000000	1.000000
9	$\overline{\wedge}_S$	8	16	16	16
10	$\overline{\overline{\wedge}}_S$	640	1024	1024	1024
11	ξ	0.25000	0.25000	0.25000	0.25000
12	NL	4	4	4	4
13	$\mathsf{BN_L}$	2	2	2	2
14	LS	0	9	9	9
15	CI	0	0	0	0
16	DU	4	4	6	4
17	$\mathsf{BN_D}$	2	3	2	3
18	PC	0	0	0	0
19	UDB	0	3	6	6
20	βU	10	16	16	16
21	DLU	4	8	8	8
22	AD	3	3	3	3
23	DPA-SNR	2.578634	2.398501	2.398501	2.128608
24	TO	3.400000	3.266667	3.466667	3.533333

Fixed Points (FP)

For a vectorial boolean mapping S, when an input value ($\varkappa$) maps upon itself in the output, it is known as fixed point (FP). Mathematically:-

$$S(\varkappa) = \varkappa \tag{2}$$

Opposite Fixed Points (OFP)

In a vectorial boolean mapping S, if an input value ($\varkappa$) maps on the inverse of itself in the output, it is known as opposite fixed point (OFP). Mathematically:-

$$S(\varkappa) = (\varkappa)' \tag{3}$$

If any S has a high number of FPs or OFPs, it is considered to lack the desired randomness so they should kept to a minimum in order to avoid statistical attacks. This can be achieved with the application of an affine transformation, as FP and OFP are affine variant properties [95].

Bit Independence Criteria (BIC)

A vectorial boolean mapping $S : F_2^n \to F_2^m$ is said to satisfy BIC, if inverting an input bit u has a changing effect on the output bit v i.e. all the avalanche variables $(\gamma_u, \gamma_v, ...)$ representing difference between bits of input and output of S become pairwise independent [99]. Mathematically, BIC is computed using correlation co-efficient of the avalanche variables:-

$$\rho(\gamma_u, \gamma_v) = \frac{cov(\gamma_u, \gamma_v)}{\sigma(\gamma_u)\sigma(\gamma_v)} \tag{4}$$

Where; $u \neq v$ and $u, v = 1, 2, ..., m$. The numerator in eq 4 denotes co-variance between two avalanche variables (γ_u and γ_v), while $\sigma(\gamma_u)$ and $\sigma(\gamma_u)$ in the denominator is the product of the same variables. For the coordinate and component functions of S, the BIC value should stay in the range of $[0, 1]$. An ideal S-box has a BIC value equal to 0. If an affine transformation is applied to S, BIC does not stay invariant [100].

Strict Avalanche Criteria (SAC)

A vectorial boolean mapping S is said to satisfy SAC such that whenever a single input bit $\varkappa$ is inverted, there is a 50 percent probability of each of the output bit changing. SAC is satisfied if hamming weight (wt) of all the coordinate and component functions of S is 1. Mathematically, it can be expressed in terms of directional derivative:-

$$S_\gamma = S(\varkappa) \oplus S(\varkappa \oplus \gamma) \tag{5}$$

Where $\gamma \in F_2^n, \gamma \neq 0, wt(\gamma) = 1$. SAC is variant under affine transformation, which means that a function not satisfying SAC could be transformed to a function that satisfies SAC using affine equivalence [101].

Auto Correlation Transform (ACT)

The ACT of S is denoted by $\triangle_S(\gamma, \rho)$, where $\gamma \in F_2^n$, and $\rho \in F_2^m$. Then ACT of S can be mathematically defined as follows:-

$$\triangle_S(\gamma, \rho) = \sum_{\varkappa=0}^{2^{n-1}} (-1)^{\rho \cdot (S(\varkappa \oplus \gamma) \oplus S(\varkappa))} \tag{6}$$

ACT of S is invariant under affine equivalence [91].

Absolute Indicator (AI)

The overall impact of auto correlation of a boolean function or a vectorial boolean function is studied by finding the maximum value in ACT spectrum, known as absolute indicator (AI). Let f be a Boolean function over F_2^n i.e. $f : F_2^n \to F_2$. The AI of f is defined as [88]:-

$$\overline{\wedge}_f = \max_{\gamma \in F_2^n \setminus \{0\}} |\triangle_f(\gamma)| \tag{7}$$

Whereas, $\triangle_f(\gamma)$ is the autocorrelation of the function f over F_2^n shifted with $\gamma \in F_2^n$ and calculated as:-

$$F(D_\gamma f) = \triangle_f(\gamma) = \sum_{\varkappa \in F_2^n} (-1)^{D_\gamma f} \tag{8}$$

Here $D_\gamma f = f(\varkappa) \oplus f(\varkappa \oplus a)$.

For a vectorial boolean mapping $S : F_2^n \to F_2^m$, using (6) the AI of S is defined as [102]:-

$$\overline{\wedge}_S = \max_{\gamma, \rho \in F_2^n \setminus \{0\}} |\triangle_S(\gamma, \rho)| \tag{9}$$

$\overline{\wedge}_S$ stays invariant under affine transformation. For balanced vectorial boolean functions, the value of AI is always 0. If a boolean mapping has high $\overline{\wedge}_S$, it becomes highly susceptible to cube attacks [88, 103].

Sum-of-Squares (SSI)

The SSI of a vectorial boolean mapping S is represented in terms of ACT as follows:-

$$\overline{\overline{\wedge}}_S = \sum_{\gamma \in F_2^n, , \rho \in F_2^m} \triangle_S^2(\gamma, \rho) \tag{10}$$

SSI is not variant under affine equivalence [104]. For achieving good diffusion characteristics in a cryptographic algorithm, S-boxes should have low SSI and AI values [88, 105].

3.2 Linear Cryptanalysis

The idea of this technique evolves around studying the non-linear layer of a block cipher to draw a linear approximations profile (LAT) between plaintext, key and the ciphertext to find correlations among them. Matsui introduced non-linearity as a significant criteria in the design of block ciphers [106]. Block ciphers having a highly non-linear layer are resistant towards linear cryptanalysis. To study the number of active S-boxes in the linear trails of a block cipher, J. Daemon *et al.* [107] introduced linear branch number. Theoretically, in order to resist linear (and its variant) cryptanalysis techniques an S-box should have a low linear approximation probability, high non-linearity, high order of linear branch number, equal to none linear structures, and low order correlation immunity.

Linear Approximation Table (LAT)

M. Matsui introduced linear cryptanalysis, as an effective way to define a cryptographic algorithm in terms of linear equations [59, 106, 108]. A linear approximation table (LAT) is constructed by finding the probability of occurrence P of all input (ϱ) and output (ψ) linear masks where $\varrho, \psi \in F_2^n, F_2^m$ such that $\varrho \cdot \varkappa = \psi \cdot S(\varkappa)$. LAT can be mathematically represented as follows:-

$$\mathsf{LAT}(\varrho, \psi) = |\{\#\varkappa \mid \varrho \cdot \varkappa = \psi \cdot S(\varkappa)\}| - 2^{n-1} \tag{11}$$

Definition 1 The maximum LAT table entry is measured in the form of Linear Approximation Probability (LAP), mathematically given as follows:-

$$\xi = \frac{1}{2^n} \max_{\varrho,\psi \in F_2^n, F_2^m \setminus \{0\}} \left| \mathsf{LAT}(\varrho, \psi) \right| \tag{12}$$

The LAT table is of size $2^n \times 2^m$. The maximum LAT table entry and weight of coefficients in rows and columns stays is invariant under affine transformation, however the distribution of these entries is subject to change. Upper and lower bounds on all the entries of LAT are depicted in Table 4.

Non-linearity (NL)

Non-linearity is the measure of minimum hamming distance between the nonzero component functions of S and their relative affine linear functions. NL of boolean a function (f) is measured as follows:-

$$\mathsf{NL_f} = \min_{L(\varkappa) \in AL_n} dis(f(\varkappa), L(\varkappa)) \tag{13}$$

The NL of an $n \times m$ vectorial boolean mapping S is calculated using walsh spectrum $\mathsf{W}(\gamma, \rho)$, where $\gamma, \rho \in F_2^n$:-

$$\mathsf{W}(\gamma, \rho) = \sum_{\varkappa \in F_2^n} (-1)^{(\gamma \cdot S(\varkappa) \oplus \rho \cdot \varkappa)} \tag{14}$$

$$\mathsf{NL_S} = 2^{n-1} - \frac{1}{2} \max_{\gamma \in F_2^n, \rho \in F_2^m} |\mathsf{W}(\gamma, \rho)| \tag{15}$$

A high NL value is desirable in order to resist linear cryptanalysis. It is an affine invariant property of any mapping S [109–111].

Linear Branch Number (LBN)

In block cipher design strategy, branch number is a significant property used to measure the strength of an S-box against linear cryptanalysis. An S-box with high branch number could increase the diffusion power of a cryptographic algorithm. Mathematically:-

$$\mathsf{BN_L(S)} = \min_{\gamma \in F_2^n, \rho \in F_2^m \setminus \{0\}} \{w_t(\gamma) + w_t(\rho)\} \tag{16}$$

LBN is variant under affine transformation i.e. two S-boxes can be affine equivalent of each other but they can have different values of LBN [112].

Linear Structures (LS)

J.H. Evertse defines [65]:

> A block cipher has Linear Structures (LS) when there exist subsets of input, output and key bits, such that changing all the input and key bits has the same effect on the XOR of the output bits.

Definition 2 Let $f : F_2^n \to F_2$ be a Boolean function, then for some $\gamma \in F_2^n, f(\varkappa \oplus \gamma) \oplus f(\varkappa) = c$ holds for all $\varkappa \in F_2^n$ where $c \in F_2$ is a constant, then γ is called a LS of $f(\varkappa)$. More specifically, γ is called an invariant LS of $f(\varkappa)$ if $c = 0$ and a complementary LS of $f(\varkappa)$ if $c = 1$ [105].

Definition 3 Let $S : F_2^n \to F_2^m$ be a vectorial boolean mapping if for some $\gamma \in F_2^n, S(\varkappa \oplus \gamma) \oplus S(\varkappa) = c$ holds for all $\varkappa \in F_2^n$, where $c \in F_2^m$ is a constant, then γ is called a LS of $S(\varkappa)$. More specifically, γ is called an invariant LS of $S(\varkappa)$ if $c = 0$ and a complementary LS of $S(\varkappa)$ if $c = 1$ [113].

S-boxes having LS are vulnerable to attacks more robust than exhaustive key search, such as differential and linear cryptanalysis [114]. LS is an affine variant property of any boolean mapping S [88, 115].

Correlation Immunity (CI)

CI is an independent statistical property of boolean functions depicting linear combinations between the input and output bits of f.

Similarly, a boolean mapping $S : F_2^n \rightarrow F_2^m$ is said to be k^{th} order correlation immune (given $1 < k < n$), if all its coordinate functions $\gamma \cdot S(\varkappa)$ are independent of the linear combinations in its input. So using (14), we can say that S is k-order CI when [116]:-

$$\{\mathsf{W}(\gamma, \rho) = 0 : \ \gamma \in F_2^m \backslash \{0\}, \ \rho \in F_2^n, \ \forall \ 1 \leq wt(\rho) \leq k\} \tag{17}$$

CI shows variant behavior when an affine transformation is applied to S [88]. For a good cryptographic S-box the lower is the order of CI the better. CI shares an inverse relation with NL, hence if CI holds a lower order the value of NL will be high, and vice versa.

3.3 Differential Cryptanalysis

Differential cryptanalysis is a technique that relies on exploiting chosen plaintext pairs and resulting ciphertext pairs, in order to gain the information of secret key. The pairs of plaintext and ciphertext are referred as differentials. And these differentials when combined for multiple rounds become differential characteristics of a cipher under study [59]. The probabilities of occurrence of certain output (ciphertext) differences corresponding fixed input (plaintext) differences are computed in the form of DDT. A low value of differential uniformity, high differential branch number, high value of propagation characteristics, and no undisturbed bits are a requirement for an S-box to resist against differential cryptanalysis and its variant attacks.

Difference Distribution Table (DDT)

Given two inputs: $\varkappa$ and $\varkappa'$ and their corresponding outputs: $\flat$ and $\flat'$, the respective input and output differences can be mathematically represented as:-

$$\triangle_{\varkappa} = \varkappa \oplus \varkappa' \tag{18}$$

$$\triangle_{\flat} = \flat \oplus \flat' \tag{19}$$

Where $\varkappa, \varkappa' \in F_2^n$, $\flat, \flat' \in F_2^m$. Ideally, the probability that a particular output difference ($\triangle\flat$) occurs given a particular input difference ($\triangle\varkappa$) is $\frac{1}{2^{n-1}}$. Same as LAT, the lookup table of DDT is also of the dimension $2^n \times 2^m$. Mathematically:-

$$\mathsf{DDT}(\triangle_{\varkappa}, \triangle_{\flat}) = \#\{S(\varkappa \oplus \triangle_{\varkappa}) \oplus S(\varkappa) = \triangle_{\flat}\} \tag{20}$$

When an affine transformation is applied to S, DDT preserves the maximum entry and weight of coefficients in rows and columns, however their position is subject to a change [117, 118]. Table 4 illustrates bounds on the possible values a single input difference can map to against a single output difference, except for $\triangle_{\varkappa} = 0$. Notably, the sum of all entries for a given $\triangle_{\varkappa}$ is upper bounded by 2^n.

Definition 4 The maximum achievable value in the DDT of S is called the differential uniformity (DU) of S. It can be mathematically represented as follows [119]:-

$$\mathsf{DU_S} = \max_{\triangle_{\varkappa} \neq 0, \triangle_{\flat}} \#\mathsf{DDT}(\triangle_{\varkappa}, \triangle_{\flat}) \tag{21}$$

For an S-box to resist differential cryptanalysis a smaller value of DU is required. If an affine transformation is applied to S. DU stays invariant [118].

Differential Branch Number (DBN)

The diffusion power of a vectorial boolean mapping S is determined using differential branch number (DBN). It is measured by finding the minimum of hamming distance between two distinct inputs $\varkappa$, $\varkappa'$ and their corresponding outputs $S(\varkappa)$, $S(\varkappa')$. Mathematically [120]:-

$$\mathsf{BN_D(S)} = \min_{\varkappa, \varkappa' \in F_2^n, \varkappa \neq \varkappa'} \{wt(\varkappa \oplus \varkappa') \oplus wt(S(\varkappa) \oplus S(\varkappa'))\} \tag{22}$$

An S-box having DBN greater than 2 increases the chances of having more active S-boxes in iterative ciphers. DBN does not stay invariant under affine equivalence [112].

Propagation Criteria (PC)

A vectorial boolean function $S : F_2^n \to F_2^m$ is said to satisfy propagation criteria (PC) when $S_\gamma = S(\varkappa) \oplus S(\varkappa \oplus \gamma)$ is balanced given $\gamma \in F_2^n$. Mathematically S satisfy $PC(l)$ iff [88, 105, 121]:-

$$\triangle_S(\gamma, \rho) = 0 \tag{23}$$

For $1 \leq wt(\gamma) \leq l$.

$PC(l)$ of S is not variant when an affine transformation is applied [101]. An S-box satisfies PC when $ACT_{max} = 0$. For an S-box to satisfy SAC, complying with PC is a pre-requisite [88]. S-boxes having low order $PC(l)$ have weak diffusion characteristics [87].

Undisturbed Bits (UDB)

For a specific nonzero input difference $\triangle_\varkappa \in F_2^n$ of an S-box $S : F_2^n \to F_2^m$, some of the bits in the corresponding output difference $\triangle_\rho$ remain unchanged, these specific bits are referred to as undisturbed bits (UDB) [122].

Mathematically:-

$$\triangle_\flat = \{\triangle_\rho = \rho_j \in F_2^m \ | Pr_S(\triangle_\varkappa \to \triangle_\rho) > 0\} \tag{24}$$

Here $j = (0, 1, 2, ...m-1)$, if $\rho_j = d$, when $d \in F_2$ is fixed and $\triangle_\rho \in \triangle_\flat$ then S has UDBs. UDB is invariant under affine transformation. An S-box should have no UDB in order to avoid the construction of truncated differentials. Currently, there is no theoretically proven upper bound on UDB.

3.4 Boomerang Cryptanalysis

Boomerang attack is a technique of block cipher cryptanalysis based on the similar principle as differential cryptanlysis. However, instead of drawing one differential characteristic for the entire cipher, boomerang attack divides the cipher into two sub ciphers and generates two differentials characteristics also known as boomerang distinguishers. A low value of boomerang uniformity makes an S-box resistant towards boomerang attacks.

Boomerang Connectivity Table (BCT)

The dependency between these two boomerang differentials can have an influence on their combined probability, hence it is of significance to observe the switching effect between the two. In order to achieve this purpose and simplify the analysis, C. Cid *et al.* proposed the Boomerang Connectivity Table (BCT) [123].

BCT of S is given by a $2^n \times 2^m$ defined as $\beta T(\triangle_\varkappa, \nabla_\flat)$:-

$$\begin{aligned} \beta\mathsf{T}(\triangle_\varkappa, \nabla_\flat) = \#\{\varkappa \in F_2^n \big| \ & S^{-1}(S(\varkappa) \oplus \nabla_\flat) \oplus \\ & S^{-1}(S(\varkappa \oplus \triangle_\varkappa) \oplus \nabla_\flat) = \triangle_\varkappa\} \end{aligned} \tag{25}$$

$\triangle_\varkappa \in F_2^n$ = Input difference of S
$\nabla_\flat \in F_2^m$ = Output difference of S

Boomerang Uniformity (BU)

The highest value in BCT is known as the boomerang uniformity (BU); where $[\triangle_\varkappa, \nabla_\flat] \neq 0$ [67].

$$\beta\mathsf{U} = \max_{\triangle_\varkappa, \nabla_\flat \in F_2^n, F_2^m \setminus \{0\}} \beta T(\triangle_\varkappa, \nabla_\flat) \tag{26}$$

BCT and BU of an S-box are invariant under affine transformation [67, 88].

3.5 Differential-Linear Cryptanalysis

Differential linear attack proposed by Hellman and Langford [124] is based on dividing a block cipher into two parts and then combining both differential and linear characteristics into one attack that covers the whole cipher. Hence, the complexity of a differential linear attack is primarily based on the dependency between the two parts.

Differential Linear Connectivity Table (DLCT)

Bar-On *et al* [69] proposed Differential Linear Connectivity Table (DLCT) in order to study the dependencies between two parts of the cipher so that better differential and linear attack characteristics could be drawn. The DLCT of S is a $2^n \times 2^m$ table, where rows contain input differences and columns contain output bit masks. For $\triangle_\varkappa \in F_2^n$ and $\rho \in F_2^m$, the DLCT entry $(\triangle_\varkappa, \rho)$ can be computed mathematically as follows:-

$$\mathsf{DLCT}_S(\triangle_\varkappa, \rho) = \#\{\varkappa \in F_2^n \ | \ \ \rho \cdot S(\varkappa) = \rho \cdot S(\varkappa + \triangle_\varkappa)\} - 2^{n-1} \tag{27}$$

Differential Linear Uniformity (DLU)

The differential linear uniformity (DLU) of S can be defined by taking a maximum on $\mathsf{DLCT}_S(\triangle_\varkappa, \rho)$ for all nonzero values of $\triangle_\varkappa$ and ρ. Mathematically:-

$$\Gamma_S = \{\mathsf{DLCT}_S(\triangle_\varkappa, \rho), \triangle_\varkappa \in F_2^n \backslash \{0\} \text{ and } \rho \in F_2^m \backslash \{0\}\} \tag{28}$$

$$\mathsf{DLU}_S = \max(\Gamma_S) \tag{29}$$

Under affine equivalence, DLCT and DLU are invariant [92, 125]. In order to resist against differential linear attack, an S-box should have low DLU.

3.6 Algebraic Cryptanalysis

The basic idea behind algebraic attacks involves converting the entire block cipher round function into a system of equations and then trying to solve these equations in order to deduce the secret key. Both, non-linear and linear components are transformed into polynomials. Unlike the linear component, the number of variables for nonlinear layer increases after every next round. Optimal S-boxes are better resistant towards algebraic crypltanalysis if they have a high value of algebraic degree and algebraic immunity, and high degree of interpolation polynomial.

Algebraic Degree (AD)

The polynomial representation of a boolean function $f : F_2^n \to F_2$, is known as its Algebraic Normal Form (ANF) [88], written as:-

$$\begin{aligned} f(\varkappa) = c_0 \oplus c_1\varkappa_1 \oplus c_2\varkappa_2 \oplus ... \oplus c_n\varkappa_n \oplus \\ c_{12}\varkappa_1\varkappa_2 \oplus c_{13}\varkappa_1\varkappa_2 \oplus ... \oplus c_{(n-1)n}\varkappa_{(n-1)}\varkappa_n \\ ... \oplus c_{123.....n}\varkappa_1\varkappa_2\varkappa_3...\varkappa_n \end{aligned} \tag{30}$$

Where the coefficients $c_i \in F_2$ form the elements of the truth table for ANF of $f(\varkappa)$. An n-bit vectorial boolean function $S : F_2^n \to F_2^m$ has $f_j = f_1, f_2, f_3, ...f_n$ coordinate functions and each can be uniquely represented in the form of ANF.

$$f_j(\varkappa) = \sum_{j=1}^{n} C_j \prod_{j=1}^{n} \varkappa_j \tag{31}$$

AD is defined as the number of variables having non-zero coefficients in the highest product term of the ANF. Mathematically, for S, AD can be defined as:-

$$\mathsf{AD_S} = \max_{1 \le j \le n} [deg(f_j(\varkappa))] \tag{32}$$

The AD is an affine invariant property of any mapping S [88, 115]. S-boxess having a low AD are vulnerable to higher order differential attacks. AD has an inverse relation with CI, the higher is the order of CI, the lower is AD.

Interpolation Polynomial (IP)

In 1996, Jakobsen and Knudsen introduced interpolation attack on block ciphers [126]. In this attack the round function or S-boxes are represented in the form of algebraic expressions. In either case, Lagrange interpolation technique is used to evaluate the algebraic expression. The Lagrange polynomial is constructed using as many plaintext/ciphertext pairs as the number of unknown coefficients in the algebraic representation. Attack complexity depends on number of terms or degree of the resulting polynomial expression.

For any vectorial boolean mapping $S : F_2^n \to F_2^m$ with input $\varkappa_i = \{\varkappa_1, ..., \varkappa_n\}$ and output $\flat_i = \{\flat_1, ..., \flat_n\}$ where $i = 1, ..., n$, we find the Interpolation Polynomial (IP) $P_i(\varkappa)$ as follows:

$$P_i(\varkappa) = \sum_{i=1}^{n} \flat_i \prod_{j=1; j \neq i}^{n} \frac{\varkappa - \varkappa_j}{\flat_i - \flat_j} \tag{33}$$

IP is invariant under affine equivalence [127], and a low degree of IP makes any S-box susceptible to interpolation attack.

3.7 Side Channel Analysis

Attacks on cryptographic implementations have evolved significantly since Kocher's first attempt to use physical leakages from a cryptosystem to extract sensitive information. Due to the increasing threat, designers are always trying to come up with efficient ways to resist against side channel attacks [128]. Starting from the design of components such as S-boxes with good cryptographic properties to resist side channels and moving up to the overall cipher level by employing countermeasures such as boolean or polynomial masking. Properties such as DPA SNR and transparency order are nowadays actively used to determine an S-box's

resilience against DPA attacks. However, striking a perfect balance between the metrics related to traditional cryptanalysis and side channel analysis is an open research area. Currently, designers try to achieve cryptographic profiles that are well suited with the requirements of a particular infrastructure or standardization process (as in NIST LWC). In ideal terms, for an S-box to be resistant towards attacks such as DPA, it needs to posses a low DPA SNR and transparency order.

DPA SNR

Differential Power Analysis Signal to Noise Ratio (DPA SNR) was introduced by Sylvain G. *et al.* in order to improve the quality of leakges from CMOS circuits by modelling ghost peaks [72]. DPA SNR of $S : F_2^n \rightarrow F_2^m$ can be mathematically represented in form of walsh spectrum $\mathsf{W}(\gamma, \rho)$ (14), as follows:-

$$\mathsf{DPA_{SNR}(S)} = m2^{2n}\left(\sum_{\gamma \in F_2^n}\left(\sum_{\rho \in F_2^m, wt(\rho)=1} \mathsf{W}(\gamma,\rho)\right)^4\right)^{-\frac{1}{2}} \tag{34}$$

As per the authors, DPA SNR increases when resistance of S against linear and differential cryptanalysis increases and vice versa. Thus highlighting that alongside protected implementations, the choice of non-linear component also plays an important role in a block cipher's resistance against side channel attacks. DPA SNR of S is variant under affine transformation [95].

Transparency Order (TO)

Emmanuel P. *et al.* extended the concept of (DPA SNR) to evaluate the leakages in a multi-bit DPA setup using hamming weight power model [73].

It is mathematically represented as follows:-

$$\begin{aligned}\mathsf{TO} = \max_{\beta \in F_2^m}\left(\left|m - 2wt(\beta)\right|\right) \times \frac{1}{2^{2n}-2^n} \times \\ \left(\sum_{\gamma \in F_2^n}\left|\sum_{\rho \in F_2^m, wt(u)=1}(-1)^{\rho.\beta}\triangle_S(\gamma,\rho)\right|\right)\end{aligned} \tag{35}$$

If an S-box has small value of TO, it is considered highly resistant against DPA attacks [73]. When affine transformation is applied to an S-box, TO does not stay invariant [95].

4 Discussion and Results

We have given the details of our findings on Romulus, ASCON/ ISAP, Elephant, Photon-Beetle, and GIFT-COFB in Tables 6-7 against dedicated cryptographic profiles. We briefly explain them in subsequent subsections.

4.1 Diffusion Metrics

If we look at the basic avalanche characteristics of all these S-boxes they satisfy the criteria of balancedness. This helps reduce the chances of getting any high probability linear approximations, in turn assuring the resistance of these S-boxes towards linear cryptanalysis [93]. The S-boxes under analysis are bijective, so they satisfy the criteria of permutation. From the bounds discussed in Table 4, we have developed an understanding that ideally the S-boxes should have a full cycle length for order of permutation. Presumably, S-boxes having short iterative periods are vulnerable to attacks. In order to avoid such attacks designers can use affine equivalence to improve the order of permutation of these S-boxes [62, 63, 97, 98].

Out of the six, Ascon/ ISAP S-box has a FP at $\varkappa = 255$. Photon-Beetle/ Elephant/ GIFT-COFB, each has one OFPs at $\varkappa = 14/8/3$. S-boxes having FPs can alter the overall diffusion power that an iterative cipher has to offer and make it vulnerable to invariant subspace attacks, it may be rectified using affine equivalent S-box.

The upper bounded BIC value for all the S-boxes indicates that the input and output avalanche vectors are fully correlated.

Subsequently, none of the S-box satisfies the principles of completeness and avalanche depicted by their SAC failure. The AI values for all the S-boxes achieve the upper bound, and the values for that of SSI seem a bit better but do not satisfy the lower bound requirement. As discussed earlier, for an S-box to satisfy SAC, one of the prerequisites is compliance with PC. In Tables 6-7 we can see that all S-boxes have PC = 0, which again points towards the weak avalanche profile. These findings indicate that an attacker can utilize this information to mount statistical attacks on the underlying cipher [99, 129].

4.2 Linear Metrics

Security towards linear cryptanalysis attacks is ensured when an S-box has a low LAP and higher non linearity. Our results show that all 6 S-boxes under analysis have achieved the desired bounds for both properties. The LBN of all 6 S-boxes is closer to the LB, which is opposite to the ideal requirements. However, if the design requires it, LBN can be improved using affine transformations. The presence of LS makes it possible for the cipher to leak significant amount of information if specific group(s) of bits in the input are flipped. All the S-boxes are first order correlation immune, which makes them secure against zero-correlation attacks.

4.3 Differential and Boomerang Metrics

Almost Perfect Nonlinear (APN) S-boxes, in odd dimensions are differentially 2 uniform [63]. The only odd dimension case in S-boxes under study is of Ascon/ ISAP, and since its has a DU: 8. The remaining S-boxes have a DU within the desired bounds. The DBN of Elephant and Photon-Beetle S-box satisfies the UB, Ascon/ ISAP is closer to the UB, and for Romulus and GIFT-COFB DBN value stands on the LB. A good DBN ensures more number of active S-boxes across multiple rounds in block ciphers. The UDB are detected in all 6 S-boxes. In [122] authors have extensively described how the presence of UDB in an S-box impacts other cryptographic properties, such as the occurrence of LS, as we can see in Tables 6-7.
Tezcan et al. used these UDB and LS to devise 4 and 5 round impossible, truncated and improbab differentials, and break 5 out of 12 Ascon rounds [130].
In regards to boomerang cryptanalysis, the BU for all S-boxes is attaining the UB, which is opposite to the required bounds in order to be secure against Boomerang attacks.

4.4 Differential-Linear Metrics

Combined attacks make it easier for an attacker to break a cipher by defining short differential and linear characteristics, as in the case of differential-linear cryptanalysis. Hence, attaining the LB on DLU is crucial to gain resistance against these attacks. In case of S-boxes under analysis, we can observe from Tables 6-7, that the DLU is a little way up from the LB, hence paving a way for differential-linear attack with a reduced complexity.

4.5 Algebraic Metrics

Previously, we have talked about the inverse relation between CI and AD, and we observed that all 6 S-boxes have a CI = 0. So given the inverse relation, AD of all S-boxes should be obtaining the UB, which in our case is true. AD determines the complexity of an S-box's ANF, the higher the degree is the more complex it is to launch an algebraic attack on a cipher. S-boxes like those of Ascon/ ISAP having an AD = 2 are referred to as quadratic and those having AD = 3 are known as cubic. The functions that posses and AD = 1 are known as affine.

4.6 Side Channel Metrics

During design and analysis phase, DPA SNR and TO of S-box are the two metrics that can be used to determine a cipher's resistance towards SCA (DPA) attacks. From the conventional cryptanalysis perspective, S-boxes having a high NL and low DU are prone to SCA attacks and have a high resistance towards differential and linear cryptanalysis, and vice versa. Hence, finding the ideal balance between the two axes of attack metrics is crucial to the security of a lightweight block cipher. Since the S-boxes of LWC finalists vary in size (4, 5 and 8 bits), a direct comparison of the results we obtained of their side-channel metrics is not fair, since the required optimal bounds for each size are different (see Table 4). Hence to draw a meaningful comparison, we normalize the DPA SNR and TO using the ideal or worse case bounds as a reference point.

- DPA SNR can be normalized using the identity-case bound [72], as follows:

$$\mathsf{DPA_{SNR}(I)} = \sqrt{\mathsf{m}} \tag{36}$$

Here, in the case of a balanced S-box m is the number of input/output bits. We now define the normalized DPA SNR as follows:-

$$\mathsf{DPA_{SNR}(norm)} = \frac{\mathsf{DPA_{SNR}(S)} - \mathsf{DPA_{SNR}(I)}}{\mathsf{DPA_{SNR}(S)}} \tag{37}$$

The results of the suggested normalization are in the range $[0, 1]$. Here, a value 0 indicates that the S-box under analysis has a DPA SNR equal to that of an identity S-box, which theoretically is the best DPA SNR possible for an S-box to be resistant towards DPA attacks. For example, in the case of 8-bit S-box, the identity has a DPA SNR 2.82 and the DPA SNR of Romulus is 6.312455. The normalized DPA SNR in the 8-bit case is 0.552, suggesting that Romulus S-box potentially leaks 55.2% more than the identity S-box. In the case of 4-bit sbox, the identity has a DPA SNR 2, while GIFT, PHOTON and Elephant have DPA SNR 2.128608 and 2.398501, respectively. The normalized DPA SNR in the case of GIFT is

0.064304, and in the case of PHOTON and Elephant is 0.1992505, respectively. The normalization in the case of 4-bit S-boxes suggests GIFT has the lowest leakage amongst the three 4-bit S-boxes, as it leaks only 6.4304% more than the 4-bit identity S-box.

- TO can be normalized using the worse-case (highest leakage) bound [73], as follows:-

$$\mathsf{TO}_{\mathsf{highest-leakage}} = \mathsf{m} \tag{38}$$

Here, in the case of a balanced S-box m is the number of input/output bits. Based on the worse-case bound, we now define the normalized TO as follows:-

$$\mathsf{TO(norm)} = \frac{\mathsf{TO}_{\mathsf{highest-leakage}} - \mathsf{TO_S}}{\mathsf{TO}_{\mathsf{highest-leakage}}} \tag{39}$$

The results of this normalization lie in the range [0,1], where a factor 0 depicts that the TO is the same as the worst-case scenario, i.e., the maximum TO value, implying the highest leakage in the case of DPA attacks. Any value greater than 0 suggests relative improvement in the TO value and hence reduced leakage. For example, in the case of 8-bit S-box, the worse-case TO is 8 and the TO of Romulus is 7.174510. The normalized TO in the 8-bit case is 0.1031, suggesting that Romulus S-box potentially leaks 10.31% less than the worse-case S-box.

5 Exploring Trade-offs in S-box Design

Based on our analysis in Section 4, several finalist S-boxes exhibit weaknesses in classical cryptographic metrics — such as fixed points, differential uniformity, non-linearity, linear structures, etc. So to explore the possibility of improving the cryptographic robustness of S-boxes beyond those used in the NIST LWC finalists, we generated a new 4×4 bit test S-box using the PEIGEN [75] tool for S-box evaluation and generation, as shown in Table 8, using the following constraints:-

- Permutation: ✓
- Differential Uniformity: 4
- Algebraic Degree: 3
- Linear Structures: 0
- Implementation Cost: 8

In PEIGEN, cost is a composite metric that captures the implementation efficiency in terms of both hardware and software, focusing on the following traits:-

- Gate Equivalent (GE): refers to a 2-input NAND gate unit,
- Bitslice Gate: for software implementations (optimized 32-bits),
- Circuit depth in terms of latency (depth vs area), and
- Multiplicative complexity: minimizing number of non-linear operations (for side channel secure ciphers where masking and other countermeasures are involved).

Table 8: Proposed 4-bit S-box

4-bit	0	4	5	1	c	9	6	7	3	a	e	8	b	2	f	d

Fixing the implementation cost ensures that the resultant S-box implementation lies within the acceptable practical bounds for lightweight cryptography implementations, while retaining the desired cryptographic profile.

5.1 Comparison and Analysis

Table 7, highlights the comparison between the S-box new 4-bit S-box and and the 4-bit S-boxes from GIFT-COFB, Photon-Beetle and Elephant. From the classical cryptanalysis perspective all four S-boxes have the same differential uniformity, non-linearity, linear approximation, algebraic degree and correlation immunity. A noticeable difference occurs in the properties of the new S-box when compared to the other three, as follows:-

- The values for BIC and SAC are better.
- No linear structures and undisturbed bits.
- Boomerang uniformity has improved.

Some of the trade-offs that exist in the properties of the new S-box are as follows:-

- 3 fixed points are present in the new S-box while the others have null.

- DPA-SNR value of 2.5786 is a little higher than for all three finalists, indicating slightly weaker resistance to side-channel (DPA) leakage, but offers optimal resistance against conventional cryptanalysis.

- TO of 3.4 is a little higher than that of Elephant (3.26), but a little lower than that of PHOTON and GIFT-COFB, indicating a reasonable balance between leakage and classical security.

The current findings underscore that even when the classical cryptanalysis properties are optimized within practical bounds, striking a perfect balance with the side-channel metrics may not be possible. In practice, identifying such balanced S-boxes remains a trial-and-error process that involves testing multiple generation strategies and parameter choices until an acceptable trade-off is found. Moreover, it is important to emphasize that the S-box alone does not define the overall security of a lightweight block cipher. Resistance to differential and linear cryptanalysis, as well as to side-channel analysis, also depends heavily on other design aspects such as the diffusion layer, round constants, and key schedule, etc. A strong S-box is therefore only one building block of a well-rounded cryptographic primitive.

6 Scope and Limitations

Our research presents a comprehensive evaluation of the cryptographic properties of S-boxes used in finalist ciphers of the NIST LWC competition. For the sake of clarity and accuracy it is important that we acknowledge the scope and limitations of our analysis.

Firstly, we would like to clarify that our analysis of S-boxes is conducted from a theoretical and metric-based perspective. We do not claim to perform any practical side-channel attacks (e.g., DPA, SPA) or cryptanalytic attacks (e.g., differential, linear) on the full/reduced-rounds structure of NIST LWC finalists.

Strong S-boxes contribute significantly to overall cipher security. We have evaluated the S-boxes individually, based on well-established cryptographic metrics listed in Table 3. Such compact analysis is a crucial first-step in determining the strength of the confusion layer when designing a new cipher, but it should be noted that full cipher-level cryptanalysis and side-channel analysis requires holistic evaluation – involving linear layers, modes of encryption, masking strategies, implementation environments, and leakage models. These are beyond the scope of this study and can be seen as potential future work.

Therefore, we specifically refrain from extrapolating our S-box component-level findings to make any assertions on the overall security strength of the cipher.

7 Conclusion

Since the announcement of NIST lightweight cryptography competition, a considerable number of attacks have been published for exploiting the vulnerabilities in the non-linear component of the competitors under consideration. This paper presents a detailed cryptographic security analysis of the S-boxes of six finalists, examining the 24 cryptographic properties that are relevant to established attack methods (see3). These six S-boxes exhibit characteristics such as high SAC and BIC values, degree-2 polynomials, and undisturbed bits — that may increase the susceptibility to known differential, linear, and boomerang attacks. The existence of degree 2 polynomials is the primary source of linear structures, followed by undisturbed bits. Improving the S-box design may, therefore, help improve their overall security margin of these offered by these permutations.

8 Declarations

Author Contribution Statement:

All authors contributed equally to the writing of the manuscript.

Author Competing Interest statement: Sajid Ali Khan has position on editorial board of Discover Computing, and was not involved in the review or decisions related to this manuscript. The other authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration:

Not applicable

Ethics and Consent to Participate declarations:

Not applicable

Consent for publication Declaration:

Not applicable

Ethics, Consent to Participate, and Consent to Publish declarations: Not Applicable

Availability of Data: The data that support the findings of this study are available from the corresponding author, upon request.

Preprint: A preprint of this article is available at [131]

References

[1] Subramanian, S., Mozaffari-Kermani, M., Azarderakhsh, R., Nojoumian, M.: Reliable hardware architectures for cryptographic block ciphers led and hight. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **36**(10), 1750–1758 (2017) https://doi.org/10.1109/TCAD.2017.2661811

[2] Bassham, L., Çalık, Ç., McKay, K., Turan, M.S.: Submission requirements and evaluation criteria for the lightweight cryptography standardization process. US National Institute of Standards and Technology (2018)

[3] Turan, M.S., McKay, K., Chang, D., Calik, C., Bassham, L., Kang, J., Kelsey, J., et al.: Status report on the second round of the nist lightweight cryptography standardization process. National Institute of Standards and Technology Internal Report **8369** (2021)

[4] Division, C.S.: Finalists - lightweight cryptography: Csrc. CSRC

[5] Turan, M.S., McKay, K., Chang, D., Kang, J., Waller, N., Kelsey, J.M., Bassham, L.E., Hong, D.: Status report on the final round of the nist lightweight cryptography standardization process. NIST (2023)

[6] CSRC, N.-: Announcing lightweight cryptography selection — $csrc_2023$. NIST — CSRC (2023)

[7] Tezcan, C.: Analysis of ascon, drygascon, and shamash permutations. Cryptology ePrint Archive, Report 2020/1458 (2020)

[8] Li, Y., Zhang, G., Wang, W., Wang, M.: Cryptanalysis of round-reduced ascon. Science China Information Sciences **60**(3), 1–2 (2017)

[9] Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Cryptanalysis of ascon. Topics in Cryptology — CT-RSA 2015, 371–387 (2015)

[10] Duarte-Sanchez, J.E., Halak, B.: In: Halak, B. (ed.) A Cube Attack on a Trojan-Compromised Hardware Implementation of Ascon, pp. 69–88. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-62707-2_2

[11] Erlacher, J., Mendel, F., Eichlseder, M.: Bounds for the security of ascon against differential and linear cryptanalysis. IACR Transactions on Symmetric Cryptology **2022**(1), 64–87 (2022) https://doi.org/10.46586/tosc.v2022.i1.64-87

[12] El Hirch, S., Mella, S., Mehrdad, A., Daemen, J.: Improved differential and linear trail bounds for ascon. IACR Transactions on Symmetric Cryptology **2022**(4), 145–178 (2022) https://doi.org/10.46586/tosc.v2022.i4.145-178

[13] Leander, G., Tezcan, C., Wiemer, F.: Searching for subspace trails and truncated differentials. IACR Transactions on Symmetric Cryptology **2018**(1), 74–100 (2018) https://doi.org/10.13154/tosc.v2018.i1.74-100

[14] Baksi, A., Breier, J., Chen, Y., Dong, X.: Machine learning assisted differential distinguishers for lightweight ciphers. 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), 176–181 (2021) https://doi.org/10.23919/DATE51398.2021.9474092

[15] Dobraunig, C., Eichlseder, M., Mendel, F.: Heuristic tool for linear cryptanalysis with applications to caesar candidates. Advances in Cryptology – ASIACRYPT 2015, 490–509 (2015)

[16] Kannwischer, M.J., Pessl, P., Primas, R.: Single-trace attacks on keccak. IACR Transactions on Cryptographic Hardware and Embedded Systems **2020**(3), 243–268 (2020) https://doi.org/10.13154/tches.v2020.i3.243-268

[17] Udvarhelyi, B., Bronchain, O., Standaert, F.-X.: Security analysis of deterministic re-keying

with masking and shuffling: Application to isap. International Workshop on Constructive Side-Channel Analysis and Secure Design, 168–183 (2021). Springer

[18] CUI, Y., XU, H., QI, W.: Milp-based linear attacks on round-reduced gift. Chinese Journal of Electronics **31**(1), 89–98 (2022) https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/cje.2020.00.113

[19] Cao, M., Zhang, W.: Related-key differential cryptanalysis of the reduced-round block cipher gift. IEEE Access **7**, 175769–175778 (2019) https://doi.org/10.1109/ACCESS.2019.2957581

[20] Eskandari, Z., Kidmose, A.B., Kölbl, S., Tiessen, T.: Finding integral distinguishers with ease. Selected Areas in Cryptography – SAC 2018, 115–138 (2019)

[21] Ji, F., Zhang, W., Zhou, C., Ding, T.: Improved (related-key) differential cryptanalysis on gift. International Conference on Selected Areas in Cryptography, 198–228 (2020). Springer

[22] Sun, L., Wang, W., Wang, M.: Linear cryptanalyses of three aeads with gift-128 as underlying primitives. IACR Transactions on Symmetric Cryptology **2021**(2), 199–221 (2021)

[23] Zhu, B., Dong, X., Yu, H.: Milp-based differential attack on round-reduced gift. Cryptology ePrint Archive, Paper 2018/390 (2018). https://eprint.iacr.org/2018/390

[24] Inoue, A., Minematsu, K.: Gift-cofb is tightly birthday secure with encryption queries. Cryptology ePrint Archive, Paper 2021/737 (2021). https://eprint.iacr.org/2021/737

[25] Jang, K., Kim, H., Eum, S., Seo, H.: Grover on gift. Cryptology ePrint Archive, Paper 2020/1405 (2020). https://eprint.iacr.org/2020/1405

[26] Picek, S., Ege, B., Papagiannopoulos, K., Batina, L., Jakobović, D.: Optimality and beyond: The case of 4×4 s-boxes. 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 80–83 (2014) https://doi.org/10.1109/HST.2014.6855573

[27] Jana, A., Paul, G.: Differential fault attack on photon-beetle. Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security, 25–34 (2022) https://doi.org/10.1145/3560834.3563824

[28] Dobraunig, C., Mennink, B.: Key recovery attack on photon-beetle. NIST, Gaithersburg, MD, USA, Tech. Rep (2020)

[29] Inoue, A., Iwata, T., Minematsu, K.: Analyzing the provable security bounds of gift-cofb and photon-beetle. Cryptology ePrint Archive, Paper 2022/001 (2022). https://eprint.iacr.org/2022/001

[30] Guo, J., Peyrin, T., Poschmann, A.: The photon family of lightweight hash functions. Advances in Cryptology – CRYPTO 2011, 222–239 (2011)

[31] Cui, T., Sun, L., Chen, H., Wang, M.: Statistical integral distinguisher with multi-structure and its application on aes. Information Security and Privacy, 402–420 (2017)

[32] Jean, J., Naya-Plasencia, M., Peyrin, T.: Multiple limited-birthday distinguishers and applications. Selected Areas in Cryptography – SAC 2013, 533–550 (2014)

[33] Zhou, H., Zong, R., Dong, X., Jia, K., Meier, W.: Interpolation attacks on round-reduced elephant, kravatte and xoofff. The Computer Journal **64**(4), 628–638 (2021)

[34] Joshi, P., Mazumdar, B.: Single event transient fault analysis of ELEPHANT cipher. CoRR **abs/2106.09536** (2021) 2106.09536

[35] Meraneh, A.H., Clavier, C., Le Bouder, H., Maillard, J., Thomas, G.: Blind side channel on the elephant lfsr. SECRYPT 2022 (2022)

[36] Beyne, T., Chen, Y.L., Dobraunig, C., Mennink, B.: Multi-user security of the elephant v2 authenticated encryption mode. Selected Areas in Cryptography, 155–178 (2022)

[37] Alagic, G., Bai, C., Katz, J., Majenz, C., Struck, P.: Post-quantum security of the (tweakable) fx construction, and applications. Cryptology ePrint Archive, Paper 2022/1097 (2022). https://eprint.iacr.org/2022/1097

[38] Tolba, M., Abdelkhalek, A., Youssef, A.M.: Impossible differential cryptanalysis of reduced-round skinny. Progress in Cryptology - AFRICACRYPT 2017, 117–134 (2017)

[39] Habu, M., , Minematsu, K., Iwata, T.: Matching attacks on romulus-m. Cryptology ePrint Archive, Report 2022/369 (2022)

[40] Dong, X., Hua, J., Sun, S., Li, Z., Wang, X., Hu, L.: Meet-in-the-middle attacks revisited: Key-recovery, collision, and preimage attacks. Cryptology ePrint Archive, Report 2021/427 (2021)

[41] Hadipour, H., Sadeghi, S., Eichlseder, M.: Finding the impossible: Automated search for full impossible-differential, zero-correlation, and integral attacks. Cryptology ePrint Archive, Paper 2022/1147 (2022) https://doi.org/10.1007/978-3-031-30634-1_5 . https://eprint.iacr.org/2022/1147

[42] Shi, D., Sun, S., Derbez, P., Todo, Y., Sun, B., Hu, L.: Programming the demirci-selçuk meet-in-the-middle attack with constraints. Advances in Cryptology – ASIACRYPT 2018, 3–34 (2018)

[43] Qin, L., Dong, X., Wang, X., Jia, K., Liu, Y.: Automated search oriented to key recovery on ciphers with linear key schedule: Applications to boomerangs in skinny and forkskinny. IACR Transactions on Symmetric Cryptology **2021**(2), 249–291 (2021) https://doi.org/10.46586/tosc.v2021.i2.249-291

[44] Bijwe, S., Chauhan, A.K., Sanadhya, S.K.: Implementing grover oracle for lightweight block ciphers under depth constraints. Information Security and Privacy, 85–105 (2022)

[45] Tezcan: Truncated, impossible, and improbable differential analysis of ascon. Cryptology ePrint Archive, Report 2016/490 (2016)

[46] Peng, S., Hu, K., He, J., Wang, M.: Improved key recovery attacks of ascon. In: Cryptographers' Track at the RSA Conference, pp. 123–146 (2025). Springer

[47] Nguyen, V.S., Grosso, V., Cayrel, P.-L.: Correlation power analysis on ascon with multi-bit selection function. International Conference on Security and Cryptography (SECRYPT) (2025)

[48] Jana, A.: Differential fault attack on ascon cipher. International Conference on Cryptology in India, 53–72 (2024). Springer

[49] Zhai, D., Bai, W., Fu, J., Gao, H., Zhu, X.: Improved 2-round collision attack on iot hash standard ascon-hash. Heliyon **10**(5) (2024)

[50] Fu, Q., Luo, Y., Yang, Q., Song, L.: Preimage and collision attacks on reduced ascon using algebraic strategies. Cybersecurity **8**(1), 1–17 (2025)

[51] Zhu, B., Dong, X., Yu, H.: Milp-based differential attack on round-reduced gift. Topics in Cryptology – CT-RSA 2019, 372–390 (2019)

[52] Jana, A., Paul, G.: Differential fault attack on spn-based sponge and siv-like ae schemes. Journal of Cryptographic Engineering **14**(2), 363–381 (2024)

[53] Krämer, J., Struck, P., Weishäupl, M.: Committing ae from sponges: Security analysis of the nist lwc finalists. IACR Transactions on Symmetric Cryptology **2024**(4), 191–248 (2024) https://doi.org/10.46586/tosc.v2024.i4.191-248

[54] Dong, X., Zhao, B., Qin, L., Hou, Q., Zhang, S., Wang, X.: Generic mitm attack frameworks on sponge constructions. Annual International Cryptology Conference, 3–37 (2024). Springer

[55] Zhang, J., Wang, H., Tang, D.: Impossible boomerang attacks revisited: Applications to deoxys-bc, joltik-bc and skinny. IACR Transactions on Symmetric Cryptology **2024**(2), 254–295 (2024) https://doi.org/10.46586/tosc.v2024.i2.254-295

[56] Ahmadian, Z., Khalesi, A., M'Foukh, D., Moghimi, H., Naya-Plasencia, M.: Improved differential meet-in-the-middle cryptanalysis. Advances in Cryptology – EUROCRYPT 2024, 280–309 (2024)

[57] Song, L., Fu, Q., Yang, Q., Lv, Y., Hu, L.: Generalized impossible differential attacks on block ciphers: application to skinny and forkskinny. Designs, Codes and Cryptography, 1–45 (2025)

[58] Perrin, L.P.: On the properties of s-boxes: A study of differentially 6-uniform monomials over finite fields of characteristic 2 (2013)

[59] Heys, H.M.: A tutorial on linear and differential cryptanalysis. Cryptologia **26**(3), 189–221 (2002)

[60] Ishfaq, F.: A matlab tool for the analysis of cryptographic properties of s-boxes. Capital University (2018)

[61] Seitkulov, Y., Ospanov, R., Yergaliyeva, B.: On cryptographic properties of s-boxes. Engineering Journal of Satbayev University **143**(4), 96–103 (2021)

[62] Nitaj, A., Susilo, W., Tonien, J.: A new improved aes s-box with enhanced properties. Cryptology ePrint Archive, Paper 2020/1597 (2020) https://doi.org/10.1007/978-3-030-55304-3

[63] afify*, E.w., sobky, W.I., Twakol, A., Alez, R.A.: Algebraic construction of powerful substitution box. International Journal of Recent Technology and Engineering (IJRTE) **8**(6), 405–409 (2020) https://doi.org/10.35940/ijrte.d8279.038620

[64] Zahid, A.H., Rashid, H., Shaban, M.M.U., Ahmad, S., Ahmed, E., Amjad, M.T., Baig, M.A.T., Arshad, M.J., Tariq, M.N., Tariq, M.W., *et al.*: Dynamic s-box design using a novel square polynomial transformation and permutation. IEEE Access **9**, 82390–82401 (2021)

[65] Evertse, J.-H.: Linear structures in blockciphers. Workshop on the Theory and Application of of Cryptographic Techniques, 249–266 (1987). Springer

[66] Nyberg, K.: Modifications of bijective s-boxes with linear structures. Cryptography and Communications **15**(3), 617–625 (2023)

[67] Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic sboxes. IACR Transactions on Symmetric Cryptology, 290–310 (2018)

[68] Tezcan, C., Özbudak, F.: Differential factors: Improved attacks on serpent. International Workshop on Lightweight Cryptography for Security and Privacy, 69–84 (2014). Springer

[69] Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: Dlct: a new tool for differential-linear cryptanalysis. Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part I 38, 313–342 (2019). Springer

[70] Kim, H., Kim, S., Hong, D., Sung, J., Hong, S.: Improved differential-linear cryptanalysis using dlct. Journal of The Korea Institute of Information Security & Cryptology **28**(6), 1379–1392 (2018)

[71] Canteaut, A.: Lecture notes on cryptographic boolean functions. Inria, Paris, France **3** (2016)

[72] Guilley, S., Hoogvorst, P., Pacalet, R.: Differential power analysis model and some results.

CARDIS, 127–142 (2004)

[73] Prouff, E.: Dpa attacks and s-boxes. International Workshop on Fast Software Encryption, 424–441 (2005). Springer

[74] Naseer, M., Tariq, S., Riaz, N.: Substitution layer analysis of nist lightweight cryptography competition finalists. 2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 659–664 (2022) https://doi.org/10.1109/IBCAST54850.2022.9990069

[75] Bao, Z., Guo, J., Ling, S., Sasaki, Y.: SoK: Peigen – a platform for evaluation, implementation, and generation of s-boxes (2019)

[76] Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1. 2: Lightweight authenticated encryption and hashing. Journal of Cryptology **34**(3), 1–42 (2021)

[77] Dobraunig, C., Eichlseder, M., Mangard, S., Mendel, F., Mennink, B., Primas, R., Unterluggauer, T.: Isap v2.0. NIST Lightweight Cryptography (2020)

[78] Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Todo, Y.: Gift-cofb. NIST (2019)

[79] Bao, Z., Chakraborti, A., Datta, N., Guo, J., Nandi, M., Peyrin, T., Yasuda, K.: Photon-beetle authenticated encryption and hash family. NIST Lightweight Compet. Round **1**, 115 (2019)

[80] Beyne, T., Chen, Y.L., Dobraunig, C., Mennink, B.: Elephant v2. NIST Lightweight Cryptography (2021)

[81] Guo, C., Iwata, T., Khairallah, M., Minematsu, K., Peyrin, T.: Romulus (2021)

[82] Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The skinny family of block ciphers and its low-latency variant mantis. Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36, 123–153 (2016). Springer

[83] Cubero, J.A.Á.: Vector boolean functions: Applications in symmetric cryptography (2015) https://doi.org/10.13140/RG.2.2.12540.23685

[84] Khadem, B., Rajavzade, S.: Construction of side channel attacks resistant s-boxes using genetic algorithms based on coordinate functions. arXiv preprint arXiv:2102.09799 (2021)

[85] O'Connor, L.: Properties of linear approximation tables. Fast Software Encryption (FSE), 131–136 (1995)

[86] Bakunina, E., Dykyi, O.: Synthesis method for s-boxes satisfying the criterion of correlation immunity of boolean and 4-functions. Journal of Discrete Mathematical Sciences and Cryptography, 1–13 (2022)

[87] Álvarez-Cubero, J.A., Zufiria, P.J.: Cryptographic Criteria on Vector Boolean Functions. InTech, ??? (2012)

[88] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, ??? (2021)

[89] Sarkar, S., Syed, H.: Bounds on differential and linear branch number of permutations. Cryptology ePrint Archive (2017)

[90] Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. application to skinny and aes. IACR Transactions on Symmetric Cryptology, 118–141 (2019)

[91] Canteaut, A., Kölsch, L., Li, C., Li, C., Li, K., Qu, L., Wiemer, F.: Autocorrelations of vectorial boolean functions. International Conference on Cryptology and Information Security in Latin

America, 233–253 (2021). Springer

[92] Canteaut, A., Kolsch, L., Li, C., Li, C., Li, K., Qu, L., Wiemer, F.: On the differential-linear connectivity table of vectorial boolean functions. arXiv preprint arXiv:1908.07445 (2019)

[93] Farwa, S., Shah, T., Idrees, L.: A highly nonlinear s-box based on a fractional linear transformation. Springer **5**(1), 1–12 (2016)

[94] Sagdıçoglu, S.: Cryptological viewpoint of boolean functions (2003)

[95] Picek, S., Yang, B., Mentens, N.: A search strategy to optimize the affine variant properties of s-boxes. International Workshop on the Arithmetic of Finite Fields, 208–223 (2016). Springer

[96] Musukwa, A., Sala, M., Zaninelli, M.: On some cryptographic properties of boolean functions and their second-order derivatives. arXiv preprint arXiv:1909.10586 (2019)

[97] Cui, J., Huang, L., Zhong, H., Chang, C., Yang, W.: An improved aes s-box and its performance analysis. International Journal of Innovative Computing, Information and Control **7**(5), 2291–2302 (2011)

[98] Seghier, A., Li, J., Sun, D.Z.: Advanced encryption standard based on key dependent s-box cube. IET Information Security **13**(6), 552–558 (2019)

[99] Webster, A., Tavares, S.E.: On the design of s-boxes. Conference on the theory and application of cryptographic techniques, 523–534 (1985). Springer

[100] Ao, T., Rao, J., Dai, K., Zou, X.: Construction of high quality key-dependent s-boxes. Nonlinearity (Ns) **13**(14), 15 (2017)

[101] Sağdıçoğlu, S.: Cryptological viewpoint of boolean function. Master's thesis, Middle East Technical University (2003)

[102] Canteaut, A., Kölsch, L., Wiemer, F.: Observations on the dlct and absolute indicators. Cryptology ePrint Archive (2019)

[103] Dinur, I., Shamir, A.: Breaking grain-128 with dynamic cube attacks. Fast Software Encryption, 167–187 (2011)

[104] LI, Z., JIANG, N., ZHUO, Z.: Further results on autocorrelation of vectorial boolean functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2022–1096 (2023)

[105] Zhang, X.-M., Zheng, Y.: Gac—the criterion for global avalanche characteristics of cryptographic functions. J. UCS The Journal of Universal Computer Science: Annual Print and CD-ROM Archive Edition Volume 1• 1995, 320–337 (1996)

[106] Matsui, M.: Linear cryptanalysis method for des cipher. Workshop on the Theory and Application of of Cryptographic Techniques, 386–397 (1993). Springer

[107] Daemen, J., Rijmen, V.: The wide trail design strategy. Cryptography and Coding: 8th IMA International Conference Cirencester, UK, December 17–19, 2001 Proceedings 8, 222–238 (2001). Springer

[108] Matsui, M.: The first experimental cryptanalysis of the data encryption standard. Annual International Cryptology Conference, 1–11 (1994). Springer

[109] Meier, W., Staffelbach, O.: Nonlinearity criteria for cryptographic functions. Workshop on the Theory and Application of of Cryptographic Techniques, 549–562 (1989). Springer

[110] Waqas, U., Afzal, S., Mir, M.A., Yousaf, M.: Generation of aes-like s-boxes by replacing affine matrix. 2014 12th International Conference on Frontiers of Information Technology, 159–164

(2014). IEEE

[111] Carlet, C., Crama, Y., Hammer, P.L.: Vectorial boolean functions for cryptography. (2010)

[112] Sarkar, S., Mandal, K., Saha, D.: On the relationship between resilient boolean functions and linear branch number of s-boxes. International Conference on Cryptology in India, 361–374 (2019). Springer

[113] Baksi, A., Bhasin, S., Breier, J., Khairallah, M., Peyrin, T., Sarkar, S., Sim, S.M.: Default: Cipher level resistance against differential fault attack. Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27, 124–156 (2021). Springer

[114] Dobbertin, H., Leander, G.: A survey of some recent results on bent functions. International Conference on Sequences and Their Applications, 1–29 (2004). Springer

[115] Nizam Chew, L.C., Ismail, E.S.: S-box construction based on linear fractional transformation and permutation function. Symmetry **12**(5), 826 (2020) https://doi.org/10.3390/sym12050826

[116] Mukherjee, C.S., Roy, D., Maitra, S.: Design and Cryptanalysis of ZUC: A Stream Cipher in Mobile Telephony. Springer, ??? (2021)

[117] Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic sboxes. IACR Transactions on Symmetric Cryptology **2018**(3), 290–310 (2018) https://doi.org/10.13154/tosc.v2018.i3.290-310

[118] Bao, Z., Guo, J., Ling, S., Sasaki, Y.: Peigen–a platform for evaluation, implementation, and generation of s-boxes. IACR Transactions on Symmetric Cryptology, 330–394 (2019)

[119] Hasan, S.U., Pal, M., Stănică, P.: The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials. IEEE Transactions on Information Theory **68**(1), 679–691 (2021)

[120] Sarkar, S., Syed, H.: Bounds on differential and linear branch number of permutations. Australasian conference on information security and privacy, 207–224 (2018). Springer

[121] Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R., Vandewalle, J.: Propagation characteristics of boolean functions. Advances in Cryptology—EUROCRYPT'90: Workshop on the Theory and Application of Cryptographic Techniques Aarhus, Denmark, May 21–24, 1990 Proceedings 9, 161–173 (1991). Springer

[122] Makarim, R.H., Tezcan, C.: Relating undisturbed bits to other properties of substitution boxes. International workshop on lightweight cryptography for security and privacy, 109–125 (2014). Springer

[123] Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: a new cryptanalysis tool. Annual International Conference on the Theory and Applications of Cryptographic Techniques, 683–714 (2018). Springer

[124] Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. Advances in Cryptology—CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings 14, 17–25 (1994). Springer

[125] Jeong, J., Koo, N., Kwon, S.: New differentially 4-uniform permutations from modifications of the inverse function. Finite Fields and Their Applications **77**, 101931 (2022) https://doi.org/10.1016/j.ffa.2021.101931

[126] Jakobsen, T., Knudsen, L.R.: The interpolation attack on block ciphers. Fast Software Encryption: 4th International Workshop, FSE'97 Haifa, Israel, January 20–22 1997 Proceedings 4,

28–40 (1997). Springer

[127] Calvi, J.-P.: Lectures on multivariate polynomial interpolation (2005)

[128] Kocher, P., Jaffe, J., Jun, B., Rohatgi, P.: Introduction to differential power analysis. Journal of Cryptographic Engineering **1**, 5–27 (2011)

[129] Singh, A., Agarwal, P., Chand, M.: Analysis of development of dynamic s-box generation. Comput. Sci. Inf. Technol **5**(5), 154–163 (2017)

[130] Tezcan, C.: Truncated, impossible, and improbable differential analysis of ascon. Cryptology ePrint Archive (2016)

[131] Naseer, M., Tariq, S., Riaz, N., Ahmed, N., Hussain, M.: S-box security analysis of nist lightweight cryptography candidates: A critical empirical study. arXiv preprint arXiv:2404.06094 (2024)