The Reality of Backdoored S-Boxes - An Eye Opener

Shah Fahd[a], Mehreen Afzal[a], Waseem Iqbal[a,*], Dawood Shah[b], Ijaz Khalid[b]

[a]*Department of Information Security, National University of Sciences and Technology, H-12, Islamabad, 44000, Pakistan*
[b]*Department of Mathematics, Quaid-i-Azam University, Islamabad, 45320, Pakistan*

Abstract

The analysis of real-life incidents has revealed that state-level efforts are made to camouflage the intentional flaws in the mathematical layer of an S-Box to exploit the information-theoretic properties, i.e., Kuznyechik. To extract and investigate the common features in the backdoored S-Box(es), this research thoroughly examines them from the perspective of 24 cryptanalytic attack vectors available in the open literature. We have debunked the earlier claims by the backdoor engineers that their designs are stealthy against statistical distinguishers. A backdoored architecture fulfils the notions of randomness but lacks the strength to resist sophisticated cryptanalytic attacks. Our analysis has revealed that during the backdoor insertion phase, a malicious designer compromises vital cryptographic properties, prominently the algebraic degree, differential trails, avalanche characteristics and leaving the open ground for hybrid attacks. It is observed that these mappings attain the upper bound of BCT, FBCT and DLCT, thus paving the way for hybrid attacks with high probability.

Keywords: Information Security, Cryptography, Backdoors, S-Box, Cryptanalysis, Quotient Groups, Nontrivial Subspaces, Linear Structures

1. Introduction

For millennia the famous Ceaser Cipher remained unbreakable. Al-Kindi exploited the natural language redundancies by observing the frequency distribution of alphabets in monoalphabetic ciphers. Claude Shannon coined the idea of confusion and diffusion to mitigate the risk of language redundancies [1, 2]. Lucifer [3], and DES [4] are engineered by the team of cryptographers at IBM on the principles devised in [1, 2]. With time matured and well-designed modern-day block ciphers are implemented and deployed worldwide [5, 6, 7, 8, 9]. Considering the importance of an S-Box as a nonlinear component, cryptographers put their best efforts into the design phase for mandated security [10, 11]. The ciphertext does not reveal any information about the plaintext, and the statistical distinguisher observes no pattern. Cryptanalysts tried to develop the latest attacks for exploiting the nonlinear properties of S-Box(es) [12, 13]. These attacks helped the cryptographic community in refining the design process [14].

The cracking of a well-designed cryptosystem is infeasible in polynomial time for adversaries. To defy the mandated security, the hostile agencies force the designers to blanket intentional weaknesses. The academia has pointed out the possibility of cryptographic abuses via subliminal channels in earlier manuscripts [15, 16]. Adam Yung proposed the initial drafts on bugging the asymmetric cryptographic implementations via the SETUP framework in [17, 18]. Interestingly, the kleptographic attacks only work in a black box evaluation model.

Vincent Rijmen and Preneel formally constructed the design-level trapdoors in a block cipher by hiding highly linear probabilistic relationships in the S-Box [19]. The proposed trapdoor was impractical due to the mighty lookup tables and unearthed in [20]. KG Paterson pioneered the construction of a design-level backdoor in DES-like cryptosystems on the principles of imprimitive group actions [21]. Harpes extended the linear attack suggested in [13] to the partitioning cryptanalysis by exploiting the nontrivial partitions. The authors claimed that the partitions could be used to construct the structural backdoors in iterative ciphers. Filiol questioned the security of AES-like designs in the Black Hat Europe [1] and challenged the research community to uncover the combinatorial backdoor in the Backdoored Encryption Algorithm (BEA-1), claimed to be resistant against distinguishing statistical attacks [22, 23]. The Council for European Professional Informatics Societies (CEPIS) has unanimously declared that access to strong encryption algorithms for secure communication is a fundamental right of European citizens, and undermining the security of communication systems for lawful access is unacceptable. Edward Snowden has shown that hostile agencies influence the cryptographic standardisation process in real-world politics. The examples are not limited to the widespread deployment of the bugged Clipper chip by the Clinton administration [24], NIST Dual EC-DRBG backed by NSA [25] and Kuznyechick by the Russian government [26]. Russian cryptographers insisted that the S-Box in Kuznyechik belonged to a random family during the ISO standardisation event. Leo Perrin raised serious concerns about the

*Corresponding Author
Email address: waseem.iqbal@mcs.edu.pk (Waseem Iqbal)

[1] https://www.theregister.com/2017/12/15/crypto_mathematical_backdoors/

S-Box engineering by proving that the permutation follows a stringent mathematical design philosophy [27, 28, 29]. The design layer maliciousness is not limited to the confidentiality-achieving algorithms; the variants of standardised hashing algorithms seem to be the victimised candidates [30, 31].

Our Contribution: The open literature on the design level backdoors in cryptographic algorithms is minimal. To our knowledge, the detailed cryptographic analysis of backdoored structures proposed by Bannier and Paterson from the perspective of hybrid cryptanalytic attacks does not exist. In this research, we identified the common artefacts in these backdoored structures per the well-established (24) cryptographic evaluation parameters and established where things go wrong in these permutations resulting in compromised vital properties. We have grouped the well-known attacks into six cryptographic profiles (1. Differential, 2. Linear, 3. Avalanche, 4. Side Channel, 5. Hybrid, and 6. Algebraic) to conclude the evaluation effectively. This research is the first of its kind to evaluate compromised permutations from a deep mathematical and cryptanalytic lens, paving the way for cipher designers to avoid minimal errors in the S-Box engineering phase.

Paper Organization: This article comprises seven sections. Section 2 shed some light on the basic definitions, terminologies and S-Box engineering. Section 3 highlights the proposed methodology for effectively acquiring results. Section 4 chalk out the philosophy of cryptographic profiling of the substitution layer. Section 5 articulates the obtained results and analysis. The mitigation and defensive strategies are drafted in section 7. In the end, section 8 concludes the article.

2. Preliminaries

The non-trivial subspaces $\mathbf{U}$ and $\mathbf{W}$ of vector space $\mathbb{V}$ over $\mathbb{F}_2^n$ partitions the vector space into distinctive cosests. For any two positive integers $(m, n \geq 2)$, an S-Box $\mathcal{S} : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$, is a vectorial boolean function. Whereas $m = n$, S is a bijection and a surjection for $m > n$. For a vector $x = (x_0, x_1 \ldots, x_n) \in \mathbb{F}_2^n$, the Hamming weight $\omega(x) = \sum_{i=1}^{n} x_i, \forall\ x_i = 1$, is the sum of l's in the vector. Let $\mathcal{F}_n$ be the set of all boolean functions with n variables. For every $f \in \mathcal{F}_n$, $\omega(f) \in [0, 2^n]$, f is said to be balanced iff $\omega(f) = 2^{n-1}$ [2]. $\mathcal{S}$ is considered balanced if for every $\lambda \in \mathbb{F}_2^n$, the bias of $\lambda \cdot S(x)$ is zero. The polarity of $f(x)$ is represented by $\widehat{f}(x) = (-1)^{f(x)}$. The Walsh co-efficient of $\mathcal{S}$ at $(\vartheta, \nu) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$ is $W_S(\vartheta, \nu) = \sum_{x \in \mathbb{F}_2^m} (-1)^{\vartheta \cdot S(x) \oplus x \cdot \nu}$. The derivative of $\mathcal{S}$ in the direction of ϑ is denoted by $D_\vartheta = \mathcal{S}(x) \oplus \mathcal{S}(x \oplus \vartheta)$.

2.1. S-Box Engineering

S-Box is pivotal in securing a symmetric primitive; therefore, utmost care is taken in the design phase. The generation of S-Box is categorised into three classes, i.e., Mathematical Designs [32, 33, 34, 35, 9, 36], Random Generation [37, 38, 39, 40] and Heuristic-Based techniques [41, 42, 43]. The mathematical design ensures a stringent cryptographic profile, i.e., differential, linear and avalanche characteristics. Nyberg proved that the directional derivative of nonlinear permutations constructed on the principle of an inversion over Galois Fields has four unique solutions [44]. Moreover, she argued that the constructions proposed in [45] have a significant distance from the set of all affine functions. Sometimes the wrong choices of mathematical primitives for constructing a cryptographic permutation turned out to be disastrous [46, 47]. The permutation generated by a random phenomenon is not encouraged due to the weak cryptographic profile. Conor et al. outlined the distribution of differentials and bounded the higher probability in the Difference Difference Distribution Table (DDT) of a bijective mapping [48, 49]. Their study establishes that expecting a differentially 4 uniform cryptographic profile from randomly generated permutations is infeasible in polynomial time [3]. In the heuristic-based design process, a designer specifies a particular expected cryptographic profile and generates random mappings till the desired candidate is found. These types of constructions are used in ANUBIS, Skipjack and Kalyna.

2.2. Some Insights on the Backdoored S-Box(es)

For a vector space $\mathbb{V}$ over $\mathbb{F}_2^n$, the corresponding non-trivial subspaces $\mathbf{U}$, $\mathbf{W}$ partitions the vector space. Let $\mathbb{F}_2^n/\mathbf{U}$ and $\mathbb{F}_2^n/\mathbf{W}$ be the non-empty quotient spaces. There exists a transformation $\mathcal{S} : \mathbb{F}_2^n/\mathbf{U} \longmapsto \mathbb{F}_2^n/\mathbf{W}$, or simply for every $u \in \mathbf{U}$, $w \in \mathbf{W}$, $x, y \in \mathbb{F}_2^n$, the relation $\mathcal{S}(x \oplus u) = y \oplus w$ holds true. These types of transformations can be found in the work of Harpes [50], KG Paterson [21], and Bannier [51]. In addition, we have not analyzed the hidden sum-based backdoors in our research [52].

3. Proposed Methodology

For the practical analysis and comparison of backdoored S-Box layer in ciphers proposed by Bannier and KG Paterson, we have picked the S-Box(es) from the well-known designs (DES), APN and optimal classes. The main goal of this study is to deeply analyse the backdoored nonlinear layer in the constructions available in open literature from the dimensions of 23 different cryptanalytic parameters. For precise compilation, the similar cryptanalytic vectors are grouped into six unique cryptographic profiles 1. Differential, 2. Linear, 3. Avalanche characteristics, 4. Side Channel Analysis, 5. Hybrid attacks, and 6. Algebraic profile. We have studied the behaviour of malicious construction with respect to the above-mentioned profiles and bench-marked with the known designs, i.e., DES, APN and Optimal constructions.

4. Cryptographic Profiling of S-Boxes

Cryptanalytic attacks are modelled to assess the strengths and weaknesses of the substitution layer. The designer assumes that the bricklayer transformation in the underlying algorithm

[2] A function with $\omega(f) \equiv 0 \mod 2^n$ is constant

[3] The probability that the directional derivative of a random permutation will have 4 unique solutions at maximum is $P = 2^{-1359.530}$

is highly nonlinear and does not belong to the affine group. An S-Box with a higher Differential Branch Number (DBN) and lesser solutions of the directional derivative guarantees immunity against the differential cryptanlysis. A thorough analysis is mandatory to penetrate the nonlinear transformations for extracting meaningful information. The evaluation vectors are grouped in unique cryptographic profiles to avoid complex jargon and messy things in a 25-dimensional complex parametric table. Each profile is the abstract representation of similar attack parameters clustered together in subsequent sub-sections. A fine-grained mathematical design follows a stringent cryptographic profile with nominal (null) deviations from the ideal profile.

4.1. Differential Profile

Four decades ago, Adi Shamir and Brickell questioned the security of the S-Box layer in DES [53, 54]. Biham and Shamir studied the propagation of fixed plaintext differences in DES for key recovery via differential cryptanalysis (DC) [55]. The practicality of DC remained infeasible against DES, but it has set a benchmark for S-Box engineering and changed the way cryptosystems are imagined, designed and evaluated. The competition(s)/standardisation of symmetric cryptographic primitives remained focused on the heuristics of DC. It exploits the irregular differential probabilities of an S-Box. Cryptographic permutations with uniform differential probabilities (perfect nonlinear) exist in a Utopian world; however, the concept of Almost Perfect Nonlinear (APN) can also be realised as an alternative [56, 57]. The existence of APN for $n - bits$ such that ($n \mod 2 \equiv 0$ and $n \neq 6$) is an open research problem. Nyberg invented the differentially 4-uniform permutations with optimal cryptographic bounds [44]. Seberry et al. [58] commented on the reasons for the weaknesses in the DES S-Box layer against DC. Furthermore, she argued that the lower differential uniformity does not guarantee the security of a Feistel structure alone, and the frequency of non-zero entries in the first column of DDT also matters. In [59], the authors defined 'Robustness' to assess block ciphers with surjective S-Box as a nonlinear composition layer. The AES designers introduced the notion of differential branch number (DBN) for evaluating the diffusion properties of cryptographic permutation against DC [5]. With time it has evolved, and more sophisticated versions have been published as high-order differential attacks [60, 61]. Tezcan et al. suggested that the fixed derivatives in the component function lead to undisturbed bits, paving the path for Truncated and Improbable differential attacks [62, 63]. Rijmen et al. interpreted the distribution of differential probabilities of an S-Box when Xor is used as the key addition layer [64]. The study focused on the distribution of differentials in random and non-random mappings. Hawkes et al. [49] demonstrated the differential probabilities in the presence of modular addition or multiplication as the key mixing mechanism. In [65], authors introduced the terminology of Modular Differential Profile (MDP). They claimed that the MDP unearths the intentional weaknesses, which remained impossible in the presence of DDT.

Definition 4.1. An S-Box is deferentially ∂-uniform ($\partial \equiv 0 \mod 2$), if for all $\Delta\vartheta \in \mathbb{F}_2^m \setminus 0$, $x \in \mathbb{F}_2^m$ and $\Delta\nu \in \mathbb{F}_2^n$ in a $2^m \times 2^n$ Difference Distribution Table (DDT), ∂ is the maximum number of solutions for Eqn 1.

$$\begin{aligned} \#(\Delta\vartheta, \Delta\nu) &= \{S(x) \oplus S(x \oplus \Delta\vartheta) = \Delta\nu\} \\ \partial &= \max_{\Delta\vartheta \in \mathbb{F}_2^{m*}, \Delta\nu \in \mathbb{F}_2^n} \#(\Delta\vartheta, \Delta\nu) \end{aligned} \tag{1}$$

DDT's largest coefficient is upper bounded by 2^n, and the lower bound is 2, which is only possible for APN.

Definition 4.2. An $m \times n$ S-Box is differential $\mathfrak{R}$ Robust, if for $\partial \neq 0$, and the frequency $\psi \neq 0$ of non-zero entries in the DDT for $\Delta\vartheta \neq 0$ and $\Delta\nu = 0$.

$$\mathfrak{R} = (1 - \frac{\partial}{2^m})(1 - \frac{\psi}{2^m}) \tag{2}$$

$\mathfrak{R}$ is bounded by $1 - \frac{1}{2^{n-1}}$ and $(1 - \frac{1}{2^{n-1}}) \times (1 - \frac{1}{2^m})$ for an $n - bit$ bijective and $m \times n$ surjective mappings respectively.

Definition 4.3. The percentage of impossible differentials in the DDT table of an $m \times n$ S-Box is denoted by

$$\Omega_S\,\% = \frac{\{x | S(x) \oplus S(x \oplus \Delta\vartheta) = 0\}}{2^{m+n}}, \forall x, \Delta\vartheta \in \mathbb{F}_2^m \tag{3}$$

Definition 4.4. Let $\omega(\vartheta)$, and $\omega(\nu)$ be the hamming weights of the non-zero vectors ϑ and ν in $\mathbb{F}_2^n$, the differential branch number (DBN) of $\mathcal{S}$ is denoted by $\lceil \frac{2n}{3} \rceil \geq \mathcal{B}_\mathrm{d}(S) \geq 1$

$$\mathcal{B}_\mathrm{d}(S) = \min_{\vartheta, \nu \neq \vartheta} \{\omega(\vartheta \oplus \nu) + \omega(S(\vartheta) \oplus S(\nu))\} \tag{4}$$

Definition 4.5. Foe every two elements $\vartheta, \nu \in \mathbb{Z}_2^{m^*} \times \mathbb{Z}_2^n$, a transformation is said to be modular differential uniform Υ if the equation 5 is satisfied for the maximum number of occurrences.

$$\begin{aligned} M^{(S)}_{(\vartheta,\nu)} &= |\{x : S(x + \vartheta) - S(x) \mod 2^n = \nu\}| \\ \Upsilon_S &= \max_{\vartheta \neq 0 \in \mathbb{Z}_2^m, \nu \in \mathbb{Z}_2^n} N_B(M^{(S)}_{(\vartheta,\nu)}) \end{aligned} \tag{5}$$

4.2. Linearity Profile

To suppress the linear relationships in a block cipher Shannon inked the idea of confusion and diffusion. Confusion is achieved by bricklayer transformation in SPN [5], and incompatible group operations in Add-Rotate-XOR (ARX) architectures [73]. The designer aims to construct cryptographic permutations with high Non-Linearity ($\mathcal{NL}$) [45]. The attacker abuses the nonlinear layer by finding statistically good linear approximations for key recovery. In contrast to DC, Matsui [13] shattered DES by exploiting approximation of the boolean function with high Linear probability ($\mathcal{LP}$). Zajac et al. claimed that the linear probabilities in Linear Approximation Table (LAT) must be reconsidered as Modular Linear Probability (MLP) in the presence of modular addition as a key mixing step [65]. In [74], he also questioned the vulnerable arrangement of S-Box(es) in the confusion layer. Rijmen et al. introduced the notion of Linear Branch Number(LBN) for a better assessment of the diffusion layer [5]. For better safeguarding against linear attacks, the

Article	S-Box	∂	$\Re$	Υ_S	$\mathcal{B}_d(S)$	ψ	$\Omega_S\%$	S-Box	∂	$\Re$	Υ_S	$\mathcal{B}_d(S)$	ψ	$\Omega_S\%$
DES [4]	DES-S0	16	0.316	12	2	37	20.52	DES-S1	16	0.363	11	2	33	21.38
	DES-S2	16	0.316	11	2	37	20.31	DES-S3	16	0.469	11	2	24	31.44
	DES-S4	16	0.387	15	2	31	23.43	DES-S5	16	0.363	11	2	33	19.53
	DES-S6	16	0.340	13	2	35	22.7	DES-S7	16	0.328	10	2	36	22.85
APN [66, 44] [67, 68, 69] [70, 71]	A-S0	2	$1-2^{-4}$	5	2	-	51.46	A-S1	2	$1-2^{-4}$	5	2	-	51.46
	A-S2	2		4	2			A-S3	2		5	2		
	A-S4	2		4	2			A-S5	2		4	2		
	A-S6	2		4	2			-	-	-	-	-	-	
Optimal [72]	S0	4	$1-2^{-3}$	5	2	-	62.11	S1	4	$1-2^{-3}$	4	2	-	62.11
	S2	4		4	2		62.11	S3	4		5	2		58.59
	S4	4		4	2		58.59	S5	4		4	2		58.59
	S6	4		4	2		58.59	S7	4		5	2		58.59
KG-Paterson [21]	KG-S0	24	0.2246	12	1	41	29.88	KG-S1	24	0.2637	16	1	37	30.95
	KG-S2	24	0.2832	12	1	35	30.46	KG-S3	24	0.2441	16	1	39	28.32
	KG-S4	24	0.2441	11	1	39	32.91	KG-S5	24	0.3223	18	2	31	30.47
	KG-S6	24	0.2930	14	1	34	31.74	KG-S7	24	0.2246	16	2	41	31.15
Bannier [51]	B4-S0	4	$1-2^{-3}$	4	2	-	62.10	B4-S1	6	$1-2^{-3}$	4	2	-	63.28
	B4-S2	8		6	2		67.57	B4-S3	10		4	2		70.71
Bannier [51]	B5-S0	32	$1-2^{-4}$	8	2	-	88.67	B5-S1	2	$1-2^{-4}$	5	2	-	51.46
	B5-S2	12		6	2		69.33	B5-S3	32		4	2		88.67
	B5-S4	12		5	2		69.33	B5-S5	-	-		-		
Bannier [51]	B6-S0	16	$1-2^{-5}$	6	2	-	78.93	B6-S1	16	$1-2^{-5}$	6	2	-	69.99
	B6-S2	14		8	2		71.21	-	-	-	-	-		

Table 1: Differential Profile

designer prefers to use components with good diffusion properties, i.e., Maximum Distance Separable (MDS) matrix [75]. To better understand cryptographic permutations, Hendrik identified the idea of linear structures [76] and explained more elaborately in [77, 78]. Ideally, an optimal S-Box must have a large distance to the set of all affine functions, lower linear probability, higher LBN, lower MLP and does not inherit linear structures.

Definition 4.6. For all the $\vartheta, \nu \neq 0 \in \mathbb{F}_2^m \times \mathbb{F}_2^n$, the equation 6 approximates the $m \times n$ S-Box $\mathcal{S}$ with non-zero probability.

$$LAT_S(\vartheta,\nu) \stackrel{\text{def}}{=} \#\left\{\chi \mid \chi \in \mathbb{F}_2^n, \bigoplus_{i=0}^{m-1} \chi[i]\cdot\vartheta[i] = \bigoplus_{i=0}^{n-1} S(\chi)[i]\cdot\nu[i]\right\}$$
$$\mathcal{LP}(S) \stackrel{\text{def}}{=} 2^{-m} \times \max_{\vartheta,\nu\neq 0} LAT_S(\vartheta,\nu) \tag{6}$$

Definition 4.7. Let $\mathcal{A}_n$ be the set of all affine boolean functions with n variables and $\mathcal{B}_n$ contains the component functions of $\mathcal{S}$. Non-linearity measures the minimum hamming distance between all the functions in $\mathcal{B}_n$ and $\mathcal{A}_n$. $\mathcal{NL}$ can be expressed in terms of Walsh coefficients as,

$$\mathcal{NL}(S) = 2^{n-1} - \frac{1}{2}\max_{\vartheta\in\mathbb{F}_2^n\setminus 0, \nu\in\mathbb{F}_2^n} |W_S(\vartheta,\nu)| \tag{7}$$

According to the SCV bounds, for $n \equiv 0 \mod 2$, equation 7 is bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$ and $2^{n-1} - 2^{\frac{n-1}{2}}$ for $n \equiv 1 \mod 2$.

Definition 4.8. For all $\vartheta, \nu \neq 0 \in \mathbb{F}_2^m \times \mathbb{F}_2^n$, such that $W_S(\vartheta,\nu) \neq 0$, the linear branch number (LBN) of $\mathcal{S}$ is denoted by

$$\mathcal{B}_1(S) = \min_{W_S(\vartheta,\nu)\neq 0} \{\omega(\vartheta) + \omega(\nu)\} \tag{8}$$

LBN of $\mathcal{S}$ is bounded by $m - 1 \geq \mathcal{B}_1(S) \geq 2$.

Definition 4.9. For all $\vartheta, \nu \in \mathbb{F}_2^n\setminus 0 \times \mathbb{F}_2^n$, equation 9 approximates $\mathcal{S}$ with respect to modulo 2^n group operations.

$$\mathrm{L}^{(S)}_{(\vartheta,\nu)} = |\{x : S(x) - \vartheta \otimes x - \nu \equiv 0 \mod 2^n\}| \tag{9}$$

Definition 4.10. For an $m \times n$ transformation, $\nu \in \mathbb{F}_2^n$ is said to be a linear structure if $\omega(S(x) \oplus S(x \oplus \nu)) \equiv 0 \mod 2^m$ holds for all $x \in \mathbb{F}_2^m$.

$$\mathcal{F}_{\mathcal{LS}} = \#\{\nu | \sum_{x\in\mathbb{F}_2^n} S(x) \oplus S(x\oplus\nu) \equiv 0 \mod 2^m, \forall\, \nu \in \mathbb{F}_2^m\} \tag{10}$$

$\mathcal{F}_{\mathcal{LS}}$ is upper and lower bounded by 2^{m+n} and zero respectively [4].

4.3. Avalanche Characteristics Profile

A block cipher designed on Shannon's fundamental philosophy of confusion and diffusion should not leak statistically significant information about the processed plaintext. Kam and Davida asserted that in an SPN architecture, the output from the

[4] $\mathcal{F}_{\mathcal{LS}} = 2^{n+m}$ corresponds to an affine or linear function

Article	S-Box	$\mathcal{LP}$	$\mathcal{NL}$	$\mathcal{F}_{\mathcal{LS}}$	$\mathrm{L}^{(S)}_{(\vartheta,\nu)}$	$\mathcal{B}_1(S)$	S-Box	$\mathcal{LP}$	$\mathcal{NL}$	$\mathcal{F}_{\mathcal{LS}}$	$\mathrm{L}^{(S)}_{(\vartheta,\nu)}$	$\mathcal{B}_1(S)$
DES [4]	DES-S0	0.281	14	0	10	2	DES-S1	0.250	16	0	11	2
	DES-S2	0.250	16	0	10	2	DES-S3	0.250	16	9	10	2
	DES-S4	0.312	16	0	10	2	DES-S5	0.250	18	0	9	2
	DES-S6	0.281	14	0	10	2	DES-S7	0.250	16	0	9	2
APN [66, 44]	A-S0	0.125	12	0	5	2	A-S1	0.125	12	31	5	2
	A-S2	0.187	10	0	5	2	A-S3	0.187	10	0	5	2
[67, 68, 69]	A-S4	0.125	12	31	5	2	A-S5	0.125	12	31	5	2
[70, 71]	A-S6	0.125	12	31	5	2	-	-	-	-	-	-
Optimal [72]	S0	0.250	4	9	6	2	S1	0.250	4	9	5	2
	S2	0.250	4	9	5	2	S3	0.250	4	0	5	2
	S4	0.250	4	0	6	2	S5	0.250	4	0	5	2
	S6	0.250	4	0	5	2	S7	0.250	4	0	6	2
KG-Paterson [21]	KG-S0	0.250	16	21	8	2	KG-S1	0.250	16	21	8	2
	KG-S2	0.250	16	21	9	2	KG-S3	0.250	16	21	10	2
	KG-S4	0.250	16	21	10	2	KG-S5	0.250	16	21	9	2
	KG-S6	0.250	16	21	9	2	KG-S7	0.250	16	21	8	2
Bannier [51]	B4-S0	0.375	2	4	4	2	B4-S1	0.375	2	5	7	2
	B4-S2	0.375	2	6	5	2	B4-S3	0.500	0	19	5	2
Bannier [51]	B5-S0	0.500	0	289	5	2	B5-S1	0.125	12	31	6	2
	B5-S2	0.250	8	49	5	2	B5-S3	0.500	0	289	6	2
	B5-S4	0.250	8	49	6	2	B5-S5	-	-	-		-
Bannier [51]	B6-S0	0.500	0	189	6	2	B6-S1	0.437	4	2	6	2
	B6-S2	0.250	16	105	7	2	-	-	-	-	-	-

Table 2: Linearity Profile

substitution layer must be influenced by all the input bits [11]. Fiestel informally conceptualised the notion of the avalanche in SPN designs for gauging the statistical randomness more elaborately [79]. The avalanche characteristics ensure that a single bit change in the plaintext yields in flipping almost half of the ciphertext bits. Webster combined the notions of completeness and avalanche characteristics of an S-Box in Strict Avalanche Criterion (SAC) for a more precise statistical assessment. Bit Independence Criteria (BIC) is measured to correlate the avalanche vectors and understand the single-bit change propagation in the substitution layer [10]. Zhang et al. concluded that SAC alone is insufficient for the cryptographic evaluation of boolean functions [80]. The authors combined the Absolute Indicator (AI) and Sum of Square Indicator (SOSI) in the Global Avalanche Criteria (GAC) to fill this gap. Ideally, a good permutation ensures a good avalanche profile by satisfying the notions of SAC with low relative error, BIC close to zero, lower AI and SOSI coefficients. Avalanche characteristics profiles with higher values advocate a permutation with weak diffusion properties.

Definition 4.11. For every $\vartheta \in \mathbb{F}_2^n$ such that $\omega(\vartheta) = 1$, the function $f \in \mathcal{F}_n$ satisfies the first order SAC iff $\sum_x \widehat{f}(x) \cdot \widehat{f}(x \oplus \vartheta) = 0, \ \forall\, x \in \mathbb{F}_2^n$, the SAC error is denoted by

$$\varepsilon_S\,\% = (2 \times \frac{\omega(f(x) \oplus f(x \oplus \vartheta))}{2^n} - 1) \times 100 \tag{11}$$

SAC error is bounded by $100 \geq \varepsilon \geq 0$.

Definition 4.12. For every $x, \vartheta \in \mathbb{F}_2^n$ such that $\omega(\vartheta) \neq 0$, the change in x by ϑ is represented by $x \oplus \vartheta$. Let $\lambda \cdot \mathcal{S}(x)$ be the coordinate function and $\lambda \cdot \mathcal{S}(x \oplus \vartheta)$ be the associated avalanche vector. Bit Independence Criteria (BIC) is the maximum correlation coefficient $\wp$ between the coordinate vectors and the set of all avalanche vectors.

$$BIC = \max_{\lambda,\vartheta \in \mathbb{F}_2^n, \omega(\lambda), \omega(\vartheta) \neq 0} (\wp(\lambda \cdot \mathcal{S}(x), \lambda \cdot \mathcal{S}(x \oplus \vartheta))) \tag{12}$$

BIC is bounded by $1 \geq BIC \geq 0$

Definition 4.13. Let $\Lambda_f(\vartheta) = \sum_x (-1)^{f(x) \oplus f(x \oplus \vartheta)}, \forall x \in \mathbb{F}_2^n$ be the autocorrelation function. The absolute indicator of is the maximum autocorrelation of f for all $\vartheta \in \mathbb{F}_2^n$

$$\Lambda_f = \max_{\vartheta \in \mathbb{F}_2^n, \omega(\vartheta) \neq 0} |\Lambda_f(\vartheta)| \tag{13}$$

Definition 4.14. The sum of square indicator of a transformation is the sum of squares of all non-zero autocorrelation coefficients

$$\Im = \sum_{\vartheta \in \mathbb{F}_2^n} (\Lambda_f(\vartheta))^2 \tag{14}$$

SOSI is bounded by $2^{3n} \geq \Im \geq 2^{2n}$ [5]

4.4. Algebraic Profile

Every system in the universe can be represented in multi-set mathematical equations. The polynomial time solution of the

[5] $\Im = 2^{3n}$ and $\Im = 2^{2n}$ depicts an affine and bent function respectively

Article	S-Box	ε_S %	Λ_S	BIC	$\Im$	S-Box	ε_S %	Λ_S	BIC	$\Im$
DES [4]	DES-S0	75	48	0.466667	36736	DES-S1	87.5	56	0.522223	25984
	DES-S2	75	48	0.396825	24064	DES-S3	100	64	1.000000	40960
	DES-S4	62.5	40	0.454545	47104	DES-S5	62.5	48	0.509175	19456
	DES-S6	75	48	0.466667	34048	DES-S7	75	48	0.544705	32128
APN [67, 68] [66, 44, 69] [70, 71]	A-S0	25	8	0.333333	2048	A-S1	100	32	1.000000	2048
	A-S2	25	8	0.333333	2048	A-S3	25	8	0.333333	2048
	A-S4	100	32	1.00000	2048	A-S5	100	32	1.00000	2048
	A-S6	100	32	1.00000	2048	-	-	-		-
Optimal [72]	S0	100	16	0.57735	1024	S1	100	16	1.00000	1024
	S2	100	16	0.57735	1024	S3	50	8	0.57735	640
	S4	50	8	0.57735	640	S5	50	8	0.57735	640
	S6	50	8	0.57735	640	S7	50	8	0.57735	640
KG-Paterson [21]	KG-S0	100	64	0.6000	65536	KG-S1	100	64	0.600000	65536
	KG-S2	100	64	0.600000	65536	KG-S3	100	64	1.000000	65536
	KG-S4	100	64	1.0000	65536	KG-S5	100	64	0.447214	65536
	KG-S6	100	64	0.447214	65536	KG-S7	100	64	0.492063	65536
Bannier [51]	B4-S0	100	16	0.500000	1408	B4-S1	100	16	1.00000	1408
	B4-S2	50	16	0.577350	1408	B4-S3	100	16	0.77459	4096
Bannier [51]	B5-S0	100	32	1.00000	32768	B5-S1	100	32	1.00000	2048
	B5-S2	100	32	1.00000	8192	B5-S3	100	32	1.000000	32768
	B5-S4	100	32	1.00000	8192	-	-	-	-	-
Bannier [51]	B6-S0	100	64	0.387298	65536	B6-S1	100	64	1.00000	65536
	B6-S2	100	64	1.000000	65536	-	-	-	-	-

Table 3: Avalanche Characteristics Profile

system of equations gives the correct information about the nature of the underlying architecture. A symmetric cryptosystem is an interpretation of nonlinear boolean equations evaluated by the degree of the system. Ideally, the system of equations for a symmetric cryptosystem must not be solvable in polynomial time. An S-Box is a combination of boolean functions comprised of coordinate and component functions. The algebraic degree of the boolean function is the hamming weight of the highest exponent in equation 15. A boolean function is considered constant if no algebraic term is active in the algebraic normal form (ANF) [81]. The number of terms in the ANF must be higher to resist interpolation attacks [82, 83]. Ideally, the frequency of affine and quadratic equations must be zero to thwart linear structures in the cryptographic permutations.

Definition 4.15. A multivariate boolean function f with n variables can be represented in a unique Algebraic Normal Form (ANF) as

$$f(x_1, \ldots, x_n) = \sum_{r \in \mathbb{F}_2^n} \varphi_r \left(\prod_{i=1}^{n} x_i^{r_i} \right), \quad \varphi_r \in \mathbb{F}_2, r = (r_1, \ldots, r_n) \tag{15}$$

The algebraic degree (shortened version degree) d of f is the highest exponent $\omega(r)$ such that $\omega(r) \neq 0$ and $\varphi_r \neq 0$.

Definition 4.16. For an $m \times n$ S-Box with m variables and 2^{n+1} component functions, the degree of every function lies in the range $(0, \cdots, m)$. The algebraic spectrum of vectorial mapping is a multiset with a population of degrees.

$$\#\{\omega(r) = d, \ \exists\, d \ \in (0, \cdots, m)\} \tag{16}$$

Definition 4.17. The number of non-zero terms in equation 15 is represented by

$$\Gamma = \omega(\sum_{r \in \mathbb{F}_2^n} \varphi_r \left(\prod_{i=1}^{n} x_i^{r_i} \right), \quad \varphi_r \in \mathbb{F}_2, r = (r_1, \ldots, r_n)) \tag{17}$$

Definition 4.18. A function $g_i \in g$ is a non-trivial annihilator of f if $f * g_i = 0, \forall g_i \neq 0, 1 + f$. Algebraic Immunity (AI) of f is the minimum degree in g.

4.5. Side Channel Profile

In the early 90s, Paul Kocher hinted that insecure cryptographic implementations substantially threaten the cyber ecosystem. Secure implementation of cryptographic primitives is equally crucial as the security of the primitive itself. Timing and power patterns are leaked during the execution of unprotected cryptographic implementation leading to timing and power analysis attacks [84, 85]. With time these attacks evolved, and more sophisticated versions came out in the wild [86, 87, 88]. Sylvain et al. introduced the concept of Differential Power Analysis (DPA) Signal to Noise Ratio (SNR) for the quantification of DPA attacks on block ciphers [89]. The authors noted that an unprotected implementation is not the only root cause of DPA attacks; the choice of S-Box parameters also plays a significant role in the overall leakage. Prouff defined the Transparency Order (TO) by extending the concept of DPA SNR to assess power leakages in a multi-bit DPA using the hamming weight model [90]. The main purpose of TO is to select optimal s-boxes

Article	S-Box	Degree	Spectrum	Γ	AI	S-Box	Degree	Spectrum	Γ	AI
DES [4]	DES-S0	4	4:1, 5:14	29	2	DES-S1	4	4:3, 5:12	20	3
	DES-S2	4	4:1, 5:14	25	3	DES-S3	3	3:1, 4:6, 5:8	13	2
	DES-S4	4	4:1, 5:14	26	2	DES-S5	5	5:15	20	3
	DES-S6	5	5:15	18	3	DES-S7	4	4:1, 5:14	24	3
APN [66, 44] [67, 68, 69] [70, 71]	A-S0	3	3:31	11	2	A-S1	2	2:31	4	2
	A-S2	4	4:31	11	2	A-S3	4	4:31	11	2
	A-S4	2	2:31	5	2	A-S5	2	2:31	4	2
	A-S6	2	2:31	5	2	-	-	-	-	-
Optimal [72]	S0	2	2:3, 3:12	3	2	S1	2	2:3, 3:12	3	2
	S2	2	2:3, 3:12	3	2	S3	3	3:15	5	2
	S4	3	3:15	4	2	S5	3	3:15	4	2
	S6	3	3:15	4	2	S7	3	3:15	4	2
KG-Paterson [21]	KG-S0	2	2:1, 3:2, 4:12	6	2	KG-S1	2	2:1, 3:2, 4:12	5	2
	KG-S2	2	2:1, 3:2, 4:12	6	2	KG-S3	2	2:1, 3:2, 4:12	4	2
	KG-S4	2	2:1, 3:2, 4:12	5	2	KG-S5	2	2:1, 3:2, 4:12	5	2
	KG-S6	2	2:1, 3:2, 4:12	4	2	KG-S7	2	2:1, 3:2, 4:12	6	2
Bannier [51]	B4-S0	2	2:1, 3:14	6	2	B4-S1	2	2:1, 3:14	4	2
	B4-S2	3	3:15	5	2	B4-S3	1	1:1, 2:2, 3:12	3	1
Bannier [51]	B5-S0	1	1:3, 2:28	3	1	B5-S1	2	2:31	4	2
	B5-S2	2	2:7, 4:24	7	2	B5-S3	1	1:3, 2:28	1	1
	B5-S4	2	2:7, 4:24	7	2	-	-	-	-	
Bannier [51]	B6-S0	1	1:3, 5:60	1	1	B6-S1	5	5:63	24	2
	B6-S2	2	2:7, 4:8, 5:48	4	2	-	-	-	-	-

Table 4: Algebraic Profile

based on their algebraic profile to design cryptographic algorithms. Research suggests that s-box(es) with the same cryptographic profile shows different leakage profiles against DPA attacks. The right trade-off between traditional cryptanalysis (differential and linear profile) and a DPA attack is still an open problem.

Definition 4.19. Let $\mathcal{S}$ be an $m \times n$ mapping, such that $\vartheta \times \nu \neq 0 \in \mathbb{F}_2^m \times \mathbb{F}_2^n$ and associated Walsh coefficient $W_S(\vartheta, \nu)$, the DPA-SNR can be measured as

$$\text{DPA-SNR} = \frac{n2^{2m}}{\sqrt{\left(\sum_\vartheta \left(\sum_\nu W_S(\vartheta, \nu)\right)^4\right)}} \tag{18}$$

DPA-SNR of an $n - bit$ affine function is $\sqrt{n}$. For a balanced mapping, equation 18 is bounded by $2^{\frac{m}{2}} \geq DPA - SNR \geq 1$.

Definition 4.20. For an $m \times n$ S-Box, for all $\nu \in \mathbb{F}_2^n$ and $\alpha \in \mathbb{F}_2^n \backslash 0$, let $W_{D_\alpha S}(0, \nu)$ be the Walsh coefficient of $\mathcal{S}$ in the direction of α at point $(0, \nu)$. For a constant precharge logic $\vartheta \in \mathbb{F}_2^n$, the transparency order of $\mathcal{S}$ is calculated as

$$\mathcal{T}_S = \max_{\vartheta \in \mathbb{F}_2^n} \left(\left| n - 2 \cdot \omega(\vartheta) \right| - \frac{1}{2^{2m} - 2^m} \sum_{a \in \mathbb{F}_2^{m*}} \left| \sum_{\substack{\nu \in \mathbb{F}_2^n \\ \omega(\nu)=1}} (-1)^{\nu \cdot \vartheta} W_{D_\alpha S}(0, \nu) \right| \right) \tag{19}$$

Transparency order is bounded by $n \geq \mathcal{T}_S \geq 0$

4.6. Hybrid Attacks

The Differential and linear attacks were the game changers for designing and analysing symmetric primitives. Langford et al. proposed that both attacks can be mounted concurrently (Differential-Linear Cryptanalysis - DLC) with lower complexity [91]. The DLC distinguisher assumes that a cipher is halved into independent parts as E_i and E_j, such that the execution of the former by selecting chosen text pairs with higher differential characteristics coincides with the best linear approximations in E_j. The improved results on Serpent and IDEA [92, 93] and further improvements can be found in [94, 95]. Dunkelman parameterised the DLC attack by defining the Differential Linear Connectivity Table (DLCT) to evaluate S-Box [96]. DLCT of $m \times n$ S-Box is $2^m \times 2^n$ table, and the largest entry in the DLCT is upper bounded by 2^{n-1}. The low coefficient ascertains the best resistance of the underlying substitution layer against the attack. Boomerang attack debunked the philosophy that securing a primitive against DC by eliminating high probability characteristics in iterated ciphers is sufficient [97]. The Boomerang Connectivity Table (BCT) was introduced to precisely assess an S-Box against the boomerang attack [98]. The largest entry in BCT is bounded by 2^n, and the higher coefficients showcase the weakened resistance. The results presented were subjected to the bijective substitution layer only. Boukerrou identified the research gap and devised an algorithm to revisit the BCT notion for the surjective transformation layer as Fiestel-BCT [99]. The hybrid profile of a suitable substitution layer is accorded with lower values of DLCT, BCT and FBCT matrices.

Definition 4.21. Consider an input $x \in \mathbb{F}_2^m$, fixed input differ-

Article	S-Box	SNR(**DPA**)	$\mathcal{T}_S$	S-Box	SNR(**DPA**)	$\mathcal{T}_S$
DES [4]	DES-S0	3.611010	2.063492	DES-S1	4.503024	2.063492
	DES-S2	3.855841	2.063492	DES-S3	4.148504	2.063492
	DES-S4	3.688899	2.063492	DES-S5	3.083666	2.063492
	DES-S6	4.661485	2.063492	DES-S7	4.218889	2.063492
APN [67, 68] [66, 44, 69] [70, 71]	A-S0	3.24422	4.7096	A-S1	3.380617	4.8387
	A-S2	3.53550	4.67740	A-S3	3.53550	4.67740
	A-S4	3.38060	4.83871	A-S5	3.38060	4.83710
	A-S6	3.7139	4.83710	-	-	-
Optimal [72]	S0	2.94580	3.46660	S1	2.68530	3.53333
	S2	2.68530	3.600000	S3	2.68530	3.53333
	S4	3.108115	3.46670	S5	3.108115	3.46670
	S6	3.108115	3.46670	S7	2.80560	3.53333
KG-Paterson [21]	KG-S0	4.624828	2.063492	KG-S1	4.643048	2.063492
	KG-S2	3.313794	2.063492	KG-S3	4.718143	2.063492
	KG-S4	4.624828	2.063492	KG-S5	3.340733	2.063492
	KG-S6	3.268115	2.063492	KG-S7	4.737493	2.063492
Bannier [51]	B4-S0	3.10855	3.4667	B4-S1	3.10855	3.6667
	B4-S2	2.68530	3.4667	B4-S3	1.70500	3.35000
Bannier [51]	B5-S0	3.015113	4.25806	B5-S1	2.917300	4.838170
	B5-S2	3.77543	4.596774	B5-S3	3.015113	4.00000
	B5-S4	2.73274	4.43548	-	-	-
Bannier [51]	B6-S0	3.6300	4.90794	B6-S1	4.07084	5.186508
	B6-S2	3.677974	5.22222	-	-	-

Table 5: Side Channel Analysis

ence $\Delta \in \mathbb{F}_2^m$ and output mask $\gamma \in \mathbb{F}_2^n$, the DLCT of S-Box is

$$DLCT_S(\Delta, \gamma) = |\{x : \gamma \cdot S(x) \oplus \gamma \cdot S(x \oplus \Delta) = 0\}| - 2^{n-1}. \quad (20)$$

For $\Delta, \gamma \neq 0$, DLCT uniformity is the maximum number of occurrences for which equation 20 holds and is upper bounded by 2^{n-1}.

Definition 4.22. Let $\mathcal{S}$ be an $n-bit$ bijection and $\mathcal{S}^{-1}$ be the inverse permutation, then for all $x, \Delta\vartheta, \nabla\nu \in \mathbb{F}_2^n$, Boomerang Connectivity Table a $2^n \times 2^n$ matrix. BCT uniformity is the highest frequency for which equation 21 is satisfied.

$$\mathcal{BCT}(\Delta\vartheta, \nabla\nu) =$$

$$\#\left\{x \mid S^{-1}(S(x) \oplus \nabla\nu) \oplus S^{-1}(S(x \oplus \Delta\vartheta) \oplus \nabla\nu) = \Delta\vartheta\right\} \quad (21)$$

Definition 4.23. FBCT of an S-Box is the double derivative of x in the direction of $\Delta\vartheta, \nabla\nu \in \mathbb{F}_2^n \times \mathbb{F}_2^m$.

$$\mathcal{FBCT}_S(\Delta\vartheta, \nabla\nu) = \quad (22)$$

$$\#\left\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta\vartheta) \oplus S(x \oplus \nabla\nu) \oplus S(x \oplus \Delta\vartheta \oplus \nabla\nu) = 0\right\}$$

$\mathcal{FBCT}_S$ uniformity is analogous to the differential uniformity and upper bounded by 2^n. Ideally, a permutation resistant to the boomerang cryptanlysis has null solutions for equation 22 for every $\Delta\vartheta \oplus \nabla\nu \neq 0 \in \mathbb{F}_2^n \times \mathbb{F}_2^m$.

5. Discussion and Analysis

A malicious designer claims to inject a cryptographic weakness in the cipher's nonlinear layer without disturbing the statistical properties. And the backdoor goes undetected by a statistical distinguisher in polynomial time. We argue that whenever a change in any system is introduced, it changes its direction from the ideal conditions to accommodate the uncertainty. After a thorough cryptographic analysis of the malicious transformations and bench-marking them with the widely accepted constructions, we have debunked the earlier claims by the malicious designers.

KG Paterson [21]: The robustness to differential cryptanalysis $\mathcal{R}$ for 6×4 mappings is upper bounded by 0.908. The engineered s-boxes listed as KG-0 to KG-7 show lower values of $0.2246 \leq \mathcal{R} \leq 0.323$ as compared to the DES $0.316 \leq \mathcal{R} \leq 0.469$ in Table 1. The lower values pinpoint the significant weakness against the DC. The combination of higher $\partial = 24$, lower $\mathcal{R}$ and lower bounded DBN $\mathcal{B}_d(S) = 1$ is an open invitation for differential distinguisher-based attacks. Interestingly, the highest possible input differences in all these mappings are $\Delta 4, \Delta 8, \Delta C$ with corresponding output differences $\Delta 1, \Delta 2, \Delta 3$. For KG-0, $\Delta 4 \mapsto \Delta 1$ with probability $P_{\Delta 4 \mapsto \Delta 1} = \frac{24}{64}$, $\Delta 4 \mapsto \Delta 2$ with $P_{\Delta 4 \mapsto \Delta 2} = \frac{24}{64}$ and $\Delta 4 \mapsto \Delta 3$ with $P_{\Delta 4 \mapsto \Delta 3} = \frac{16}{64}$, the details about the probability distribution of remaining mappings can be found in Appendix-A. The study of modular differential probability Υ_S does not provide significant information on the hidden weaknesses in these mappings, thus strengthening the idea that weaknesses in the $\mathbb{F}_2^n$ remains undetected by the dis-

Article	S-Box	$DLCT_S$	$\mathcal{BCT}$	$\mathcal{FBCT}_S$	S-Box	$DLCT_S$	$\mathcal{BCT}$	$\mathcal{FBCT}_S$
DES [4]	DES-S0	24	-	24	DES-S1	20	-	28
	DES-S2	20	-	20	DES-S3	32	-	48
	DES-S4	20	-	28	DES-S5	24	-	20
	DES-S6	20	-	28	DES-S7	24	-	28
APN [66, 44]	A-S0	4	2	0	A-S1	16	2	0
	A-S2	4	2	0	A-S3	4	2	0
[67, 68, 69]	A-S4	16	2	0	A-S5	16	2	0
[70, 71]	A-S6	16	2	0	-	-	-	-
Optimal [72]	S0	8	16	8	S1	8	16	8
	S2	8	16	8	S3	4	6	4
	S4	4	10	4	S5	4	6	4
	S6	4	8	4	S7	4	10	4
KG-Paterson [21]	KG-S0	32	-	64	KG-S1	32	-	64
	KG-S2	32	-	64	KG-S3	32	-	64
	KG-S4	32	-	64	KG-S5	32	-	64
	KG-S6	32	-	64	KG-S7	32	-	64
Bannier [51]	B4-S0	8	16	8	B4-S1	8	16	8
	B4-S2	4	16	4	B4-S3	8	16	8
Bannier [51]	B5-S0	16	32	32	B5-S1	16	2	0
	B5-S2	16	32	32	B5-S3	16	32	32
	B5-S4	16	32	32	-	-	-	-
Bannier [51]	B6-S0	32	24	20	B6-S1	28	20	20
	B6-S2	32	32	32	-	-	-	-

Table 6: Hybrid Attacks Profile

tinguisher based upon modular differences [65]. The modular differences-based backdoor can be detected with the help of Υ_S. Similarly, the linear probabilities in table 2 show small deviations compared to the DES. Due to $\mathcal{F}_{\mathcal{LS}} \neq 0$, these mappings contain intersectable linear structures responsible for partitioning the input space to the output space, making them vulnerable to invariant subspace attacks and partitioning cryptanalysis with high probability. Analogous to Υ_S, the modular-based linear approximation tool $\mathrm{L}^{(\mathrm{S})}_{(\vartheta,\nu)}$ does not extract significant information on the intentional weaknesses in these mappings. Discussing the notions of completeness in table 3, it is important to note that KG-0 to KG-7 fails to satisfy them, and the average SAC error is $\varepsilon_S\% = 100$. The average absolute indicator meets the upper bound, i.e., $\Lambda_S = 2^6$ and the sum of square indicator coefficient $\Im = 65536$ is greater than $\Im = 40960$ for DES. Higher BIC coefficients indicate that the avalanche vectors are highly correlated and violate the basic philosophy of S-box engineering. The algebraic analysis shows that the component functions are quadratic. The degree 2 functions are responsible for introducing the linear structures in an S-box [62]. In contrast to DES, the side channel profile (Table 5) is not problematic in these malicious constructions. Thanks to the hybrid attacks evaluation tools proposed in [96, 98, 99], dissecting these mappings from the perspective of high-order differential cryptanalysis, we have shown that the FBCT and DLCT coefficients are attaining the upper bound in Table 6 cross-checked with Table A.9 and A.8 in Appendix A. Ideally, to resist hybrid attacks, the designer selects design primitives to suppress the coefficients in equation 20, 21 and 22. Interestingly, we exposed the hidden subspaces in these mappings when we searched the higher coefficients and associated indexes in FBCT, DLCT and DDT tables A.9, A.8 and A.7 in Appendix A. We conclude that the hidden subspaces smooth the way for high-order differential attacks.

Bannier [51]: Similar to Kenny's mappings, Bannier engineered 4, 5 and 6-bit backdoored permutations with hidden subspaces. Consequently, the cryptographic profiles highlight remarkable patterns in respective evaluation tables. Looking into the 11% non-zero differential coefficients of B5-S0 and B5-S3 in differential profile in table 1 and B.10, $\Delta 1 \mapsto \Delta 6$ with probability $P_{\Delta 1 \mapsto \Delta 6} = 1$, $\Delta 4 \mapsto \Delta 2$ with probability $P_{\Delta 4 \mapsto \Delta 2} = 1$, $\Delta 5 \mapsto \Delta 4$ with probability $P_{\Delta 5 \mapsto \Delta 4} = 1$ and $\Delta B \mapsto \Delta 8$ with probability $P_{\Delta B \mapsto \Delta 8} = 1$, $\Delta 18 \mapsto \Delta 15$ with probability $P_{\Delta 18 \mapsto \Delta 15} = 1$, $\Delta 1C \mapsto \Delta 1D$ with probability $P_{\Delta 1C \mapsto \Delta 1D} = 1$ respectively. The unitary probabilities are solely responsible for potential weaknesses against the DC. Examining the higher linear probabilities in table 2 and closely inspecting the indexes of maximum probabilities in table B.14, they are synced with the hidden subspaces. Analogous to Kenny's mappings, $\mathcal{F}_{\mathcal{LS}} \neq 0$, the component functions of these constructions are filled with linear structures, resulting in linear independent vectors when intersected. The independent linear vectors lead to preservable input and output space partitions. Consequently, the modular cryptanalytic vectors $\mathrm{L}^{(\mathrm{S})}_{(\vartheta,\nu)}$ and Υ_S remain silent on this vulnerability. Inspecting the $\varepsilon_S\% = 100$ and unity BIC in table 3, the dissatisfaction of desired completeness properties is evident. These findings are supported by the failure of global avalanche characteristics (GAC) in the light of achieved upper bounded Λ_S

and $\Im$ in table 3. The annoyance of avalanche characteristics is closely linked with affine and quadratic equations in these permutations [6]. The investigation of the side channel profile in table 5 depicts the weaknesses against DPA attacks. These intentionally weakened permutations sprout a plethora of information when inspected with hybrid cryptanalytic tools, i.e., DLCT, BCT and FBCT in table 6. These mappings give the green signal for hybrid attacks due to the resultant upper bounded DLCT, FBCT and BCT coefficients, 2^{n-1} and 2^n, respectively. Reverse engineering the indices with high BCT, FBCT, and DLCT coefficients in B.11, B.13 and B.12 connect us with the output subspace if present in the S-Box. Equivalently, it is also true that the information on of subspaces gives leverage to the malicious designer to intelligently craft the datasets for attacking the cipher with less complexity.

6. Data Availability

The verifiable detailed cryptographic analysis of the backdoored mappings, along with the $4-bit$ optimal constructions, DES and APN, is uploaded and available to the open public via accessible link [7].

7. Mitigation Techniques

The root cause of all the problems investigated in the weakened mappings is the intentional existence of linear structures, giving rise to the preservable linear subspaces and weakened avalanche characteristics. If we closely inspect the lightweight NIST competitors, the finalists are not free of the linear structures, but they don't give rise to the preservable subspaces in the respective ciphers. The main objective is to flush the design strategies responsible for the birth of linear structures, i.e., affine and quadratic equations. The utilization of highly nonlinear functions in the confusion layer without the existence of preservable linear subspaces is an effective remedial measure. Furthermore, the mappings with good differential and linear profiles but depicting visible lines in the DCLT, FBCT and BCT must be struck off without any reasonable doubt.

8. Conclusion

The realistic existence of design-level backdoors in cryptographic algorithms can never be ignored. A malicious designer embeds the mathematical weakness in an algorithm without harming the integrity of known cryptanalytic evaluation parameters. However, we believe that whenever any abnormality is introduced in a system, it shifts the direction to accommodate the intentional change. From the detailed cryptographic analysis, the changing behaviour of cryptographic evaluation vectors is evident in the malicious mappings proposed by Kenny and Bannier. Most mappings explored in this work tend to show better resistance against linear and differential cryptanalysis. The designer compromised the degree of component functions to insert linear structures, further deteriorating the completeness properties translated into weak avalanche characteristics and highly correlated vectors. It is presumed that the security claims pertaining to the conventional statistical cryptanalysis made by the cryptographic engineer must not be considered alone. The hidden weaknesses may come to light when analysed with a multifaceted lens. The analysis from multiple perspectives is mandatory for unwrapping the multilayered information regarding intentional vulnerabilities. The backdoored mappings are vulnerable to hybrid cryptanalytic attacks with high probability. The evaluation tools for detecting the modular layer backdoors remain ineffective in exposing the combinatorial backdoors in block ciphers, and vice versa.

[6] B5-S1 is an APN while B4-S0, B5-S0, B5-S3 are affine permutations

[7] `https://nustedupk0-my.sharepoint.com/:f:/g/personal/sfahd_phdismcs_student_nust_edu_pk/EnfJdtEemA5Dj_j6lTitrlUBGbQVvHueMteRmRtnKkAD7g?e=sccgHX`

Bibliography

[1] C. E. Shannon, A mathematical theory of communication, The Bell system technical journal 27 (3) (1948) 379–423.

[2] C. E. Shannon, Communication theory of secrecy systems, The Bell system technical journal 28 (4) (1949) 656–715.

[3] H. Feistel, et al., Lucifer (cipher).

[4] F. Pub, Data encryption standard (des), FIPS PUB (1999) 46–3.

[5] J. Daemen, V. Rijmen, The design of Rijndael, Vol. 2, Springer, 2002.

[6] A. Kato, M. Kanda, S. Kanno, Camellia cipher suites for tls, Tech. rep. (2010).

[7] V. Dolmatov, Gost r 34.12-2015: Block cipher" kuznyechik", Tech. rep. (2016).

[8] E. Biham, R. Anderson, L. Knudsen, Serpent: A new block cipher proposal, in: International workshop on fast software encryption, Springer, 1998, pp. 222–238.

[9] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, The 128-bit blockcipher clefia, in: International workshop on fast software encryption, Springer, 2007, pp. 181–195.

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

[11] J. B. Kam, G. I. Davida, Structured design of substitution-permutation encryption networks, IEEE Transactions on Computers 28 (10) (1979) 747–753.

[12] E. Biham, A. Shamir, Differential cryptanalysis of des-like cryptosystems, Journal of CRYPTOLOGY 4 (1) (1991) 3–72.

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

[14] H. M. Heys, S. E. Tavares, Avalanche characteristics of substitution-permutation encryption networks, IEEE Transactions on Computers 44 (9) (1995) 1131–1139.

[15] G. J. Simmons, The prisoners' problem and the subliminal channel, in: Advances in Cryptology: Proceedings of Crypto 83, Springer, 1984, pp. 51–67.

[16] Y. Desmedt, Abuses in cryptography and how to fight them, in: Advances in Cryptology—CRYPTO'88: Proceedings 8, Springer, 1990, pp. 375–389.

[17] A. Young, M. Yung, The dark side of "black-box" cryptography, or: Should we trust capstone, in: Advances in Cryptology—CRYPTO, Vol. 96, 1996, pp. 89–103.

[18] A. Young, M. Yung, Kleptography: Using cryptography against cryptography, in: Advances in Cryptology—EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings 16, Springer, 1997, pp. 62–74.

[19] V. Rijmen, B. Preneel, A family of trapdoor ciphers, in: FSE, Vol. 97, Springer, 1997, pp. 139–148.

[20] H. Wu, F. Bao, R. H. Deng, Q. Z. Ye, Cryptanalysis of rijmen-preneel trapdoor ciphers, in: Advances in Cryptology—ASIACRYPT'98: International Conference on the Theory and Application of Cryptology and Information Security Beijing, China, October 18–22, 1998 Proceedings, Springer, 1998, pp. 126–132.

[21] K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in: International Workshop on Fast Software Encryption, Springer, 1999, pp. 201–214.

[22] A. Bannier, E. Filiol, Mathematical backdoors in symmetric encryption systems-proposal for a backdoored aes-like block cipher, arXiv preprint arXiv:1702.06475 (2017).

[23] A. Bannier, E. Filiol, Partition-Based Trapdoor Ciphers, IntechOpen, Rijeka, 2017. doi:10.5772/intechopen.69485.
URL https://doi.org/10.5772/intechopen.69485

[24] M. Blaze, Key escrow from a safe distance: looking back at the clipper chip, in: Proceedings of the 27th Annual Computer Security Applications Conference, 2011, pp. 317–321.

[25] D. J. Bernstein, T. Lange, R. Niederhagen, Dual ec: A standardized back door, in: The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday, Springer, 2016, pp. 256–281.

[26] H. Yoshida, J. Hammell, Meeting report for the discussion on kuznyechik and streebog [cited 27.03.2023].
URL https://cdn.virgilsecurity.com/assets/docs/meeting-report-for-the-discussion-on-kuznyechik-and-streebog.pdf

[27] L. Perrin, Streebog and kuznyechik: Inconsistencies in the claims of their designers, in: IETF 105, 2019.

[28] A. Biryukov, L. Perrin, A. Udovenko, Reverse-engineering the s-box of streebog, kuznyechik and stribobr1, in: Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I 35, Springer, 2016, pp. 372–402.

[29] O. Dunkelman, L. Perrin, Adapting rigidity to symmetric cryptography: Towards" unswerving" designs, in: Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop, 2019, pp. 69–80.

[30] A. Albertini, J.-P. Aumasson, M. Eichlseder, F. Mendel, M. Schläffer, Malicious hashing: Eve's variant of sha-1, in: Selected Areas in Cryptography–SAC 2014: 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers 21, Springer, 2014, pp. 1–19.

[31] P. Morawiecki, Malicious keccak, Cryptology ePrint Archive (2015).

[32] J. Daemen, V. Rijmen, The rijndael block cipher: Aes proposal, in: First candidate conference (AeS1), 1999, pp. 343–348.

[33] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, Camellia: A 128-bit block cipher suitable for multiple platforms—design andanalysis, in: International workshop on selected areas in cryptography, Springer, 2000, pp. 39–56.

[34] J. Daemen, L. Knudsen, V. Rijmen, The block cipher square, in: International Workshop on Fast Software Encryption, Springer, 1997, pp. 149–165.

[35] J. Guo, T. Peyrin, A. Poschmann, The photon family of lightweight hash functions, in: Annual cryptology conference, Springer, 2011, pp. 222–239.

[36] W. Diffie, G. Ledin, Sms4 encryption algorithm for wireless networks, Cryptology ePrint Archive (2008).

[37] R. Scott, Wide-open encryption design offers flexible implementations, Cryptologia 9 (1) (1985) 75–91.

[38] G. G. Rose, P. Hawkes, Turing: A fast stream cipher, in: International Workshop on Fast Software Encryption, Springer, 2003, pp. 290–306.

[39] B. Kaliski, The md2 message-digest algorithm, Tech. rep. (1992).

[40] I. Das, S. Nath, S. Roy, S. Mondal, Random s-box generation in aes by changing irreducible polynomial, in: 2012 International Conference on Communications, Devices and Intelligent Systems (CODIS), 2012, pp. 556–559. doi:10.1109/CODIS.2012.6422263.

[41] P. S. Barreto, The anubis block cipher, NESSIE (2000).

[42] L. Knudsen, D. Wagner, On the structure of skipjack, Discrete Applied Mathematics 111 (1-2) (2001) 103–116.

[43] R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, V. Dolgov, A. Pushkaryov, R. Mordvinov, et al., A new encryption standard of ukraine: The kalyna block cipher, Cryptology ePrint Archive (2015).

[44] K. Nyberg, Differentially uniform mappings for cryptography, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, pp. 55–64.

[45] K. Nyberg, On the construction of highly nonlinear permutations, in: Advances in Cryptology—EUROCRYPT'92: Workshop on the Theory and Application of Cryptographic Techniques Balatonfüred, Hungary, May 24–28, 1992 Proceedings 11, Springer, 1993, pp. 92–98.

[46] I. Hussain, T. Shah, M. A. Gondal, M. Khan, W. A. Khan, Construction of new s-box using a linear fractional transformation, World Appl. Sci. J 14 (12) (2011) 1779–1785.

[47] J. L. Massey, Safer k-64: A byte-oriented block-ciphering algorithm, in: Fast Software Encryption: Cambridge Security Workshop Cambridge, UK, December 9–11, 1993 Proceedings, Springer, 2005, pp. 1–17.

[48] L. O'Connor, On the distribution of characteristics in bijective mappings, in: Advances in Cryptology—EUROCRYPT'93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings 12, Springer, 1994, pp. 360–370.

[49] P. Hawkes, L. O'Connor, Xor and non-xor differential probabilities, in: Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18, Springer, 1999, pp. 272–285.

[50] C. Harpes, J. L. Massey, Partitioning cryptanalysis, in: Fast Software Encryption: 4th International Workshop, FSE'97 Haifa, Israel, January 20–22 1997 Proceedings 4, Springer, 1997, pp. 13–27.

[51] A. Bannier, Combinatorial analysis of block ciphers with trapdoors, Ph.D. thesis, École Nationale Supérieure d'Arts et Métiers (2017).

[52] M. Calderini, On boolean functions, symmetric cryptography and algebraic coding theory, Ph.D. thesis, University of Trento (2015).

[53] A. Shamir, On the security of des, in: Advances in Cryptology—CRYPTO'85 Proceedings 5, Springer, 1986, pp. 280–281.

[54] E. F. Brickell, J. H. Moore, M. Purtill, Structure in the s-boxes of the des, in: Advances in Cryptology—CRYPTO'86: Proceedings, Springer, 2000, pp. 3–8.

[55] D.-l. Cryptosystems, E. B. A. Shamir, Differential cryptanalysis (1990).

[56] L. Budaghyan, C. Carlet, G. Leander, Constructing new apn functions from known ones, Finite Fields and Their Applications 15 (2) (2009) 150–159.

[57] R. Alvarez, G. McGuire, S-boxes, apn functions and related codes, in: Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, IOS Press, 2009, pp. 49–62.

[58] J. Seberry, X.-M. Zhang, Y. Zheng, Systematic generation of cryptographically robust s-boxes, in: Proceedings of the 1st ACM Conference on Computer and Communications Security, 1993, pp. 171–182.

[59] J. Seberry, X.-M. Zhang, Y. Zheng, Pitfalls in designing substitution boxes, in: Annual International Cryptology Conference, Springer, 1994, pp. 383–396.

[60] X. Lai, Higher order derivatives and differential cryptanalysis, Communications and Cryptography: Two Sides of One Tapestry (1994) 227–233.

[61] L. R. Knudsen, Truncated and higher order differentials, in: Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2, Springer, 1995, pp. 196–211.

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

[63] R. H. Makarim, C. Tezcan, Relating undisturbed bits to other properties of substitution boxes, in: Lightweight Cryptography for Security and Privacy: Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers, Springer, 2015, pp. 109–125.

[64] J. Daemen, V. Rijmen, Probability distributions of correlation and differentials in block ciphers, Journal of Mathematical Cryptology 1 (3) (2007) 221–242.

[65] P. Zajac, M. Jókay, Cryptographic properties of small bijective s-boxes with respect to modular addition, Cryptography and Communications 12 (2020) 947–963.

[66] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes, Information and Control 18 (4) (1971) 369–394.

[67] H. Dobbertin, Almost perfect nonlinear power functions on gf (2 n): a new case for n divisible by 5, in: Finite Fields and Applications, Springer, 2001, pp. 113–121.

[68] T. Beth, C. Ding, On almost perfect nonlinear permutations, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, pp. 65–76.
[69] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, University of Southern California, 1972.
[70] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.), IEEE transactions on Information Theory 14 (1) (1968) 154–156.
[71] T. P. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, On almost perfect nonlinear functions over f_2n, IEEE Transactions on Information Theory 52 (9) (2006) 4160–4170.
[72] G. Leander, A. Poschmann, On the classification of 4 bit s-boxes, in: International Workshop on the Arithmetic of Finite Fields, Springer, 2007, pp. 159–176.
[73] X. Lai, On the design and security of block ciphers, Ph.D. thesis, ETH Zurich (1992).
[74] M. Matsui, On correlation between the order of s-boxes and the strength of des, Lecture Notes in Computer Science 950 (1995) 366–375.
[75] S. Vaudenay, On the need for multipermutations: Cryptanalysis of md4 and safer, in: Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2, Springer, 1995, pp. 286–297.
[76] J.-H. Evertse, Linear structures in blockciphers, in: Advances in Cryptology—EUROCRYPT'87: Workshop on the Theory and Application of Cryptographic Techniques Amsterdam, The Netherlands, April 13–15, 1987 Proceedings, Springer, 2000, pp. 249–266.
[77] X. Lai, Additive and linear structures of cryptographic functions, in: Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2, Springer, 1995, pp. 75–85.
[78] S. Dubuc, Characterization of linear structures, Designs, Codes and Cryptography 22 (2001) 33–45.
[79] H. Feistel, Cryptography and computer privacy, Scientific american 228 (5) (1973) 15–23.
[80] X.-M. Zhang, Y. Zheng, 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 (1996) 320–337.
[81] W. Meier, E. Pasalic, C. Carlet, Algebraic attacks and decomposition of boolean functions, in: Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23, Springer, 2004, pp. 474–491.
[82] T. Jakobsen, L. R. Knudsen, The interpolation attack on block ciphers, in: Fast Software Encryption: 4th International Workshop, FSE'97 Haifa, Israel, January 20–22 1997 Proceedings 4, Springer, 1997, pp. 28–40.
[83] A. M. Youssef, G. Gong, On the interpolation attacks on block ciphers, in: Fast Software Encryption: 7th International Workshop, FSE 2000 New York, NY, USA, April 10–12, 2000 Proceedings 7, Springer, 2001, pp. 109–120.
[84] P. C. Kocher, Cryptanalysis of diffie-hellman, rsa, dss, and other systems using timing attacks, in: Extended abstract, Citeseer, 1995.
[85] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19, Springer, 1999, pp. 388–397.
[86] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, et al., Spectre attacks: Exploiting speculative execution, Communications of the ACM 63 (7) (2020) 93–101.
[87] H. Maghrebi, T. Portigliatti, E. Prouff, Breaking cryptographic implementations using deep learning techniques, in: Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings 6, Springer, 2016, pp. 3–26.
[88] M. Zhao, G. E. Suh, Fpga-based remote power side-channel attacks, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 229–244.
[89] S. Guilley, P. Hoogvorst, R. Pacalet, Differential power analysis model and some results, in: Smart Card Research and Advanced Applications VI: IFIP 18th World Computer Congress TC8/WG8. 8 & TC11/WG11. 2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS) 22–27 August 2004 Toulouse, France, Springer, 2004, pp. 127–142.
[90] E. Prouff, Dpa attacks and s-boxes, in: Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers 12, Springer, 2005, pp. 424–441.
[91] S. K. Langford, M. E. Hellman, Differential-linear cryptanalysis, in: Advances in Cryptology—CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings 14, Springer, 1994, pp. 17–25.
[92] E. Biham, O. Dunkelman, N. Keller, Differential-linear cryptanalysis of serpent, in: Fast Software Encryption: 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003. Revised Papers 10, Springer, 2003, pp. 9–21.
[93] J. Borst, Differential-linear cryptanalysis of idea, ESAT–COSIC Technical Report (1997) 96–2.
[94] G. Leurent, Improved differential-linear cryptanalysis of 7-round chaskey with partitioning, in: Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I 35, Springer, 2016, pp. 344–371.
[95] C. Blondeau, G. Leander, K. Nyberg, Differential-linear cryptanalysis revisited, Journal of Cryptology 30 (2017) 859–888.
[96] A. Bar-On, O. Dunkelman, N. Keller, A. Weizman, Dlct: a new tool for differential-linear cryptanalysis, in: 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, Springer, 2019, pp. 313–342.
[97] D. Wagner, The boomerang attack, in: Fast Software Encryption: 6th International Workshop, FSE'99 Rome, Italy, March 24–26, 1999 Proceedings, Springer, 2001, pp. 156–170.
[98] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song, Boomerang connectivity table: a new cryptanalysis tool, in: Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37, Springer, 2018, pp. 683–714.
[99] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal, M. Minier, On the feistel counterpart of the boomerang connectivity table, IACR Transactions on Symmetric Cryptology 2020 (1) (2020) 331–362.

Appendix A. KG Paterson Mappings

The imprimitive permutations-based trapdoor 6×4 mappings suggested by Paterson can be accessed here [21]. For clarity, these mappings are numbered from KG-0 to KG-7. The detailed cryptographic profiling of the 8 proposed mappings is accessible via the URL mentioned in section 6. For proof of concept and visualisation of the cryptographic vulnerabilities in these mappings, KG-0 has been elaborated in table A.7, A.8 and A.9.

Appendix B. Bannier Permutations

Bannier designed 4, 5 and 6-bit trapdoor bijections in his dissertation [51]. The permutations numbered from B4-S0 to B4-S3 represent a 4-bit family, while B5-S0 to B5-S4 and B6-S0 to B6-S2 belong to 5 and 6-bits, respectively. The extensive cryptographic profile of the 12 backdoored mappings is accessible via URL in the section 6. For a better understanding of the DDT, FBCT, BCT DLCT, and LAT tables of B5-S0 are given in table B.10, B.11, B.12, B.13, and B.14. The intersecting grey lines with highlighted coefficients in the respective tables depict the weakest links against the cryptanalytic attacks.

$\Delta\vartheta/\Delta\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	6	6	2	2	4	4	4	4	0	0	8	8	0	4	4	8
2	0	0	0	0	8	8	0	0	6	6	2	2	10	10	6	6
3	0	4	8	4	6	2	2	6	0	4	4	8	0	8	4	4
4	0	24	24	16	0	0	0	0	0	0	0	0	0	0	0	0
5	2	2	6	6	4	4	4	4	0	16	0	0	4	0	8	4
6	0	0	0	0	4	4	4	4	2	2	6	6	6	6	10	10
7	8	4	0	4	2	6	6	2	4	0	8	4	4	4	0	8
8	0	24	16	24	0	0	0	0	0	0	0	0	0	0	0	0
9	6	6	2	2	4	4	4	4	8	0	8	0	8	4	4	0
10	0	0	0	0	4	4	4	4	2	2	6	6	6	14	10	2
11	4	8	4	0	2	6	6	2	8	4	4	0	8	0	4	4
12	0	16	24	24	0	0	0	0	0	0	0	0	0	0	0	0
13	2	2	6	6	4	4	4	4	8	0	0	8	4	8	0	4
14	0	0	0	0	0	0	8	8	6	6	2	2	10	2	6	14

Table A.7: KG-0 DDT

$\Delta\vartheta/\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
1	32	-4	-8	0	0	4	0	0	0	4	16	0	0	-4	8	0
2	32	0	16	0	-16	0	-8	0	-16	0	0	0	0	0	-8	0
3	32	-8	-8	-4	0	0	-8	-4	0	8	0	4	0	0	0	-12
4	32	-8	-8	-16	32	-8	-8	-16	32	-8	-8	-16	32	-8	-8	-16
5	32	-4	0	-8	0	-12	8	-8	0	4	-8	8	0	12	-16	8
6	32	0	-8	0	-16	0	0	0	-16	0	8	0	0	0	0	0
7	32	0	0	4	0	8	0	4	0	0	8	-4	0	-8	8	12
8	32	-16	-8	-8	32	-16	-8	-8	32	-16	-8	-8	32	-16	-8	-8
9	32	12	8	0	0	4	0	0	0	-12	0	0	0	-4	8	0
10	32	0	0	-8	-16	0	-8	8	-16	0	0	8	0	0	8	-8
11	32	8	8	-4	0	0	8	-4	0	-8	0	-12	0	0	0	4
12	32	-8	-16	-8	32	-8	-16	-8	32	-8	-16	-8	32	-8	-16	-8
13	32	-4	0	8	0	4	-8	8	0	4	-8	-8	0	-4	0	-8

Table A.8: KG-0 DLCT

$\Delta\vartheta/\Delta\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64
1	64	64	0	0	24	24	0	0	40	40	0	0	24	24	0	0
2	64	0	64	0	8	0	8	0	24	0	24	0	16	0	16	0
3	64	0	0	64	16	0	0	16	24	0	0	24	32	0	0	32
4	64	24	8	16	64	24	8	16	64	24	8	16	64	24	8	16
5	64	24	0	0	24	64	0	0	40	24	0	0	24	40	0	0
6	64	0	8	0	8	0	64	0	24	0	16	0	16	0	24	0
7	64	0	0	16	16	0	0	64	24	0	0	32	32	0	0	24
8	64	40	24	24	64	40	24	24	64	40	24	24	64	40	24	24
9	64	40	0	0	24	24	0	0	40	64	0	0	24	24	0	0
10	64	0	24	0	8	0	16	0	24	0	64	0	16	0	8	0
11	64	0	0	24	16	0	0	32	24	0	0	64	32	0	0	16
12	64	24	16	32	64	24	16	32	64	24	16	32	64	24	16	32
13	64	24	0	0	24	40	0	0	40	24	0	0	24	64	0	0
14	64	0	16	0	8	0	24	0	24	0	8	0	16	0	64	0

Table A.9: KG-0 FBCT

$\Delta\vartheta/\Delta\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	8	0	0	0
3	0	8	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	8	0	0	0	0	8	0	0	0	0	0
4	0	0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	8	0	0	0	0	8	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	8	0
7	0	0	0	8	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8
9	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0
10	0	0	0	8	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	8	0	8	0	0	0	0	0	0
11	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	8
12	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0
14	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0
15	0	0	0	0	0	0	0	8	0	8	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	8	0	0
16	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0
18	0	0	0	8	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	8	0	8	0	0	0	0	0	0	0
19	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0
20	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0
22	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0
23	0	0	0	0	0	0	0	8	0	8	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	8	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	8	8	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	8	8	0	0	0
26	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	8	0	0
27	0	8	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0	0	8	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	8	8	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0	8	8
30	0	0	0	0	0	8	0	0	0	0	8	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8
31	0	0	0	8	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	8	0	0	8	0	0	0	0	0	0

Table B.10: B5-S0 DDT

$\Delta\vartheta/\Delta\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
1	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
2	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0
3	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0
4	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
5	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
6	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0
7	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0
8	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
9	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
10	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
11	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
12	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
13	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
14	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
15	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
16	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0
17	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0
18	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0
19	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0
20	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0
21	32	0	32	0	32	0	32	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	0	0	0	0	0	0	0	0
22	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0
23	32	8	32	8	32	8	32	8	0	8	0	8	0	8	0	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0
24	32	0	32	0	32	0	32	0	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
25	32	0	32	0	32	0	32	0	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
26	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8
27	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8
28	32	0	32	0	32	0	32	0	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
29	32	0	32	0	32	0	32	0	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
30	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8
31	32	8	32	8	32	8	32	8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	0	8	0	8	0	8	0	8

Table B.11: B5-S0 BCT

$\Delta\theta/\Delta\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	16	-16	-16	-16	-16	16	16	16	16	-16	-16	-16	-16	16	16	16	16	-16	-16	-16	-16	16	16	16	16	-16	-16	-16	-16	16	16
2	16	0	0	16	0	0	0	0	0	-16	-16	0	0	0	0	0	0	0	0	0	0	16	16	0	0	0	0	0	-16	0	0	-16
3	16	0	0	-16	0	0	0	0	0	-16	16	0	0	0	0	0	0	0	0	0	0	-16	16	0	0	0	0	0	16	0	0	-16
4	16	16	-16	-16	16	16	-16	-16	16	16	-16	-16	16	16	-16	-16	16	16	-16	-16	16	16	-16	-16	16	16	-16	-16	16	16	-16	-16
5	16	16	16	16	-16	-16	-16	-16	16	16	16	16	-16	-16	-16	-16	16	16	16	16	-16	-16	-16	-16	16	16	16	16	-16	-16	-16	-16
6	16	0	0	-16	0	0	0	0	0	-16	16	0	0	0	0	0	0	0	0	0	0	16	-16	0	0	0	0	0	-16	0	0	16
7	16	0	0	16	0	0	0	0	0	-16	-16	0	0	0	0	0	0	0	0	0	0	-16	-16	0	0	0	0	0	16	0	0	16
8	16	0	-16	0	0	0	0	0	-16	0	16	0	0	0	0	0	0	0	0	0	16	0	-16	0	0	0	0	0	-16	0	16	0
9	16	0	16	0	0	0	0	0	-16	0	-16	0	0	0	0	0	0	0	0	0	-16	0	-16	0	0	0	0	0	16	0	16	0
10	16	-16	0	0	0	0	0	0	0	0	-16	16	0	0	0	0	0	0	0	0	0	0	-16	16	0	0	0	0	16	-16	0	0
11	16	-16	0	0	0	0	0	0	0	0	16	-16	0	0	0	0	0	0	0	0	0	0	-16	16	0	0	0	0	-16	16	0	0
12	16	0	16	0	0	0	0	0	-16	0	-16	0	0	0	0	0	0	0	0	0	16	0	16	0	0	0	0	0	-16	0	-16	0
13	16	0	-16	0	0	0	0	0	-16	0	16	0	0	0	0	0	0	0	0	0	-16	0	16	0	0	0	0	0	16	0	-16	0
14	16	-16	0	0	0	0	0	0	0	0	16	-16	0	0	0	0	0	0	0	0	0	0	16	-16	0	0	0	0	16	-16	0	0
15	16	-16	0	0	0	0	0	0	0	0	-16	16	0	0	0	0	0	0	0	0	0	0	16	-16	0	0	0	0	-16	16	0	0
16	16	0	0	0	16	0	0	0	0	0	16	0	0	0	16	0	0	0	-16	0	0	0	-16	0	-16	0	0	0	-16	0	0	0
17	16	0	0	0	-16	0	0	0	0	0	-16	0	0	0	16	0	0	0	16	0	0	0	-16	0	-16	0	0	0	16	0	0	0
18	16	0	0	0	0	0	0	16	0	0	-16	0	0	-16	0	0	0	-16	0	0	0	0	-16	0	0	0	0	16	16	0	0	0
19	16	0	0	0	0	0	0	16	0	0	16	0	0	16	0	0	0	-16	0	0	0	0	-16	0	0	0	0	-16	-16	0	0	0
20	16	0	0	0	16	0	0	0	0	0	-16	0	0	0	-16	0	0	0	16	0	0	0	16	0	-16	0	0	0	-16	0	0	0
21	16	0	0	0	-16	0	0	0	0	0	16	0	0	0	-16	0	0	0	-16	0	0	0	16	0	-16	0	0	0	16	0	0	0
22	16	0	0	0	0	0	0	-16	0	0	16	0	0	-16	0	0	0	-16	0	0	0	0	16	0	0	0	0	-16	16	0	0	0
23	16	0	0	0	0	0	0	-16	0	0	-16	0	0	16	0	0	0	-16	0	0	0	0	16	0	0	0	0	16	-16	0	0	0
24	16	0	0	0	0	0	-16	0	0	0	16	0	-16	0	0	0	-16	0	0	0	0	0	16	0	0	0	-16	0	16	0	0	0
25	16	0	0	0	0	0	-16	0	0	0	-16	0	16	0	0	0	-16	0	0	0	0	0	16	0	0	0	16	0	-16	0	0	0
26	16	0	0	0	0	16	0	0	0	0	-16	0	0	0	0	-16	0	0	0	16	0	0	16	0	0	-16	0	0	-16	0	0	0
27	16	0	0	0	0	-16	0	0	0	0	16	0	0	0	0	-16	0	0	0	-16	0	0	16	0	0	-16	0	0	16	0	0	0
28	16	0	0	0	0	0	16	0	0	0	-16	0	-16	0	0	0	-16	0	0	0	0	0	-16	0	0	0	16	0	16	0	0	0
29	16	0	0	0	0	0	16	0	0	0	16	0	16	0	0	0	-16	0	0	0	0	0	-16	0	0	0	-16	0	-16	0	0	0
30	16	0	0	0	0	16	0	0	0	0	16	0	0	0	0	16	0	0	0	-16	0	0	-16	0	0	-16	0	0	-16	0	0	0
31	16	0	0	0	0	-16	0	0	0	0	-16	0	0	0	0	16	0	0	0	16	0	0	-16	0	0	-16	0	0	16	0	0	0

Table B.12: B5-S0 DLCT

$\Delta\vartheta/\Delta\nu$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
1	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
2	32	32	32	32	32	32	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	32	32	32	32	32	32	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
5	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
6	32	32	32	32	32	32	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	32	32	32	32	32	32	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	32	32	0	0	32	32	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	32	32	0	0	32	32	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	32	32	0	0	32	32	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	32	32	0	0	32	32	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	32	32	0	0	32	32	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	32	32	0	0	32	32	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	32	32	0	0	32	32	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	32	32	0	0	32	32	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0
17	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0
18	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0
19	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0
20	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0
21	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0
22	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0
23	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0	0	0	0	0	0	0
24	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0
25	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0
26	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32
27	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32
28	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0
29	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32	0	0
30	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32
31	32	32	0	0	32	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	32	32	0	0	32	32

Table B.13: B5-S0 FBCT

ϑ/ν	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	-0.25	-0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	-0.25	0	0	0	0	0	0	0	0	0	0
2	0	0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0
3	0	0	0	0	-0.25	0	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0	0.25	0	0
4	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	-0.25	0
5	0	0	0	0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0.25	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-0.25	-0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	-0.25
7	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	-0.25	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0
9	0	0	0	0	0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0.25	0	0
10	0	0	0	0	0	0	0	0	-0.25	-0.25	0	0	0	0	0	0	-0.25	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	-0.25	0.25	0	0	0	0	0	0	0.25	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0.25	0.25	0	0	0	0	0	0	-0.25	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	-0.25	-0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-0.25	0.25	0	0	0	0
14	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	-0.25
15	0	0	-0.25	0	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0.25	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-0.25	-0.25	0	0	0	0	0	0	0.25	-0.25	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0.25	-0.25	0	0	0	0	0	0	0.25	0.25	0	0	0	0	0	0	0	0	0	0
18	0	-0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0
19	0	0	0	0	0	0.25	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	0.25	0	0
20	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0.25	0
21	0	0	0	0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0
22	0	0	0	0	0	0	0.25	-0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	0.25
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	-0.25	0	0	0	0	0	0	-0.25	-0.25	0	0	0	0
24	0	-0.25	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0
25	0	0	0	0	0	0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	-0.25	0	0
26	0	0	0	0	0	0	0	0	-0.25	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	0.25	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-0.5	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-0.5	0	0	0	0	0	0	0	0	0
29	0	0	-0.25	0.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25	0.25	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0	-0.25
31	0	0	0.25	0	0	0	0	0	0	0	0	-0.25	0	0	0	0	0	0	0.25	0	0	0	0	0	0	0	0	0.25	0	0	0	0

Table B.14: B5-S0 LAT