Robustness of Affine and Extended Affine Equivalent Surjective S-Box(es) Against Differential Cryptanalysis

Shah Fahd[1(✉)], Mehreen Afzal[1], Dawood Shah[2], Waseem Iqbal[1], and Atiya Hai[3]

[1] National University of Sciences and Technology, Islamabad 44000, Pakistan
sfahd.phdismcs@student.nust.edu.pk,
{mehreenafzal,waseem.iqbal}@mcs.edu.pk
[2] Quaid-i-Azam University, Islamabad, Pakistan
[3] University of Surrey, Guildford, UK

Abstract. A Feistel Network (FN) based block cipher relies on a Substitution Box (S-Box) for achieving the non-linearity. S-Box is carefully designed to achieve optimal cryptographic security bounds. The research of the last three decades shows that considerable efforts are being made on the mathematical design of an S-Box. To import the exact cryptographic profile of an S-Box, the designer focuses on the Affine Equivalent (AE) or Extended Affine (EA) equivalent S-Box. In this research, we argue that the Robustness of surjective mappings is invariant under AE and not invariant under EA transformation. It is proved that the EA equivalent of a surjective mapping does not necessarily contribute to the Robustness against the Differential Cryptanalysis (DC) in the light of Seberry's criteria. The generated EA equivalent S-Box(es) of DES and other 6×4 mappings do not show a good robustness profile compared to the original mappings. This article concludes that a careful selection of affine permutation parameters is significant during the design phase to achieve high Robustness against DC and Differential Power Analysis (DPA) attacks.

Keywords: S-Box · Permutations · Block Ciphers · Cryptography · Differential Cryptanalysis · Differential Uniformity · Affine Equivalence

1 Introduction

Al-Kindi cracked the thousands-year-old Ceaser cipher by exploiting the frequency of occurrence problem in a natural language. The US intelligence agencies broke the language redundancy problem aroused due to misuse of the Russian One Time Pad (OTP) [1]. To suppress the statistics of plaintext in the resultant ciphertext, Claude Shannon coined the idea of information entropy in his landmark papers [2–4]. He proposed the concepts of Confusion and Diffusion achievable by networking substitution and permutation in a block cipher. Research

G.-V. Jourdan et al. (Eds.): FPS 2022, LNCS 13877, pp. 461–471, 2023.
https://doi.org/10.1007/978-3-031-30122-3_29

on the design and security of the substitution layer is maturing [5,6]. The engineering of S-Box remains an area of focus for the cryptographic community. A cryptanalyst intends to find the statistical vulnerabilities in its design [7–9], and a side channel analyst exploits the cryptographic implementations [10]. An S-Box is generated in multiple ways, i.e., Mathematical processing (Finite Field Inversion [11–13]), random generation [14,15] and heuristic-based approach [16,17]. The mathematical generation of S-Box needs rigorous research, but it promises an optimum cryptographic profile, i.e., Differential Uniformity (DU) [8] and Linearity [9]. The mathematician focuses on the Affine, or Extended Affine (EA) equivalent, to copy the cryptographic profile of the parent candidate [18,19]. Seberry et al. [20,21] discussed the idea of Robustness against the DC (later on will be called Robustness throughout the document) rather than focusing on the highest coefficient in the Difference Distribution Table (DDT) alone. The robustness is upper bounded by $(1-2^{-n+1})$ for $(n \equiv 1 \mod 2)$ and $(1-2^{-n+2})$ for $(n \equiv 0 \mod 2)$ for an n-bit (finite field inversion based) bijection. However, the Robustness of an $m \times n$ surjective S-Box is interesting in this regard, upper bounded by $\frac{2^{n+m-1}-2^m-2^{n-1}+1}{2^{n+m-1}}$. The realistic values deviate from the lower or upper bounds. The AE and EA equivalent S-Box retains the distribution of differential probabilities at different locations in the DDT compared to the parent profile. Evaluating Robustness in the surjective substitution layer is crucial rather than focusing on the DU alone. This article identifies and addresses the robustness problem in the AE and EA equivalent surjective mappings.

Paper Organization: Section 2 explains the preliminary mathematical notations used throughout the document. In Sect. 3, we have discussed the types and design strategies of S-Box mappings. Section 4 outlines the robustness against differential cryptanalysis. Our results are elaborated in Sect. 5, and the paper is concluded in Sect. 6.

2 Preliminaries

Definition 1. *Given two positive integers* $(m, n \geq 2)$*, an S-Box is a vectorial boolean function of the form* $\beta : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$*, mapping an m-bits to n-bits. For* $m = n$*, S is a bijection, and* $m > n$ *is a surjective mapping.*

Definition 2. *An S-Box is deferentially* δ*-uniform* ($\delta \equiv 0 \mod 2$)*, if for all* $a \in \mathbb{F}_2^m \setminus 0$*,* $x \in \mathbb{F}_2^m$ *and* $b \in \mathbb{F}_2^n$ *in a* $2^m \times 2^n$ *Difference Distribution Table (DDT),* δ *is the maximum number of occurrences for which Eq. 1 is satisfied.*

$$\begin{aligned} N_B(a,b) &= \{\beta(x) \oplus \beta(x \oplus a) = b\} \\ \delta &= \max_{\Delta a \neq 0 \in \mathbb{F}_2^m, \Delta b \in \mathbb{F}_2^n} N_B(\Delta a, \Delta b) \end{aligned} \tag{1}$$

Definition 3. *An* $m \times n$ *S-Box is differential R Robust, if for* δ*, and the frequency* ψ *of non-zero entries in the DDT for* $a \neq 0$ *and* $b = 0$*.*

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

Definition 4. *Two m-bit S-Box(es), β and β^* are affine equivalent (AE) if there exists an affine permutation $L \in \mathcal{A}_n$ and $z \in \mathbb{F}_2^m$ [18,19]*

$$\beta^* = L \circ \beta(x) \oplus z \tag{3}$$

Definition 5. *Two m-bit S-Box(es), β and β^{*} are extended affine (EA) equivalent, if there exists an affine permutation $K, L \in \mathcal{A}_n$, for some $A, c, x, z \in \mathbb{F}_2^m$ and affine function $Z(x) = A \cdot (x) \oplus z$ [18,19]*

$$\beta^{*} = K \circ \beta(x) \circ L \oplus Z(x) \tag{4}$$

3 Design of S-Box(es)

The information-theoretic security of an FN or SPN block cipher mainly depends upon an S-Box; therefore, heinous efforts are made on the design level strategies [5]. Since its inception, high-end research is contributed to its optimal design. These strategies are grouped into three (03) classes, i.e., Mathematical objects, Random Generation and Heuristic Techniques. A cryptographer expects a profile with lower δ from an S-Box. The probability distribution of differentials in a DDT is estimated in [22–24] and Theorem 9.1.1, Eqn 9.1 and 9.2 in [25]. The mathematical function-based cryptographic mappings are (not limited to) Finite Field inversion [26–31], Finite Field exponentiation [32,33], Modular Ring Exponentiation [34], and APN functions [35,36]. Like Finite Field inversion [11], not all the mathematical functions are promising for optimal cryptographic profile, $\delta = 128$ for SAFER [34] and $\delta = 10$ for E2 [37].

Based upon the results in (Theorem 9.1.1 and Eqn 9.1 [25]), the probability that a random $m \times n$ mapping will be differentially 4 uniform is negligible. For any 6×4 random mapping, the probability that it will be an APN is very low compared to any other 6×4 random mapping with $\delta = 12$. Random mappings available in the literature [38–41], key-dependent S-Box generation [42] lies in this cluster as well. A randomly generated S-Box does not guarantee an optimal cryptographic profile.

The heuristic-based mappings are the refined version of the pseudo-random mappings. A randomly generated S-Box is filtered for some set of cryptographic properties. The S-Box is accepted if the desired profile is achieved; otherwise, a new mapping is generated. The S-Box in Kuznyechick [43] was claimed to be heuristically generated but turned down by Perrin in [25]. The permutation in Anubis [44], Skipjack [45], and Kalyna [46] is the outcome of the Hill climbing technique.

The differential uniformity [11], linearity [9], Algebraic Degree [18], balancedness and linear structures [47] remains invariant under the affine equivalence. The differential branch number and linear branch number [48], Differential Power Analysis (DPA) Signal to Noise Ratio (SNR) [49], Transparency Order (TO) [50] does not remain invariant under the affine and extended affine equivalence. Lower values of DPA-SNR and TO guarantee the resistance of an S-Box against DPA attacks.

4 Robustness of Surjective S-Box(es)

Seberry explained the reasons for the weaknesses of the Data Encryption Standard (DES) against the differential Cryptanalysis [20]. The author argued that only the largest coefficient in the DDT table does not matter, and the frequency of non-zero entries in the first column of DDT is also important. For an n-bit bijection, the frequency of zero entries for the first column is $2^n - 1$, and R is upper bounded by $1 - 2^{-n+1}$. The number of non-zero entries is not strictly unitary in the DDT of $m \times n$ mapping (Page 62 - [8]). For surjective mappings, the robustness is quite interesting and bounded by $(1 - \frac{1}{2^m})(1 - 2^{-n+1})$. The robustness deviates from the lower or upper bound as proposed in [20,21].

Proposition 1. *Robustness against the differential cryptanalysis is invariant under affine equivalence.*

Proof: For any positive $x, \alpha \in F_{2^n}$, the derivative of $S(x)$ in the direction of α is $D_\alpha S(x) = S(x) \oplus S(x \oplus \alpha)$. For an affine matrix Lover F_2 and $z \in F_{2^n}$, let $S^*(x) = L \cdot S(x) \oplus z$ be the affine equivalent S-Box. The directional derivative of $S^*(x)$ can be computed in the following manner,

$$\begin{aligned} D_\alpha S^*(x) &= S^*(x) \oplus S^*(x \oplus \alpha) \\ &= L \cdot S(x) \oplus z \oplus L \cdot S(x \oplus \alpha) \oplus z \\ &= L \cdot S(x) \oplus L \cdot S(x \oplus \alpha) \\ &= L \cdot (S(x) \oplus S(x \oplus \alpha)) \\ &= L \cdot (D_\alpha S(x)) \end{aligned} \tag{5}$$

Since the robustness profile in Eq. 2 only considers the frequency of non-zero entries in the first column (which is $\beta = 0$, equivalently $D_\alpha S(x) = 0$) of DDT, An S-Box's affine preserves the distribution of coefficients (with altered positions) in the DDT. The frequency of non-zero entries in the first column remains unchanged. The affine equivalence changes the positions of coefficients in the DDT rows according to the affine matrix. The affine constant z does not play any role in managing DDT coefficients. The affine permutation parameters do not affect δ and ψ, thus preserving the values of R in Eq. 2 accordingly.

Proposition 2. *Robustness against the differential cryptanalysis is not invariant under extended affine equivalence.*

Proof: For two affine matrices A_1, A_2 over F_2, let $S^\Delta = A_1 \cdot S(A_2(x \oplus b_1)) \oplus b_2 \oplus A_3(x) \oplus b_3$ be EA equivalent S-Box of S. The directional derivative of S^Δ can be computed in the following manner,

$$\begin{aligned} D_\alpha S^\Delta(x) &= S^\Delta(x) \oplus S^\Delta(x \oplus \alpha) \\ &= A_1 \cdot S(A_2(x \oplus b_1)) \oplus b_2 \oplus A_3(x) \oplus b_3 \oplus A_1 \cdot S(A_2(x \oplus \alpha \oplus b_1)) \oplus b_2 \oplus A_3(x \oplus \alpha) \oplus b_3 \\ &= A_1 \cdot S(A_2(x \oplus b_1)) \oplus A_1 \cdot S(A_2(x \oplus \alpha \oplus b_1)) \oplus A_3(x) \oplus A_3(x \oplus \alpha) \\ &= A_1 \cdot S(A_2(x \oplus b_1)) \oplus A_1 \cdot S(A_2(x \oplus \alpha \oplus b_1)) \oplus A_3(\alpha) \\ &= A_1 \cdot (S(A_2(x \oplus b_1)) \oplus S(A_2(x \oplus \alpha \oplus b_1))) \oplus A_3(\alpha) \end{aligned} \tag{6}$$

From Eq. 6, it is evident that the directional derivative is affected by the affine permutation parameters, thus affecting the values of the directional derivative for α. The changing frequency of non-zero entries in the first column of DDT results in the variation of the Robustness profile of EA equivalent mappings.

The higher values of δ and ψ lead to weakened S-Box(es) against the differential cryptanalysis. The designer focuses on importing the exact cryptographic profile rather than stressing the affine permutation parameters. The selection of affine permutation parameters and functions is crucial in this regard. Those affine permutation parameters are of the utmost importance, which can lower the value of ψ, resulting in higher robustness. The preceding section shed some light on the actual test cases of the real-world ciphers, and optimal mappings in the 4-bit class [51,52].

5 Results

For evaluation of robustness, the S-Box(es) from a well-known cipher DES, analyzed in [20], are compared to the affine equivalent S-Box(es) for different affine permutation parameters. The 4-bit S-Box(es) with optimal cryptographic properties from [51] are combined to get 6-bit S-Box(es) of the form $\beta_1 : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$. The three 5-bit non-linear mappings from [47] are combined for achieving $\beta_2 : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^5$. For β_1 and β_2, R is upper bounded by 0.861 and 0.923 respectively. We have also randomly generated (6×5) and (6×4) mappings and their associated affine equivalent candidates[1]. The lower values of R against the affine equivalent of the DES Substitution layer in (Table 1, from [20]) is a clear indication of the weakness against DC. For the sake of convenience, the affine equivalent mappings are represented as $i, j \in [0 \dots ord(\mathcal{A}_n) - 1]$ for an affine matrix $M_i, M_j, \in \mathcal{A}_n$, for all $i \neq j$.

Following the proof in Proposition-1 and Eq. 5, the robustness profile of affine equivalent mappings in Table 3, 2 and 1 remains invariant for all the S-Box(es) under consideration. The results from Proposition-2 prove that the robustness profiles for the extended affine equivalent in Table 3, 2 and 1 do not remain invariant for the surjective mappings. For EA-S0 (EA equivalent of S0), the R values drastically drop to 0.1289 from 0.316 in Table 1. In Table 2, the values of R decline to 0.063 for EA-O3 and EA-O4. The R values for EA equivalence are not promising as the parent mappings in Table 3.

According to [49], the upper bound of DPA-SNR for 6×4 S-Box is 2^3. The higher values of DPA-SNR make an S-Box vulnerable to the DPA attack. DPA-SNR of A-S0 (5.0360) is higher than the parent S-Box DPA-SNR (3.6110). Similarly, the DPA-SNR profile of EA-S7 shows smaller values than S7 and A-7, making it more resistant to DPA attacks. The TO profile of S-Box(es) in Table 1 is altered by the affine parameters as compared to the parent mappings;

[1] The S-Box(es), their equivalent mappings and detailed cryptographic profile is available at https://drive.google.com/drive/folders/1-6DNsVdZWT_kkdhJEpZgM-A0Pjtv8wtQ?usp=sharing.

the lower value of TO against all the S-Box(es) is minimized to 2.0079 for EA-S2. The lower value of TO for the S3 in Table 1 is maximized from 2.0634 to 2.0674 in EA-S3. The values of DPA-SNR for EA-O1 and EA-O5 in Table 2 are drastically higher and approaching the higher bound, making them vulnerable to DPA attacks.

For 6×5 mappings, the DPA and TO profiles show considerable variations in Table 3. The DPA-SNR of S54 is lowered from 5.0531 to 3.729 in A-S54. On the other hand, the EA map amplifies the values against S51 and EA-S51. The TO values are maximized for EA-S54, and EA-S52 are lowered accordingly.

Table 1. Robustness Profile of DES and its Equivalent S-Box(es)

S-Box	S0	S1	S2	S3	S4	S5	S6	S7
ψ	37	33	37	24	31	33	35	36
δ	16							
R	0.316	0.363	0.316	0.469	0.387	0.363	0.340	0.328
DPA-SNR	3.6110	4.503	0.316	3.855	3.855	3.0836	4.6618	4.2188
TO	2.063492							
Affine Equivalent S-Box(es) of DES								
S-Box	A-S0	A-S1	A-S2	A-S3	A-S4	A-S5	A-S6	A-S7
ψ	37	33	37	24	31	33	35	36
δ	16							
R	0.316	0.363	0.316	0.469	0.387	0.363	0.340	0.328
DPA-SNR	5.0360	4.3813	4.3787	4.7819	4.3120	3.4148	4.8906	4.0236
TO	2.063492							
Extended Affine Equivalent S-Box(es) of DES								
S-Box	EA-S0	EA-S1	EA-S2	EA-S3	EA-S4	EA-S5	EA-S6	EA-S7
ψ	53	44	52	44	49	45	48	44
δ	16							
R	0.1289	0.2344	0.1406	0.2344	0.1758	0.2227	0.1875	0.2344
DPA-SNR	4.57711	4.3813	4.9506	3.3795	4.2350	4.7970	3.9806	3.05629
TO	2.03571	2.0555	2.0079	2.0674	2.05158	2.0238	2.0555	2.04761

Table 2. Robustness Profile of 6 × 4 Equivalent S-Box(es)

S-Box	O1	O2	O3	O4	O5
ψ	18	11	15	21	21
δ	46	54	54	48	44
R	0.2021	0.1294	0.1196	0.168	0.210
DPA-SNR	3.1459	3.2825	2.8857	3.1067	3.2356
TO	2.063492				
Affine Equivalent 6 × 4 S-Box(es)					
S-Box	A-O1	A-O2	A-O3	A-O4	A-O5
ψ	18	11	15	21	21
δ	46	54	54	48	44
R	0.2021	0.1294	0.1196	0.168	0.210
DPA-SNR	4.4216	4.0	2.5217	2.3717	3.3288
TO	2.063492				
Extended Affine Equivalent 6 × 4 S-Box(es)					
S-Box	EA-O1	EA-O2	EA-O3	EA-O4	EA-O5
ψ	46	38	38	45	46
δ	46	54	54	48	44
R	0.079	0.063	0.063	0.0742	0.0879
DPA-SNR	7.3292	5.8362	5.2277	5.0695	6.2719
TO	2.0436	2.01984	2.05157	4.0	2.0198

Table 3. Robustness Profile of 6 × 5 Equivalent S-Box(es)

S-Box	S51	S52	S53	S54
ψ	18	21	25	21
δ	34	32	32	32
R	0.3369	0.3359	0.3042	0.2734
DPA-SNR	4.1367	4.8013	4.5584	5.0531
TO	4.06394	4.0555	4.0158	4.0834
Affine Equivalent 6 × 5 S-Box(es)				
S-Box	A-S51	A-S52	A-S53	A-S54
ψ	18	21	25	21
δ	34	32	32	32
R	0.3369	0.3359	0.3042	0.2734
DPA-SNR	5.0800	4.2156	3.8318	3.7290
TO	5.0000	4.0198	5.0000	4.0119
Extended Affine Equivalent 6 × 5 S-Box(es)				
S-Box	EA-S51	EA-S52	EA-S53	EA-S54
ψ	31	27	37	29
δ	34	32	32	32
R	0.2417	0.2891	0.2109	0.2734
DPA-SNR	5.3692	5.0838	5.4433	4.9637
TO	4.0158	4.0079	4.0476	5.0000

6 Conclusion

An S-Box is designed to achieve specific cryptographic properties to satisfy the notions of information-theoretic security. The affine equivalent mappings import the desired cryptographic profile. During the importing process, the cryptographic engineer may overlook the robustness of surjective mappings. The affine permutation choices drastically affect the robustness of a surjective mapping. In our analysis, none of the 6×4 and 6×5 EA equivalent S-Box achieved good robustness compared to the parent mapping. Neglecting affine parameters may lead to a weakened mapping against the differential cryptanalysis irrespective of the parent differential uniformity. The choice of affine parameters also affects the security of an S-Box against DPA attacks. Therefore, a careful selection of affine equivalence parameters is as essential as the cryptographic profile.

References

1. Hankin, C.: Project VENONA: breaking the unbreakable code (2020)
2. Claude Elwood Shannon: A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423 (1948)
3. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
4. Shannon, C.E.: Prediction and entropy of printed English. Bell Syst. Tech. J. **30**(1), 50–64 (1951)
5. Kam, J.B., Davida, G.I.: Structured design of substitution-permutation encryption networks. IEEE Trans. Comput. **28**(10), 747–753 (1979)
6. Adams, C., Tavares, S.: The structured design of cryptographically good s-boxes. J. Cryptol. **3**(1), 27–41 (1990). https://doi.org/10.1007/BF00203967
7. Heys, H.M., Tavares, S.E.: Substitution-permutation networks resistant to differential and linear cryptanalysis. J. Cryptol. **9**(1), 1–19 (1996). https://doi.org/10.1007/BF02254789
8. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
9. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_33
10. Zhou, Y., Standaert, F.X.: S-box pooling: towards more efficient side-channel security evaluations. In: Applied Cryptography and Network Security Workshops. ACNS 2022. LNCS, vol. 13285, pp. 146–164. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-16815-4_9
11. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_6
12. Cruz Jiménez, R.A.: Generation of 8-bit s-boxes having almost optimal cryptographic properties using smaller 4-bit s-boxes and finite field multiplication. In: Lange, T., Dunkelman, O. (eds.) LATINCRYPT 2017. LNCS, vol. 11368, pp. 191–206. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25283-0_11

13. Canright, D.: A very compact s-box for AES. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 441–455. Springer, Heidelberg (2005). https://doi.org/10.1007/11545262_32
14. Arı, A., Özkaynak, F.: Generation of substitution box structures based on blum blum shub random number outputs. In: 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 677–682. IEEE (2022)
15. Artuğer, F., Özkaynak, F.: A method for generation of substitution box based on random selection. Egypt. Inform. J. **23**(1), 127–135 (2022)
16. Freyre-Echevarrıa, A.: On the generation of cryptographically strong substitution boxes from small ones and heuristic search. In: 10th Workshop on Current Trends in Cryptology (CTCrypt 2021), p. 112 (2021)
17. Opirskyy, I., Sovyn, Y., Mykhailova, O.: Heuristic method of finding bitsliced-description of derivative cryptographic s-box. In: 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 104–109. IEEE (2022)
18. Canteaut, A., Roué, J.: On the behaviors of affine equivalent sboxes regarding differential and linear attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 45–74. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_3
19. Fuller, J.E.: Analysis of affine equivalent Boolean functions for cryptography. PhD thesis, Queensland University of Technology (2003)
20. Seberry, J., Zhang, X.M., Zheng, Y.: Systematic generation of cryptographically robust s-boxes. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 171–182 (1993)
21. Seberry, J., Zhang, X.-M., Zheng, Y.: Pitfalls in designing substitution boxes. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 383–396. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48658-5_35
22. Daemen, J., Rijmen, V.: Probability distributions of correlation and differentials in block ciphers. J. Math. Cryptol. **1**(3), 221–242 (2007)
23. O'Connor, L.: On the distribution of characteristics in bijective mappings. J. Cryptol. **8**(2), 67–86 (1995). https://doi.org/10.1007/BF00190756
24. Hawkes, P., O'Connor, L.: XOR and Non-XOR differential probabilities. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 272–285. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_19
25. Perrin, L.P.: Cryptanalysis, reverse-engineering and design of symmetric cryptographic algorithms. PhD thesis, University of Luxembourg, Luxembourg (2017)
26. Daemen, J., Rijmen, V.: The rijndael block cipher: AES proposal. In: First Candidate Conference (AeS1), pp. 343–348 (1999)
27. Aoki, K., et al.: Camellia: a 128-bit block cipher suitable for multiple platforms — design and analysis. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44983-3_4
28. Daemen, J., Knudsen, L., Rijmen, V.: The block cipher square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052343
29. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_13

30. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74619-5_12
31. Diffie, W., Ledin, G.: SMS4 encryption algorithm for wireless networks. Cryptology ePrint Archive (2008)
32. Perrin, L.P., Udovenko, A.: Exponential s-boxes: a link between the s-boxes of belt and kuznyechik/streebog. IACR Trans. Symmetric Cryptol. **2016**(2), 99–124 (2017)
33. Agievich, S., Afonenko, A.: Exponential s-boxes. Cryptology ePrint Archive (2004)
34. Massey, J.L.: SAFER K-64: a byte-oriented block-ciphering algorithm. In: Anderson, R. (ed.) FSE 1993. LNCS, vol. 809, pp. 1–17. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-58108-1_1
35. Bilgin, B., Bogdanov, A., Knežević, M., Mendel, F., Wang, Q.: FIDES: lightweight authenticated cipher with side-channel resistance for constrained hardware. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 142–158. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40349-1_9
36. Matsui, M.: New block encryption algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052334
37. Kanda, M., et al.: E2-a new 128-bit block cipher. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **83**(1), 48–59 (2000)
38. Scott, R.: Wide-open encryption design offers flexible implementations. Cryptologia **9**(1), 75–91 (1985)
39. Rose, G.G., Hawkes, P.: Turing: a fast stream cipher. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 290–306. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39887-5_22
40. Kaliski, B.: The MD2 message-digest algorithm. Technical report (1992)
41. Das, I., Nath, S., Roy, S., Mondal, S.: Random s-box generation in AES by changing irreducible polynomial. In: 2012 International Conference on Communications, Devices and Intelligent Systems (CODIS), pp. 556–559 (2012)
42. Kazlauskas, K., Kazlauskas, J.: Key-dependent s-box generation in AES block cipher system. Informatica **20**(1), 23–34 (2009)
43. Dolmatov, V.: GOST R 34.12-2015: block cipher kuznyechik. Technical report (2016)
44. Barreto, P.S.L.M.: The anubis block cipher. NESSIE (2000)
45. Knudsen, L., Wagner, D.: On the structure of skipjack. Discret. Appl. Math. **111**(1–2), 103–116 (2001)
46. Oliynykov, R., et al.: A new encryption standard of Ukraine: the Kalyna block cipher. Cryptology ePrint Archive (2015)
47. Bannier, A.: Combinatorial Analysis of Block Ciphers With Trapdoors. PhD thesis, École Nationale Supérieure d'Arts et Métiers (2017)
48. Sarkar, S., Syed, H.: Bounds on differential and linear branch number of permutations. In: Susilo, W., Yang, G. (eds.) ACISP 2018. LNCS, vol. 10946, pp. 207–224. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93638-3_13
49. Guilley, S., Hoogvorst, P., Pacalet, R.: Differential power analysis model and some results. In: Quisquater, J.-J., Paradinas, P., Deswarte, Y., El Kalam, A.A. (eds.) CARDIS 2004. IIFIP, vol. 153, pp. 127–142. Springer, Boston, MA (2004). https://doi.org/10.1007/1-4020-8147-2_9
50. Li, H., Zhou, Y., Ming, J., Yang, G., Jin, C.: The notion of transparency order, revisited. Comput. J. **63**(12), 1915–1938 (2020)

51. Leander, G., Poschmann, A.: On the classification of 4 bit s-boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73074-3_13
52. Zhang, W., Bao, Z., Rijmen, V., Liu, M.: A new classification of 4-bit optimal s-boxes and its application to present, rectangle and SPONGENT. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 494–515. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48116-5_24