Block Cipher's Substitution Box Generation Based on Natural Randomness in Underwater Acoustics and Knight's Tour Chain

Muhammad Fahad Khan1,2, Khalid Saleem1, Tariq Shah 3, Mohmmad Mazyad Hazzazi 4, Ismail Bahkali 5, Piyush Kumar Shukla 6

1 Department of Computer Science, Quaid-i-Azam University, Islamabad, Pakistan
2 Department of Software engineering, Foundation University Islamabad, Pakistan
3 Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
4 Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
5 Department of Information Sciences, King Abdulaziz University Jeddah, 21589, Saudi Arabia
6 Department of Computer Science & Engineering, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, Madhya Pradesh, India

ABSTRACT
The protection of confidential information is a global issue and block encryption algorithms are the most reliable option for securing data. The famous information theorist, Claude Shannon has given two desirable characteristics that should exist in a strong cipher which are substitution and permutation in their fundamental research on "Communication Theory of Secrecy Systems." block ciphers strictly follow the substitution and permutation principle in an iterative manner to generate a ciphertext. The actual strength of the block ciphers against several attacks is entirely based on its substitution characteristic, which is gained by using the substitution box(S-Box). In the current literature, algebraic structure-based and chaos-based techniques are highly used for the construction of S-boxes because both these techniques have favourable features for S-box construction, but also various attacks of these techniques have been identified including SAT solver, Linear and differential attacks, Gröbner-based attacks, XSL attacks, Interpolation attacks, XL-based attacks, Finite precision effect, chaotic systems degradation, predictability, weak randomness, chaotic discontinuity, Limited control parameters. The main objective of this research is to design a novel technique for the dynamic generation of S-boxes that are safe against the cryptanalysis techniques of algebraic structure-based and chaos-based approaches. True randomness has been universally recognized as the ideal method for cipher primitives design because true random numbers are unpredictable, irreversible, and un reproducible. The biggest challenge we faced during this research was how can we generate the true random numbers and how can true random numbers utilized for strengthening the s-box construction technique. The basic concept of the proposed technique is the extraction of true random bits from underwater acoustic waves and to design a novel technique for the dynamic generation of S-boxes using the chain of knight’s tour. Rather than algebraic structure and chaos-based, our proposed technique depends on inevitable high-quality randomness which exists in underwater acoustic waves. The proposed method satisfies all standard evaluation tests of S-boxes construction and true random numbers generation. Two million bits have been analyzed using the NIST randomness test suite, and the results show that underwater sound waves are an impeccable entropy source for true randomness. Additionally, our dynamically generated S-boxes have better or equal strength, over the latest published S-boxes (2020 to 2021). According to our knowledge first time, this type of research has been done, in which natural randomness of underwater acoustic waves has been used for the construction of block cipher’s Substitution Box.

KEYWORDS: Encryption, Substitution Box, Randomized Decision Making, Randomness, Chaotic Encryption, Entropy Source, Knight’s Tour, Chaotic Maps, Chaos

1. INTRODUCTION
Information security is the protection of secret data from illegal access, disclosure, inspection, destruction, disruption, and modification. The protection of confidential information is a global issue and block encryption algorithms are the most reliable option [1]. Block cipher is a branch of deterministic algorithm that works on the static length of bits, which is called block. Block cipher algorithms split the plaintext into various blocks of size k, to generate the same number of encrypted...
blocks of size n. Block ciphers encrypt one block at a time and the size of the output block is always equal to the input block and the transformation from input block to output block is done through the key whitening operation. Block cipher merged the confusion-diffusion primitives iteratively using a round function to generate an encrypted text. AES, DES, GOST, BLOWFISH are the most prominent block ciphers of the industry, that used the same strategy. For the block encryption algorithms such as AES, GOST, BLOWFISH, DES, linear-differential attacks are the most powerful attacks [2-6]. In the differential attack, the basic purpose is to detect the sequential patterns from the encrypted text and for this purpose, the attacker tries to apply a specific set of inputs to trace the change in output. In the linear attack, the basic purpose is to find the linear relation among the plain text, cipher text with the corresponding keys. The responsibility to create a randomized relation among ciphertext and the key is on the confusion component, also the confusion component is totally responsible to provide resistance against the linear and differential attacks [1-11]. Block cipher’s confusion component is generally known as substitution(S-box) which transforms $k$ input bits into $m$ output bits through $S: \{0,1\}^k \rightarrow \{0,1\}^m$, transforms vector $z = [z_{n-1}, z_{n-2}, z_{n-3} ... z_0]$ into output vector $k = [k_{n-1}, k_{n-2}, k_{n-3} ... k_0]$.

As S-box is the only nonlinear primitive of block cipher, so the block cipher strength depends on its design. Cipher designers used various approaches to construct good quality S-boxes. Chaos-based and algebraic structure-based techniques are highly used for the construction of S-boxes. Chaos-based and algebraic structure-based techniques have favourable features for S-box construction, but many cryptanalysis of these techniques have been identified in the current literature. These cryptanalysis are described in the following section 3. Underwater acoustic is generated by a diverse nature of sound sources such as underwater volcanoes, snapping shrimp, reverberation, vibrating objects, breaking waves, marine life, man-made sources, rain, geological activities, scattering waves, reflection waves, random motion of water molecules, lightning strikes, ice cracking, earthquake, compression and decompression of water molecules [12-22]. Due to these diverse nature of sound sources, inevitably high-quality randomness exists in the amplitude characteristic of the underwater acoustics, which was our main source of inspiration because true randomness has been universally recognized as the ideal primitive for cryptography. True random numbers (TRN) are unpredictable, irreversible, and unreproducible that’s why cipher researchers endorsed the true random number for cryptographic primitives design [23-30].

The main idea of this research paper is, extraction of true random bits from underwater acoustic waves and to design a novel technique for the dynamic generation of cryptographic S-boxes using the chain of knight’s tour. The main benefit of our approach is that, the proposed technique depends on the natural randomness of underwater acoustic waves for the construction of S-boxes and that’s why various existing chaos and algebraic structure-based attacks are bypassed for our proposed technique.

The rest of the paper is arranged as follows. Section-2 presents our main contribution, Section-3 shows the potential cryptanalysis and attacks, Section-4 describes the proposed methodology for the dynamic generation of strong S-Boxes, Section-5 presents results and discussion, section-6 shows the conclusion.

2. CONTRIBUTION
   i. A novel technique is proposed based on combination selection, for the generation of true random numbers from the randomness which exists in the amplitude property of underwater acoustics. As an assessment, two million bits have been analyzed using the NIST randomness test suite, and results show that underwater acoustic waves are an impeccable entropy source for TRNG.

   a. Knight’s tour-based, a novel technique is proposed, for the dynamic generation of S-boxes and as a result attacks of algebraic and chaos based techniques are not applicable and irrelevant for our proposed technique.
According to our knowledge first time, this type of research has been done, in which natural randomness of underwater acoustic waves has been used for the construction of Block Cipher's Substitution Box.

3. POTENTIAL ATTACKS OF EXISTING S-BOX DESIGNS

As we said before, chaos-based and algebraic structures-based techniques are widely used for the construction of Shannon's confusion primitive but many attacks of these techniques have been identified in the current literature including Gröbner-based attacks [2-8], SAT solver [9-11,31-35], Linear and differential attacks [36-50], XSL attacks [51-55], Interpolation attacks [51,56-58], XL-based attacks [59-61], finite precision effect [62-67], chaotic systems degradation [61-63,68-69], predictability [70-71], weak randomness [62-63,65-66,67-77], chaotic discontinuity [65-67,72-73], limited control parameters [78-81].

The main objective of this research is to design a novel technique for the dynamic generation of S-boxes that are safe against the attacks of algebraic structure-based and chaos-based techniques. Rather than algebraic structure and chaos-based, our proposed technique depends on inevitable high-quality randomness which exists in underwater acoustics waves. The basic concept of the proposed technique is the extraction of true random bits from underwater acoustic waves and to design a novel technique for the dynamic generation of S-boxes using the chain of knight’s tour.
Khan, Muhammad Fahad, et al. "Block Cipher’s Substitution Box Generation Based on Natural Randomness in Underwater Acoustics and Knight’s Tour Chain." Computational Intelligence and Neuroscience 2022 (2022). https://doi.org/10.1155/2022/8338508
TABLE 1: Results of NIST randomness Test Suite

| Type of Test                                      | P-Value           | Conclusion |
|--------------------------------------------------|-------------------|------------|
| 01. Frequency Test (Monobit)                     | 0.8461758819031635 | Random     |
| 02. Frequency Test within a Block                | 0.5166228701210154 | Random     |
| 03. Run Test                                     | 0.2609970420138874 | Random     |
| 04. Longest Run of Ones in a Block               | 0.34640251063536204 | Random   |
| 05. Binary Matrix Rank Test                      | 0.09949346113140206 | Random    |
| 06. Discrete Fourier Transform (Spectral) Test   | 0.832838521091328  | Random     |
| 07. Non-Overlapping Template Matching Test       | 0.22184797295460362 | Random   |
| 08. Overlapping Template Matching Test           | 0.16413619193258017 | Random   |
| 09. Maurer's Universal Statistical test          | 0.4051810932845413 | Random     |
| 10. Linear Complexity Test                       | 0.4394606534399792 | Random     |
| 11. Serial test:                                 | 0.5703210920746249 | Random   |
| 12. Approximate Entropy Test                     | 0.5412977586951687 | Random   |
| 13. Cumulative Sums (Forward) Test               | 0.9081561782752144 | Random     |
| 14. Cumulative Sums (Reverse) Test               | 0.7420961383854099 | Random     |
| 15. Random Excursions Test:                      |                   |            |
| State:                                          | Chi Squared       | P-Value    | Conclusion |
| -4                                              | 3.1940558536339703 | 0.6700965365355721 | Random |
| -3                                              | 8.322704313725493  | 0.1393246937222086 | Random |
| -2                                              | 2.215579649802308  | 0.818611392928053 | Random |
| -1                                              | 10.373856209150327 | 0.06530924791189864 | Random |
| +1                                              | 5.49281045751634   | 0.358734843928551 | Random |
| +2                                              | 1.97863099330267   | 0.8520935894148005 | Random |
| +3                                              | 0.872903529411762  | 0.9721522155809542 | Random |
| +4                                              | 2.2030722493078865 | 0.8203920781040164 | Random |
| 16. Random Excursions Variant Test:              |                   |            |
| State:                                          | Counts            | P-Value    | Conclusion |
| -9.0                                            | 1743              | 0.3503620748973999 | Random |
| -8.0                                            | 1791              | 0.2231318786599762 | Random |
| -7.0                                            | 1861              | 0.0970096546916874 | Random |
| -6.0                                            | 1837              | 0.09426256021374013 | Random |
| -5.0                                            | 1775              | 0.17515792247265105 | Random |
| -4.0                                            | 1675              | 0.32181454622986 | Random |
| -3.0                                            | 1588              | 0.6391395377015844 | Random |
| -2.0                                            | 1605              | 0.43375610043914314 | Random |
| -1.0                                            | 1572              | 0.4476990724652935 | Random |
| +1.0                                            | 1601              | 0.1993153588782468 | Random |
| +2.0                                            | 1629              | 0.30147752489003166 | Random |
| +3.0                                            | 1609              | 0.523032983174088 | Random |
| +4.0                                            | 1609              | 0.589348273539888 | Random |
| +5.0                                            | 1662              | 0.42637406860618 | Random |
| +6.0                                            | 1783              | 0.1678955379041649 | Random |
| +7.0                                            | 1876              | 0.0827802734496795 | Random |
| +8.0                                            | 1869              | 0.1135773370125223 | Random |
| +9.0                                            | 1818              | 0.20668955769990105 | Random |

4. PROPOSED METHODOLOGY
The proposed method consists of two phases, the first phase is true random numbers generation based on underwater acoustics and the second phase is dynamic generation of S-boxes based on Knight's tour chain. Architecture diagram of the proposed system is depicted in Figure-1.

4.1 TRUE RANDOM NUMBERS GENERATION BASED ON UNDERWATER ACOUSTICS
In this phase, first of all, long-term underwater acoustics recordings were acquired from the doi based dataset of the Australian Antarctic Data Centre (AADC) [82]. In the dataset, the average duration of each recording is sixty minutes. Out of thousands of long-term underwater acoustic recordings, we randomly selected the 96 long-term underwater acoustic recordings but proposed technique can take any multiple of 16 files as entropy.
sources. Secondly, these recordings are divided into blocks of size 16 and then the amplitude difference of every 0.5 sec is calculated. Due to the diverse nature of sound sources, the difference of each amplitude with other amplitudes is random, this was our main source of inspiration. Other characteristics of underwater sound like frequency and timber contain low-quality randomness that’s why we chose the amplitude characteristic for this research. To calculate the amplitude differences, we used the combination selection strategy by using \( n! / r! \cdot (n-r)! \). In our case, the value of the n is 16 and the value of r is 2. The entire step-by-step process of this phase from underwater acoustic files input to the random bits generation is represented in the flowchart of Figure-2. The amplitude differences calculation step is depicted in FIGURE-3 and here long term underwater acoustic recording represented as \( R_1, R_2, ..., R_{16} \). Two million bits have been analyzed using the NIST randomness test suite and in the Table-1, results of the NIST tests show that underwater acoustic waves are an impeccable entropy source for true randomness. There are many random extractors based on hash functions, machine learning, chaos machine, physical unclonable functions, and probabilistic methods but among all these types of random extractors, Von Neumann random extractor is the simplest and fastest method that’s why we chose Von Neumann random extractor as post processing method.

4.2 DYNAMIC GENERATION OF S-BOXES BASED ON KNIGHT'S TOUR CHAIN
The knight's tour is more than a 1400-year-old puzzle game whose objective is to discover the legal moves on the chessboard in the way that, it explores every cell only once and in our proposed methodology we utilized the chain of \( 8 \times 8 \) knight’s tour for the generation of S-boxes. First of all true random numbers are acquired and divided into blocks of 64 length size, then each 64 length block is converted into the \( 8 \times 8 \) chessboard matrix. Based on the knight tour rules, we traversed each element of the chessboard matrix however only unique elements are considered for S-box elements, and a similar procedure is repeated for coming chessboards until the completion of required length of the S-box. Initial position of first block of the knight's tour chain is calculated through \( r = TRNG [0] \mod 8 \), \( c = TRNG [1] \mod 8 \) and the initial positions of other knights' tour chains are dependent on the second last and the last element of the S-box, which are calculated through \( r = S-box [n-1] \mod 8 \), \( c = S-box [n] \mod 8 \). The entire step-by-step process of this phase from true random numbers input to dynamic S-boxes generation is represented in the flowchart of Figure-4. This phase is depicted in the following Figure-5. The reverse S-box algorithm is shown in the following. From the dynamically generated S-boxes stream, we picked two S-boxes randomly as sample which are shown in Table 2a and 2b, and their reverse S-boxes are also shown in Table 2c and Table 2d respectively. The maximum nonlinearity score of our sample S-boxes is higher or equal to the recently published S-boxes (from 2020 to 2021).

5. RESULTS AND EVALUATION
In the results and evaluation section, our proposed S-boxes are evaluated by standard S-box evaluation criteria which includes Nonlinearity Score, Bit Independence Criterion, Linear Approximation Probability, Strict Avalanche Criterion and Differential Approximation Probability.
FIGURE 4: Flowchart of Dynamic S-boxes Generation based on Knight's Tour Chain
Khan, Muhammad Fahad, et al. "Block Cipher's Substitution Box Generation Based on Natural Randomness in Underwater Acoustics and Knight's Tour Chain." Computational Intelligence and Neuroscience 2022 (2022).
https://doi.org/10.1155/2022/8338508

| TABLE 2a: Substitution box 1 |
|-----------------------------|
| 106 220 5 24 1 124 20 104 96 88 240 170 9 115 246 86 |
| 197 230 174 155 76 185 175 31 142 103 239 122 40 113 208 228 |
| 78 21 218 29 110 85 43 70 27 120 66 28 189 126 36 232 |
| 138 165 234 16 243 23 160 235 97 48 90 101 98 250 6 45 |
| 38 73 141 53 81 71 203 206 2 135 252 111 145 92 238 63 |
| 130 186 180 123 192 4 251 89 196 84 58 143 32 59 82 198 |
| 112 224 247 64 177 178 148 184 233 200 222 107 105 195 201 187 |
| 154 236 163 109 219 254 137 210 241 204 212 139 34 248 249 74 |
| 202 253 52 47 226 19 12 3 114 207 118 171 91 193 217 144 |
| 169 237 13 57 131 30 121 95 33 14 199 119 146 100 166 182 |
| 255 72 215 209 188 77 99 35 116 242 18 87 132 102 158 152 |
| 150 62 211 55 164 80 162 125 225 133 183 117 179 51 205 60 |
| 65 8 15 213 69 223 41 54 176 46 244 194 0 156 172 39 |
| 56 161 227 147 93 129 67 168 221 245 25 136 17 214 128 167 |
| 61 229 22 11 153 94 149 151 50 216 49 159 37 10 127 7 |
| 26 83 44 134 42 231 79 75 68 108 173 157 140 191 181 190 |

| TABLE 2b: Substitution box 2 |
|-----------------------------|
| 254 240 187 11 151 155 153 100 103 201 144 0 72 14 158 63 |
| 180 209 138 2 169 27 60 186 21 97 52 109 251 248 95 19 |
| 124 71 10 107 58 210 26 203 90 168 121 250 66 226 50 104 |
| 176 46 65 93 6 183 245 134 86 216 7 44 238 207 16 110 |
| 202 99 17 165 217 167 80 55 128 82 75 200 40 182 147 174 |
| 196 156 120 192 116 136 164 188 48 5 152 166 33 62 230 137 |
| 12 9 102 61 223 54 159 34 59 246 195 213 170 51 253 229 |
| 126 122 140 241 98 77 237 179 47 191 30 130 118 185 224 243 |
| 45 36 227 149 106 239 68 221 189 219 150 108 13 161 154 112 |
| 242 172 23 178 135 131 160 231 129 244 31 255 173 39 233 205 |
| 198 89 20 18 215 8 249 139 181 212 53 163 157 127 208 64 |
| 105 85 142 184 145 29 37 175 111 125 222 4 117 232 76 87 |
| 84 35 42 123 49 235 24 92 101 91 204 194 79 133 96 32 |
| 15 69 67 146 190 88 83 1 141 119 177 234 132 38 74 236 |
| 252 3 28 78 22 220 57 43 211 225 199 41 94 197 143 70 |
| 206 73 162 56 25 228 218 81 115 114 171 113 148 193 247 214 |
### TABLE 2c: Reverse S-box 1

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 204 | 4 | 72 | 135 | 85 | 2 | 62 | 239 | 193 | 12 | 237 | 227 | 134 | 146 | 153 | 194 |
| 51 | 220 | 170 | 133 | 6 | 33 | 226 | 53 | 3 | 218 | 240 | 40 | 43 | 35 | 149 | 23 |
| 92 | 152 | 124 | 167 | 46 | 236 | 64 | 207 | 28 | 198 | 244 | 38 | 242 | 63 | 201 | 131 |
| 57 | 234 | 232 | 189 | 130 | 67 | 199 | 179 | 208 | 147 | 90 | 93 | 191 | 224 | 177 | 79 |
| 99 | 192 | 42 | 214 | 248 | 196 | 39 | 69 | 161 | 65 | 127 | 247 | 20 | 165 | 32 | 246 |
| 181 | 68 | 94 | 241 | 89 | 37 | 15 | 171 | 9 | 87 | 58 | 140 | 77 | 212 | 229 | 151 |
| 8 | 56 | 60 | 166 | 157 | 59 | 173 | 25 | 7 | 108 | 0 | 107 | 249 | 115 | 36 | 75 |
| 96 | 29 | 136 | 13 | 168 | 187 | 138 | 155 | 41 | 150 | 27 | 83 | 5 | 183 | 45 | 238 |
| 222 | 213 | 80 | 148 | 172 | 185 | 243 | 73 | 219 | 118 | 48 | 123 | 252 | 66 | 24 | 91 |
| 143 | 76 | 156 | 211 | 102 | 230 | 176 | 231 | 175 | 228 | 112 | 19 | 205 | 251 | 174 | 235 |
| 54 | 209 | 182 | 114 | 180 | 49 | 158 | 223 | 215 | 144 | 11 | 139 | 206 | 250 | 18 | 22 |
| 200 | 100 | 101 | 188 | 82 | 254 | 159 | 186 | 103 | 21 | 81 | 111 | 164 | 44 | 255 | 253 |
| 84 | 141 | 203 | 109 | 88 | 16 | 95 | 154 | 105 | 110 | 128 | 70 | 121 | 190 | 71 | 137 |
| 30 | 163 | 119 | 178 | 122 | 195 | 221 | 162 | 233 | 142 | 34 | 116 | 1 | 216 | 106 | 197 |
| 97 | 184 | 132 | 210 | 31 | 225 | 17 | 245 | 47 | 104 | 50 | 55 | 113 | 145 | 78 | 26 |
| 10 | 120 | 169 | 52 | 202 | 217 | 14 | 98 | 125 | 126 | 61 | 86 | 74 | 129 | 117 | 160 |

### TABLE 2d: Reverse S-box 2

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 215 | 19 | 225 | 187 | 89 | 52 | 58 | 165 | 97 | 34 | 3 | 96 | 140 | 13 | 208 |
| 62 | 66 | 163 | 31 | 162 | 24 | 228 | 146 | 198 | 244 | 38 | 21 | 226 | 181 | 122 | 154 |
| 207 | 92 | 103 | 193 | 129 | 182 | 221 | 157 | 76 | 235 | 194 | 231 | 59 | 128 | 49 | 120 |
| 88 | 196 | 46 | 109 | 26 | 170 | 101 | 71 | 243 | 230 | 36 | 104 | 22 | 99 | 93 | 15 |
| 175 | 50 | 44 | 210 | 134 | 209 | 239 | 33 | 12 | 241 | 222 | 74 | 190 | 117 | 227 | 204 |
| 70 | 247 | 73 | 214 | 192 | 177 | 56 | 191 | 213 | 161 | 40 | 201 | 199 | 51 | 236 | 30 |
| 206 | 25 | 116 | 65 | 7 | 200 | 98 | 8 | 47 | 176 | 132 | 35 | 139 | 27 | 63 | 184 |
| 143 | 251 | 249 | 248 | 84 | 188 | 124 | 217 | 82 | 42 | 113 | 195 | 32 | 185 | 112 | 173 |
| 72 | 152 | 123 | 149 | 220 | 205 | 55 | 148 | 85 | 95 | 18 | 167 | 114 | 216 | 178 | 238 |
| 10 | 180 | 211 | 78 | 252 | 131 | 138 | 4 | 90 | 6 | 142 | 5 | 81 | 172 | 14 | 102 |
| 150 | 141 | 242 | 171 | 86 | 67 | 91 | 69 | 41 | 20 | 108 | 250 | 145 | 156 | 79 | 183 |
| 48 | 218 | 147 | 119 | 16 | 168 | 77 | 53 | 179 | 125 | 23 | 2 | 87 | 136 | 212 | 121 |
| 83 | 253 | 203 | 106 | 80 | 237 | 160 | 234 | 75 | 9 | 64 | 39 | 202 | 159 | 240 | 61 |
| 174 | 17 | 37 | 232 | 169 | 107 | 255 | 164 | 57 | 68 | 246 | 137 | 229 | 135 | 186 | 100 |
| 126 | 233 | 45 | 130 | 245 | 111 | 94 | 151 | 189 | 158 | 219 | 197 | 223 | 118 | 60 | 133 |
| 1 | 115 | 144 | 127 | 153 | 54 | 105 | 254 | 29 | 166 | 43 | 28 | 224 | 110 | 0 | 155 |
Algorithm: ReverseSbox (S-box)

in: 2D array of integers, sbox[16][16]; out: 2D array of integers, ReverseSbox [16][16];
1: ReverseSbox → [16][16]
2: for row → 0 … (16) do
3:     for col → 0 … (16) do
4:         rowIS → sbox row,col div 16
5:         colIS → sbox row,col mod 16
6:         value → row*16+col
7:     ReverseSbox rowIS,colIS →value
8: end for
9: end for
10: return ReverseSbox

5.1 NONLINEARITY

Among all cryptographic properties, nonlinearity is the most important one. The main purpose of S-box is to gain nonlinear change from secret message to the ciphered message. For a strong encryption scheme, the mapping between input and output in an S-box must be nonlinear. The nonlinearity of cryptographic algorithm is represented by nonlinearity score. Nonlinearity is defined as the smallest difference of Boolean function to the bunch of affine functions. The nonlinearity score determine the total number of bits altered to get the closest affine function in the Boolean truth Table. It calculates the distance between the set of all affine functions and Boolean function. When the initial distance is obtained, the nearest affine function is achieved by inverting the bit values in the truth Table of Boolean function. By using walsh spectrum, the nonlinearity of Boolean function is computed through [46]:

\[
N_g = 2^{n-1}(1 - 2^{-n} \max_{\varphi \in \mathbb{GF}(2^n)} |S(g)(\varphi)|) \tag{1}
\]

\[S_{(g)}(\varphi) = \sum_{\varphi \in \mathbb{GF}(2^n)} (-1)^{g(x) \oplus x \varphi} \tag{2}\]

Where \(\varphi\) is a n-bit vector and \(\varphi \in \mathbb{GF}(2^n)\). \(x \varphi\) represents the bit-wise dot product of \(x\) and \(\varphi\):

\[x \varphi = x_1 \oplus \varphi_1 + x_2 \oplus \varphi_2 \cdot \cdot \cdot + x_n \oplus \varphi_n.\]
S-box having high nonlinearity creates difficult for attacker to perform linear cryptanalysis. The maximum nonlinearity scores of our proposed Sbox-1 and Sbox-2 are 110 and 110 respectively, which is higher or equal to the recently published S-boxes. Detailed comparative analysis is shown in the following table-3.

### TABLE 3: Nonlinearity of state-of-the-art S-boxes

| Recently Published S-boxes | Maximum Nonlinearity Achieved | Recently Published S-boxes | Maximum Nonlinearity Achieved |
|---------------------------|-------------------------------|---------------------------|-------------------------------|
| [83],[2021]               | 108                           | [98],[2021]               | 110                           |
| [84],[2021]               | 110                           | [99],[2021]               | 110                           |
| [85],[2021]               | 108                           | [100],[2021]              | 108                           |
| [86],[2020]               | 108                           | [101],[2021]              | 110                           |
| [87],[2020]               | 110                           | [102],[2020]              | 102                           |
| [88],[2020]               | 108                           | [103],[2020]              | 107                           |
| [89],[2020]               | 108                           | [104],[2020]              | 104                           |
| [90],[2020]               | 108                           | [105],[2020]              | 106                           |
| [91],[2020]               | 104                           | [106],[2020]              | 105                           |
| [92],[2020]               | 108                           | [107],[2020]              | 106                           |
| [93],[2020]               | 106                           | [108],[2020]              | 108                           |
| [94],[2020]               | 108                           | [109],[2020]              | 108                           |
| [95],[2020]               | 110                           | [110],[2020]              | 108                           |
| [96],[2021]               | 108                           | [111],[2021]              | 108                           |
| [97],[2021]               | 110                           | [112],[2021]              | 108                           |

### 5.2 Strict Avalanche Criteria (SAC)

Strict avalanche criteria is the another crucial property for evaluating and according to SAC, if a single input bit is altered, all output bits will shift with probability of 1/2. SAC examined the effects of avalanche affects in encryption scheme. The modification at the input series induces a significant change in output series. SAC computes the number of output bits altered caused by inverting a single bit of input. To make the system more reliable, the output vector needed to be deviate with half probability, when one bit of input is inverted. Dependency matrix is determined to evaluate the SAC property. For an S-box that satisfies SAC property all values were close to the ideal value of 0.5 in its dependence matrix. Dependency matrix offsets computed through equation 3 [46]. The SAC results of S-box1 and Sbox-2 are shown in Table 4a, 4b and scores of our Sbox-1 and Sbox-2 are 0.495 and 0.50 respectively which are the ideal scores for the secure S-boxes.

\[
S(g) = \frac{1}{n^2} \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} \left( \frac{1}{2} - Q_{r,w}(g) \right)
\]

Where

\[
Q_{r,w}(g) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} gw(x) \oplus gw(x \oplus e_r)
\]

\[
e_r = [0, 1, 0, 1, 2, \ldots, 0, n] \top
\]

\(\top\) is the transpose of matrix \(\theta_{r,w} = 0, r \neq w \quad \text{or} \quad \theta_{r,w} = 1, r = w\)

#### TABLE 4a: SAC results of Sbox-1

| r   | w   | \(0.500000\) | \(0.562500\) | \(0.468750\) | \(0.453125\) | \(0.500000\) | \(0.421875\) | \(0.453125\) | \(0.500000\) |
|-----|-----|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| 0.500000 | 0.562500 | 0.468750 | 0.453125 | 0.500000 | 0.421875 | 0.453125 | 0.500000 |
| 0.437500 | 0.515625 | 0.468750 | 0.515625 | 0.500000 | 0.546875 | 0.437500 | 0.500000 |
| 0.468750 | 0.546875 | 0.484375 | 0.515625 | 0.500000 | 0.531250 | 0.546875 | 0.500000 |
| 0.453125 | 0.500000 | 0.500000 | 0.484375 | 0.453125 | 0.515625 | 0.546875 | 0.500000 |
| 0.468750 | 0.562500 | 0.500000 | 0.500000 | 0.484375 | 0.437500 | 0.500000 | 0.500000 |
| 0.406250 | 0.546875 | 0.593750 | 0.484375 | 0.453125 | 0.390625 | 0.531250 | 0.500000 |
| 0.437500 | 0.484375 | 0.578125 | 0.453125 | 0.515625 | 0.546875 | 0.437500 | 0.484375 |
| 0.546875 | 0.515625 | 0.531250 | 0.500000 | 0.562500 | 0.437500 | 0.515625 | 0.515625 |

#### TABLE 4b: SAC results of Sbox-2
The coefficient of correlation is used to determine the cipher's strength. When the changes in output bits are a crucial parameter in determining the cipher's strength, the BIT Independent Criterion (BIC) parameter for the S-box is required to make system design incomprehensible. The bit independence of the avalanche variables for a given set of avalanche vectors must be pair-wise independent. By modifying the input bits, BIC is used to study the behaviour of the output bits. When the output bits behave independent of one another, the S-box holds the BIC property. If any single input bit \( i \) is inverted, BIC states that output bits \( j \) and \( k \) will alter independently. This will enhance the effectiveness of confusion function. The coefficient of correlation is used to determine the independence among pair of avalanche variables. High bit independence is required to make system design incomprehensible. The bit independence of the \( j^{th} \) and \( k^{th} \) bits of \( B^{e_{i}} \) is [46]:

\[
BIC(b_j, b_k) = \max_{1 \leq i \leq n} |corr(b_{j}^{e_i}, b_{k}^{e_{i'}})|
\]

S-box function (h) is described as : \( h: \{0, 1\}^n \rightarrow \{0, 1\}^n \)

BIC parameter for the S-box function is expressed as :

\[
BIC(h) = \max_{1 \leq j, k \leq n} BIC(b_j, b_k)
\]

The change in output bits is a crucial parameter in determining the cipher's strength. When the changes in output bits contrast with the input bit sequence shows sufficient independence, the mapping technique will be difficult to understand.

### Table 5A: BIC Independent Matrix of Sbox-1

|       | 0.480469 | 0.484375 | 0.464844 | 0.509766 | 0.507812 | 0.517578 | 0.521484 |
|-------|----------|----------|----------|----------|----------|----------|----------|
| 0.480469 | 0.511719 | 0.513672 | 0.484375 | 0.486328 | 0.476562 | 0.494141 |          |
| 0.484375 | 0.511719 | 0.498047 | 0.507812 | 0.494141 | 0.509396 | 0.486328 |          |
| 0.464844 | 0.513672 | 0.498047 |          | 0.494141 | 0.508589 | 0.501953 | 0.496094 |
| 0.509766 | 0.484375 | 0.507812 | 0.494141 |          | 0.509766 | 0.480469 | 0.470703 |
| 0.507812 | 0.486328 | 0.494141 | 0.508589 | 0.509766 |          | 0.494141 | 0.498047 |
| 0.517578 | 0.476562 | 0.503906 | 0.501953 | 0.480469 | 0.494141 |          | 0.509766 |
| 0.521484 | 0.494141 | 0.486328 | 0.496094 | 0.470703 | 0.490847 | 0.509766 |          |

### Table 5B: BIC Independent Matrix of Sbox-2

|       | 0.501953 | 0.498047 | 0.501953 | 0.488281 | 0.529297 | 0.486328 | 0.484375 |
|-------|----------|----------|----------|----------|----------|----------|----------|
| 0.501953 | 0.500000 | 0.501953 | 0.484375 | 0.513672 | 0.466797 | 0.509766 |          |
| 0.498047 | 0.500000 | 0.507812 | 0.527344 | 0.474609 | 0.507812 | 0.486328 |          |
| 0.501953 | 0.501953 | 0.507812 | 0.519531 | 0.523438 | 0.515625 | 0.521484 |          |
| 0.488281 | 0.484375 | 0.527344 | 0.519531 | 0.523438 | 0.515625 | 0.521484 |          |
| 0.529297 | 0.513672 | 0.474609 | 0.521484 | 0.523438 | 0.478516 | 0.503906 |          |
| 0.486328 | 0.466797 | 0.507812 | 0.494141 | 0.515625 | 0.478516 |          | 0.519531 |
| 0.484375 | 0.509766 | 0.486328 | 0.511719 | 0.521484 | 0.503906 | 0.519531 |          |

### 5.4 Linear Approximation Probability (LP)
LP is the cryptographic property which measures the resistance of S-box against the linear attacks. LP analysis intends to measure the maximum imbalance of the event. LP is measured by determining the total number of coincident input bits with the output bits. The input bits uniformity must be identical to the output bits. Each input bit is individually evaluated and its results are tested in the output bits. γ1 and γ2 masks are selected randomly to determine the mask of all output and input values. The mathematical expression of determining Linear Approximation Probability is as follows [46]:

\[
\text{LP}_f = \max_{\gamma_1, \gamma_2 \neq 0} \left| \frac{\#(x \in X, x x = S(x) \neq S(x) \oplus \Delta y)}{2^n} \right|
\]

(7)

Where γ1 and γ2 represent the input and output mask in the above expression. Linear approximation probability is calculated by using these masks. X represents the set of all possible inputs and \(2^n\) is the total number of elements in the set. S-box with low LP value is robust enough against different linear approximation attacks.

5.5 Differential Approximation Probability (DP)

The resistance of S-box to the differential attacks is assessed through the DP. DP is the probability of particular change in output bits caused by the change in input bits. An S-box must possess differential uniformity which means that each input differential is connected to the specific output differential. The XOR values of all output must have equal probability to the XOR values of all input. The differential uniformity is measured by using expression [46]:

\[
\text{DP} (\Delta x \rightarrow \Delta y) = \frac{\#(x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y)}{2^n}
\]

(8)

Where X represents the set of all possible input values, \(2^n\) is the total number of elements in set. The maximum differential probability value a system could achieve is 4/256. The lowest value of DP means the high security of the S-box against differential approximation attacks. In Tables 6a and 6b, we can see that our randomly picked Sbox-1 and Sbox-2 fully fill the DP criterion.

TABLE 6a: DP of Sbox-1

| x    | 0.0000 | 0.0234 | 0.0312 | 0.0234 | 0.0234 | 0.0312 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 |
|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| y    | 0.3125| 0.0234 | 0.0156 | 0.0312 | 0.0234 | 0.0312 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 |

TABLE 6b: DP of Sbox-2

| x    | 0.0000 | 0.0234 | 0.0312 | 0.0234 | 0.0156 | 0.0234 | 0.0312 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 | 0.0234 |
|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
6. CONCLUSION
The protection of confidential information is a global issue and block encryption algorithms are the most reliable option. The actual strength of the block encryption algorithms against several attacks is entirely dependent on S-Boxes. Current in the literature, algebraic structure-based, and chaos-based techniques are highly used for the construction of S-boxes because both these techniques have favourable features for S-box construction, but many attacks of these techniques have been identified. In this paper, we purposed a novel technique for the dynamic generation of S-boxes that is safe against the existing attacks of algebraic structure-based and chaos-based techniques. True randomness has been universally recognized as the ideal method for security primitive because true random numbers are unpredictable, irreversible, and un reproducible. Rather than algebraic structure and chaos-based, our proposed technique depends on inevitable high-quality randomness which exists in underwater acoustics waves. According to our knowledge first time, this type of research has been done, in which natural randomness of underwater acoustic waves and knight’s tour problem has been used for the generation of Block Cipher’s Substitution Box. The proposed method satisfies all standard evaluation tests of S-boxes construction and true random numbers generation. Additionally, our dynamically generated S-boxes have better or equal strength, over the latest published S-boxes (2020 to 2021). In the future, we will extend this research for automatic key generation and optimization using knight’s tour.

Data Availability
The datasets analysed during the current study are available in the Australian Antarctic Data Centre repository at https://data.aad.gov.au/metadata/records/AAS_4102_longTermAcousticRecordings

Conflicts of Interest
The authors declare no conflicts of interest.

Acknowledgments

REFERENCES
1. Khan, M. F., Saleem, K., Alshara, M. A., & Bashir, S. (2021). Multilevel information fusion for cryptographic substitution box construction based on inevitable random noise in medical imaging. Scientific reports, 11(1), 1-23.
2. Bulygin, S., Brickenstein, M.: Obtaining and Solving Systems of Equations in Key Variables Only for the Small Variants of AES. Mathematics in Computer Science 3(2), 185–200 (Apr 2010)
3. Buchmann, Johannes, Andrei Pyshkin, and Ralf-Philipp Weinmann. "Block ciphers sensitive to Gröbner basis attacks." In Cryptographers’ Track at the RSA Conference, pp. 313-331. Springer, Berlin, Heidelberg, 2006.
4. Buchmann, Johannes, Andrei Pyshkin, and Ralf-Philipp Weinmann. "A zero-dimensional Gröbner basis for AES-128." In International Workshop on Fast Software Encryption, pp. 78-88. Springer, Berlin, Heidelberg, 2006.
5. Cid, Carlos, and Ralf-Philipp Weinmann. "Block ciphers: algebraic cryptanalysis and Gröbner bases." In Gröbner bases, coding, and cryptography, pp. 307-327. Springer, Berlin, Heidelberg, 2009.
6. Pyshkin, Andrey. "Algebraic cryptanalysis of block ciphers using Gröbner Bases." PhD diss., Technische Universität, 2008.
7. Zhao, Kaixin, Jie Cui, and Zhiqiang Xie. "Algebraic cryptanalysis scheme of AES-256 using Gröbner basis." Journal of Electrical and Computer Engineering 2017 (2017).
8. Faugère, Jean-Charles. "Interactions between computer algebra (Gröbner bases) and cryptology." In Proceedings of the 2009 international symposium on Symbolic and algebraic computation, pp. 383-384. 2009.
9. Gwynne, Matthew, and Oliver Kullmann. "Attacking AES via SAT." PhD diss., BSc Dissertation (Swansea), 2010.
10. Jovanovic, Philipp, and Martin Kreuzer. "Algebraic attacks using SAT-solvers." Groups Complexity Cryptology 2, no. 2 (2010): 247-259.
11. Semenov, Alexander, Oleg Zaikin, Ilya Otpuschennikov, Stepan Kochemazov, and Alexey Ignatiev. "On cryptographic attacks using backdoors for SAT." In Thirty-Second AAAI Conference on Artificial Intelligence. 2018.
12. R. S. Dietz and M. J. Sheehy, Transpacific detection of myojin volcanic explosions by underwater sound. Bulletin of the Geological Society 2 942–956 (1954).
13. M. A. McDonald, J. A. Hildebrand & S. M. Wiggins, Increases in deep ocean ambient noise in the Northeast Pacific west of San Nicolas Island, California, J. Acoust. Soc. Am. 120, 711–718 (2006).
14. Ocean Noise and Marine Mammals, National Research Council of the National Academies (The National Academies Press, Washington DC, 2003).
15. Mohl, B., Wahlberg, M., Madsen, P. T., Miller, L. A., & Surlykke, A. (2000). Sperm whale clicks: Directionality and source level revisited. The Journal of the Acoustical Society of America, 107(1), 638–648. https://doi.org/10.1121/1.428329
16. Watkins, W. A. (1980). Acoustics and the Behavior of Sperm Whales. In R.-G. Busnel & J. F. Fish (Eds.), Animal Sonar Systems (pp. 283–290). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4684-7254-7_11
17. Levenson, C. (1974). Source level and bistatic target strength of the sperm whale ( Physeter catodon ) measured from an oceanographic aircraft. The Journal of the Acoustical Society of America, 55(5), 1100–1103. https://doi.org/10.1121/1.1914660
18. Watkins, W. A., & Schevill, W. E. (1977). Sperm whale codas. The Journal of the Acoustical Society of America, 62(6), 1485. https://doi.org/10.1121/1.381678
19. Cummings, W. C., & Thompson, P. O. (1994). Characteristics and seasons of blue and finback whale sounds along the U.S. west coast as recorded at SOSUS stations. The Journal of the Acoustical Society of America, 95(5), 2853–2853. https://doi.org/10.1121/1.409514
20. Clark, C. W. (1982). The acoustic repertoire of the Southern right whale, a quantitative analysis. Animal Behaviour, 30(4), 1060–1071. https://doi.org/10.1016/S0003-3472(82)80196-6
21. Thompson, P. O., Cummings, W. C., & Ha, S. J. (1986). Sounds, source levels, and associated behavior of humpback whales, Southeast Alaska. The Journal of the Acoustical Society of America, 80(3), 735–740. https://doi.org/10.1121/1.393947
22. Frankle, A. S. (1994). Acoustic and Visual Tracking Reveals Distribution, Song Variability and Social Roles of Humpback Whales in Hawaiian waters.(Megaptera Novaegaeangliae) (p. 142). Manoa HI: University of Hawaii.
23. Pironio, Stefano, et al. "Random numbers certified by Bell’s theorem." Nature 464.7291 (2010): 1021.
24. Bernardo-Gavito, Ramón, et al. "Extracting random numbers from quantum tunnelling through a single diode." Scientific Reports 7.1 (2017): 17879.
25. Sunar, Berk, William J. Martin, and Douglas R. Stinson. "A provably secure true random number generator with built-in tolerance to active attacks." IEEE Transactions on computers 56.1 (2006): 109-119.
26. Ray, Biswajit, and Aleksandar Milenković. "True random number generation using read noise of flash memory cells." IEEE Transactions on Electron Devices 65.3 (2018): 963-969.
27. Aghamohammadi, Cina, and James P. Crutchfield. "Thermodynamics of random number generation." Physical Review E 95.6 (2017): 062139.
28. Lee, Kyungroul, et al. "TRNG (True Random Number Generator) method using visible spectrum for secure communication on 5G network." IEEE Access 6 (2018): 12838-12847.
29. Marangon, Davide Giacomo, et al. "Long-term test of a fast and compact quantum random number generator." Journal of Lightwave Technology 36.17 (2018): 3778-3784.
30. Jinomeiq, Liu, Wei Baoduui, and Wang Xinmei. "One AES S-box to increase complexity and its cryptanalysis." Journal of Systems Engineering and Electronics 18, no. 2 (2007): 427-433.
31. Cho, Joo Yeon. "Linear cryptanalysis of reduced-round PRESENT." In Cryptographers’ Track at the RSA Conference, pp. 302-317. Springer, Berlin, Heidelberg, 2010.
32. Selçuk, Ali Aydin. "On probability of success in linear and differential cryptanalysis." Journal of Cryptology 21, no. 1 (2008): 131-147.
33. Blondeau, Céline, and Benoît Gérard. "Multiple differential cryptanalysis: theory and practice." In International Workshop on Fast Software Encryption, pp. 35-54. Springer, Berlin, Heidelberg, 2011.
45. Jing-mei, Liu, Wei Bao-dian, Cheng Xiang-guo, and Wang Xin-mei. "Cryptanalysis of Rijndael S-box and improvement." Applied Mathematics and Computation 170, no. 2 (2005): 958-975.

46. Khan, Muhammad Asif, Asim Ali, Varun Jeoti, and Shahid Manzoor. "A chaos-based substitution box (S-Box) design with improved differential approximation probability (DP)." Iranian Journal of Science and Technology, Transactions of Electrical Engineering 42, no. 2 (2018): 219-238.

47. Hermelin, Miia, and Kaisa Nyberg. "Linear Cryptanalysis Using Multiple Linear Approximations." IACR Cryptology ePrint Archive 2011 (2011): 93.

48. Lu, Jiqiang. "A methodology for differential-linear cryptanalysis and its applications." Designs, Codes and Cryptography 77, no. 1 (2015): 11-48.

49. Tiessen, Tyge, Lars R. Knudsen, Stefan Kölbl, and Martin M. Lauridsen. "Security of the AES with a Secret S-Box." In International Workshop on Fast Software Encryption, pp. 175-189. Springer, Berlin, Heidelberg, 2015.

50. Canteaut, A., & Roué, J. (2015, April). On the behaviors of affine equivalent sboxes regarding differential and linear attacks. In Annual international conference on the theory and applications of cryptographic techniques (pp. 45-74). Springer.

51. Youssef, A.M., Gong, G.: On the Interpolation Attacks on Block Ciphers. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 109–120. Springer, Heidelberg (2001)

52. Cid, C.: Some Algebraic Aspects of the Advanced Encryption Standard. In: Dobbertin, H., Rijmen, V., Sowa, A. (eds.) Advanced Encryption Standard – AES, pp. 58–66. No. 3373 in Lecture Notes in Computer Science, Springer Berlin Heidelberg

53. Cid, C., Leurent, G.: An Analysis of the XSL Algorithm. In: Roy, B. (ed.) Advances in Cryptology - ASIACRYPT 2005, pp. 333–352. No. 3788 in Lecture Notes in Computer Science, Springer Berlin Heidelberg

54. Choy, Jiali, Huihui Yap, and Khoongming Khoo. "An analysis of the compact XSL attack on BES and embedded SMS4." In International Conference on Cryptology and Network Security, pp. 103-118. Springer, Berlin, Heidelberg, 2009.

55. Choy, Jiali, Guanhan Chew, Khoongming Khoo, and Huihui Yap. "Cryptographic properties and application of a generalized unbalanced Feistel network structure." In Australasian Conference on Information Security and Privacy, pp. 73-89. Springer, Berlin, Heidelberg, 2009.

56. Dinur, Itai, Yunwen Liu, Willi Meier, and Qingju Wang. "Optimized interpolation attacks on LowMC." In International Conference on the Theory and Application of Cryptology and Information Security, pp. 535-560. Springer, Berlin, Heidelberg, 2015.

57. Li, Chaoyun, and Bart Preneel. "Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree." In International Conference on Selected Areas in Cryptography, pp. 171-193. Springer, Cham, 2019.

58. Courtois, Nicolas T. "The inverse S-box, non-linear polynomial relations and cryptanalysis of block ciphers." In International Conference on Advanced Encryption Standard, pp. 170-188. Springer, Berlin, Heidelberg, 2004.

59. Courtois, N.T., Pieprzyk, J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In: Zheng, Y. (ed.) Advances in Cryptology — ASIACRYPT 2002, pp. 267–287. No. 2501 in Lecture Notes in Computer Science, Springer Berlin Heidelberg

60. Diem, Claus. "The XL-algorithm and a conjecture from commutative algebra." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2004.

61. Makoto Sugita, Mitsuru Kawazoe, and Hideki Imai. Relation between the XL Algorithm and Gröbner Basis Algorithms. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E89-A:11–18, 2006.
62. Li, Chengqing, et al. "Dynamic analysis of digital chaotic maps via state-mapping networks." IEEE Transactions on Circuits and Systems I: Regular Papers 66.6 (2019): 2322-2335.

63. Liu, Yunqi, et al. "Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation." International Journal of Bifurcation and Chaos 27.03 (2017).

64. Deng, Yashuang, et al. "A general hybrid model for chaos robust synchronization and degradation reduction." Information Sciences 305 (2015): 146-164.

65. Khan, Muhammad Fahad, et al. "A Novel Design of Cryptographic SP-Network Based on Gold Sequences and Chaotic Logistic Tent System." IEEE Access 7 (2019): 84980-84991.

66. Hua, Zhongyun, et al. "2D Logistic-Sine-coupling map for image encryption." Signal Processing 149 (2018): 148-161.

67. Khan, Muhammad Fahad, Adeel Ahmed, and Khalid Saleem. "A novel cryptographic substitution box design using gaussian distribution." IEEE Access 7 (2019): 15999-16007.

68. Zhang, Leo Yu, et al. "A chaotic image encryption scheme owning temp-value feedback." Communications in Nonlinear Science and Numerical Simulation 19.10 (2014): 3653-3659.

69. Hua, Zhongyun, Binghang Zhou, and Yicong Zhou. "Sine chaotification model for enhancing chaos and its hardware implementation." IEEE Transactions on Industrial Electronics 66.2 (2018): 1273-1284.

70. Hua, Zhongyun, and Yicong Zhou. "Image encryption using 2D Logistic-adjusted-Sine map." Information Sciences 339 (2016): 237-253.

71. Hua, Zhongyun, and Yicong Zhou. "Dynamic parameter-control chaotic system." IEEE transactions on cybernetics 46.12 (2015): 3330-3341.

72. Zhou, Yicong, Long Bao, and CL Philip Chen. "A new 1D chaotic system for image encryption." Signal processing 97 (2014): 172-182.

73. Xie, Eric Yong, et al. "On the cryptanalysis of Fridrich's chaotic image encryption scheme." Signal Processing 132 (2017): 150-154.

74. Parvaz, R., and M. Zarebnia. "A combination chaotic system and application in color image encryption." Optics & Laser Technology 101 (2018): 30-41.

75. Alawida, Moatsum, Je Sen Teh, and Azman Samsudin. "An Image Encryption Scheme based on Hybridizing Digital Chaos and Finite State Machine." Signal Processing (2019).

76. Li, Chengqing. "Cracking a hierarchical chaotic image encryption algorithm based on permutation." Signal Processing 118 (2016): 203-210.

77. Wu, Xiangjun, et al. "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system." Information Sciences 349 (2016): 137-153.

78. Pak, Chanil, and Lilian Huang. "A new color image encryption using combination of the 1D chaotic map." Signal Processing 138 (2017): 129-137.

79. Chen, Guo, Yong Chen, and Xiaofeng Liao. "An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps." Chaos, solitons & fractals 31.3 (2007): 571-579.

80. Alawida, Moatsum, et al. "A new hybrid digital chaotic system with applications in image encryption." Signal Processing 160 (2019): 45-58.

81. Cao, Chun, Kehui Sun, and Wenhai Liu. "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map." Signal Processing 143 (2018): 122-133. short quantity of randomness [119-122]

82. Miller, B.S., Milnes, M. and Whiteside, S. (2021) Long-term underwater acoustic recordings 2013-2019, Ver. 4, Australian Antarctic Data Centre - doi:10.26179/h7xa-y729. Accessed: 2022-03-05

83. U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, "A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings," Arabian J. Sci. Eng., pp. 1–13, May 2021, doi: 10.1007/s13369-021-05666-9

84. S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permuted elliptic curves," Inf. Sci., vol. 558, pp. 246–264, May 2021
on scheme based on a new hybrid chaotic

 Address. 2022. "Block Cipher’s Substitution Box Generation Based on Natural Randomness in Underwater Acoustics and Knight’s Tour Chain." Computational Intelligence and Neuroscience 2022 (2022). https://doi.org/10.1155/2022/8338508

85. B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, “Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box,” Symmetry, vol. 13, no. 129, pp. 1–20, 2021
86. W. Gao, B. Idrees, S. Zafar, and T. Rashid, “Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(2^8)),” IEEE Access, vol. 8, pp. 136736–136749, 2020
87. S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, “A power associative loop structure for the construction of non-linear components of block cipher,” IEEE Access, vol. 8, pp. 123492–123506, 2020.
88. Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, “An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map,” IEEE Access, vol. 8, pp. 54175–54188.
89. H. Liu, A. Kadir, and C. Xu, “Cryptanalysis and constructing S-box based on chaotic map and backtracking.” App. Math. Comput., vol. 376, pp. 1–11, Jul. 2020.
90. M. B. Farah, A. Farah, and T. Farah, “An image encryption scheme based on a new hybrid chaotic map and optimized substitution box,” Nonlinear Dyn., vol. 99, pp. 3041–3064, 2020.
91. Bin Faheem, Z., Ali, A., Khan, M. A., Ul-Haq, M. E., & Ahmad, W. “Highly dispersive substitution box (S-box) design using chaos”. ETRI Journal.2020
92. Z. B. Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, “Highly dispersive substitution box (S-box) design using chaos,” ETRI J., vol. 42, pp. 1–14, Aug. 2020
93. A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, “Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications,” Sci. Rep., vol. 10, no. 1, p. 116, Dec. 2020
94. D. Lambić, “A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design,” Nonlinear Dyn., vol. 100, no. 1, pp. 699–711, Mar. 2020.
95. Q. Lu, C. Zhu, and X. Deng, “An efficient image encryption scheme based on the LSS chaotic map and single S-box,” IEEE Access, vol. 8, pp. 25664–25678, 2020.
96. N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, “A novel scheme of substitution-box design based on modified Pascal’s triangle and elliptic curve,” Wireless Pers. Commun., vol. 116, no. 4, pp. 3015–3030, Feb. 2021.
97. H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, “A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm,” Multimedia Tools Appl., vol. 80, no. 5, pp. 7333–7350, Feb. 2021.
98. M. Long and L. Wang, “S-box design based on discrete chaotic map and improved artificial bee colony algorithm,” IEEE Access, vol. 9, pp. 86144–86154, 2021.
99. R. Soto, B. Crawford, F. G. Molina, and R. Olivares, “Human behaviour based optimization supported with self-organizing maps for solving the Sbox design problem,” IEEE Access, vol. 9, pp. 84605–84618, 2021.
100. W. Yan and Q. Ding, “A novel S-box dynamic design based on nonlinear transform of 1D chaotic maps,” Electronics, vol. 10, no. 11, p. 1313, May 2021.
101. P. Zhou, J. Du, K. Zhou, and S. Wei, “2D mixed pseudo-random coupling PS map lattice and its application in S-box generation,” Nonlinear Dyn., vol. 103, no. 1, pp. 1151–1166, Jan. 2021
102. ÖzKaynak, F. (2020). “On the effect of chaotic system in performance characteristics of chaos-based S-box designs”. Physica A: Statistical Mechanics and its Applications.
103. A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, “Secure data encryption based on quantum walks for 5G Internet of Things scenario,” IEEE Trans. Netw. Service Manage., vol. 17, no. 1, pp. 118–131, Mar. 2020
104. Muhammad, Z. M. Z., & ÖzKaynak, F. (2020, February). “A Cryptographic Confusion Primitive Based on Lotka–Volterra Chaotic System and Its Practical Applications in Image Encryption”. In 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (pp. 694-698).
105. A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, “Quantum inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications,” Sci. Rep., vol. 10, no. 1, pp. 1–16, Dec. 2020.
106. Artuğer, F., & ÖzKaynak, F. (2020). “A novel method for performance improvement of chaos-based substitution Boxes”. Symmetry, 12(4), 571.
107. Lambić, D. (2020). “A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design”. Nonlinear Dynamics, 1-13.
108. H. Liu, A. Kadir, and C. Xu, “Cryptanalysis and constructing S-box based on chaotic map and backtracking.” Appl. Math. Comput., vol. 376, Jul. 2020, Art. no. 125153.
109. Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, “An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map,” IEEE Access, vol. 8, pp. 54175–54188, 2020
110. Cassal-Quiroga, B. B., & Campos-Canton, E. (2020). “Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map”. Mathematical Problems in Engineering, 2020.
111. Siddiqui, Nasir, Amna Naseer, and Muhammad Ehatish-ul-Haq. "A novel scheme of substitution-box design based on modified Pascal’s triangle and elliptic curve." Wireless Personal Communications 116.4 (2021): 3015-3030.
112. Hua, Zhongyun, et al. "Design and application of an S-box using complete Latin square." Nonlinear Dynamics 104.1 (2021): 807-825.