An Analysis of the Post Quantum and Classical Security of 4x4 and 16x4 S-Boxes and Their Implementations in Simplified-AES

Christopher Dunne[1]

Capitol Technology University, cdunne@captechu.edu

Abstract. Grover's algorithm is a quantum searching algorithm that poses a threat to symmetric cryptography. Due to their smaller key sizes, lightweight cryptographic algorithms such as Simplified-AES face a much more immediate threat from Grover's algorithm than traditional cryptographic algorithms. By analyzing different S-boxes, it was discovered that the S-box 946C753AE8FBD012 may be more quantum resistant than the S-box that Simplified-AES uses, 94ABD1856203CEF7. In addition to this, 16x4 S-boxes (or 4 4x4 S-boxes) showed to be significantly more quantum secure than 4x4 S-boxes. This is because the number of gates needed to model a 2^nx4 S-box increases at an exponential rate. It was also found that this property extends to 2^nx8 S-boxes, implying the existence of a more quantum secure 8x8 S-box that AES could use. However, an increase in quantum security does not equate to an increase in classical security, as some of the least quantum secure S-boxes analyzed displayed some of the best classical security. Finally, an alteration of Simplified-AES that used a 16x4 S-box was found that displayed better classical and quantum security than Simplified-AES and did not require an increase in key size.

Keywords: Grover's Algorithm, 16x4 S-box, Simplified-AES, Quantum Security

1 Introduction

Grover's algorithm is a quantum searching algorithm able to find values in $\sqrt{N}$ steps, where N is the amount of unstructured data being searched. This differs from classical algorithms which need to make an average of $\frac{N}{2}$ checks [20]. It can be used to perform brute force attacks to determine the key used in a symmetric encryption algorithm. To do this, one must implement the encryption algorithm used on a quantum computer. As such, the quantum cost of such an implementation directly impacts the cost of Grover's algorithm, wherein quantum cost refers to the number of gates needed to model said implementation.

This is especially true regarding lightweight cryptography. Lightweight cryptography is a branch of cryptography that aims at enabling devices with limited resources to perform cryptography. This is because many Internet of Things (IoT) devices have limited memory, power, and processing speed that can be dedicated to performing cryptographic algorithms [21]. Lightweight cryptography has become increasingly prevalent given the rise of IoT devices. In 2021 there were 11.28 billion IoT devices, and this figure is predicted to reach 29.42 billion by 2030 [22].

Given the limited resources, lightweight cryptography uses smaller keys than standard encryption algorithms. Not only does this reduce the security of lightweight cryptographic algorithms, but these algorithms will be the first algorithms that Grover's algorithm may pose a threat to. IonQ is currently working on IonQ Forte, a quantum computer with 32 quantum bits (qubits) [19], which is enough qubits to perform an attack via Grover's algorithm on Simplified-AES (S-AES). It is because of this that lightweight cryptographic algorithms should be limited to ephemeral data with a short lifespan. As such, even minor increases in the security of lightweight cryptographic algorithms are greatly beneficial.

One aspect of symmetric encryption algorithms that can be modified is the construction and implementation of substitution boxes (S-boxes). These are precomputed tables that map an input value to an output value. This paper analyzes how the construction of an S-box impacts its respective quantum cost, and if the use of multiple variably assigned S-boxes provides better quantum security against Grover's algorithm.

1.1 Methodology

The original plan was to modify the S-box used in S-AES and perform a brute force attack on this modified version of S-AES via Grover's algorithm. S-AES is a lightweight cryptographic algorithm whose structure is identical to AES. It has a key and block size of 16-bits and has two rounds [13].

This would be achieved by modifying the work done by Kyung-Bae Jang, Gyeong-Ju Song, Hyun-Ji Kim, and Hwa-Jeong Seo in a paper entitled "Grover on Simplified AES". This paper managed to create an efficient quantum implementation of S-AES that only used 32 qubits for a 16-bit plaintext and 16-bit key. A tool called LIGHTER-R was used to generate the quantum circuit for the S-box that did not require the use of any ancilla qubits [5].

LIGHTER-R was originally going to be used to generate the quantum circuits for the modified S-boxes which would then replace the substitution circuit and be run through Grover's algorithm. IBM Quantum (IBMQ) would be used in conjunction with Qiskit to model these results. However, LIGHTER-R produced inconsistent results that could not be replicated. In addition to this, memory constraints prevented the modified versions of S-AES from being run in Qiskit. As such, SageMath was used to generate the algebraic normal form (ANF) of various S-boxes which was then used to create a quantum circuit for said S-box. Grover's algorithm was then used to perform a known plaintext attack on a quantum circuit that XOR-ed a key with a plaintext before running said plaintext through the S-box. A known plaintext attack was performed instead of a brute force attack because it required less resources to simulate.

Afterwards, three possible full implementations of S-AES that use 16x4 S-boxes were tested. This was proceeded by classical analysis performed through the National Institute of Standards and Technology (NIST) statistical test suite on said algorithms and modified versions of S-AES that use different S-boxes. This process was then repeated on implementations using the three 16x4 randomly generated S-boxes that required the most quantum gates to model.

2 S-Box Construction

Four sets of four S-boxes were created. They were broken into these groups because a 16x4 S-box would also be tested that consisted of each S-box in the set. This S-box would use two bits from the provided key to determine which S-box would be used on the plaintext. The first set of S-boxes were created using the same methodology as the S-boxes from S-AES and AES. They served as the base set of S-boxes that the other sets would modify to meet various criteria.

The S-box that S-AES uses was generated by inverting values as an element of GF(2^4) using the prime polynomial $x^4 + x + 1$. These values were then multiplied by a matrix and had a vector added to them. This produces the equation below, wherein b_n is the nth bit of the inverted input [13].

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

This process was used to create each of the S-boxes in the first set of S-boxes, with the prime polynomials used being $x^4 + x + 1$ (i.e., the S-box that S-AES uses), $x^4 + x^3 + 1$, and $x^4 + x^3 + x^2 + x + 1$. Since there are only three prime polynomials in GF(2^4), the fourth S-box was generated using a rotated matrix and the prime polynomial $x^4 + x + 1$. The 16x4 S-box formed from Set 1 can be seen in Table 2.

The second set that was created aimed at analyzing S-boxes that produced a unique output for any given input. This was achieved by progressively shifting each S-box in the first set of S-boxes to the left. Afterwards, repeat occurrences of an output for any given input were swapped with the next value in the S-box that would not cause a collision.

The third set aimed at analyzing S-boxes that had no collisions with the input, i.e., no output values are identical to the input values. This was done by taking the first set of S-boxes and swapping any values that resulted in a collision with the next value in the S-box that would not cause said collision. Finally, the fourth set of S-boxes aimed at analyzing S-boxes that had no collisions with each other or the plaintext. This was generated by repeating this process on the second set of S-boxes. The resulting set of S-boxes can be seen in Table 1.

Table 1: Sets 1-4

	S-Box 1	S-Box 2	S-Box 3	S-Box 4
Set 1	94ABD185 6203CEF7	940756EB FD1C2A83	946C753A E8FBD012	9E518BDA 67F3C402
Set 2	94ABD185 6203CEF7	40756EBF D1C2A839	6C573AE8 FBD01294	18BDA673 CF4920E5
Set 3	94ABD185 6203ECF7	940756EB FD1C2A83	946C735A E8FDB012	9E518BDA 67F34C02
Set 4	94ABD185 6203ECF7	40756EBF D1C2A839	6C573AE8 FBD01294	18BDA673 CF49205E

2.1 S-Box Quantum Circuit Construction

It is possible to express an S-box as a series of polynomials, or their ANF. This can be used to reduce the quantum cost needed to perform Boolean functions on a quantum computer [4]. SageMath was used to calculate the ANF of each S-box. The ANF of S-box 1 of Set 1 is depicted below, with y_n being the nth output bit and x_n being the nth input bit. The ANF of the other S-boxes can be found in Appendix A.

$$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1$$
$$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3$$
$$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$$
$$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3 \oplus 1$$

This can be converted to a quantum circuit by using a multi-controlled X (MCX) gate whose target is the register y_n and whose controls are the registers in $\{x_0, \ldots, x_n\}$. The controls for each MCX gate are dictated by which x values are being multiplied together. Doing this for the equation above results in the quantum circuit depicted in Figure 1.

Table 2: 16x4 S-box formed by Set 1

	0b000000	0b000001	0b000010	0b000011
0b000000	0x9	0x4	0xA	0xB
0b000100	0xD	0x1	0x8	0x5
0b001000	0x6	0x2	0x0	0x3
0b001100	0xC	0xE	0xF	0x7
0b010000	0x9	0x4	0x0	0x7
0b010100	0x5	0x6	0xE	0xB
0b011000	0xF	0xD	0x1	0xC
0b011100	0x2	0xA	0x8	0x3
0b100000	0x9	0x4	0x6	0xC
0b100100	0x7	0x5	0x3	0xA
0b101000	0xE	0x8	0xF	0xB
0b101100	0xD	0x0	0x1	0x2
0b110000	0x9	0xE	0x5	0x1
0b110100	0x8	0xB	0xD	0xA
0b111000	0x6	0x7	0xF	0x3
0b111100	0xC	0x4	0x0	0x2

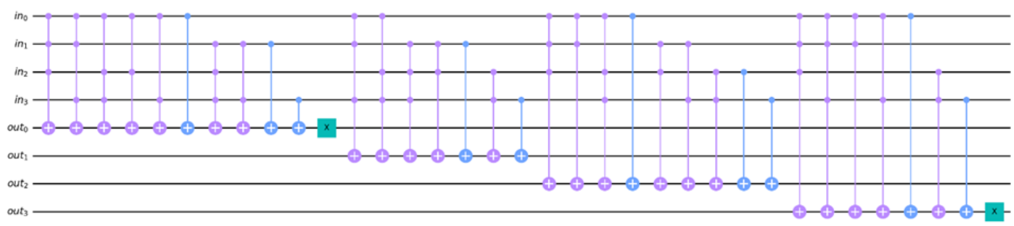


Figure 1: Quantum circuit for S-box 1 of Set 1 (94ABD1856203CEF7)

3 Quantum Cost of S-Boxes

Quantum particles must be trapped in a low energy state to allow the performance of meaningful operations. Reducing the number of gates needed for a quantum algorithm reduces the cost of performing said algorithm, as it reduces the number of necessary quantum computations and therefore the time atoms need to stay in a specific state. This is important as it reduces the likelihood of the occurrence of decoherence. Decoherence can cause a spin flip of quantum particle and can cause trapped atoms to be excited into higher vibrational modes [16].

Table 3 depicts the resulting cost of the quantum circuit for the ANF of each S-box. It lists the number of MCX gates with n controls. An MCX gate with 0 controls is equivalent to an X gate. Table 4 depicts the cost of a 16x4 S-box generated from each set. It should be noted that the quantum circuits depicted in Table 3 require 8 qubits, while the circuits in Table 4 require 10 qubits. This is because a 16x4 S-box requires 2 additional bits to determine what S-box should be used. It should also be noted that using a rotated matrix to generate S-box 4 in Set 1 had no impact on the cost of performing said S-box.

3.1 Analyzing Quantum Cost of Random S-Boxes

This process was repeated on a set of 1,500 randomly generated 4x4 S-boxes and a set of 800 randomly generated 16x4 S-boxes. Table 5 and Table 6 list the MCX gates needed

Table 3: Cost of each S-box in Sets 1 through 4

MCX Controls	Set 1 S-Box 1	Set 1 S-Box 2	Set 1 S-Box 3	Set 1 S-Box 4	Set 2 S-Box 1	Set 2 S-Box 2	Set 2 S-Box 3	Set 2 S-Box 4
0	2	2	2	2	2	1	2	1
1	10	9	13	10	10	6	8	10
2	12	14	19	12	12	11	13	14
3	11	7	7	11	11	6	6	7
Total Gates	35	32	41	35	35	24	29	32
MCX Controls	**Set 3 S-Box 1**	**Set 3 S-Box 2**	**Set 3 S-Box 3**	**Set 3 S-Box 4**	**Set 4 S-Box 1**	**Set 4 S-Box 2**	**Set 4 S-Box 3**	**Set 4 S-Box 4**
0	2	2	2	2	2	1	2	1
1	10	9	13	10	10	6	8	10
2	11	14	17	11	11	11	13	14
3	10	7	7	10	10	6	6	6
Total Gates	33	32	39	33	33	24	29	31

Table 4: Cost of each 16x4 S-box formed by Sets 1 through 4

MCX Controls	Set 1	Set 2	Set 3	Set 4
0	2	2	2	2
1	10	17	10	17
2	22	26	21	25
3	48	39	45	38
4	27	32	25	33
5	10	10	8	12
Total Gates	119	126	111	127

to run the 3 most costly randomly generated 4x4 and 16x4 S-boxes respectively. The 16x4 S-boxes were created by combining 4 randomly generated 4x4 S-boxes. A list of all the S-boxes generated and their associated costs can be found in Appendix B.

The most expensive randomly generated 4x4 S-box was 7FAC98B234516D0E, which required the same number of gates as the most expensive 4x4 S-box generated by hand (946C753AE8FBD012). The most expensive 16x4 S-box that was generated by hand was formed from Set 4, requiring 127 gates. However, the randomly generated S-box CB91D538E7A20F64A217C6534D8EBF09D14A58BF792C630E58B214C790E6DFA3 required 150 gates. This is approximately 3.659 times more gates than the most expensive 4x4 S-box found, and an increase of 23 gates compared to the 16x4 S-box generated from Set 4.

It should be noted that all the 16x4 S-boxes depicted in Table 6 were more expensive than the hand generated 16x4 S-boxes depicted in Table 4. This is even though each 16x4 S-box in Table 6 had at least one collision with the input, and at least one collision between the different 4x4 S-boxes used to generate the 16x4 S-box. This implies that reducing these collisions in 16x4 S-boxes does not increase said S-box's quantum security.

Table 5: Cost of the 3 most expensive randomly generated 4x4 S-boxes

	S-Box		
MCX Controls	7FAC98B234516D0E	FD8716ABCE459320	C2BA7FD51408E396
0	3	4	2
1	8	9	12
2	19	14	15
3	11	13	11
Total Gates	41	40	40

Table 6: Cost of the 3 most expensive randomly generated 16x4 S-boxes

	S-Box		
MCX Controls	CB91D538E7A20F64 A217C6534D8EBF09 D14A58BF792C630E 58B214C790E6DFA3	70812A3B496DCEF5 89C62357BA4ED01F 841CEAB73265DF09 0386F4127B95ECAD	6A543D18EC27F09B 9ADC7F3E502816B4 FC1BE0568A423D79 309C7BA2D8F4E651
0	2	3	2
1	10	19	13
2	42	38	38
3	48	44	52
4	36	37	34
5	12	8	8
Total Gates	150	149	147

4 Using Grover's Algorithm to Perform a Known Plaintext Attack

A known-plaintext attack is an attack wherein the attacker has access to both the ciphertext and plaintext of an encryption algorithm. Such an attack aims at figuring out the key used to encrypt the plaintext [15]. Performing a known plaintext attack with Grover's algorithm is cheaper than performing a brute force attack using Grover's algorithm. This is because Grover's algorithm will only need to search through the possible values of a key as opposed to the values for both the key and the plaintext.

Using Grover's algorithm, a known plaintext attack was performed on an algorithm that XOR-es a 4-bit key to a 4-bit plaintext that is then ran through an S-box (Algorithm 1). This performs the add round key and substitution steps of round 1 of S-AES on a 4-bit block. The shift rows, mix columns, and second add round key steps were excluded due to memory and time constraints. Two different implementations of a 16x4 S-box were tested. The first implementation (Algorithm 2) used the first and last bit of the key to determine what S-box to use (acting as x_4 and x_5) and the second implementation (Algorithm 3) appended two bits to the key that determined what S-box to use (once again acting as x_4 and x_5).

These algorithms serve as a simplified single round version of S-AES that requires fewer resources to model and operates on a single plaintext block. Below is the pseudocode for these algorithms, wherein BitToInt is a function that converts a bitstream to an integer value and *sbox* is a list of values between 0x0 and 0xF that represent the S-box being used.

Algorithm 1

```
Input: bitstream[4] pt, bitstream[4] key, list[16] sbox
bitstream[4] ct
i = 0
while i < 4 do
    ct[i] = pt[i] ⊕ key[i]
    i = i + 1
end while
ct = sbox[BitToInt(ct)]
```

Algorithm 2

```
Input: bitstream[4] pt, bitstream[4] key, list[64] sbox
bitstream[4] ct
i = 0
while i < 4 do
    ct[i] = pt[i] ⊕ key[i]
    i = i + 1
end while
bitstream[2] b
b = [key[0], key[3]]
box = BitToInt(b) * 2^4                ▷ Which 4x4 S-box to use
ct = sbox[box+BitToInt(ct)]
```

Algorithm 3

```
Input: bitstream[4] pt, bitstream[6] key, list[64] sbox
bitstream[4] ct
i = 0
while i < 4 do
    ct[i] = pt[i] ⊕ key[i]
    i = i + 1
end while
bitstream[2] b
b = [key[4], key[5]]
box = BitToInt(b) * 2^4                ▷ Which 4x4 S-box to use
ct = sbox[box+BitToInt(ct)]
```

5 Construction of Grover's Algorithm

5.1 Oracle Construction

To construct Grover's algorithm, one must create an oracle that is used to find a desired state [20]. The oracle for a known plaintext attack on a 4x4 S-box and a known ciphertext of 1100 is depicted in Figure 2 registers key, plaintext (pt), ciphertext (ct), expected, and passed. Had LIGHTER-R been used to generate the oracle, the ciphertext register would not be necessary. This is because LIGHTER-R is able to construct quantum circuits for reversible ANF representations of S-boxes that do not need an ancilla register and require fewer gates, significantly reducing the cost associated with an S-box's quantum circuit [7]. The first thing the oracle does is XOR the key register with the plaintext register. This is done by using a series of controlled-X gates on the key and plaintext registers. An S-box is then used on the plaintext and ciphertext registers, with the plaintext register acting as x_0 through x_3 and the ciphertext register acting as y_0 through y_3.

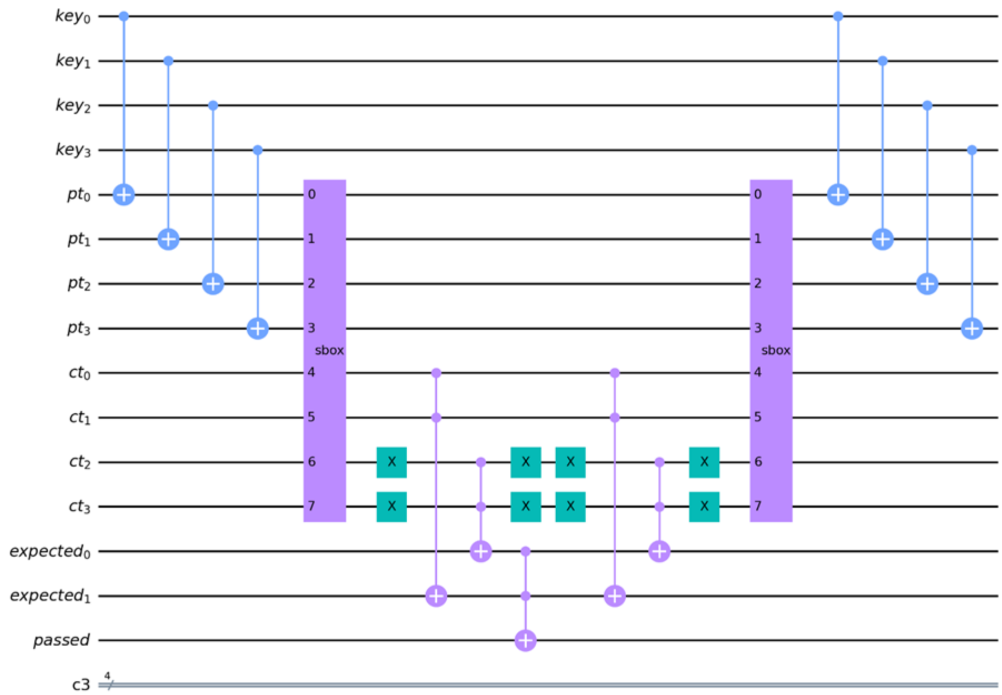


Figure 2: Quantum oracle for S-AES

The ciphertext register is then tested to see if it is in the randomly chosen state $|1100\rangle$. This is done using the 2-qubit expected register. The first qubit of this register is used to check the 0's of the ciphertext and the second qubit being used to check the 1's of the ciphertext. This is done by applying an X gate on qubits that should be in the state $|0\rangle$. A controlled-X gate is then applied, using these qubits as its control and the first qubit of the expected register as its target. It is then followed by another X gate on the ciphertext qubits in question. If the known ciphertext does not contain any zeroes, the first qubit of the expected register can either be removed or initialized to the state $|1\rangle$. Another controlled-X gate is then ran using the qubits that should be in the state $|1\rangle$ as the control, and the second qubit of the expected register being its target. If the known ciphertext does not contain any zeroes, the second qubit of the expected register can either be removed or initialized to the state $|1\rangle$.

A controlled-X gate is then run using the expected register as its control and the passed register as its target to determine if the ciphertext register is in the desired state. The process of checking the 1's and 0's of the ciphertext, running the S-box, and XORing the key with the plaintext is then repeated. Doing this sets everything back to the state they were in originally.

This process was repeated for 16x4 S-boxes. Figure 3 depicts the oracle for Algorithm 2, while Figure 4 depicts the oracle for Algorithm 3. Once again, a known ciphertext of 1100 is being looked for. As seen in Figure 4, the two additional bits of the key in Algorithm 3 are not XORed with the plaintext.

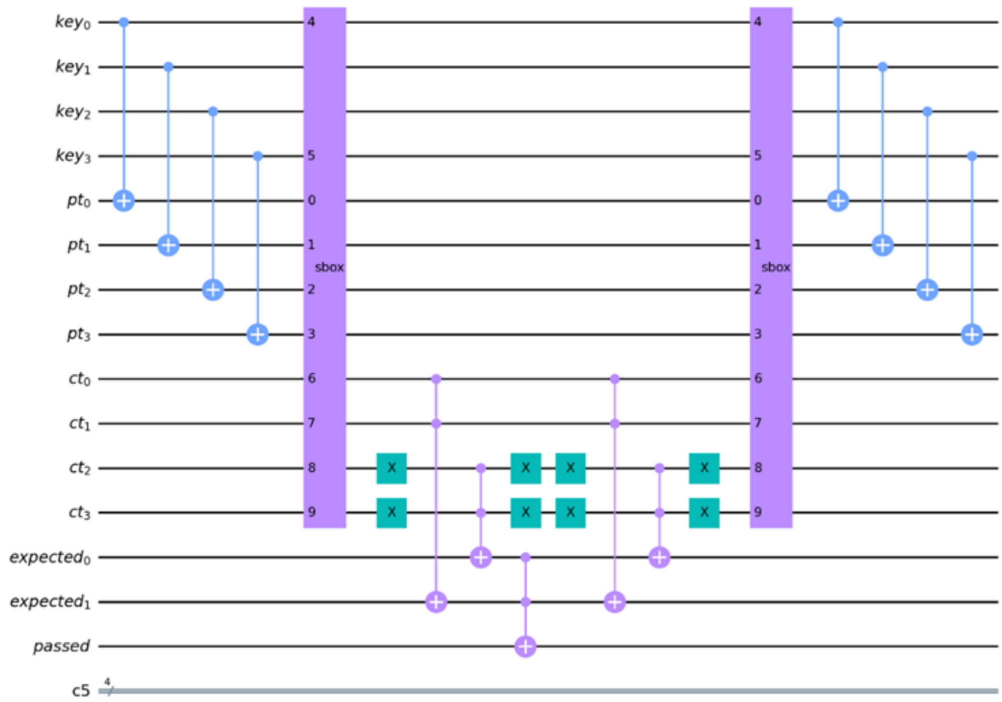


Figure 3: Quantum oracle for Algorithm 2

5.2 Assembling Grover's Algorithm

To find the 4 to 6-bit key used to generate the known ciphertext from a known plaintext, one must perform 2 searches. The plaintext register will also need to be initialized to its known value. This is done by applying a X gate on each plaintext qubit that is meant to be a $|1\rangle$. Finally, the passed register will need to be initialized to the state $|-\rangle$. An example of this is shown in Figure 5, wherein a known plaintext of 1101 is being looked for using a single 4x4 S-box. After the oracle is run, a diffuser is applied to the key register. The diffuser rotates the key register closer to the states that satisfy oracle [20].

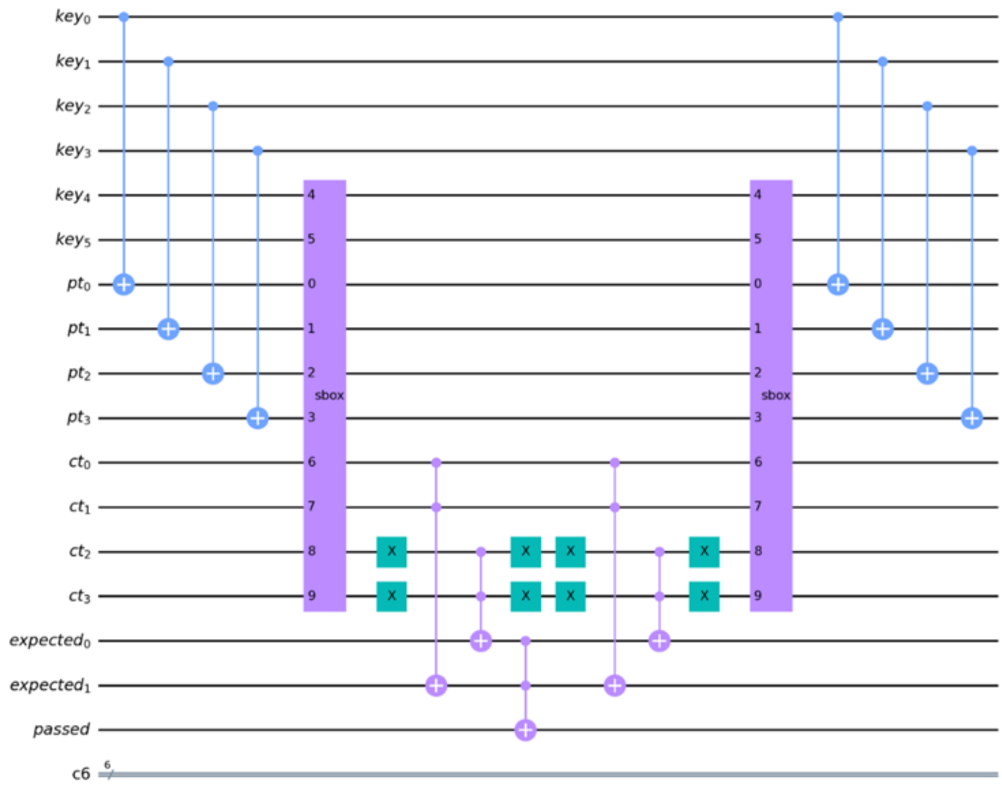


Figure 4: Oracle for Algorithm 3

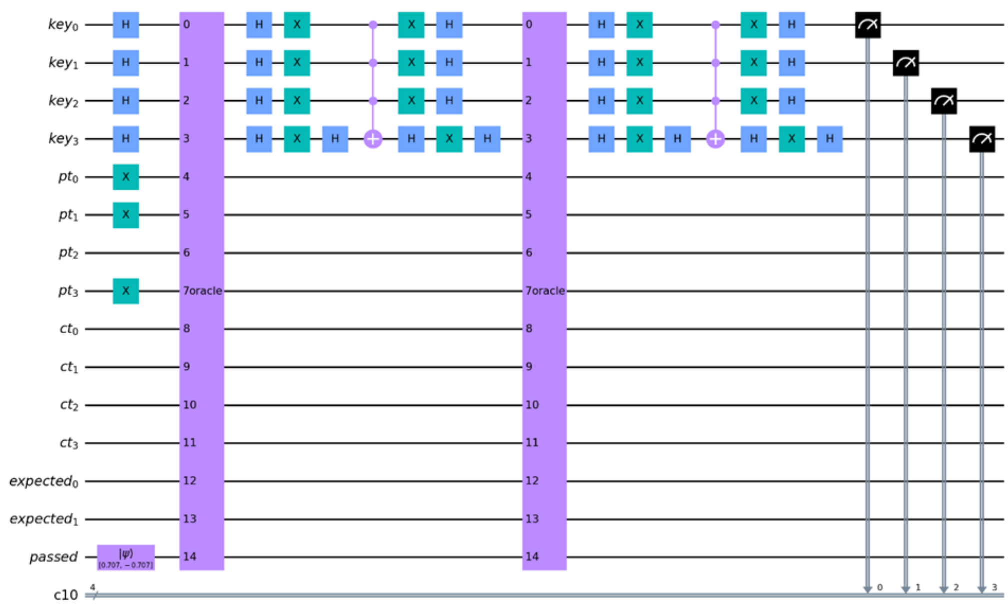


Figure 5: An example of Grover's algorithm that is looking through a 4x4 S-box to find what produces the plaintext 1101

6 Results

Table 7 lists 3 sets of randomly generated plaintext ciphertext pairs that were used to perform a known plaintext attack. Figures 6, 7, and 8 show the results of performing a known plaintext attack via Grover's algorithm on Algorithms 1, 2, and 3 respectively with the randomly generated plaintext 0110 and randomly generated ciphertext 0100. These tests were performed using Qiskit via IBMQ. These figures only depict the results of performing the attack on Set 1. The rest of the results of each of these attacks on 16x4 S-box algorithms can be seen in Appendix C. The results of a known plaintext attack on Algorithm 1 had an average of 932.146 out of 1024 shots being correct with a standard deviation of 8.636. Comparable results were present when performing this attack on Algorithm 2, having an average of 930.5 out of 1024 shots being correct with a standard deviation of 9.987. However, instead of finding only 1 valid key, it found 4. Such a result means that Algorithm 2 is unable to provide authentication.

Table 7: Randomly generated plaintext ciphertext pairs

Plaintext	Ciphertext
0000	0110
0011	1011
0110	0100

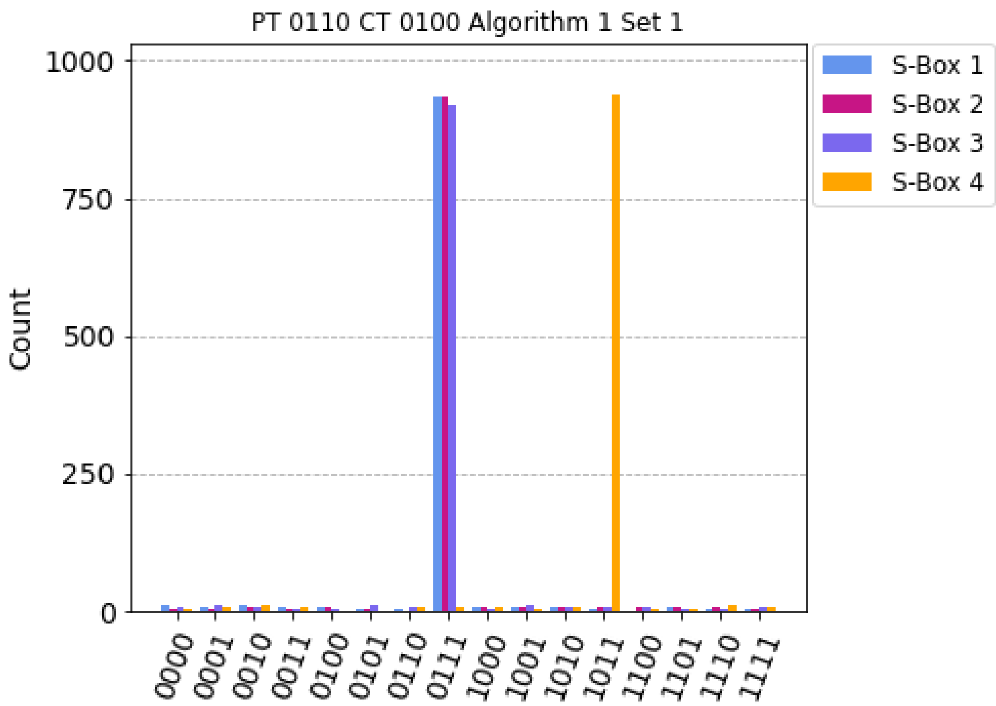


Figure 6: Results of performing a known plaintext via Grover's algorithm on Algorithm 1

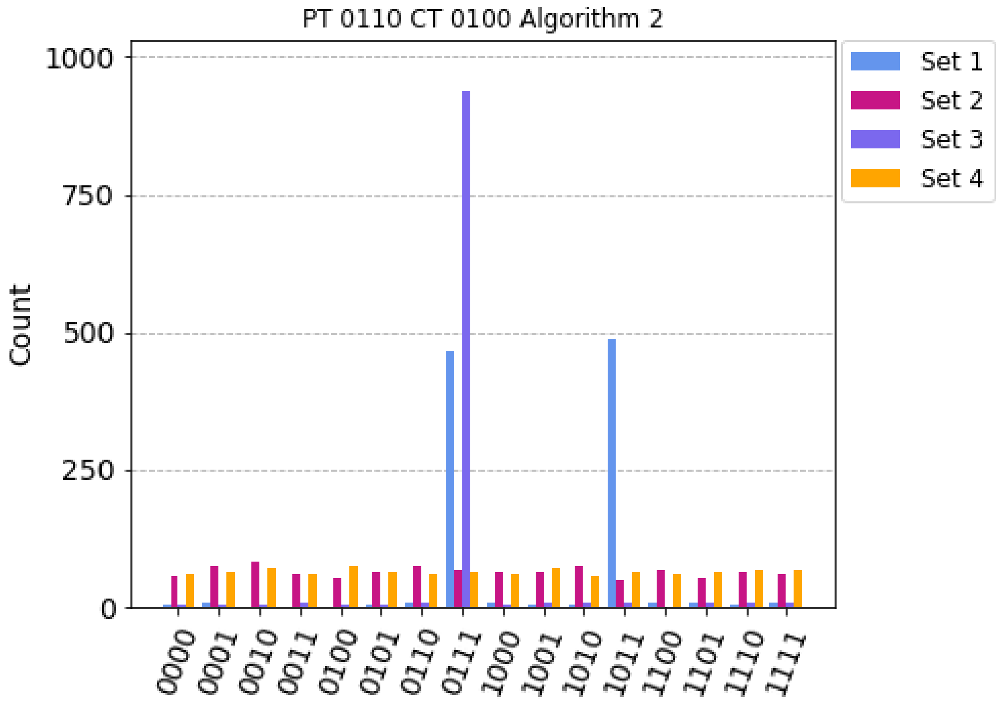


Figure 7: Results of performing a known plaintext via Grover's algorithm on Algorithm 2

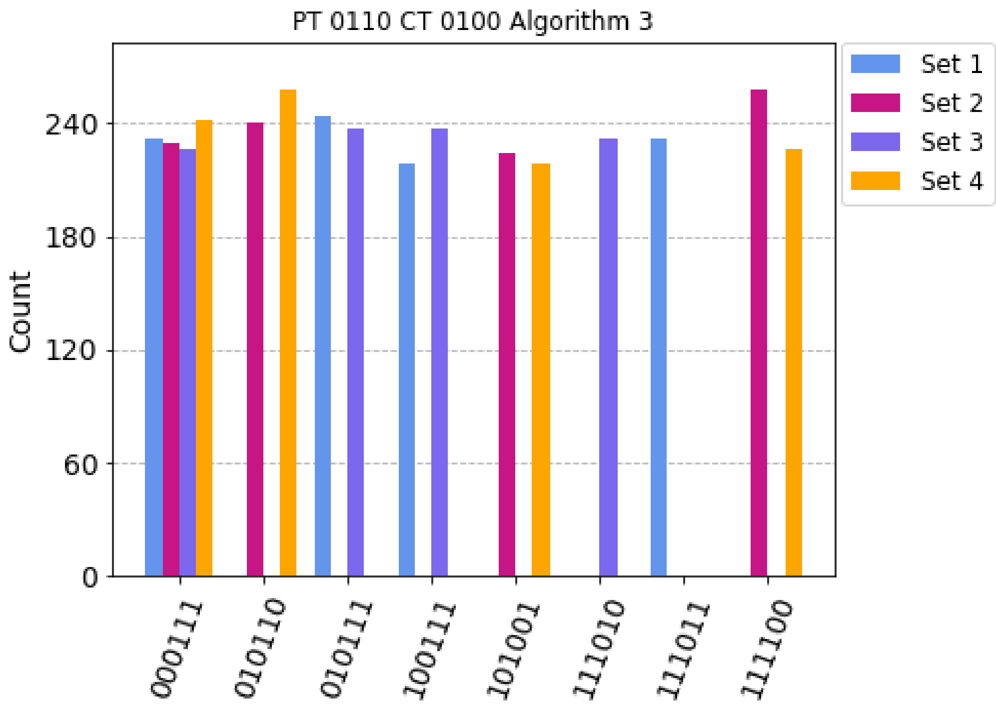


Figure 8: Results of performing a known plaintext via Grover's algorithm on Algorithm 3

6.1 Analyzing ALG 2

However, when Grover's algorithm was run on Algorithm 2, results were very inconsistent. Figure 7 best demonstrates this, as the attack only found a valid key when using the S-boxes in Set 1 and 3. Furthermore, Set 1 yielded two possible keys (0111 and 1011) while Set 3 only yielded one possible key (0111). Sets 2 and 4 did not find any valid keys because no keys exist that could produce the ciphertext 0100 from the plaintext 0110. Since the value that is XORed with the plaintext also decides which S-box to use, the plaintext will only be XORed with one of 4 values before being put through a specific S-box. Table 8 depicts what key values correlate to each S-box for any particular set.

XORing a plaintext before putting it through an S-box serves to create permutations that are computationally indistinguishable from a random permutation. To do this, a function must map each n-bit input to exactly one random n-bit output, with the input being the key XORed with a 4-bit plaintext block [23]. However, ALG 2 fails at doing this. Table 9 shows the output of Algorithm 2 using Set 1 for any given key and a plaintext of 0x0. One can see that a ciphertext of 0x4, 0x7, and 0xD are produced multiple times, while a ciphertext of 0x0, 0x5, and 0xC are never produced. As such, it fails at providing a computationally random permutation.

Table 8: Keys applicable to nth S-box in Algorithm 2

S-Box	Key			
S-Box 1	0 (0000)	2 (0010)	4 (0100)	6 (0100)
S-Box 2	1 (0001)	3 (0011)	5 (0101)	7 (0111)
S-Box 3	8 (1000)	A (1010)	C (1100)	E (1110)
S-Box 4	9 (1001)	B (1011)	D (1101)	F (1111)

Table 9: Output of Algorithm 2 when using Set 1 for any given key and a plaintext of 0x0

	S-Box 1				S-Box 2				S-Box 3				S-Box 4			
Key	0	2	4	6	1	3	5	7	8	A	C	E	9	B	D	F
CT	9	A	D	8	4	7	6	B	E	F	D	1	7	3	4	2

6.2 Analyzing Algorithm 3

In contrast, Algorithm 3 supplies a computationally random permutation since each n-bit plaintext input has an equally likely chance of being mapped to any other n-bit ciphertext. However, each ciphertext generated has 4 possible keys that could be used to decrypt it. Ideally, given a key size of n-bits, an attacker should have a $\frac{1}{2^n}$ chance of guessing the correct key. However, when Algorithm 3 is implemented, an attacker has a $\frac{4}{2^4}$ or $\frac{1}{16}$ probability of guessing the key instead of a $\frac{1}{2^8}$ or $\frac{1}{64}$ chance of guessing the key. While this does not provide ideal security, it provides the same amount of security as Algorithm 1, as an attacker would also have a $\frac{1}{16}$ chance of guessing the correct key.

It is because of this that Grover's algorithm must run the same number of times for all three algorithms evaluated. As such, the only benefit that Algorithm 3 provides is an increased cost of the oracle used to perform Grover's algorithm. As depicted in Tables 3 and 4, if Algorithm 3 was ran using Set 4, the S-box subcircuit would require 127 gates. Whereas if Algorithm 1 was ran using S-box 3 of Set 4, the S-box subcircuit would only require 24 gates.

Since each oracle subcircuit applies two S-box subcircuits, and since the oracle had to be run twice, this meant that the S-box subcircuit had to be run a total of 4 times for each known plaintext attack performed. Therefore, given the scenario outlined above, Algorithm 3 would require 412 more gates in total than Algorithm 1. In addition to this, Algorithm 3 requires 2 more qubits to perform a known plaintext attack than an attack performed on Algorithm 1. However, this increase in gates and qubits can be circumvented by just testing on a single specific S-box, i.e., by using Algorithm 1.

7 Implementation in S-AES

It might be possible to overcome the security holes present in Algorithms 2 and 3 by implementing them in the full S-AES algorithm. To do this for Algorithm 2, the S-AES algorithm was largely unmodified. The key expansion algorithm was left unchanged, using the first S-box from the set to perform the key expansion. The only step that was changed was the substitution step, wherein the previous round key was used to determine which S-box to use (i.e., W_0W_1 was used in round 1 and W_2W_3 was used in round 2 to determine which S-box to use). Figure 9 depicts this process. The high and low bits of K_0 are used to determine which S-box to use on Block 1, while the high and low bits of K_1 are used to determine which S-box to use on Block 0. This implementation will be referred to as ALG 2. It serves to perform a version of S-AES that uses a 16x4 S-box without increasing the key size.

7.1 Implementing Algorithm 3 in S-AES

Implementing Algorithm 3 in S-AES required a lot more changes to S-AES. The first thing that had to be modified was the key expansion algorithm. Key expansion in S-AES operates by breaking the 16-bit key into 4 4-bit nibbles (K_0 through K_3) that are then used to form 6 8-bit words (W_0 through W_5). These nibbles are then rotated and put through a S-box before adding the round constant g. The first round of this process is depicted in Figure 10.

To implement Algorithm 3, the key size needed to be increased to 24 bits, with these additional bits forming the nibbles K_4 and K_5. K_4 and K_5 are then used to form α_0, which determines which S-box to apply on each plaintext nibble in round 1. Before performing the key expansion, $K_0(\kappa_0\kappa_1)$ and $K_2(\kappa_2\kappa_3)$ are swapped with K_4 and K_5 to form α'_0. $\kappa_0\kappa_1$ are then used to determine which S-box to use on W_1.

α'_0 is then expanded using a process that mirrors the original key expansion algorithm used by S-AES. 2 2-bit words (ω) are formed from α'_0, with ω_0 being formed from $\kappa_0\kappa_1$ and ω_1 being formed from the rotated $\kappa_3\kappa_2$. The substitution step is skipped and ω_1 is XORed with the constant ρ (0b1000) before being XORed with ω_0 to form ω_2. ω_2 is then XORed with ω_1 to form ω_3, with $\omega_2\omega_3$ forming α_1. α_1 is then used to determine which S-box to use on each plaintext nibble in round 2. Figure 11 depicts this process.

To calculate W_5W_6, this process, excluding the key expansion of α_1, is repeated. This implementation is referred to as ALG 3 Double Swap. Another implementation was tested that did not swap K_4K_5 with K_0K_2 when calculating W_5W_6, with this implementation being referred to as ALG 3 Single Swap.

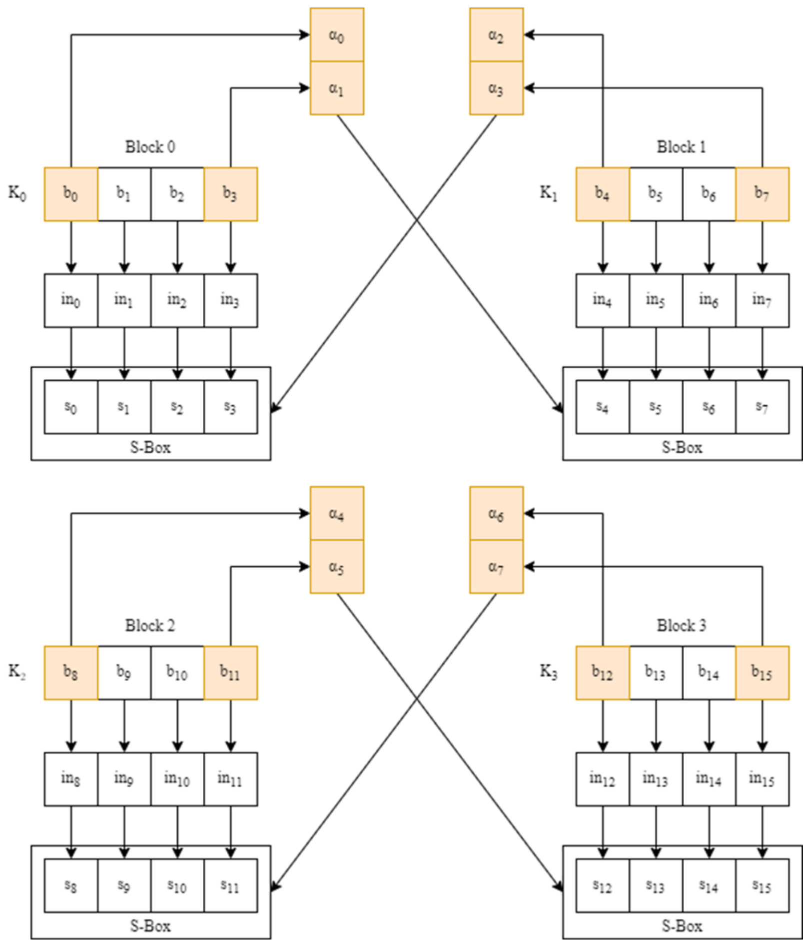


Figure 9: ALG 2

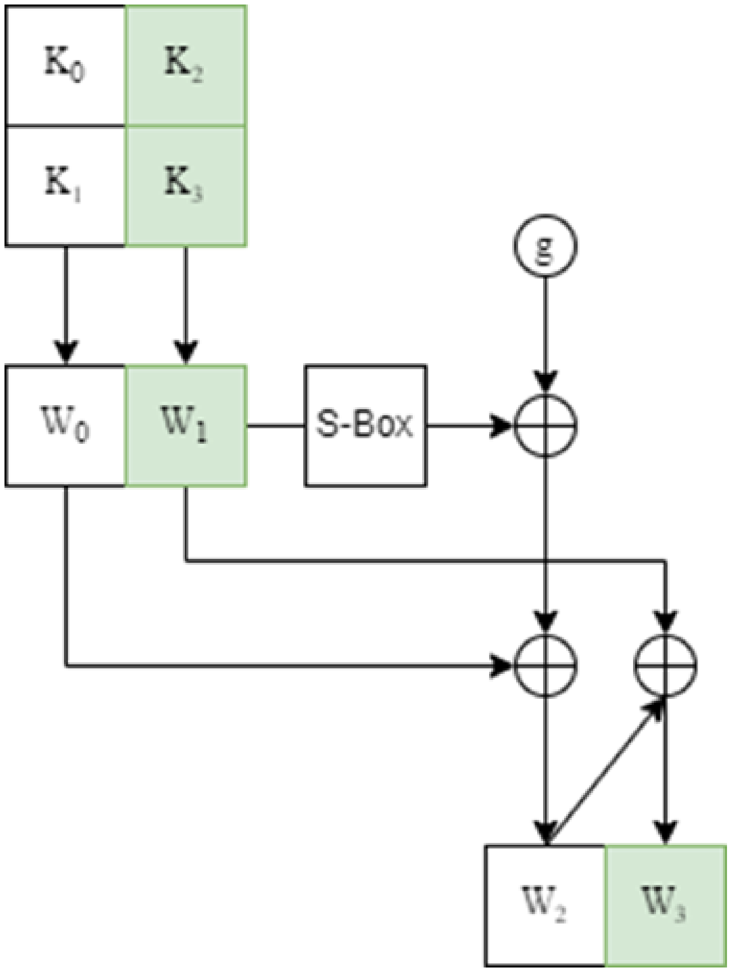


Figure 10: S-AES key expansion algorithm

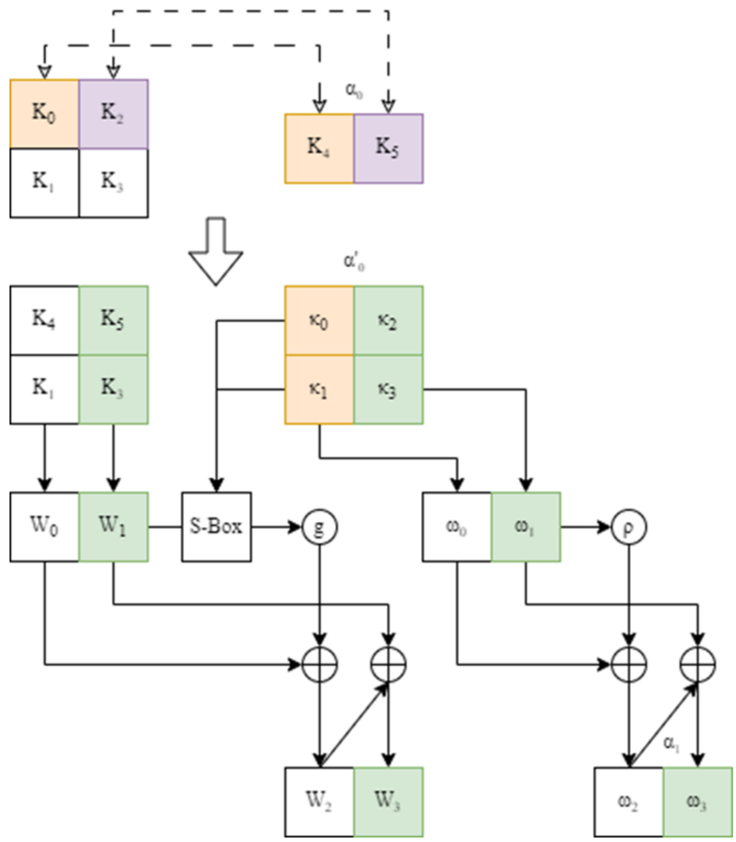


Figure 11: ALG 3

8 Analyzing Full S-AES Implementations of ALG 2 and 3

Running Grover's algorithm on these modified versions of S-AES was too resource intensive. As such, every possible key was used on 3 randomly generated plaintexts (as well as the plaintext 0x0000) to determine how many keys generated the same ciphertext given a specific plaintext. When doing this, the S-box S-AES used was always set to the first S-box of the set being tested. This was done to see how resistant each implementation was to a known plaintext attack of an unmodified version of S-AES that uses the first S-box of a 16x4 S-box.

The average results of performing this test on each set is depicted in Figures 12 and 13. Table 10 provides the average minimum, maximum, mean, median, variance, and standard deviation of these tests.

The distribution of keys that correlated to identical outputs is statistically identical between S-AES and ALG 2. They were also statistically identical between ALG 3 Double Swap and ALG 3 Single Swap. Roughly 36.76% of the possible 2^{16} 16-bit outputs (or around 24,094) could not be generated by S-AES or ALG 2. Another 36.85% of the possible outputs (or around 24,149) could only be generated with a single key. On average, each ciphertext produced by ALG 3 could be generated with 256 different keys. This is because a 24-bit key is being applied to a 16-bit plaintext block that will produce a 16-bit plaintext block.

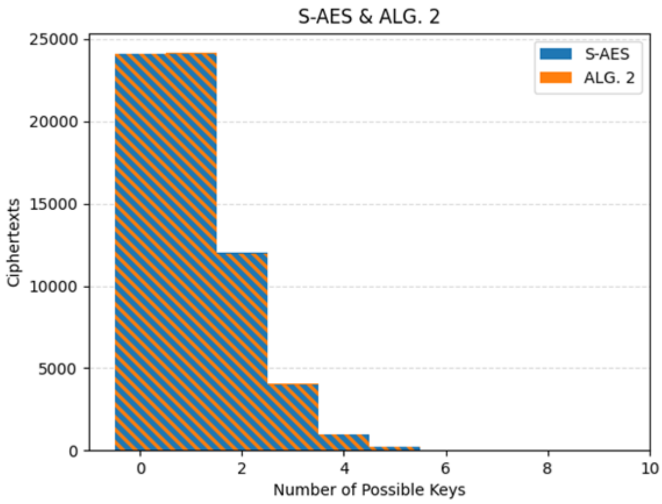


Figure 12: Key distribution of S-AES and ALG 2

8.1 Effectiveness of ALG 3 Double Swap & Alg 3 Single Swap

ALG 3 Double Swap and ALG 3 Single Swap were designed to prevent an attacker from being able to use any possible value for the additional 8 bits when attacking the algorithm. Five random ciphertexts that could be generated from the plaintext 0xD3AE with 256 possible keys were selected from ALG 3 Double Swap and ALG 3 Single Swap. Each key that could generate the ciphertext in question was then analyzed to see how many of the possible values for K_4K_5 generated said ciphertext. If all 2^8 of these values can be used, an attacker would be able to ignore these additional 8 bits.

Doing so revealed that ALG 3 Double Swap, on average, used 62.34% of the possible K_4K_5 values. Doing this on ALG 3 Single Swap had similar results, with it using an

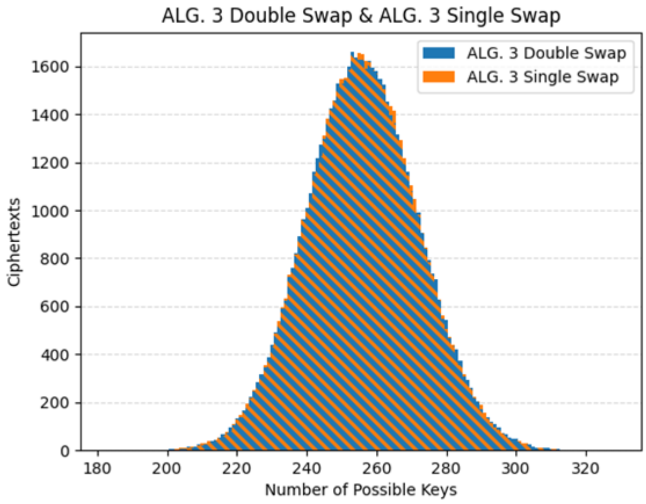


Figure 13: Key distribution of ALG 3 Double Swap and ALG 3 Single Swap

Table 10: Keys per ciphertext

	Average Minimum	Average Maximum	Average Mean	Average Median	Average Variance	Average Standard Deviation
S-AES	0	7.75	1	1	1	1
ALG 2	0	7.75	1	1	1	1
ALG 3 Double Swap	192.5	325.25	256	256	255.805	15.993
ALG 3 Single Swap	190	325	256	256	256.63	16.023

average of the 63.67% possible K_4K_5 values. This difference is most likely due to the small sample size. It is likely that repeating this test on all the ciphertexts that could be generated with 256 different keys would result in a near identical ratio between the two algorithms.

8.2 The Ability of S-AES, ALG 2, and ALG 3 to Provide Authentication

IoT devices are found in many settings such as the military, industrial, and healthcare fields. Many of these devices are required to provide confidentiality, integrity, and authentication of transmitted data. Authentication is provided using shared keys that transform a plaintext into a ciphertext, wherein the same key must be used to decrypt the ciphertext to a valid plaintext value [10]. This is especially true for IoT devices in the medical field, as the security of patient data is a top priority. Due to the various applications and benefits provided by IoT devices, the healthcare industry has been quick to adopt IoT devices [8].

Due to the distribution of keys, ALG 3 could never provide authentication. Since there will always be more keys than possible ciphertexts, there will always be more than one possible valid key that could be used to authenticate data. However, ALG 2 was equally as capable of providing authentication as S-AES was. This is because their key distributions were nearly identical.

To provide ideal authentication, each ciphertext should map to exactly one key given a specific plaintext. However, encryption algorithms can still provide authentication if they produce collisions such that it is difficult to find x values that compose of a key and plaintext that satisfy the equation $encryption(x_1) = encryption(x_n)$. This is best done with hashing algorithms but can still be performed through the use of encryption algorithms [9].

Due to the constraints of lightweight cryptographic algorithms (i.e., their limited computational costs and limited key space) any lightweight algorithm that has an x value that satisfies the above equation a collision in it would be easy to find. Seeing as there are only around 36.85% possible values of x that do not cause a collision in S-AES or ALG 2, both algorithms fail at providing adequate authentication. However, the lack of differentiation between the number of collisions amongst the two algorithms would imply that implementations of ALG 2 on algorithms such as AES would not impact their ability to provide authentication.

9 Statistical Analysis of These Implementations

One of the criteria that encryption algorithms must provide is their ability to act as random number generators [18]. NIST has provided a statistical test suite that can be used to analyze random number generators and cryptographic algorithms. It works under the null hypothesis that the sequence being analyzed is random. This test suite performs 15 tests that measure the randomness of an algorithm to produce a *P-value*. This is the probability that a test statistic will produce values that are equal to or worse than the test statistic value. A *P-value* of 1 indicates perfect randomness, while a *P-value* of 0 indicates that the sequence analyzed is completely non-random [1]. Information about each test can be seen in [1].

The implementations of ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap were analyzed using this test suite. In addition to this, versions of S-AES that used each S-box in each set of S-boxes were also analyzed. The algorithms generated 60 bitstreams of 100,000 bits each. This was done by generating 60 random 32-bit input values for the different versions of S-AES and ALG 2, as well as 60 random 40-bit input values for ALG 3 Double Swap and ALG 3 Single Swap. These values were then fed into their respective algorithms, being incremented by one until each bitstream had the necessary number of bits.

Appendix D lists the *P-value* associated with as well as the percentage of bitstreams that passed each test. Tables 11 lists the results for implementations of S-AES that use S-box 1 and 3 of Set 1. S-box 1 of Set 1 is the S-box that S-AES uses, and S-box 3 of Set 1 was the most expensive 4x4 S-box found. Table 12 lists the results of implementations of ALG 2, ALG 3 Single Swap, and ALG 3 Double Swap that use Set 4, as it composed the most expensive 16x4 handmade S-box.

9.1 Test Flaws

Fine tuning each test performed was infeasible, as 49 different algorithms ended up being tested. As such, several tests produced questionable results. This is most apparent in the various tests that had a *P-value* of 0 despite having a very high pass rate. Furthermore, only 3 Random Excursions and Random Excursions Variant tests could be performed on each algorithm. In addition to this, the only Discrete Fourier Transform (FFT) tests that did not result in a *P-value* of 0 were the ones ran on ALG 2. Finally, only one Muarer's "Universal Statistical" test could be performed on each algorithm tested.

Table 11: Statistical analysis results of S-AES using its default S-box (S-box 1 of Set 1) and the most quantum expensive 4x4 S-box found (S-box 3 of Set 1)

	S-Box 1		S-Box 3	
	P-val	Passed	P-val	Passed
Frequency	0	100%	0.299	100%
Block Frequency	0.178	93.33%	0.016	98.33%
Sums 1	0	100%	0.001	100%
Sums 2	0	100%	0.01	100%
Runs	0	100%	0.773	100%
Longest Run	0.324	98.33%	0.706	98.33%
Rank	0.437	100%	0.195	93.33%
FFT	0	16.66%	0	71.66%
Non-Overlapping	0.256	99.06%	0.247	98.96%
Overlapping	0.804	98.33%	0.195	98.33%
Universal	0.83	—	0.886	—
Entropy	0.407	100%	0.02	100%
Excursions	—	100%	—	96.87%
Excursion Variants	—	100%	—	93.05%
Serial 1	0.74	100%	0.148	100%
Serial 2	0.233	100%	0.773	100%
Linear Complexity	0.773	100%	0.054	100%
Average Pass Rate	94.0%		97.0%	
100% Pass Rate	11		10	

9.2 Analysis of Results

Apart from the Binary Matrix Rank and FFT tests, each algorithm passed each test more than 80% of the time. ALG 3 Double Swap and ALG 3 Single Swap tended to have low pass rates of the rank test, with ALG 3 Double Swap consistently having a significantly lower pass rate than ALG 3 Single Swap when performing this test. ALG 3 Double Swap also tended to have lower pass rates than ALG 3 Single Swap across every test performed, implying that ALG 3 Single Swap is more secure than ALG 3 Double Swap. Finally, the only algorithm that consistently passed every single test, including FFT, was ALG 2. Each test performed on this algorithm had a pass rate of 90% or more, implying that ALG 2 was the most classically secure algorithm tested.

The Binary Matrix Rank test is used to look for linear dependencies among fixed length substrings of a binary stream [1]. Failure of this test implies that the various values produced by an encryption algorithm are dependent on each other and are therefore not random. Such a dependence makes algorithms susceptible to linear cryptanalysis that can be used to perform key recovery attacks [14]. The FFT test is used to find repetitive patterns that are near each other [1]. These patterns can be exploited by cryptanalysts to recover the plaintext [3].

ALG 2 was also the algorithm that had the highest average pass rate of 99% of all tests performed passing when used in conjunction with Set 4. Despite this, the unmodified version of S-AES had the highest number of tests that had a 100% pass rate for each *P-value* generated, as 11 of the performed tests had a 100% pass rate. ALG 3 Double Swap using Set 4 performed the worst, having an average pass rate of 89% and with only 3 tests having a 100% pass rate.

Table 12: Statistical analysis results of implementations of ALG 2 and 3 using the most expensive handmade 16x4 S-box (Set 4)

	ALG 2		ALG 3 Double Swap		ALG 3 Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.378	98.33%	0.111	95.0%	0.195	100%
Block Frequency	0.001	98.33%	0.254	98.33%	0.233	98.33%
Sums 1	0.276	96.66%	0	91.66%	0.091	100%
Sums 2	0.888	100%	0	91.66%	0.025	100%
Runs	0.254	100%	0.834	98.33%	0.324	100%
Longest Run	0	96.66%	0.74	100%	0.067	98.33%
Rank	0.122	100%	0	58.33%	0.091	93.33%
FFT	0.804	96.66%	0	0.0%	0	71.66%
Non-Overlapping	0.303	98.99%	0.486	98.72%	0.498	98.96%
Overlapping	0.06	100%	0.135	98.33%	0.991	98.33%
Universal	0.461	—	0.713	—	0.621	—
Entropy	0.35	98.33%	0.028	98.33%	0.005	100%
Excursions	—	93.75%	—	98.61%	—	96.87%
Excursion Variants	—	100%	—	96.28%	—	93.05%
Serial 1	0.005	100%	0.534	100%	0.378	100%
Serial 2	0.834	100%	0.888	100%	0.437	100%
Linear Complexity	0.148	100%	0.35	95.0%	0.602	100%
Average Pass Rate	99.0%		89.0%		97.0%	
100% Pass Rate	8		3		8	

9.3 Avalanche Criterion

Another desirable property of encryption algorithms is their ability for small changes in an input to produce significant changes to the output. To achieve this effect, each output bit should have a 50% chance of changing when any individual bit of the input is flipped. This is known as the Strict Avalanche Criteria (SAC) [17]. While the SAC requires each bit to have an exactly 50% chance of changing, such a criterion is very hard to achieve, and it is more useful as a means of measuring a sample's divergence from the SAC. As such, algorithms are considered to meet the generalized SAC when each bit has a probability close to 50% of changing [12].

This was tested by generating 2,500 random plaintexts and keys for each implementation. Each bit in the input was then iterated through to measure the ciphertext produced when said bit was flipped. Furthermore, this test was also applied on a version of S-AES that used each S-box from each set of generated S-boxes. Table 13 lists the average chance that each bit had of changing, and Appendix E contains charts depicting the chance of each individual bit changing for each implementation tested.

Across all four sets analyzed, the bits when running ALG 2 ranged from having a 47.76% to a 51.14% chance of changing. Results were near identical with ALG 3 Double Swap and ALG 3 Single Swap, with bits ranging from having a 48.89% to 51.17% chance of changing. Similarly, each modified version of S-AES produced results that ranged from 48.35% to 53.21%.

Overall, each bit across all the algorithms tested in Table 13 ranged from having a 49.28% to a 50.63% average chance of changing when any given input bit is changed. As such, ALG 2, ALG 3 Double Swap, ALG 3 Single Swap, and each implementation of

S-AES tested met the generalized SAC.

Table 13: SAC test results of Sets 1 through 4

	Set 1						
	ALG 2	ALG 3 Double Swap	ALG 3 Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.65%	49.28%	49.98%	49.76%	50.52%	49.78%	49.87%
	Set 2						
	ALG 2	ALG 3 Double Swap	ALG 3 Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.60%	50.02%	50.04%	49.72%	50.02%	49.92%	50.23%
	Set 3						
	ALG 2	ALG 3 Double Swap	ALG 3 Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.83%	49.94%	49.93%	49.63%	50.55%	49.90%	50.01%
	Set 4						
	ALG 2	ALG 3 Double Swap	ALG 3 Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.65%	50.04%	49.87%	49.80%	49.89%	49.98%	50.63%

10 Analyzing Randomly Generated 16x4 S-Boxes

When analyzing the quantum cost of the ANF of the randomly generated 16x4 S-boxes, multiple S-boxes were found that were more expensive than the S-boxes analyzed in Sets 1 through 4. Table 6 lists the three most expensive randomly generated 16x4 S-boxes. The individual 4x4 S-boxes that produced the three most expensive 16x4 S-boxes were categorized into Sets 5 through 7, as depicted in Table 14. Table 15 depicts the cost of the quantum circuit for the ANF of each of these S-boxes. Appendix A lists the ANF of each of these S-boxes.

Table 14: Sets 5-7

	S-Box 1	S-Box 2	S-Box 3	S-Box 4
Set 5	CB91D538 E7A20F64	A217C653 4D8EBF09	D14A58BF 792C630E	58B214C7 90E6DFA3
Set 6	70812A3B 496DCEF5	89C62357 BA4ED01F	841CEAB7 3265DF09	0386F412 7B95ECAD
Set 7	6A543D18 EC27F09B	9ADC7F3E 502816B4	FC1BE056 8A423D79	309C7BA2 D8F4E651

Table 15: Quantum costs of Sets 5 through 7

	MCX Controls						Total
	0	1	2	3	4	5	Gates
Set 5							
S-Box 1	2	7	19	9	0	0	37
S-Box 2	2	9	11	8	0	0	30
S-Box 3	3	7	10	7	0	0	27
S-Box 4	2	9	7	8	0	0	26
16x4 S-Box	2	10	42	48	36	12	150
Set 6							
S-Box 1	3	11	18	8	0	0	40
S-Box 2	1	6	10	3	0	0	20
S-Box 3	1	9	10	8	0	0	28
S-Box 4	0	10	14	9	0	0	33
16x4 S-Box	3	19	38	44	37	8	149
Set 7							
S-Box 1	2	7	13	11	0	0	33
S-Box 2	2	8	10	11	0	0	31
S-Box 3	4	9	11	8	0	0	32
S-Box 4	2	8	15	6	0	0	31
16x4 S-Box	2	13	38	52	34	8	147

11 Statistical Analysis of Randomly Generated 16x4 S-Boxes

To see if Sets 5 through 7 also provided classical security, each of these S-boxes were analyzed using the NIST statistical test suite and tested to see if they met the generalized SAC. The same procedure used when analyzing Sets 1 through 4 was once again used on Sets 5 through 7. The NIST statistical test suite was ran on versions of S-AES that use S-box 1 of each set, ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap. These algorithms (as well as versions of S-AES that use each S-box in Sets 5 through 7) were then analyzed to measure the likelihood of each bit changing in accordance to a single bit flip in the input to measure their compliance with the SAC. Table 16 and Table 17 contains the results of performing the NIST statistical test suite on Set 5, and Table 18 contains the results for the SAC tests. Appendix D lists the results of running the NIST statistical test suite on each implementation tested, and Appendix E lists charts depicting the chance of each individual bit changing for each implementation tested.

11.1 Analysis of Statistical Tests

Table 19 depicts the results of running implementations of ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap using Set 5, the most expensive 16x4 S-box analyzed in terms of quantum gates. Table 20 depicts the algorithms that performed the best and worst when running statistical tests using Sets 5 through 7. These results were generated using ALG 2 and ALG 3 Double Swap respectively, with both algorithms using Set 6.

Despite requiring the most gates, implementations of ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap that used Set 5 tended to perform worse than implementations that used Sets 6 or 7. Using Set 6 in conjunction with ALG 3 Double Swap resulted in the worst performance with an average pass rate of 86% and only 3 *P-values* that had a

Table 16: Statistical analysis results of implementations of S-AES using each S-box from Set 5.

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.074	100%	0	100%	0.378	100%	0.534	100%
Block Frequency	0.001	100%	0	100%	0.602	100%	0	96.66%
Sums 1	0.001	100%	0	100%	0.233	100%	0.672	100%
Sums 2	0.018	100%	0	100%	0.637	100%	0.637	100%
Runs	0.039	100%	0.534	100%	0.672	100%	0.233	100%
Longest Run	0.501	100%	0.672	100%	0.233	100%	0.254	100%
Rank	0.407	98.33%	0.862	96.66%	0.706	100%	0.672	98.33%
FFT	0	16.66%	0	21.66%	0	30.0%	0	8.33%
Non-Overlapping	0.303	99.15%	0.333	99.03%	0.314	99.14%	0.305	98.86%
Overlapping	0.74	98.33%	0.95	98.33%	0.932	100%	0.911	98.33%
Universal	0.53	—	0.3	—	0.338	—	0.898	—
Entropy	0.025	100%	0.001	100%	0.035	100%	0.501	100%
Excursions	0.361	100%	0.016	97.36%	—	100%	—	100%
Excursion Variants	0.293	100%	0.009	99.7%	—	100%	—	100%
Serial 1	0.862	96.66%	0.213	100%	0.469	100%	0	100%
Serial 2	0.834	100%	0.195	100%	0.407	100%	0.862	100%
Linear Complexity	0.911	98.33%	0.991	98.33%	0.672	100%	0.602	98.33%
Average Pass Rate	94.21%		94.44%		95.57%		93.67%	
100% Pass Rate	10		9		14		10	

100% pass rate. In contrast, using Set 6 in conjunction with ALG 2 resulted in the best performance. These results had an average pass rate of 99%, with 11 *P-values* that had a 100% pass rate.

11.1.1 Analysis of S-Box 3 of Set 5

When the NIST statistical test suite was ran on implementations of S-AES that used S-boxes from Sets 5 through 7, there was a massive outlier when S-box 3 of Set 5 was tested. The results of this test are depicted in Table 21. This test produced 14 *P-values* that had a 100% pass rate. This was the highest number of *P-values* out of the 49 different algorithms tested. It also had an average *P-value* of 0.442, which is the 4th highest average *P-value*.

This could be due to a poor choice of parameters, or it could be due to an anomaly from the inputs fed into the algorithm. However, if it is not, this would imply that the S-box D14A58BF792C630E was the most classically secure 4x4 S-box tested. This is even though this S-box only required 27 gates to create its quantum oracle. The ANF of this S-box is listed below, and Figure 14 depicts what its quantum oracle would look like.

$$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_1 \oplus x_3$$
$$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_2 \oplus x_3$$
$$y_2 = x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2$$
$$y_3 = x_0x_1x_2 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$$

Table 17: Statistical analysis results of implementations of ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap using Set 5

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.254	100%	0.009	91.66%	0.706	100%
Block Frequency	0.568	100%	0	91.66%	0.031	100%
Sums 1	0.299	100%	0	90.0%	0.437	100%
Sums 2	0.01	100%	0	86.66%	0.299	100%
Runs	0.011	100%	0.122	95.0%	0.834	98.33%
Longest Run	0.035	100%	0.254	95.0%	0.195	98.33%
Rank	0.74	98.33%	0	28.33%	0	73.33%
FFT	0.009	90.0%	0	0.0%	0	45.0%
Non-Overlapping	0.303	98.94%	0.462	98.59%	0.462	98.91%
Overlapping	0.602	96.66%	0.672	100%	0.534	98.33%
Universal	0.79	—	0.021	—	0.956	—
Entropy	0.011	100%	0.834	100%	0.888	100%
Excursions	—	94.64%	—	98.42%	—	97.91%
Excursion Variants	—	98.41%	—	100%	—	99.07%
Serial 1	0.082	100%	0.407	96.66%	0.888	100%
Serial 2	0.74	100%	0.568	100%	0.602	100%
Linear Complexity	0.163	96.66%	0.568	98.33%	0.74	100%
Average Pass Rate	98.35%		85.64%		94.32%	
100% Pass Rate	9		4		8	

Table 18: SAC test results of Sets 5 through 7

	Set 5						
	ALG 2	Double Swap	Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.78%	49.86%	49.88%	50.19%	49.87%	49.94%	49.55%
	Set 6						
	ALG 2	Double Swap	Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.48%	50.06%	50.12%	50.07%	49.48%	50.36%	50.10%
	Set 7						
	ALG 2	Double Swap	Single Swap	S-AES (S-Box 1)	S-AES (S-Box 2)	S-AES (S-Box 3)	S-AES (S-Box 4)
Average	49.49%	49.48%	49.95%	49.83%	49.12%	50.26%	50.04%

11.2 Analysis of SAC Tests

While each bit had an average chance of changing that is close to 50% when using Sets 5 through 7, each individual bit did not have a near 50% chance of changing. This is best shown in Figure 15. When using S-AES with S-box 2 of Set 7, bits b_7 and b_{11} only had a 44.76% and 44.93% chance of changing respectively. This is the lowest probability that a single bit had of changing across all the tests performed on implementations of S-AES with different S-boxes. When using ALG 2 with Set 6, bit b_5 only has a 46.61% chance

Table 19: Statistical analysis results of ALG 2 and ALG 3 implementations using Set 5

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.254	100%	0.009	91.66%	0.706	100%
Block Frequency	0.568	100%	0	91.66%	0.031	100%
Sums 1	0.299	100%	0	90.0%	0.437	100%
Sums 2	0.01	100%	0	86.66%	0.299	100%
Runs	0.011	100%	0.122	95.0%	0.834	98.33%
Longest Run	0.035	100%	0.254	95.0%	0.195	98.33%
Rank	0.74	98.33%	0	28.33%	0	73.33%
FFT	0.009	90.0%	0	0.0%	0	45.0%
Non-Overlapping	0.303	98.94%	0.462	98.59%	0.462	98.91%
Overlapping	0.602	96.66%	0.672	100%	0.534	98.33%
Universal	0.79	—	0.021	—	0.956	—
Entropy	0.011	100%	0.834	100%	0.888	100%
Excursions	—	94.64%	—	98.42%	—	97.91%
Excursion Variants	—	98.41%	—	100%	—	99.07%
Serial 1	0.082	100%	0.407	96.66%	0.888	100%
Serial 2	0.74	100%	0.568	100%	0.602	100%
Linear Complexity	0.163	96.66%	0.568	98.33%	0.74	100%
Average Pass Rate	98.35%		85.64%		94.32%	
100% Pass Rate	9		4		8	

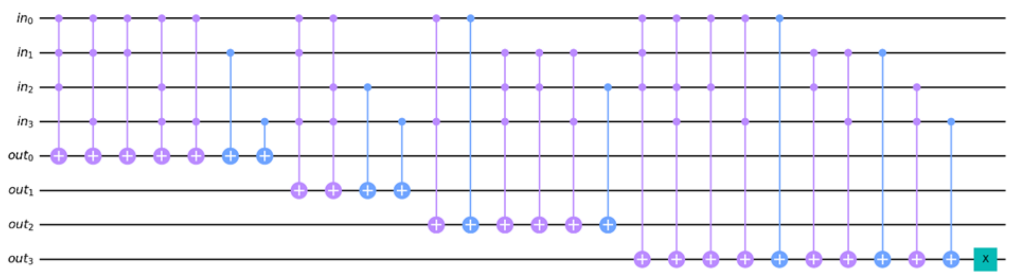


Figure 14: Quantum oracle of the ANF of S-box 3 of Set 5

of changing. This is the lowest probability that a single bit had of changing throughout all the tests performed on ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap. The individual bits that had the highest chance of changing are not of concern, as across all 49 different algorithms analyzed the highest chance any single bit had of changing was only 51.28% (specifically bit b_1 of ALG 2 when using Set 7).

S-box 2 of Set 7 performed the worst in this test, which is not surprising as it was a randomly generated S-box. Furthermore, this S-box had the lowest quantum cost out of all 28 4x4 S-boxes analyzed, with it only needing 20 quantum gates for a quantum circuit of its ANF.

Table 20: The best and worst performing algorithms across Sets 5 through 7, both of which are from Set 6

	ALG 2		Double Swap	
	P-val	Passed	P-val	Passed
Frequency	0.054	100%	0.378	96.66%
Block Frequency	0.672	100%	0	100%
Sums 1	0.031	100%	0.437	95.00%
Sums 2	0.007	96.66%	0.135	95.00%
Runs	0.706	100%	0.005	93.33%
Longest Run	0.049	98.33%	0.672	98.33%
Rank	0.082	100%	0	25.00%
FFT	0.122	100%	0	0.00%
Non-Overlapping	0.271	99.21%	0.522	98.79%
Overlapping	0.054	100%	0.637	100%
Universal	0.213	—	0.076	—
Entropy	0	96.66%	0.091	98.33%
Excursions	—	100%	—	100%
Excursion Variants	—	100%	—	93.05%
Serial 1	0.074	100%	0.568	95.00%
Serial 2	0.233	100%	0.932	96.66%
Linear Complexity	0.276	98.33%	0.932	98.33%
Average Pass Rate	99.0%		86.0%	
100% Pass Rate	11		3	

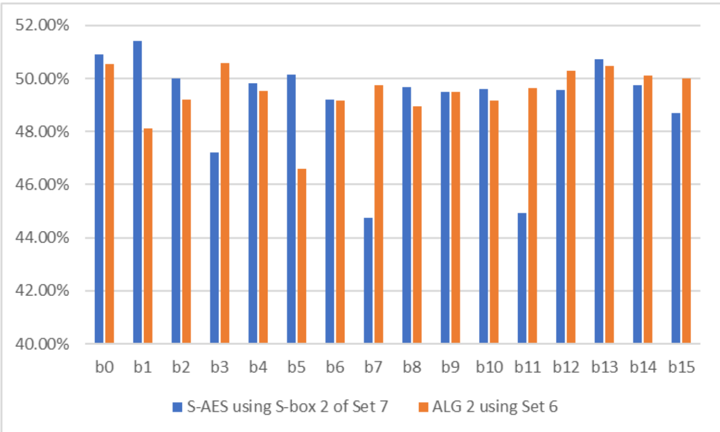


Figure 15: SAC test results of S-AES using S-box 2 of Set 7 and ALG 2 using Set 6

12 Overall Observations and the Correlation Between Quantum and Classical Security

Table 22 lists the range of average pass rates amongst the different implementations of S-AES, ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap. Based on these results, it is clear that ALG 2 performed better than any of the other algorithms tested.

The most quantum secure 4x4 S-box found (S-box 3 of Set 1, or 946C753AE8FBD012) only had an average pass rate of 94%. The 4x4 S-box that produced the highest average pass rate, S-box 4 of Set 4, or 18BDA673CF49205E, was also the 4x4 S-box that had the

Table 21: Statistical analysis results of an implementation of S-AES using S-box 3 of Set 5 (D14A58BF792C630E)

	P-val	Passed
Frequency	0.378	100%
Block Frequency	0.602	100%
Sums 1	0.233	100%
Sums 2	0.637	100%
Runs	0.672	100%
Longest Run	0.233	100%
Rank	0.706	100%
FFT	0	30.00%
Non-Overlapping	0.314	99.14%
Overlapping	0.932	100%
Universal	0.338	—
Entropy	0.035	100%
Excursions	—	100%
Excursion Variants	—	100%
Serial 1	0.469	100%
Serial 2	0.407	100%
Linear Complexity	0.672	100%
Average Pass Rate	96.0%	
100% Pass Rate	14	

highest FFT pass rate of 80%. This is abnormally high, as the average FFT pass rate of S-AES was only 25.35%. S-box 3 of Set 5, or D14A58BF792C630E, had the highest number of *P-values* with a 100% pass rate. As such, these two 4x4 S-boxes were some of the most secure 4x4 S-boxes analyzed. This is even though they only required 27 to 31 gates to model their ANF. The 4x4 S-box that required the most quantum gates to model its ANF, S-box 3 of Set 1 (or 946C753AE8FBD012) only had an average pass rate of 94%.

Table 22: Range of average pass rates for each implementation of each algorithm tested

Algorithm	Range of Average Pass Rates
S-AES	93 – 97%
ALG 2	98 – 99%
ALG 3 Single Swap	94 – 97%
ALG 3 Double Swap	86 – 89%

The most quantum secure 16x4 S-box, or Set 5, had one of the worst performances when ran through the NIST statistical test suite when implemented in ALG 2. It was the only 16x4 S-box that had an average pass rate of 98%, as all the other 16x4 S-boxes had an average pass rate of 99% when implemented in ALG 2. Furthermore, Set 5 produced the worst results when implemented in ALG 3 Single Swap, but one of the best results when implemented in ALG 3 Double Swap.

This implies a lack of correlation between quantum security and classical security, i.e., better quantum security does not necessarily equate to better classical security. This is further supported by what happened to the Supersingular Isogeny Key Encapsulation (SIKE) algorithm. This was an algorithm that was believed to be quantum secure but was cracked in about an hour using a nine-year-old Intel Xeon process [11].

13 Analysis of n-Length S-Boxes

13.1 Analysis of 2^nx4 S-Boxes

To see how increasing the number of 4x4 S-boxes used to construct variably assigned S-boxes impacts the quantum security of an algorithm, S-boxes with the dimensions 2^nx4 were tested to see how increasing n impacted the quantum security of said S-box. Doing so enabled the analysis of S-boxes with dimensions ranging from 4x4 ($n = 2$) to 1024x4 ($n = 10$). Each S-box required $n - 2$ bits to determine which 4x4 S-box to use. Figure 16 depicts the average number of gates needed to model each 2^nx4 S-box and Figure 17 depicts the number of 4x4 S-boxes are needed to construct each 2^nx4 S-box.

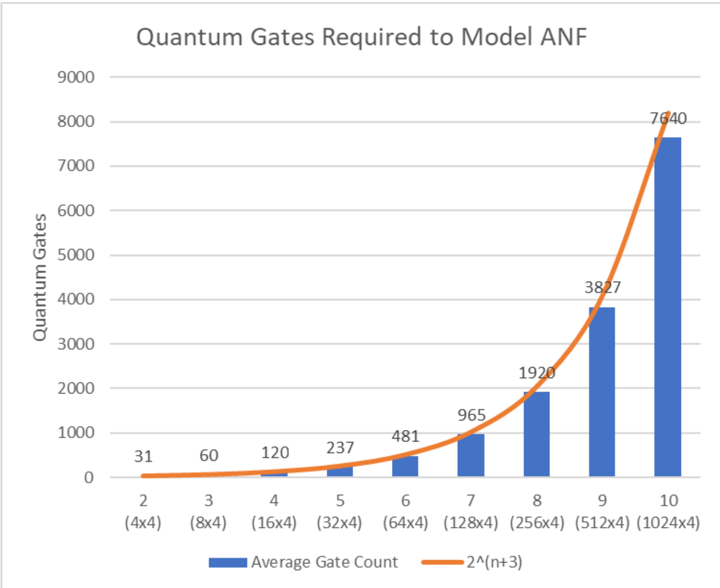


Figure 16: Number of gates needed to model the ANF of a 2^nx4 S-box

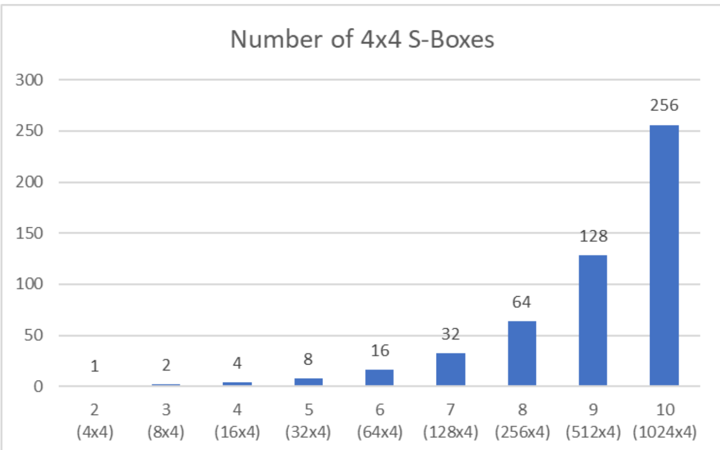


Figure 17: Number of 4x4 S-boxes required for a 2^nx4 S-box

As n increased, both the number of S-boxes and the number of gates required increased at an exponential rate, while the number of additional bits needed increased at a linear rate. The average number of necessary gates increased at a rate of approximately 2^{n+3}, while the number of necessary S-boxes increased at a rate of 2^{n-2}.

A regular 4x4 S-box maps a single input to one of 16 (N) values. As such, a classical device will need to perform an average of 8, or $N/2$, searches each time it runs something through an S-box during the encryption or decryption process. The value of N in a variably assigned S-box is equal to 2^{n+2}. Therefore, the average number of searches a classical device will need to make when performing said S-box will be 2^{n+1}.

13.2 Analysis of 2^nx8 S-Boxes

AES uses an 8x8 S-box. As such, this test was repeated on 2^nx8 S-boxes. This was performed on 3 randomly generated S-boxes. The results of doing so are depicted in Figure 18. Due to computational costs, only 3 different values of n could be analyzed. Similar to 2^nx4 S-boxes, the number of gates required to model the ANF of an 2^nx8 S-box also increased at an exponential rate. This rate of increase was approximately equal to 2^{n+7}.

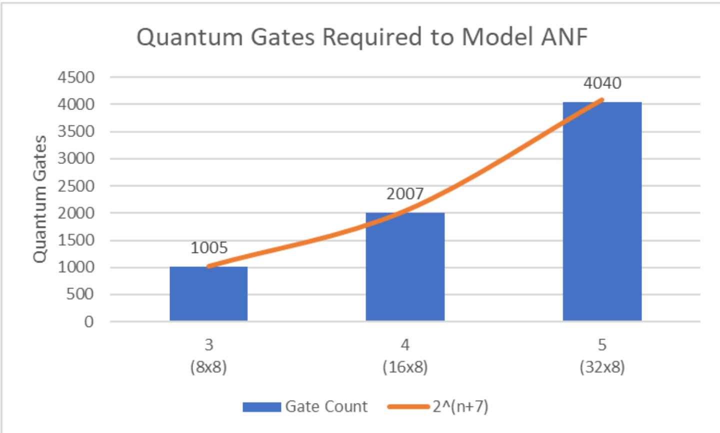


Figure 18: Number of gates needed to model the ANF of 2^nx8 S-boxes

13.2.1 AES S-Box Implications

The ANF of AES' S-box is depicted in Appendix F, and the necessary gates required to model said S-box's ANF in a quantum environment is depicted in Table 23. Based on this, the S-box that AES uses requires slightly less than 1024 gates, which is the expected average number of gates necessary to model an 8x8 S-box. This implies that there is a more quantum secure 8x8 S-box that AES could use.

14 Conclusion

Throughout this paper, an alteration to S-AES was tested that provided better classical and better quantum security. This algorithm, ALG 2, used a 16x4 S-box instead of a 4x4 S-box, using bits in the key to determine which S-box to use. While ALG 2 provided better classical and quantum security, quantum security does not necessarily result in classical security. This was demonstrated by how the most quantum secure 4x4 S-box (946C753AE8FBD012), as well as the most quantum secure 16x4 S-boxes tended to result in comparatively poor performances when analyzed with the NIST statistical test suite. The

Table 23: MCX gates needed to model the ANF of AES' S-box

MCX Controls	Amount
0	4
1	35
2	97
3	245
4	268
5	236
6	107
7	25
Total Gates	1017

two S-boxes that displayed the best classical security were the S-boxes 18BDA673CF49205E and D14A58BF792C630E. These S-boxes required 31 and 27 gates respectively to model their ANF in a quantum environment. Both values are less than the expected average of 32 gates needed to model a 4x4 S-box.

When trying to optimize the quantum security of an S-box, it is important to select the S-box whose ANF requires the most XOR operations. Doing so will maximize the cost necessary to run Grover's algorithm on said S-box. This suggests that an S-box that uses the prime polynomial $x^4 + x^3 + x^2 + x + 1$ (specifically the S-box 946C753AE8FBD012) is more quantum secure than the prime polynomial that S-AES currently uses ($x^4 + x + 1$). This is because an ANF implementation of said S-box requires 41 quantum gates, whereas an ANF implementation of the S-box that S-AES uses only requires 35 quantum gates. While this is only a minor increase in security, it could be very beneficial in protecting ephemeral data with a short lifespan. This is especially true of lightweight cryptography, wherein security is compromised to allow devices with limited resources to provide partial protection to data [2].

It was also demonstrated that the number of gates needed to model the ANF of variably assigned S-boxes increases at an exponential rate, as does the number of searches that need to be performed during the encryption and decryption process. Specifically, the rate of increase in the number of required quantum gates to model a 2^nx4 S-box increases at a rate approximately equal to 2^{n+3} while the number of required quantum gates to model a 2^nx8 S-box increases at a rate approximately equal to 2^{n+7}. This implies that AES could use a more quantum secure S-box, as the S-box that it currently uses only requires 1017 gates to model instead of the expected 1024 gates. However, the methods used to construct the quantum circuits for the S-boxes analyzed throughout this paper could be greatly improved. Tools such as LIGHTER-R can generate quantum circuits of S-boxes that do not require additional qubits and use fewer gates. It does this by generating a reversible ANF [6]. As such, this expected rate of growth in quantum cost could probably be significantly reduced.

When designing these larger S-boxes, it is important to analyze the ANF of the S-box as a whole instead of the ANF of each individual 4x4 S-box composing said larger S-box. Furthermore, reducing the collisions between an S-box and the plaintext or amongst the other S-boxes in a 16x4 S-box does not increase the quantum security of said S-box. The most quantum secure 16x4 S-box was found to be the randomly generated S-box CB91D538E7A20F64A217C6534D8EBF09D14A58BF792C630E58B214C790E6DFA3, requiring a total of 150 quantum gates to model. Since 16x4 S-boxes have an n value of 4, they are expected to require an average of 128 quantum gates to model in a quantum environment. As such, this randomly generated 16x4 S-box is in the upper bounds of the possible 16x4 S-boxes. Despite this, there could be an even more secure 16x4 S-box, as this S-box was found from a small sample size of only 800 randomly generated 16x4 S-boxes.

15 Further Work

15.1 Improved Quantum Circuit Construction

While the ANF of an S-box was used to generate their respective quantum circuit, there are alternative and more efficient methods of doing so. Tools such as LIGHTER use a graph-based meet-in-the-middle approach to calculate the smallest implementation needed to implement an S-box. It then computes good implementations of the smaller functions to reduce the time and memory requirements of said implementation [7]. This approach has been built on through LIGHTER-R, which uses this approach to generate reversible ANF representations that do not need extra qubits and require fewer gates [6]. The S-boxes assessed throughout this paper should be analyzed to see if the strengths and weaknesses discovered still hold true when using this alternate approach. This alternate approach should also be analyzed to see how it impacts the rate of growth of the number of required gates needed to model 2^nx4 and 2^nx8 S-boxes in a quantum environment.

15.2 Improved & Alternate ALG 2 Implementations

It might be possible to further increase the quantum security of ALG 2 by using the 16x4 S-box in the key expansion algorithm. Alternatively, instead of just using the first 4x4 S-box in ALG 2's 16x4 S-box, one could use the most expensive 4x4 S-box that composes said S-box. Doing so should increase its quantum security without increasing the cost associated with performing encryption and decryption. Finally, an implementation of ALG 2 on AES should be tested. Since S-AES and AES share the same structure, this should require minimal alterations to ALG 2.

15.3 Analysis of Algorithms in a Quantum Environment

The full S-AES, ALG 2, ALG 3 Double Swap, and ALG 3 Single Swap algorithms could not be implemented in a quantum environment due to computational and time constraints. Further analysis of the ALG 3 implementations is probably unnecessary as ALG 2 outperformed said algorithm and ALG 3 provided lackluster classical security. However, analyzing S-AES and ALG 2 in a quantum environment still holds merit and should be further investigated.

A ANF of Each Set and Their Corresponding 4x4 S-Boxes

Algebraic Normal Form of 4x4 S-Boxes

Set 1 S-Box 1 (94ABD1856203CEF7)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 1 S-Box 2 (940756EBFD1C2A83)

$y_0 = x_0x_1x_3 \oplus x_0x_3 \oplus x_0 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus 1$
$y_1 = x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_3$

$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus 1$

Set 1 S-Box 3 (946C753AE8FBD012)

$y_0 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$
$y_1 = x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus 1$

Set 1 S-Box 4 (9E518BDA67F3C402)

$y_0 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3$
$y_3 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 2 S-Box 1 (94ABD1856203CEF7)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 2 S-Box 2 (940756EBFD1C2A83)

$y_0 = x_0x_1x_3 \oplus x_0x_3 \oplus x_0 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus 1$
$y_1 = x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus 1$

Set 2 S-Box 3 (946C753AE8FBD012)

$y_0 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$
$y_1 = x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus 1$

Set 2 S-Box 4 (9E518BDA67F3C402)

$y_0 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3$
$y_3 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 3 S-Box 1 (94ABD1856203ECF7)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 3 S-Box 2 (940756EBFD1C2A83)

$y_0 = x_0x_1x_3 \oplus x_0x_3 \oplus x_0 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus 1$
$y_1 = x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus 1$

Set 3 S-Box 3 (946C735AE8FDB012)

$y_0 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus 1$

Set 3 S-Box 4 (9E518BDA67F34C02)

$y_0 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3$
$y_3 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_3 \oplus 1$

Set 4 S-Box 1 (94ABD1856203ECF7)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 4 S-Box 2 (40756EBFD1C2A839)

$y_0 = x_1 \oplus x_2x_3 \oplus x_3$
$y_1 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2$
$y_2 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus 1$
$y_3 = x_0x_1x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2 \oplus x_3$

Set 4 S-Box 3 (6C573AE8FBD01294)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_1 = x_0x_1x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus 1$
$y_2 = x_0x_1x_2 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_2 \oplus 1$
$y_3 = x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_2x_3 \oplus x_3$

Set 4 S-Box 4 (18BDA673CF49205E)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_3$
$y_3 = x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3$

Set 5 S-Box 1 (CB91D538E7A20F64)

$y_0 = x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2$
$y_1 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_2x_3 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1 \oplus x_2x_3 \oplus 1$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus 1$

Set 5 S-Box 2 (A217C6534D8EBF09)

$y_0 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3$
$y_1 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$
$y_2 = x_0x_1 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 5 S-Box 3 (D14A58BF792C630E)

$y_0 = x_0x_1x_2 \oplus x_0x_2 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_1x_2 \oplus x_3$
$y_2 = x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus 1$
$y_3 = x_0x_1x_2 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$

Set 5 S-Box 4 (58B214C790E6DFA3)

$y_0 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1$
$y_2 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$
$y_3 = x_0x_1x_2 \oplus x_0x_2 \oplus x_0 \oplus x_1x_3 \oplus x_1 \oplus x_3$

Set 6 S-Box 1 (70812A3B496DCEF5)

$y_0 = x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_3 \oplus 1$
$y_2 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_2 \oplus 1$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3$

Set 6 S-Box 2 (89C62357BA4ED01F)

$y_0 = x_0x_1 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_3$
$y_1 = x_0x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_3$
$y_2 = x_0x_2x_3 \oplus x_1 \oplus x_2x_3$
$y_3 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus 1$

Set 6 S-Box 3 (841CEAB73265DF09)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_1 \oplus x_3$
$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_2 \oplus x_3$
$y_2 = x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2$
$y_3 = x_0x_1x_2 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$

Set 6 S-Box 4 (0386F4127B95ECAD)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0 \oplus x_2 \oplus x_3$
$y_1 = x_0x_2x_3 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1 \oplus x_2$

Set 7 S-Box 1 (6A543D18EC27F09B)

$y_0 = x_0x_1 \oplus x_0x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2$
$y_1 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus 1$
$y_2 = x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_0 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus 1$
$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_3$

Set 7 S-Box 2 (9ADC7F3E502816B4)

$y_0 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_1x_2x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$

Set 7 S-Box 3 (FC1BE0568A423D79)

$y_0 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_2 \oplus x_3 \oplus 1$
$y_1 = x_0 \oplus x_1x_3 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$
$y_2 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_3 \oplus 1$
$y_3 = x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_2 \oplus x_1x_2x_3 \oplus x_1 \oplus x_2x_3 \oplus 1$

Set 7 S-Box 4 (309C7BA2D8F4E651)

$y_0 = x_0x_2 \oplus x_0 \oplus x_1x_2 \oplus x_2x_3 \oplus 1$
$y_1 = x_0x_1x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1 \oplus x_2x_3 \oplus x_3 \oplus 1$
$y_2 = x_0x_1 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2 \oplus x_3$
$y_3 = x_0x_1x_3 \oplus x_0x_2 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_3$

Algebraic Normal Form of 16x4 S-Boxes

Set 1

$y_0 = x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_3x_4 \oplus x_3 \oplus 1$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4 \oplus x_1 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_5 \oplus x_3$

$y_2 = x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_4 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2 \oplus x_3$

$y_3 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3 \oplus 1$

Set 2

$y_0 = x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_3x_4 \oplus x_3 \oplus 1$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4 \oplus x_1 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_5 \oplus x_3$

$y_2 = x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_4 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2 \oplus x_3$

$y_3 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3 \oplus 1$

Set 3

$y_0 = x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_3x_4 \oplus x_3 \oplus 1$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_5 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4 \oplus x_1 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_2x_5 \oplus x_3$

$y_2 = x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_4 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_3x_4 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2 \oplus x_3$

$y_3 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3 \oplus 1$

Set 4

$y_0 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_3x_4 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_5 \oplus x_3 \oplus x_4 \oplus x_5 \oplus 1$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_5 \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_0x_5 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_5 \oplus x_2x_4 \oplus x_3x_4x_5 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3 \oplus x_4x_5 \oplus x_5$

$y_2 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_5 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3 \oplus x_4 \oplus x_5$

$y_3 = x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_3 \oplus x_4x_5 \oplus x_4 \oplus x_5 \oplus 1$

Set 5

$y_0 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus$

$x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2 \oplus x_5$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_4 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4 \oplus x_1x_4 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_3x_4x_5 \oplus x_3 \oplus x_4x_5 \oplus x_4$

$y_2 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4x_5 \oplus x_4 \oplus 1$

$y_3 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0x_5 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3x_4x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_5 \oplus x_3x_4x_5 \oplus x_3x_4 \oplus x_3x_5 \oplus x_4x_5 \oplus 1$

Set 6

$y_0 = x_0x_1x_2x_5 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2 \oplus x_3 \oplus x_4x_5 \oplus x_4 \oplus x_5 \oplus 1$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_5 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3 \oplus x_4x_5 \oplus x_4 \oplus x_5 \oplus 1$

$y_2 = x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_5 \oplus x_0x_4 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4 \oplus x_1x_3 \oplus x_1x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_2 \oplus x_3x_4x_5 \oplus x_4x_5 \oplus x_4 \oplus x_5 \oplus 1$

$y_3 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4x_5 \oplus x_3x_5 \oplus x_4 \oplus x_5$

Set 7

$y_0 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_4 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0x_5 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_4 \oplus x_2 \oplus x_3x_4x_5 \oplus x_3x_5 \oplus x_4x_5 \oplus x_4 \oplus x_5$

$y_1 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_5 \oplus x_0x_2 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_3x_5 \oplus x_4x_5 \oplus x_4 \oplus 1$

$y_2 = x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_5 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_5 \oplus x_2 \oplus x_3x_4x_5 \oplus x_3x_4 \oplus x_3x_5 \oplus x_4 \oplus 1$

$y_3 = x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1x_4 \oplus x_0x_1 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_5 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4x_5 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0 \oplus x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_3x_4x_5 \oplus x_3x_5 \oplus x_3 \oplus x_4 \oplus x_5$

B Randomly Generated 4x4 & 16x4 S-Boxes

Randomly Generated 4x4 S-Boxes

S-Box	Total Gates	S-Box	Total Gates	S-Box	Total Gates	S-Box	Total Gates
B9A53E18D2CF4706	28	7F143A20B698E5CD	29	9EBC678415DAF032	31	92570F4E13D86BCA	30
EA86DC91B04732F5	32	43A5B7DF6E2108C9	32	DB93F210A8EC6745	26	645D9F73A0EBC182	31
F24B731DC9658E0A	32	0B74D58E92613CFA	26	15B3FEC8907D6A42	27	EB37094621FAD58C	30
E9D4A180B763C5F2	37	258C9EB0F146AD73	34	FD501B48C7963E2A	36	3956D018EA2F47BC	30
B358FA7ED12690C4	27	25EDF68174CB90A3	28	A7960FBE2C31845D	21	5AEBD63C2081F794	33
DE2C0F7B9156A834	37	0D5A7E29FC8134B6	26	AD6901C34B7285FE	27	29DAB7F6C40E1358	35
D6310A495FB2EC78	31	C064B9135A2DF7E8	35	23F0A1E4B6C859D7	33	57FD810CE269AB34	29
E1C34B0765F928AD	29	714C29853FDA6B0E	29	AD9C35284BE076F1	29	9FE6C2758D431AB0	30
DA31C8F067EB2954	33	689FB0DE2A1745C3	30	B3E81495A62D7FC0	36	642BAC810DF573E9	30
FD2345CA98E60B71	31	9B41DCE052FA7386	30	04DB62C9AE7531F8	23	ED6F9814B7A0325C	36
57D01BC864A29FE3	26	2A9DF5EB374018C6	30	FD9A1CB604E52873	34	68735F2DCB4AE910	28
E1DFA06CB7824539	36	568CB94327EDA1F0	32	401B7FEC5DA69238	31	32807A4D69CF1EB5	28
A7D4E98B23C510F6	26	37F2809DBA6E1C45	24	19E48D0F23C57B6A	26	B3C28190F5DA467E	29
CA196D7B05F48E23	30	5260C78B9A14FE3D	35	D0A3E4FC86B91257	31	60C93B71FEA482D5	36
18DA6BE23FC47095	32	2CA71B0465D9FE38	29	D648AC2953107EFB	33	0F78E54AB126D9C3	32
B687F0C9D412A53E	25	A4D1806C9E32B57F	30	68B091E45F3A7C2D	37	BE6CA19F70D45382	35
15F260AE9B743DC8	27	CE1538926704BDFA	34	425BDE09A37186CF	30	D7EA61280B45C3F9	34
2CADF5E06193B847	25	F78A30DE24BC1695	38	89DCB435A71F206E	27	48CDA09F625E7B13	32
1C9A3D60BF8E4572	33	E0F95872D63A4B1C	30	6BA9E051C7D8F432	31	9E403C2D71865ABF	30
836CE49057D2ABF1	27	CE732804D915AB6F	30	74B1FC860AD293E5	24	3A9DB56417FEC802	31
E53D9A867BC1240F	30	31589AC46F2EB70D	29	68FDC132E0A79B45	34	46F7BA98E13C502D	31
DF91045CEAB62387	29	42F5BC31D96A8E07	25	CE3987621F40B5AD	31	A43D7B109CF8256E	33
D45BC96E38A7F012	27	065A289C4DFE3B71	29	47EADF92386B1C50	36	AD0479E63B8C2F51	37
490DFC7AB16832E5	32	1628DB4E7F0A53C9	34	67F2548A9DBE130C	34	A2EF6D5193CB4078	25
0589CA1DB37E24F6	28	D326C0A9FE5B4817	35	EA0CF25341D7B968	29	FD8716ABCE459320	40
E0AD4762F13C85B9	30	3DBC275A04F91E68	31	E1CBF96DA3458720	32	C4A0782963B1FDE5	32
68BCA945307ED2F1	33	A0D74C581EB6329F	30	E4B62073C159DFA8	31	9E8631F274DBA50C	34
C4169528FD3EAB70	28	1DCA7B84E65F2039	26	7FAC98B234516D0E	41	48CA5F37E0912D6B	31
02AE869B143F7D5C	30	ADBF0354E6C19287	31	E06FBC91AD238547	29	970E26A53FDB14C8	29
04F8273DC916E5AB	25	7F30B564E1C829DA	26	A813FB645C92ED70	32	C31E84AD0F26579B	33
D314F9C82B76EA50	36	C2BA7FD51408E396	40	F72A690B84DE1C53	30	391BA7E82064CDF5	24
D3791FBAC652408E	27	A8F25197E6CD043B	31	2CBA67081FED4539	30	54B0AE789D26CF31	31
609F7DBC24A183E5	30	4A05BE2F1D9863C7	33	29AF7EC041D63B58	29	F21536A078BDEC94	29
5E46FC2018A793DB	27	4FD2510AE396B87C	30	87B5AF0D92E136C4	23	1BD264CA78950FE3	24
2BD946158F0AE3C7	29	A5096842F1B7C3DE	31	67DE9B42C305F1A8	33	13F0A6EBD94257C8	33
3E69015F7A48D2CB	25	B3E92405FD8A61C7	33	328E51C406D79FBA	36	6DEA8534170CF92B	35
38A19546FD2BE7C0	32	DB96E8A0215734CF	24	5B03A872C96E4DF1	33	BA3CDF2E96704158	29
EC6B3A24897DF051	31	EBC13674A28590DF	26	2A41C63FE98D70B5	32	65F8730B2A9CD4E1	31
B702149D53AF8CE6	38	E4C5B0D6327A891F	32	BA2E3C41F685097D	35	378E0A49C2FB51D6	30
4862D5BF7C1AE903	20	C8D9612A0F3EB547	25	C69F5348EB072D1A	32	AE3017F9B85D64C2	33
5DFB28C30A91764E	27	3CFDA107964528BE	25	9D8B35C217EA04F6	30	F9D10274BCEA6385	32
B07AD491CF5E8236	32	F702B3C61D4A598E	21	D21EF3954B8A607C	24	D3140FE56C9BA872	31
DFC0284BE573916A	30	DBEC37654A2F9108	29	EF4B216A7D09C835	34	8405DAB9FE1267C3	34
6853DF09C42E17BA	32	9D8CF4A2B0E15763	24	635DB1EC972A084F	36	4586B0739F2DCEA1	33
CAE4798625D30BF1	31	E3D2061A8F5BC497	35	59184E0CB673D2AF	26	84329E01CBA7D56F	32
DB7081AC3F29E654	33	A7E8C60D45F9B321	35	62C0E1FB549D83A7	29	17C620D5AF8E4B93	36
8E75BF2694130DAC	28	4F3B7920156EDCA8	33	F9CEA1B80D274563	30	514F278ABCE906D3	30
B827EF01D659C34A	28	FD0423B91CA7586E	37	251DF04397E68BAC	32	E29D1A567C084FB3	34
8AE761F2D0B5C439	30	5AD48E06713BFC92	27	FB74038916C5DE2A	32	F7AB459180E62D3C	30
39D0F26E417CBA58	37	80CDF2613459BE7A	34	F396EA4207D5C1B8	33	02E7536C48FA1BD9	26
E86F9B75C430D21A	34	29ED0C87F6134BA5	26	593F7AC01BDE4268	27	B197EFC43680D52A	30
15948F6ED7BAC203	28	DF50671AC4E9328B	31	643E0F87DBC15A92	31	8A71D0435CE2B9F6	32
8AF379D1C4B260E5	30	6BD875943CEA201F	30	4C39B78D50F12AE6	28	97FBC1A62D5083E4	29
64B903187CEDF2A5	24	C28A314D9E5F760B	29	6D3CB0174859EF2A	30	D053F8A4B91672EC	36
83109725BCADE46F	26	87AEC2DF354B1609	28	D7E24C965B038A1F	28	9CB72A8140F3D56E	25
DA9185F42CE63B70	34	517894DABF2C360E	25	13BD64E789F0C2A5	30	69FB7D03C154EA28	31
493EA0572DB8F1C6	28	68DA9FB2731E40C5	32	DAB34CE6912785F0	36	680917EB4D3F2C5A	30
F7C149E5D3B0A286	30	B527FD6C81094E3A	34	14D5CBE82309A7F6	32	203BC57AD689E4F1	31
7BCDEA6358021F49	32	89A56DE12CB73F40	32	B25A849EC76D130F	34	90AF68C512E47B3D	31
9658FD43BC12A70E	35	C70D519B86F423AE	29	2AB47F36ED1C8590	30	2D985067EBA31FC4	31
B839DF0526EA41C7	25	54D9361FE7B2A80C	30	BF29C13ADE650478	37	723DF860CAEB9145	30
8A476ED0913BC52F	28	F160D7A48EC5B392	31	79AC138BDF65E204	29	72964EB3805CFDA1	35
C205361E8DA794BF	38	B576AFED841092C3	28	70CDA483256FE9B1	31	3580E6DAF179C42B	33
1DC805F39476EB2A	20	95AB76321FECD084	33	78FA941C20BD563E	33	BC7F06A32951DE48	29
D0EFA59C3B714268	29	3C145609287DABFE	33	16BD025F7EA8349C	32	C1DF3AB59E048672	35
F51CE2038B79DA64	27	05E6C9A3BF8D7142	23	3B71F62C40AED598	31	62F07D5C19EA834B	31
0C4D3F896E7A25B1	27	7F048CBD1E39256A	32	7C6035F94A18D2EB	35	42A05961BE7FDC83	32
36792B4E018DCAF5	30	74C3526D0EAF891B	31	FCA8467E30D5291B	31	418EAD7025C6FB39	26
AF5BE872C1D43906	32	8ED34F76B5A2C190	28	436589AF1E7D2BC0	20	A9851E7BCD2F6043	28
D0284E6BA7C3F591	33	9064A17DBF35EC82	31	14CEAFBD73568902	27	D597A0FC3E21846B	31
9CB84F23A156D7E0	34	FD14A09EB657C283	32	0C678DF9342EA51B	29	3947F2AC0B5D681E	25
7D4FEB26CA085139	36	18F9AB724E5C036D	35	CE6580B4DA19F327	25	A48921BD7FC3065E	35
5EA83B769CD40F21	37	85D7294B1F6AC3E0	32	9FC850172DBE6A43	24	2176DB5F93E840AC	32
60F8D2E53791BA4C	32	AD632E798FC1045B	19	18CF942375E06ABD	27	8AEC2F0369754B1D	31
D1A47293BE68FC05	36	92451EC7680FA3DB	31	EAD108946532CBF7	29	186E309C4BFD25A7	29
F9A84B3CE7D15062	27	B41A2586C937F0ED	31	47369051B2DAEFC8	33	D019752B48AE63FC	34
A7491B3E506C82FD	35	7CA34E2105BD689F	36	A5B813EC94D76F02	33	15CDB9F826A734E0	26
4A93B7EDC8F10562	33	C63E14F09582BDA7	37	8F05E2D6B934C17A	26	9E78C21F350AB46D	29
62347FDBA5198EC0	30	E71A3598FBC0624D	35	18BFDC3A2754069E	31	CA5BD2E348061F97	27
3652E1A8C07F4D9B	35	236FB8ADC740E519	26	B0CE51A9F67324D8	35	9021ACB75F643D8E	29
72CB01E843F56DA9	28	95F8027B16E4AC3D	33	056E398A4FBC271D	29	5DEC403B62FA7819	28
47CF62E839D105BA	22	1D0AB9547386FC2E	31	4E7952683FC0AB1D	23	70C68B13FEDA5942	33
86EC1FA29537DB40	28	731D2A48E069CB5F	28	09426CDF78351BAE	27	847ED2F0C9A6315B	31
2B6E95D8401AC73F	26	C139A528F46D0BE7	31	91C430B56827DAFE	31	0672B5D8341CA9EF	26
5EF8170A93CD42B6	30	DA145372C68B9EF0	30	85C7F46D21A0B93E	37	9AEB7D04163582CF	28
75BCA30186942FED	37	F98130C25E6D7B4A	34	E8A3416C2D5B07F9	32	F01A4568DB92EC73	34
3FA618527BD0C49E	23	0651A24BDF893EC7	23	D91A7BC082E546F3	34	7514C29DB86A30EF	32
85641F2EAC307D9B	37	01F2973A84BC5D6E	33	54FE91A7C6308BD2	25	80AE65FB179D324C	32
5719A2364FB8C0ED	31	4B072CF18395A6DE	29	031CBAE468D7F952	27	814E9D30AF62B75C	20
1F05968BA72C3D4E	27	023517CBF8D6EA94	25	35A8406ECB7D2F19	28	4ACE6B3591870F2D	33
0937DF82BE541AC6	34	718D3AC246B5E9F0	32	8CF5D1AB76E40923	28	B65F7AE014283CD9	32
4916ECD8A0FB2537	29	13ADC56B748F02E9	24	86B1593472FA0DEC	34	56E74B01832D9FCA	26
0F5B7A8C346ED921	23	0F25AE3BD79184C6	34	38C6529A17D0BEF4	35	D9B6FE5830417CA2	33

61D38542B7F09CEA	36	18075EDBFC96A423	30	0BC294DF71638A5E	29	90475A136C8FB2DE	33
E2CAB638105F4D97	29	FA90347852DEB6C1	27	859742ED3AF6BC01	31	8CBE546137092ADF	24
03B856F147E2ACD9	24	F04159E7DA8C362B	31	40D9BA815C276E3F	26	396FBCD4015278AE	33
8DCB71A42E9605F3	32	94D71E2F3068B5CA	30	728E05F16ADB9C43	26	536E98204ACFDB71	33
23E7546BC0D1AF98	29	78394FD0AB5E62C1	37	A4605DF8739E21CB	33	16A794CF25ED38B0	30
67D043FE9CB1852A	28	5DE61CB427A9F380	28	8E021C9743ADB5F6	24	137E4BF529086DAC	30
BFCDA60E39258417	31	ABD045E6F978213C	32	9CB81256D0AE4F37	25	8CD791B620F35AE4	25
9F6AE014BDC35287	25	9264FD105A837CBE	29	BDAF1590C46E7238	35	6834F702ECBD159A	28
A4279FCE513860DB	31	0FACE61978B523D4	31	1FB3AD0846E5279C	30	B0C73E659D284F1A	32
AB7F48C539ED2061	31	7AB1D40F5E3692C8	27	74D0263A8F9B1C5E	39	14D29FC5B360EA78	31
D0F583CE14AB7629	30	B4FD20E83A96517C	32	08153DA49F62E7CB	27	B0CD579A3F8E4261	33
9A614E2D5830F7CB	33	EA318D7C2B64F950	32	95E4278A610C3DBF	34	984DA675F23E01CB	23
3A745DB2FE0C6981	35	03AEC76F84B521D9	28	ABF2193ED807645C	30	728ED6FB1A54930C	36
1A094FCD352EB786	24	6A47CFB82D50391E	33	5E7B6093DF281CA4	37	BD21C6FA0394E758	31
6012D5F834AB9EC7	33	382C1D0ABF954E67	29	48CD36215FBA9E07	31	3659124EF0ABD7C8	27
B75EAC380261F9D4	35	50234A8FD9B71CE6	28	E39D6250AB1F874C	30	D75E016A9C48FB23	34
2AC1E0BD6F598437	27	C12E76839DB04F5A	32	768ADB320FC594E1	33	415BC9EA3D7628F0	26
01438C257BEA9DF6	30	A7234C0B856DE9F1	31	4136BDEF972C5A08	29	A3F5B6148D902CE7	33
83AFB4E52967DC10	30	8325AD106CFB74E9	26	39E480C65AF7DB21	31	6201FA5C398EDB74	33
A79CF801B64532DE	29	D57E3A2694C8FB10	26	F0C7952D1A863EB4	31	92E37F4CD01B8A65	32
274EC30B51A68FD9	32	C9BD78A1EF340625	32	91874F6023BD5ACE	29	D392A7C158640EBF	28
A840FD2B651379CE	31	567FB4E8A139DC02	33	34AD291E0C6FB578	29	6B035A1D294F78EC	30
6D503AF9E8B4271C	32	8347C0A92B65DF1E	27	E2D41038B6CA7F95	32	269C03874F5B1DEA	30
F29E5B04137D86AC	34	6D1EAF84C29703B5	30	86753F9B40C2EA1D	29	8A4502F9E6C73DB1	25
502A6734B9DC18FE	35	60AE5B317842F9CD	31	1F98B4D732065EAC	32	4BC72DAF3695E180	28
6AC807BF214E9D35	32	37FED105289BCA46	26	B2C50167FED943A8	25	128653C9BDFEA704	31
A301D287C4B96FE5	30	DC69BA7142E05F83	30	FC3D95B1678A402E	35	502AB4F791C38ED6	34
78FDE4CB5A613092	31	2B536D7FAE4109C8	33	5C34D7601AEFB892	25	10DC4E26AB8F3795	28
C5490FB716E3AD28	33	C6BE5719024DAF83	32	DE6A209CB3815F47	31	7F24C981D605A3BE	31
4EDF0A8BC2561379	20	0476A2381CF59BED	27	01ADE958C6B423F7	29	2416DAEF9BC58073	30
6B3C42DA107F985E	33	F69BD0E2714A3C58	31	DF439BC867E2501A	24	530216849EABCFD7	27
91BCF8A2D506E437	31	8FE1094BCD5A3627	31	2697AF8BD5E3C401	29	AF89B2D05C47E136	26
E7495210C8AD6B3F	34	6EFB0D5382C1749A	32	23FDB1579AE48C06	30	ED0C8F54AB732916	34
71D86CB04A2F5E39	26	BA765F01432CE89D	31	934D05CB761A82FE	31	451FEBA79326C0D8	33
96384C205DEB71AF	36	C7BA1362D0958FE4	29	A8E3C570B94F1D62	31	2F9B3D64C05A187E	31
A723D854B9601CFE	29	C3975BEF68A2401D	35	986AC237BE10D54F	30	79CD12FEA84356B0	38
A369D8FC7BE20541	29	21C3A964E58DBF70	26	913C578DA02BEF64	25	0CB3F7D528691EA4	27
5C74DF08A326B9E1	27	E7A45BF836219C0D	35	DB8F23C07E59614A	38	4C3A61750FE8DB92	29
EC140AD538769B2F	34	6E3104D8C79B2FA5	26	287F14B90C53AD6E	27	50AB4E6F8CD19723	32
A5DBF68C049E2317	33	E28BA974D35FC160	38	4BC91820F365E7DA	28	19E2A60F84DC753B	27
E7AC50B2438DF961	35	B2D6E41C0F53A798	35	BA0F59E8764CD321	27	4ED70A869B21FC53	16
7C0623A8D51FBE49	40	A716FC895B30D42E	37	856B2D9CF7E30A41	27	A286ED3150B9C7F4	33
BDA908245FC3E716	30	8C67B1E25D40A39F	36	041EFA96C58372BD	31	D94F0BC5A2871E36	36
DE60BCF95473128A	26	257D0C69F38BA14E	33	476D03CE5B8F192A	22	0C5A4F6293B8D17E	29
AB920F7DCE835164	31	A45F329CE708BD61	29	81EFD5C6B3947A02	25	352ACE6910B874FD	33
276E90F3184AB5DC	26	6E89C1A457D02BF3	32	D74BEA2563F10C98	35	1D29A4CB05E736F8	31
DF9BAE7318C56240	24	14E9235F807ACD6B	31	C397D45F6EA8B201	33	A02F5796314EBDC8	33
950328D4716CFAEB	33	6C47D2851FA3BE09	34	8413C9D07AF2E56B	31	F8A2567419D0BCE3	40
DB04C938A5761FE2	25	4E3F6570D91AC28B	31	3C5F7A94B260ED18	27	D8E9724CB350AF16	34
A7F51DB8049C2E63	32	D7369EF42801AC5B	31	1203C7854F69BEDA	22	EADC6B89F3410527	25
267E83094A1FCD5B	29	A365EF729B81CD04	29	9AF52D6174BE30C8	31	541C8AF0E26379DB	27
65B97342DC8A01EF	30	1BD874035AFE629C	32	291B7C3406DAFE58	27	EB620D3847C5FA91	31
56480F3C92EAD1B7	29	A9EFD852BC743106	26	E05D8FBA3C429761	29	38BE71F625D9A0C4	27
6F8C4315E7A92BD0	32	FD645E829CB1A703	30	9DE31A87B54C06F2	35	B0F36D178A592C4E	31
C5E07DBA643F9218	33	25D83E61BA7F094C	28	0E4C698F5A13BD72	23	4F7836DE5C0B21A9	24
15E87F2DB396A04C	32	82A35B67EFCD1490	24	9CE7D6F02B381A54	31	BE54AD3689C10F27	27
B65E2CDA9083471F	32	3E7256CB49F8D1A0	34	5DBE42AF968C7103	36	F84A03D169B2C5E7	35
8B4E7FA2C3D59610	32	290C731BFD64E658A	34	B3A49F7E1DC65208	29	8EC32957F064AB1D	29
CFBAD0926314785E	23	8F96014DA52BCE37	25	623154EF789BADC0	34	846BD9321CAF750E	25
5D8BF6E13420CA97	31	1D7C90AE36B8F452	29	96732014BEA85CDF	36	FE05792BDA8C3416	36
93410F75D6CA8E2B	27	A178DB50943CF6E2	35	4E013B56F879CD2A	24	276FCAB03591E84D	27
E26F948703B1CAD5	34	563E10A84FCDB792	31	B5ED186C2934A07F	32	2058EF34B9DA17C6	28
DEA467530912F8CB	33	6ACB3E012487F59D	27	E0AFC4153B962D78	33	C51EB94283A7F6D0	26
8CAE61B27F9340D5	32	CD54109B37F6E8A2	25	0CBE93AD746128F5	32	89A5F23D04E16C7B	27
7BA0CEF4328D5961	37	6F1EC794328BD50A	24	6FD23901E48C57BA	30	82FD015A439BC7E6	30
790B3A5ECF4D8612	35	9AFBE51326D0748C	36	983027B64D1CFA5E	27	1279DC6AB48FE350	26
F5AC61934EB07D28	31	C290A54F17BDE386	36	5CF6E20389AB417D	27	B12574E9DC03A68F	34
3FE168B5A2D0794C	24	D5BE6A08372C941F	32	CD1B89036F5AE724	27	EC4280D1ABF93576	34
68B1947C0DF32EA5	30	DC8703514B69EAF2	33	920D5EF36CAB8471	27	15EBFD370A49C286	30
6BE4A53280F197DC	30	06FCA5D89437EB21	33	3F0AD56BC879421E	29	DE1759A64B382F0C	34
BD950E182637F4CA	30	56FBA2D4C18E9730	36	419EFA02583C7DB6	24	D9F0415EC72BA863	30
BEAD53086C492F71	31	6048B7E1ACD293F5	30	0AE749516C238FBD	27	43DBA08C71E259F6	32
5807C213E49F6DAB	29	9DA30B1C4F825E67	39	A9DBE6873FC12045	28	86A1FCD720E9B534	27
B6F28D0EA53C4791	25	D45A9FB7E132806C	28	AD57340CB96FE128	33	D2B319745C0FE86A	32
10683E4297FABCD5	22	4C6F12B7DEA50938	27	D0F9A687EB2C4315	28	2379C081EA56FD4B	33
B546E20D18F3A9C7	33	87B19F423DC6AE50	30	F3E674D2B589C0A1	33	4BC076EDAF983215	30
E5B79C1F06D43A82	35	29E68B430AFCD571	27	15462E3D8CFA0B79	24	4FCAE98612B705D3	28
6BFDC370E4912A58	31	FC274AB5ED913806	32	4E603A928D1FC75B	33	1E360F5DCB79482A	30
78E901F5C63D4AB2	37	A490D71FC258B36E	29	D2F9E786431ACB05	34	4B5E98CF1DA03762	31
8F35BA04E67C129D	27	01387DACB9E5642F	34	61A2375C40FEDB98	31	14F90E67BA528DC3	26
905C7D18B324FA6E	29	0C61E592DBFA3478	29	05F1D26C389A7B4E	35	68A427D39CBE15F0	34
704E89CD126B5FA3	40	1F63A72C59DE0B84	35	E90361D8F2C4BA75	28	A3BD9EF6842C0715	34
4C391E8B5F6720AD	29	2543BFE76981A0DC	26	01B628DE975C4FA3	34	2B914E0D75C63A8F	30
7B1AC9FE6D304528	35	8C5E42073F6D9A1B	29	6D138A29BC45FE70	36	81A6CB325F70E49D	29
81D20346FC7AEB59	28	6E48F1A50329D7BC	28	0A2D1BF53E94C876	26	87DC9361EFB5A042	29
CDB03F8E1A624975	30	F28D4E150BC97A63	38	4658FB9EC27103DA	32	D82EC6103A495FB7	35
BFEC149578A23D60	30	251D96B47EFC083A	32	DE7921B46803F5AC	28	F64521B7083ED9AC	32
E56F4A8237B901DC	26	A2B309F6874CD1E5	26	CD70E8635BF4A921	31	A5C64E2908D1B73F	30
F2389A7B6E0DC514	35	9AF728C03B54ED16	28	9683410CF2BA7D5E	31	0A8563E2F94B1DC7	31
25FDC143EB697A80	34	5019E7FA823CD6B4	35	D48735012CE6BA9F	32	36CAF702BE95D841	31
543079CDBEF618A2	29	23D75AC0FB19864E	29	CD83157BA9E2064F	22	20FBC618D9E3A475	32
F17C82E965DA30B4	31	41AF809275EC3B6D	31	3147025BECF8AD69	28	E6092C8A437BFD15	34
C1AE0BF4D2867395	28	D402C13BE86A79F5	30	76A801E9423CBFD5	28	3B769ADFE025481C	22
F43BA68E205DC917	35	A35ED9827C014F6B	33	FD4A12C69E8375B0	28	6EFA2B0548D7C391	25
D9F670835E142CBA	30	3465FA7B8D2901EC	32	EBC34D09A56821F7	29	68F0E27359C4A1DB	25
62BD7854AC0F31E9	32	4FDE0981C3A6275B	23	1025FDC3EAB94678	27	2FE01BC9584A6D73	24
02481CDE6A573B9F	24	0E9357B6F1D842AC	34	9A4E8B5276C0DF13	28	E51A2784C3D96BF0	34
DE3165C27094ABF8	29	1E5FC7A82D493B60	26	738D9BFE5261CA40	30	FA86539DC7BE4102	33
346B15E8CF0297AD	33	7243AE10D698FB5C	34	2B34FE18975DA0C6	34	6821EBC5A7F0394D	29
E3D24F58901BCA76	30	826954C1B07EAF3D	31	23D6E05A1BF4C978	29	D35A7824F10EC6B9	26
FDA268E34071C5B9	30	E14C8F7B02DA9635	36	86E14AB359D7FC20	32	AF14850D36BE792C	22
20DEA6C1B583947F	26	EF14625BAD9780C3	32	7A2586C0E19BD34F	32	89E07354B26FDCA1	35
8BFA5C9E032417D6	30	45901DFE27A68B3C	28	4528A3C90E6B17FD	25	5C0DBE94738F61A2	35
012E36A547BF8D9C	28	F74C9E635B8AD021	31	27BCE94A6318D50F	30	A570C8E6B2149DF3	32

7F264BA59C13DE80	36	30976FED841C25AB	35	8F5301C9D4AB2E67	29	FC960EB423751DA8	37
9C378514DBA206FE	29	690E54A3BDC278F1	35	596408CE21A7BF3D	35	8B7DA3C9641E5F02	27
912CD65FA8B473E0	32	A49D38B7EC5F2601	29	6A79C5F128E0DB43	28	20AB5397D48CE1F6	28
3A26B1E45CD7089F	28	D83F659C702BA1E4	33	5DBC3706E82A4F19	32	27F198EB4C63A05D	37
CB9DF73A615E8402	31	C16D3EBA089524F7	31	70D86915B2EF34AC	32	4930C8D5271BF6EA	26
10D7C493F86E5A2B	31	9A1C07542D836EBF	30	D1509F682AE3B47C	32	258E7FB031694CAD	31
34D20C951EFA7B68	25	94C2B730FA6D18E5	32	FA8D93564E17BC02	35	4A92C75BD6308EF1	29
543F02D6A79B8C1E	31	931B547AED0F2C86	28	2506CA1849FE37BD	31	6DCB78351F92E40A	28
FA891B6C3705E24D	31	6F01C2ED35479A8B	27	D9734F0A2CE865B1	33	314CD2EA597F860B	35
F310D6429C57A8EB	31	B53C84AF1D9E6072	23	4D6F75EA91B2C308	25	C8E9B6A4705D132F	24
15AFCB8630729ED4	37	B2C0D8496FAE5713	34	2D90347816A5BCFE	29	B2D5841EF0639C7A	34
3A4D572C80F61BE9	26	7142B5D9AE68F0C3	30	BCA7452D8F3069E1	31	780C2149ADB3E65F	34
5E021D493B7F68CA	26	678159DEAFC230B4	29	E92B3C45D167F0A8	37	95A708E46F31D2CB	29
67E2D39B08A4C15F	34	3E0954C61A28DF7B	29	E14BC87F09A3D265	28	9C4FD316A5B2E870	28
B3D0CAEF57946812	31	623ADF197B805C4E	31	73DA851FCEB29604	31	D2A176BF38405C9E	31
518BC37AEFD04926	36	EB5C317A60D2F948	35	3C40DB2891765EFA	34	3280E19C6A7BF4D5	34
01FA7D582943CBE6	30	0D9FAE6184325B7C	28	6A9C5F720D348BE1	31	15C6A38F92E7B0D4	35
713A62BC0E8FD549	28	79832CE16FB05D4A	32	362B4D91A087E5FC	36	107BF5D8432A96CE	27
986025D7AB1F43CE	25	2D3EF8B901C4A675	32	1C72B6E4D59F0A38	27	BF35A24687DCE019	30
2678013E5D49FBAC	28	095CDBA4F17E2386	26	A39081E2D47BF5C6	22	8A21BD6F079E4C53	30
7B5FC9A360E84D12	29	A68734DE0F92BC15	34	FDA8541EB6790C32	29	19BD54FA23E860C7	25
7DCF2695EA40813B	29	1DF9EC403268B75A	36	A8D9C6BE051F3427	27	6BEF53A82701DC94	29
482E5D360F7B9A1C	22	DFC673E21509A84B	21	4DF8C261BE7035A9	30	81506A9DC4EF273B	25
5A2EC908F37BD164	37	34E0FAB75926C18D	29	E8BA9C72504F163D	33	F524B1A60D8E397C	34
ABDEF8C163942570	24	A8D9F2106E4CB753	32	BDCA75E8460921F3	32	4516723E08DB9FAC	26
26EBA9D54C17F038	27	70D91F25A63CB48E	33	71F0CE594A326D8B	29	672DEA1345908CBF	22
760D3F1C8EB5A492	33	1C5692AD4E7FB803	36	C827056D31ABF4E9	26	327E4FAC8B0561D9	30
70A53DB69EC1F248	29	F1CB608975423ADE	31	7E86B15F4DA239C0	28	6DB1F53C2479E80A	26
8B29D1754C6EFA30	28	5E476DC0BA398F21	29	0816F3257D9CB4AE	27	5D13E70AF649C28B	29
FBA967D8135C042E	31	7CE49A183B526DF0	36	04CB9D126E75A38F	24	A417BE68C5D239F0	34
5470D9C12FBA63E8	31	B3806F7425E1D9AC	28	4EC87BF916D2350A	28	59EAC3F06B2487D1	29
EB9A720C1D63F548	33	583017A49DFECB62	29	C607D2458A1FEB93	28	E85C97BAF613420D	33
A7D2C86F495B310E	33	C6F021473AB95DE8	33	E72051BCF6943A8D	35	18FD746E0532C9BA	34
B47E6F2D59A0813C	28	36FD94CA7EB85102	25	EA213C4896BF507D	35	E631D28C0BF54A79	30
C7EFD2B150A69438	31	B23A841ED97F6C50	26	8FC619A32475B0ED	31	81B47F9C6E5DA032	31
43752FC0A6EB89D1	33	0D359B4E12FC687A	34	BD6753C4218E0F9A	32	C475FE968D021BA3	32
721DB8E903C6A5F4	31	79A3285EF10BCD64	31	3A4058D9EB27CF61	33	D9A037B5C1E62F84	29
49830EAFD16752CB	29	5C8AE1702B496FD3	36	A62043987CF1BED5	32	3480F16D9C5EA72B	33
31A68F5B09C74ED2	33	3B476A2C1ED8F059	30	1FE30C6DB5A72948	27	079BC6D523A481FE	29
92D6F5BC718E03A4	25	9D867FB15EC0342A	28	6A8DC590F34B1E27	29	B9A0F142D5C7E863	24
E69B357F82D410AC	30	9A87401F5E326CBD	33	C25E04379BA68D1F	32	2C5DB7AF84361E90	30
EA02146FD3987BC5	32	12E3CF5496708ADB	31	1B2408CA79563EFD	23	B8D0C965374F1A2E	29
2DAC789635FB104E	31	E2480F6B9D7A51C3	28	E89623D74CA1BF50	32	67C1FE48B0D2593A	26
D0BCF3698E142A75	36	1AF3784D6EB5092C	28	B710A9D64E382C5F	40	175832FA6BCE4D90	32
7E69452C8BD0A1F3	28	E02B957CF46381DA	26	23B197D08F45EC6A	34	F2B690C4A5D7E138	25
F264E03C57891ADB	35	85604ABE391C27FD	33	D5E34B6F917C08A2	27	A4F8BD2165370CE9	32
69DFE83C14B2A057	31	AE50B493C72F18D6	34	0E8C5D72F4B6A319	28	75408D92C3AE6FB1	33
04D38CFB6A7592E1	25	5DA791B4F0EC2638	31	ECB80F91462A3D75	30	42ED8F1A396C075B	33
02DE69547BF3CA18	35	015A43F697CDBE28	25	9E48F5C207DB316A	32	7531D8C4E9B20FA6	30
2610C97D5E843FAB	29	F5E3CB2718A04D96	36	F27981C5DE340A6B	33	7142E3CA0D6F958B	29
9C46F0EABD723185	32	C9A42F718D03BE65	28	1908D2E5367ABC4F	22	FC1D36E5AB824907	31
8DA2FB610439E75C	28	4D3A96BF01C2758E	31	BD23EF76A8590C41	33	25ABDC308E1F7469	28
035DA9127E46CF8B	27	8FCB0519A46D237E	23	416D9FEB7A53208C	28	804EC693DA127F5B	27
E024AFC3B798651D	31	BE6CD8054F9312A7	33	BF924C71DE5306A8	31	B3ED10597A6F48C2	29
29DE4C356B87A1F0	28	2DF7C94AB163E085	34	93F6875E1DA2B0C4	33	3A512B869D47E0FC	28
D4F3A0EC18B52976	26	3290AC7ED685F41B	37	64EC579A1082BDF3	24	42B57D19FA83C06E	27
85C31709BEA264FD	31	5C8B1E749D02F63A	32	489B7ED5FA106C32	35	9EF1B073D5C2A486	34
E8407F2635A1CBD9	38	B3FE8A4175DC0629	28	9A06F1C8BD3752E4	31	7CAE631804F529DB	35
AC3B95E0FD481762	29	03724B6EC8FAD951	29	41C69A32EB08DF57	27	A0B58C71FED43926	32
CA76EF95240318BD	27	7514C6F0E3829ADB	29	67CE08B493A25DF1	29	83BC2F409156DAE7	33
52CB30946DE871AF	30	403B2E9678AF1CD5	30	C6B0219EFD5874A3	32	6D8BE0FC759A2143	30
E8415B37A09D26FC	30	2F8013C46DB5A97E	37	546D37B01FE8AC29	32	1563DC07E2F8B4A9	30
0D5348F7C9BEA261	29	8795BD1A4FE623C0	32	0293EC4B6FA1758D	27	76C918025B4AEF3D	33
5A3E2B81640FD79C	34	57982EDF6C134A0B	31	5CDE03F629A47B18	27	96B8C41A02EF573D	39
AB26E05D94CF8371	31	C9523068BA4E1FD7	35	C1BA568093247EFD	35	B64139D20E7A58CF	36
C4F6017D392BE8A5	24	7A01824EC965B3DF	38	0AFDE8C213746B59	26	682C173DA09E5FB4	27
270F983154EABC6D	29	498DCEA3F5B61072	31	CD34A861B209F5E7	27	F1B65D78A30E924C	30
CD374BE596F201A8	29	9A65DF1843EBC207	27	405F3A689C1E72DB	29	C1254A70D8E3BF69	30
9365DC8012BEA4F7	33	B34785C02AFE16D9	28	4BE61C93A7582DF0	26	C75FE34891AD02B6	30
F37B0D26C981A5E4	31	39678DFCA5EB4102	31	3D9256A1F4B8C7E0	36	27B4E693F5DA0C81	35
42C3BD57E109FA86	34	4E5D6CFA38927B10	24	7316DB2EAF5C4809	30	0A53B8D6EC2947F1	25
E8B592374C61A0FD	39	3502E8A6BC1D974F	30	546A3FC091D8BE27	27	BA3E260C759481DF	28
EA8902B4617DC3F5	32	7D180C9E5AF4B263	30	F6493E0175B28DCA	30	9D80471632FBEAC5	26
B67DC05A31F2E498	31	D8EAF570B6C34291	29	7601A4BCE8D2935F	32	84BED19F253C60A7	25
69BC03178A524DFE	35	517B08249A3CEF6D	23	BE5894A3D027C6F1	27	A4B81F750C29E63D	27
B9C07416EA85F2D3	30	781B0DE2F495C36A	24	81AFB94C605E7D32	31	35E09BC268DF741A	26
4DBAE5629831F07C	32	975C2A3EB8F140D6	28	D96B74821EAC05F3	26	9CF267E58A1B04D3	30
C12763985AEFDB04	27	F604C175BE38DA29	32	7EB64923DCFA8105	24	561E398C2DFA74B0	32
29E05FA684BD1C73	34	2CAE97D8304FB561	29	3BCAF9E175D08426	32	70981D6BCFA24E53	36
C1D93BA56E478F20	28	F197248ADBC635E0	26	9678FC1B425AE03D	31	2910EBD7F6384CA5	32
4CE1B3D7A8596F02	31	B970D256F8E3C41A	30	71BC235E806D94AF	32	D47652CF0AB9E813	28
980742A3C1FD5BE6	32	2B8EA056473F9C1D	29	2EC869301A45F7DB	27	C358B17DAFE29046	32
E40BD729183AC6F5	26	2670FCEA39B1584D	29	DC56F120ABE87349	30	FC601B87359DE4A2	31
4138C50ADB9F2E76	34	CA2198E53FD074B6	32	F78356940BAC2D1E	39	B2F8013ED7694AC5	32
B4C6253F0D7E98A1	27	F357142B9ACD08E6	36	1FB084DC2967EA53	32	2D9A8437FB65E1C0	32
982D6FA473C01EB5	32	5846ADE92C7013FB	37	C59E3F70A1D8462B	25	B4F29D05E817AC63	34
61DF20C9854B3A7E	35	70216D3EFCB48A95	24	A213ED08C54FB679	28	C1E52F6D38B0A794	31
20FCE647D1A35B89	30	8C652AB9D3E1047F	34	2BC310D78A6E495F	32	5C2B89014A673FDE	31
FB0D893CE6524A71	33	2145D3A9B76E8C0F	34	9F30A657BD2C48E1	27	410CAEF9657D2B83	26
B6DF3E7A92184C05	34	6B32048579C1DEFA	32	D1032C94BE5F78A6	32	960BEC1D24735AF8	31
564AB1097C28E3DF	32	874CD29FA510E6B3	28	2F1E7053CBD498A6	26	8DC12EB906A5F734	29
EB25A38F96407C1D	29	81E3D49056ACBF72	25	6A37DB4E9052C81F	34	FB3C6AED71490825	28
05CA7F34B892D1E6	30	4D8E09F136725ABC	28	B8EF6AD519720C43	38	4D0BC685AE13F297	29
AEC7B8259034D61F	34	50F892A73614DCEB	23	91D0CABE285473F6	26	0A9B684CF5ED3217	27
2D0491E68F573CBA	34	5AF610C289E7B34D	39	C823D04AF1EB7659	32	BAD87195CE2F3460	30
5CDA9EFB72134086	36	84D7F690125AECB3	28	6A019C4ED528F73B	35	CB7EF54D329860A1	35
51034FE92B68DAC7	33	4A9026BCDE8513F7	33	DE257FC830B964A1	31	0F56BE2137A8DC49	34
DB9A20C534F681E7	29	92F8D541E3CAB076	30	4C8A9F6E20B371D5	24	A3F4D28BE501C697	29
EB20D9FC6815473A	32	D4CE830A67B512F9	26	710693AC4D25FE8B	31	9C30EB457D8A261F	30
0714BFDAE2986C53	32	5BE790382614CFDA	30	541ADE723B068FC9	28	70A4925EBF16C38D	37
53F10E7984DB2A6C	32	3AD50742FEB6918C	32	DEA9574063BCF218	27	9FE3B1A0625C78D4	35
D492CAE5F137068B	31	0FC5A7819E2463DB	29	41C9D8BA3F256E70	26	2D6E04AF75B8C193	32
45FD9BA38E21C076	28	94378BF1DACE0562	31	ACE5D6208FB34197	33	35F6D19784ECA02B	33
501D9CEA7824F6B3	20	2DC875E69A314BF0	32	AFB174982E3DC560	32	71CE58A23940FBD6	28

431A2FD9B58607EC	34	D4E3786CAF9521B0	24	B872EA53C9D6F014	33	02AEC7D9153648FB	25
78B9F4E021A5D63C	32	CB70D25F3A19648E	31	79453DB81E26F0AC	26	5CA19D7FB80E3264	37
2B487C9F56ED13A0	26	F5BE31DCA4960827	35	2B3A1E0F6975CD48	19	1FEA0CB794D63582	31
7985ABD301E62FC4	39	6F9AC2DE73B01485	36	9D45EF03B8A1762C	36	E2A4D3B1F58976C0	28
F5123BAE67C4098D	31	B3E16D0248F795CA	34	EF69AC407DB31825	28	A4F2E85D6079CB13	30
6E7C2DB309514AF8	21	E57F9DB38602C14A	40	712D83B9CAE405F6	34	B21AF964C80D57E3	34
27E8FCDA1964B035	34	67BEF12AD09C5843	30	BE5D14679A0F8C32	33	0CF674ED9B21A835	32
46EA8DC70F39521B	31	AFB60E2D389C5174	31	0DF7A32B98E654C1	29	E4879D063A1BC5F2	37
D238CF679BE154A0	34	4C2DF56B901E78A3	28	D486F71C93E052BA	28	1DE9B3270AC8F465	30
8B421390DFC7AE65	30	8FE24BD0A3965C71	33	08DF7B2CE64A3951	25	7DAB460159FE2C83	30
4FAD3E5C09618B27	27	B50AD81764293EFC	40	F1C4BD236A9E8075	30	BEDF826703459CA1	35
495EB2DFA806317C	34	AF482D7360C519EB	31	21F38B05A4C9D67E	31	6CB891A74FD2E503	30
1B286A95743DCEF0	30	43B5ADC2F768E910	40	1AD6B80E24C593F7	31	F850ED439B127CA6	30
C8AF43D56179EB20	26	E378654D10AB92FC	28	89B16EA0DF435C27	31	57FE10A6B82C49D3	30
397405C6DE1A2B8F	30	6FA72CEBD3054198	31	B1ECA96035724DF8	29	4C0A729FB6D3518E	25
A254D90813BF6CE7	29	DA5B4F60931287CE	25	F8756D91240BE3CA	34	625971E4BA08FC3D	23
0C43F5AE819672BD	27	B84235A6E70DCF19	34	1D8B45F03A762EC9	28	3F2C6195ABDE0478	33
C9341A06FED2B587	37	4E3B7FAC029165D8	25	9B1625A0F783CE4D	31	5AD3F4879C0E6B21	29
8CFD503A96E2B417	27	9FC265A0718E4D3B	27	2153769FA08CEBD4	27	01E7F39C48BAD256	30
29631B07E54FDCA8	27	6BDEA53479F0C218	33	86127DECF9A4B530	32	F2AB3E0D7C548196	30
E207D931CA84FB56	28	EBD4A93581CF0627	31	80D2B9E47356CA1F	30	B8407C26A1DF935E	31
A163F458B702D9CE	27	2F7ADBE58104936C	32	0F7C2ED68A95413B	29	31B587E0D42F6C9A	34
059F7D8BCA3612E4	29	0276A1E4CF538BD9	30	1672495E80DC3BFA	34	10F82A94E6C35D7B	29
79581CFA36ED2B40	38	6109D2EB853A4C7F	36	AC980D6E372B41F5	32	4095B632A1C87EFD	35
7F092BCDE63514A8	31	240F3D5C9AEB7681	31	D3E29108745CFAB6	26	AF2475DE986C1B03	28
62DFA71EB903C458	27	86247CE5AB1D390F	32	869FBE134C7DA025	30	48F19367D05B2CEA	24
07A9C24B31F58E6D	27	17E928D4A53F06CB	27	985B371A42FC6DE0	32	E8721C39054D6FBA	38
28410CAD35769EBF	26	DAE7B9F85061342C	30	89105EBCFD746A32	25	0B5827FC3AE9D461	25
847D9F5B60E1AC32	35	31DE0764BAC985F2	23	6EB9D874F30C152A	32	3F1905B42C76ADE8	27
81CA526E0D4F97B3	26	A5D089731F64C2BE	33	65BCD84970FEA321	25	2D5041E7CAB38F69	30
F423079DE5BCA186	32	0729B1C5834FDEA6	34	4F8190CDB3AE5276	34	9C6A703F5128DB4E	29
D4235FB068AE9C71	31	4CE65B301DA287F9	20	4D1CEAF6529830B7	25	E3C4FAD280675B91	29
0A8F1DCB253746E9	30	C7DAE38905126B4F	26	1B6AEDFC97803245	26	BAE29178D40C65F3	30
CB3218E76FAD4590	34	D9EC104A7BF26853	34	306487915AC2BEFD	27	1275FCE0A8B943D6	28
5B09321746DFAEC8	31	35EB17FD628C09A4	29	9B56D7F83024ECA1	27	5AD3C016928E47FB	31
9C148F2AD6075B3E	27	07BA19258E36C4FD	23	B71839CFEDA45062	29	145D8BFA69732EC0	32
1BCA8DE3F4076529	26	47E59F8361CB0DA2	29	A98D3F72B5E4061C	32	3B952701E846DAFC	20
89D071E563AC4FB2	35	025F3DBCA96E8741	23	10E8F42CB35769AD	29	04C9FBEA3586127D	25
E09435BCDFA72186	30	8716C492E5B3AF0D	29	3F74ECD126A0B598	29	9BCF367D01E42A85	30
86A57E40FCD39B12	31	6F45E89A72B10DC3	34	09E5243C67A8FD1B	31	43DA0EBC9768F521	23
52F9EC7B34681A0D	33	37B5F9EAC284160D	27	093EC2A8D1B47F65	28	856397EB0F1DC24A	28
A054F267C3B1E9D8	37	0F74A21C85963DBE	29	E7B6A2D4C89013F5	26	6BD593817E0C2F4A	32
BEC1FD345728609A	32	51A37D80CEF9642B	33	D342A980CB76F1E5	30	4871CA90E26D5B3F	26
7AE59F2B04D1863C	32	3FEC1A58490D27B6	32	A86051E3274FBCD9	32	5B0F6378CA2E9D14	31
7C19DF6E8A54B203	34	F820EC417AD596B3	36	8A29130F6BCD57E4	29	5C63D7B094F2E18A	30
D3A7BEF82C145609	30	E381756BF4CDA209	36	89031BE24DA75CF6	26	297DA14E68BC5F30	20
C1E2079F3485BD6A	32	CD56832EA40FB791	29	A6D47B8FE15923C0	30	F034716CA59DB28E	35
1ADE8743C6F5B290	26	4E83DB20C17F5A96	26	68F3E051C2A94B7D	25	125A4B6CF908DE73	30
A72FBDE94036C815	32	3E984C0B2567A1FD	39	2EBC4056F1DA9873	26	C2E67F583B1DA490	24
AFD0849E53C261B7	27	4856C91E23D7ABF0	28	3A8DBF917426E50C	28	94F80761CEB53A2D	29
31045ABDF8726EC9	36	0FD6E8453AC9B721	29	07F854CEAB63192D	31	63BE812540D97FAC	26
65C9DA02F3E8B741	35	34692A1BDF8EC075	26	378D4162BFAC095E	25	F430DC865BEA7912	29
072CE849ABF1D563	26	BFD03794E521AC86	26	5C6BA9284F13E70D	29	23FDE647A9810C5B	27
D20BC589761EAF34	33	B647089F3ECAD512	27	82BAE63419D7CF50	32	7CA53FD4620E189B	35
2AFB67D3C984105E	31	9DB8AF415237C6E0	26	D2B16E4ACF705398	31	7C96248150DEA3BF	32
B1F83674A50CDE29	34	75E0219ABF6843DC	26	96E8D7450F1AB2C3	32	69CA140D7F53EB28	35
6D8E92375BF14A0C	30	0523D7B9CE46F8A1	29	4E109623AD587FCB	31	B1395E640C2A8D7F	28
07ACB5924836E1DF	26	B9D4A26E817530CF	28	18BF40329AD57CE6	30	B6719FA3802C54DE	37
F7893E05BCA2D461	33	EB2A89F1D047C356	32	3058ED7ACFB29146	28	B1687495FA320ECD	29
47902A8CF536BD1E	31	97F8B31540CD6A2E	29	EF48653D7201ACB9	28	475AD69FE1CB3028	23
D35CA672498B0EF1	31	58CA7BD2F3146E09	30	1C04B8D32A7F9E65	28	E2BF861A3D074C95	26
235FC1AE749D068B	29	1792C0A3FEB654D8	31	54E3DBA8C072196F	26	DF7C3925841AE06B	31
4CB26D95AE807F13	32	61B9A23854CE0D7F	32	8FBC50A4D23761E9	30	9E1F750B36C28DA4	29
EB3F07859DA6421C	30	30E975FB8D6C24A1	29	781A0F52ED46B9C3	30	A3986FE4D071C5B2	29
E23ADB4FC5170869	32	CD279BA4135E680F	34	D2785E6301F9BC4A	32	AF04CBD836E75129	26
52EF468CBD01A397	27	1A80943B2CD7E6F5	28	AD069B3EFC574281	21	3F8BA1CD9E642507	33
BA70419CE6D3258F	30	F5ABD263C90714E8	37	7D3B4C6928F10EA5	24	F6ADC57402E983B1	37
1BE03C5974AD6F28	27	0F6745EC1293BAD8	33	D1895CFB73064AE2	33	4C8D71E5FAB60932	27
4BD1ECAF78326905	36	7A6C1B523F948ED0	34	B84F0EC93761A52D	35	18AE76B0F5324CD9	34
68E3BACF517920D4	33	ACD2E49850FB6371	31	270B16DE539FC48A	32	123F65BD80E7A4C9	34
16A24F5ED9C7B380	30	9BD1C7E3540A86F2	25	E084C61FA7DB2395	28	5C6F7D08921EAB34	23
8BAF5134E72D609C	28	24968D3A17B5CFE0	24	FE0C1326B458A7D9	38	78BF0C964231DE5A	38
DC3F0BA8297E4561	35	298BD031A546FEC7	27	B791D5E0A43F86C2	23	6E1AC0B729F5D384	23
A935C176D42FB0E8	27	31E8CA4D2F750B69	32	948A1FE7D6C0B523	28	D7A89E30542F6C1B	31

Randomly Generated 16x4 S-Boxes

S-Box	Total Gates	S-Box	Total Gates	S-Box	Total Gates	S-Box	Total Gates
69DE7C85FA41320B 376E5084BA1C29FD CE24F10A387DB956 871ABE20C5F493D6	128	9721F380A6ECBD45 DC5417E3FA8209B6 B76C03948DE52F1A C35B46DE02971A8F	126	21CEB59A67DF0348 A5DBE46093C1F827 D438FA6CBE570291 F80B1E4A25C79D36	122	5A3042198DFCB76E 7D580B3EF4912C6A 63DE2C405178BFA9 59E84C3B176A0D2F	112
38D6E4B02C9A751F 0A57B3DE19FC4628 5D9B4078621CA3EF 24F5E1D6073A8B9C	126	EBDC26A45803197F 4ED0CFA7395B2186 108D3E62CB7A594F 64E829FDC5A1B730	124	0B728F3CA5D41E96 B3285D76E41AC9F0 9087F15A3E2DB46C 1EBCDA7F29403568	115	90CF1DE2847635AB 426F7ECA91053DB8 4F9D586A7C23B1E0 12BFD98673EA54C0	118
4856EF7A21C39D0B 3A569D4081E7CF2B A5C7FE94316B0D82 5D21349C870EAF6B	133	682C13AEFD495B70 5E71948CB63F20DA 863209A4C1B57FDE C345E0D9AF78B216	134	F9CE2A57483B0D61 98AB57F346C1E02D E1F807BD95A2C643 931FDA2B4E5807C6	112	2CA049D7635F81EB 45A69BDE3C827F01 1549EC80DF27A36B EB6783CA421905FD	115
6930E5182BA47DCF 1482B5EF0D6C379A		C0495261F3DB8EA7 CA289E7B04F5D361		F16E9D582A7B40C3 4B7DCE95A368F120		604F5A712CB983DE 08E46FC9DA3B7125	

EF3DBAC852604917 A60FD427CB3E5891	123	3F628D1A0749C5BE 43AECB8D7026591F	130	709B6AFC4381DE25 FC81B73AD9540E26	124	94C75E68D3F21A0B 12A0F84DC93B576E	121
AE4B2C8D06F35719 46B7CF298A0315DE 328AD60BE1CF9457 D6054132B78CA9FE	119	869D1ECA57023F4B 120D437AC8B5EF69 F9BE75CD12430A68 796A8E1DB24F53C0	118	E6413D27B9C8A0F5 870CEBF2394A61D5 4B2851FAD63C097E 78BA91C3ED504F62	135	5032D6A9C71EB8F4 B814DC6E5F09273A 3A90E542CF1B8D67 6897E510FDBA432C	116
3178E29FA65BC0D4 4CADE209F573681B 4A6BE132DC0879F5 58204C1B69E37DFA	134	5DC7FEA68B430291 B6D387A540F2EC91 7B9C04E13F85A2D6 784C5A0F3BD6192E	115	09B5CA6ED14F8732 7F01E639C5B24AD8 3BD20A561C8EF947 082F43751A9DBEC6	116	1BCE6FA897235D40 CEF48921D0B5A376 C3158AF72609ED4B D8B349E72F6AC105	120
8C3F70D612AB945E 6BE13F872CAD9405 2017A4C59DBE386F 429137AC0DFB6E85	116	C2156F4B3AD9E078 C9834AF517E60D2B 4DA9F67E02CB3581 9453E2A8F7B601CD	123	FEC596307B2A14D8 1CFB53E0AD829476 40BDA5286F73E9C1 86FD29CB4750A3E1	115	25D3CB18076A9FE4 37F150BC4A9E862D DE12A36F9C7B5480 516BEFCA97D42038	113
52D740B869C1EFA3 FA984C52E3D601B7 275BDAEF4106C983 29D31A8CF4705E6B	125	FB6C87921EA403D5 3D8B7C2A156F49E0 6F14E902C3AD587B 7A98F2D63540BEC1	137	179F25ACD60B38E4 701DB6F2A48E593C 4ABF02E17839D56C 34E7CBD658AF0129	122	6170FA9B2C54D3E8 647B2FC8E03195DA D507C684931F2EAB 54A68F17BD3C209E	115
5E173CD6092B4F8A 98425D301FB7AEC6 F49D3EA275086BC1 A7B59F0CED638412	115	8BD713294056CEFA 5C8723D0469EBA1F 34F971C8D05EB62A 87ED062C4593B1FA	114	80E19CD6AF273B45 13EAFD65894B2C70 30479EDB6851AF2C 5D2EFA94B017836C	130	5A6DF0172BCE4893 DC15BA42E9F70638 8D069A2E15B74F3C 9CF35407ED681BA2	125
0BA915C2E8F73D64 9A2FECD45086B137 CBDA38045F6719E2 D14B85029F36EC7A	128	45A07B1FC9D6E832 1ABCF58934726E0D F270534861DABE9C 1435EC78BA029F6D	115	45738CE9FBA0216D 20C8793E1A4DFB56 56217FBC9E03A4D8 FCBA9538D60417E2	113	B80D1752EAC9F463 2A4C0EFD51863B79 2CE9BA1564D7038F 362980EBC1D4AF57	131
DAEC60735182FB49 7F369E01B2C84AD5 F6CEB57213A4D809 B4E29D6A10735C8F	126	8763CDE429BAF015 E65D729A43801FCB ED78C10634F2B59A FB7302CE8D95461A	112	E4A3F08D25B1769C D8AEF7B926035C41 1B6753E29C48FAD0 361780EFBD4259CA	110	DA5C71E34029FB86 CD0F6A354E81B729 06E19A47FB385C2D C6EF107DB329845A	100
36E052FD8B794AC1 6BD93280A715E4FC 458BEFC69D7A2031 7290C543A1FDE68B	125	EF98ABD6723154C0 A3C9B568E02D174F 9C34B7E50FD682A1 C378B4D601AEF295	118	98DC7E04B15FA362 94E2AB07F31CD685 FD24A7C08563E91B D31F5690784BECA2	107	7DF0B15CA43E6892 9C365E4B7FD2A810 51E97B420ADC3F68 704A1ED63285FB9C	112
B3258A640D9FEC17 CB789F6D245E301A 0ACD584E1379F6B2 916B7F0D8C253E4A	122	51CD8B796AE3024F 47EC8F0B59A613D2 1359E8047D6CFAB2 B106CEF97243D5A8	111	0F416E28CAB9D357 4C916F58E03BD2A7 3278BDCF4E05A961 13F9E7BDC42508A6	122	7DF6259CEB03A841 38C6420A5BEDF791 E1AF35B0287946CD E2F74A36509DB8C1	111
8AE645C209FB73D1 9C83A0E5B217F6D4 21D9E4C768B0F53A BA4F2675019E83DC	120	BD5F7108AEC63294 D9F68351E0A7CB24 158F607EC4A29DB3 E7125A9D60CFB843	118	3F410DE756AB8C29 398EB521A47C06FD B3A4D6E8C927015F 2C571F63A48E0D9B	123	31E087FDAC49B265 9AC0352746EFD18B 4B5C0763DA1F982E F02D14C8E9A36B75	120
F93517428ED06CAB 4BD7C56A912FE038 18BA23E60CF9D475 2E08A71934B56FCD	121	657FD913CE8042BA A978ECBF416D5203 4BA105C26E87F3D9 1C3F74AB590E86D2	119	265E137CA4BF089D 85A6C7EB2FD94310 A7EF84C2610BD359 428B9CF761AED350	110	ED2B6F850A17C439 197B50843DA62ECF D835AB2C6049F7E1 10937FA64CB25ED8	121
104A639FB7CE528D E0B6C5F3987DA241 FCB574A08132E69D 8BC920AF7ED16543	126	9D48E6B31FA5C072 F461CB039875EDA2 5A3F68497BE210CD 3D1AB850CEF72469	116	86E23F10DA745B9C 3ECDF60A758B9241 E824B536F1C0D9A7 56A8134D7E9C2B0F	106	F93AD2085B1E47C6 C84A06F37D2195EB 473581C2A0BD9E6F E3C5DA0F9276841B	115
C176F28BE59AD340 671F9A40D2C53BE8 0A3179D542E6C8FB 503C2AF948167BDE	103	57F64E20983DA1CB 25D7689E43A1F0BC 2AEB01493CD86F57 CFD809E32A146B57	109	FD35704BC19A82E6 BF63CD7A98405E12 C206DB579A834F1E 89327D41BC5A60EF	112	37A8BD195C46E02F 9B350246EFA817CD 804F325E916CDA7B 1F3C45E69A87B2D0	118
1BD0F86C2E379A45 1E385D4B0C7629FA B9A064137D2E85FC BF53E7D8419A062C	124	95476E20FB1CAD38 E0DA91845C37B62F 7D94EF52BAC60381 7E8921A6FD5B430C	130	E795A4B3F2801C6D F590BA21846E3CD7 6034F5ABC987DE21 EF0249B37A6C581D	115	0C1F386BE924DA75 05219E78CD4F36BA 503B1F96C2EDA478 684CF729015EDBA3	118
927A543DF0B861EC 7B8F65DC10AE4329 DF6A98E1750B2C34 AF71B6043E85DC92	109	EB4C20D76A518F93 85DE93A4F1B62C07 AD6E89104C7FB523 C34920FA17E8D65B	119	40531D7E2A9CF86B 0CF316B59E2A4D87 A7D10CF5389E642B DF10EB452CA78936	126	F3DBC407A5E19286 3190C6F845AEDB72 B062C7ED983F15A4 26C7E1B09A4DF358	119
E4592CFDA6B38701 4AFEB72069D8C531 53260AC7419EBFD8 AD274E539B8CF106	124	3BA71D25C9640E8F CB1E63247A5FD809 39B265AFE8C0417D 027BA8C46913E5DF	134	8A47F5E209DC36B1 016F3A8C7E25DB49 6DC4A395E087B1F2 371E6ADF5948B0C2	113	4AD6C27E59BF8310 BE0516892AD743FC 14E9F56D78BC320A 48A013E695B27FCD	117
1C0AB92D45F8E763 23BDE9C4F1A65708 BE82F793A16C4D50 6538AC21D9470BEF	112	BC20D46E5A8173F9 90E543261ACBF87D 27FC86DBA53041E9 68A7940C5E3F1DB2	115	B9137DC5E68F024A 70E9631C2D4F8A5B BF5402ECAD671938 90F5B64D32A71CE8	119	E9D281657F4CA03B B2307A64C59F81ED 7A4028E35FC96B1D FC1A374895206BED	127
7F06D1495EC2A3B8 401FD853CE927B6A 81D2E960FBA754C3 96C723BD5A184F0E	121	56FA9BE72C48D301 5B216F8EDA790C34 D028EAC4756BF391 52B9063CDAEF7184	123	326E4B7FAC815D09 AF30C9D52468E17B 9F3A172B8D560C4E 0D739CEF8A24B516	112	86ECAF3470D1B259 A80CBE7423F6159D 78EF52D4A9BC3601 3F162A7D0C8E94B5	134
2830C4AFE61BD957 74E6C2AD309F51B8 D3F2CA91E46057B8 06CB4EA58D3F7129	112	3DAF68B4507EC912 32A065EDB179C84F 32A16C5B98FE0D47 374961C5F2DAEB08	101	7B05F4AE8D2C3169 E2AF04983CB5167D 73809C1EA26F54BD C8DB192A5E7403F6	112	C5B729F38A14D60E 1069B85E2A4DF73C F46CDB8AE3021795 4D693BA1528F7E0C	122
0F4DB3965218CA7E AD3F704E9512BC68 10DEC28B679A54F3 124F0E5C697BA38D	117	1F650CE3D2B97A84 C7A65E1830F2D9B4 720E68934FD5AC1B 59CAD7031EB426F8	117	598EBA701DFC3642 DF3B7A681204C95E BAFC154E2068739D 867DE402B19FA5C3	112	C0B7A32EF156D849 1E39B8750CF46A2D 7B6293AE1D045FC8 D1C26AE074839FB5	130
84EF13A592C6DB07 036F179CEA4B852D 4569182CB07AD3FE F8C92350B71AD4E6	122	F2567A3C0DE9B481 A4709CF1BDE52836 CBD6723EF981045A 4F5ACDE60189327B	127	F682BC930AED7514 FC2795B106ED834A 637E4B529F01CA8D 0DF86C7A54E912B3	110	C5DF78910326AE4B 9EA512BF6034C87D B2E753F048A61DC9 45C8ABD176FE2093	126

BD27E1539C8FA604 9E1834A062C7F5BD DCF18B4A0693E257 87A4D5BFC120E963	118	E978450A631DCF2B 17EF3280A69BDC45 D3F20A7C195B684E F06E285BC91374AD	107	ACDF450972368BE1 B2345C18760F9EDA 98F2E17C4D5BA063 685130DBE427AFC9	116	872EB0A4165DFC93 AB0618F52934ED7C 1F9E425AB08C7D63 92D08375CA4B6EF1	113
7195BD46E2AF8C03 843296DA5EF107BC 5A7D0C6FEB128493 E5D61CA984037F2B	129	7A93C284EDB105F6 2B8FE1C074D59A63 EC318B2760D5FA49 E0DBF74A9C358162	125	F104B78C5EA3D692 F81562ADE437B09C FED5693A2140BC87 1D80427B96C5AE3F	118	80B4AF96751DE3C2 97085FB1E3A6D4C2 B0D7FA5C6231498E A15F826039E47CBD	111
50E7FD418932A6BC D3AC2158F74960EB 3495C2FE10AD876B 0C1856EAB7D34F92	121	84E976A51B3DF20C B9F682C1A4D75E03 95F70BC83E12AD46 201A98DBF6E75C34	113	205BCA78F19DE463 1A790E6C52B843FD 3C1E02D97F5A86B4 AFB6291078435EDC	108	0A532E7419BF86DC 6A9C758024FDE1B3 13A0E965BF2D4C78 34579CDE1A2B0F68	117
7956F2401CD8BE3A FCB92D516AE87340 7A38BD2509CE461F 75B89160FDE324CA	126	7ACED59F23604B81 310FD5276A849CEB 1D4B68F7A209E35C BD09FA5C8761E234	131	F47B0A5D692138EC 85E7C3AB9142D06F 75269B3ED14C8F0A 874DEB5F63029A1C	120	B5FC3A7D91E48206 3B5AC82074DE9F16 85B92D463C0F1EA7 534D82F16AE079BC	118
F0AC941BD63287E5 36875DCF94B1E0A2 DE4095A7B2F1683C BD136F2A450C89E7	131	BF795D804A3EC126 E3C416FD20BA8957 1260BCA7DE38495F A42C1657EDF98B03	122	D2973CAFB8056E14 3F6C49D1085EA2B7 F95DCA2673B1408E F23DE6C4790B58A1	133	4B50A3C61F9278ED 3CB742A8F109DE56 4DAF5197CE28B306 CB536D42908FE7A1	129
6312FDC80AB75E49 3AB27E6104F859DC 56C4182E3A70D9FB D6F3B8540CE127A9	130	A52B43968D17EF0C EA8D5C612F3B9047 C278D61F43A9E0B5 5C72F984DE3A6B10	118	9C8EDBF253614A07 6D0AB2E9714835CF 8B4A317F2C09E5D6 0E98DC7F3B4621A5	132	15A2FD07984B3CE6 1C9F4AE0D6375B82 84E379126B0DACF5 7401B362F9C8ED5A	106
E2F9A14CD8B56307 92EC547F1D086BA3 6FB21037DCA8954E E4931CB8670AF5D2	121	5D612490F3C8A7BE AFC36E4957D8120B F9EC0A2DB5481736 26BEFC98D5347A01	129	648F593CB1AED720 BA901D354E7F2C68 E5601BA98723FC4D 8312E5B0AD746CF9	126	B7948F0C52AE13D6 A938726B40EF1C5D 274035D9A1C6BE8F 4021E637C8B5D9AF	122
0E1CD3BF75A89642 6C512FD347BA809E 249FC38D56E71A0B EA3F602C74B9518D	119	072EBF4C96D351A8 3A6E92CB0F4D7158 F15CA8463B970DE2 3C417D689EF25A0B	127	14C0F8A9E62D3B57 C9E730F14D56AB82 EB890DC7F5A41632 150A48DE936FC7B2	119	F54702963ADC18EB 59EF0C137D2846AB BE6520D17F9483CA E6FCA4173B2D9085	120
EAF37C45160B982D 9FCA7183DEB64520 97B8EC25360A4DF1 09D3271CFE86AB54	115	196AFD35CE4270B8 CA9BF071E36482D5 453B867FA0C29DE1 D7B2E0CF5386149A	124	9C35E4F02A6D7B81 D05A719682F3BCE4 5BD9867E4F2A301C 9B27C06DF4A5831E	117	DC158F073B9E4A26 D674F5B2CA80139E F279B4513CADE086 DCB1975460FAE382	111
BE179D53026FA8C4 0983F2E7156DB4CA 4BC5A927EF0618D3 7FEA503BC492D168	123	938D26FBA5470E1C C6A1F480E95237DB 58210AEDFB4C3796 7F1C98B3402E65DA	128	5C496E0D712AF8B3 7635D2409B81CFEA 6857F102CBAD94E3 0A548C637E9D1BF2	113	8561A2F73DE40BC9 FB7AC06421D359E8 287EF9B53C60DA41 E2C58D3A0916B7F4	129
7E50926814FCA3BD D4AF586BCE721093 0C123875D9BF4A6E E210C5973FBD48A6	118	5ADE64FC192B0873 3BFD04798651C2AE 4F70185E36CBD92A F0E39A1B6DC72485	124	CF0A6948ED1327B5 10478F6E5BA3D92C B85231A649DE7F0C C73FD9065E8B214A	110	871AC4BF6D0E2953 F4379A20E5C1D8B6 ED14BF9235AC0768 953CD48AB607F21E	113
43F208AB967CD15E 0E63BF8542C1A9D7 F3AC104B97DE5286 7C09D1E324FA5B86	120	EBA2C0F7931654D8 8DF19A50247EB3C6 6AB0157D3EF8C249 B784C6F5A0D39E12	125	0471FB6A39E25D8C 5AC4F2E18DB37690 FD5C7A46928B1E30 D2EC0731A4F59B68	133	42E768F03DBC95A1 60DB137C85AE492F A03E4DC5B916F278 5F7C9DB416AE3028	117
DEF1809A723B45C6 C63ED190B57428AF 5B7684CF9A0312DE 6ADF3257C0B9481E	123	8A243FEB60C7D591 3B64A5FD980EC127 70BC65EFD2318A94 70259F361ACED8B4	121	2CF9B8E4175A60D3 C128706439BF5ADE B3F4E28A96C17D50 EBC176FD983A2054	127	E5041CD627983FBA 36F79B204DA81CE5 6AFB8CE410253D97 71C0DF968AB52E34	133
F6439752B108ECDA 109B3AE6C74D28F5 E64BA38CF109D752 E0D2AFC3719865B4	133	386AF5204179CDBE 1A89BF02DC7E3654 5DBC0F876E3912A4 7EA3185BC42DF609	118	BD1A50C6943728EF 32D8FE9540CB716A 279F1ED8C40B6A53 579F428DA603EBC1	119	2AF316E5B7408CD9 925EC613BD04AF87 5DCA8F321974BE60 2590DC6A834E17BF	106
BE365DC4081FA792 791BA5D4CFE36028 F6B87912D4A0E3C5 5A87C10B2E43F69D	117	749EFD803B52AC16 7EB2C950A1634DF8 1F705ED2A49C8B36 DAC4E812F7096B35	116	59E8A1D627F034CB 12FCAD03B46879E5 2A34E1DBC587960F B976A4D520F8C13E	119	7138BADF05249CE6 0D91F762B3A84E5C 9DE6F07245B13C8A B9C0A4E7F16358D2	129
823C4917BFDA0E65 94F6A1257CBD8E30 D697582A1BEC0F34 693AF1E4DC025B87	139	C5671B90AE3F842D DF85B20643A71EC9 79CB105E823D4F6A 9ED3BC5F471A0826	130	7F4A5E10D6C39B82 5AC763F810D42EB9 5430E17AD2CB9F86 9DFC0E874253A1B6	124	2F61D50B8ECA7349 DC4201E368B7A95F 84762059DAE3FBC1 F36947015ED28BAC	122
36ECB0D12857FA94 A326B0EF91C74D58 76C04BF891E53AD2 D8619FA753C240BE	121	F1B75AD8023C496E 347C91DA0B2F65E8 A2B4F7CE9610853D B13A79F0D842E65C	126	BEAF6370D8142C95 0D2FC5BA7469E138 CF53698D27E01BA4 1A208CB3FE7D9654	101	0DA4C219F657E8B3 A0819E356D2B7C4F E24D5B7310FA9C86 074E18B639DF25CA	122
F6B25D7830149ECA 15A836FBCE24079D A0317BDC4862E9F5 51C4679E20DB8AF3	112	6C0E9D7AF15423B8 E158702D349AFB6C D84012EAB679F35C 2083CE5A974BD16F	136	E7F230C46BD58A91 6BEC8AF4571903D2 B719F580C62EDA43 BEF20437D68C195A	122	9580AEB36D4C71F2 9FBED5480A12367C 30B1624CE95A87FD 59F0B1348E6D2AC7	117
8A402519DBF7C3E6 480DFC27E3591BA6 E912CDB63580A4F7 E5A721603D9B4FC8	121	B23A8C1475FD609E 7ACD03FE6928541B 7C8FE0214DB3596A 89364CEBF7A2510D	111	E9CB1F8A3560D427 2E74C3F0D8A5619B 319AD02C7B548F6E 6E8F4BD02A39C715	122	285701EDB63F9C4A 5964EA1783B0CDF2 7385F940ED2C6A1B 3F102D7A45BE8C69	108
B2F9108DE7AC5634 A587F0DE49CB6132 AB6590C43E81F72D F7A134B596D802EC	120	72801536D4EBFC9A 6A3FB4895DE702C1 961C32DF7AEB4508 6B3CD0A29F71E458	129	2A8DCE93B06F5147 7B6C1382A4E0DF59 0C87FD49152EAB36 2EAB04CD395F6187	119	7C152A08F93EBD46 B46D512E3AF790C8 2F1DAB64583E7C09 B9425D876FEC0A31	141
71CD2AB5E096843F 51746E8BC29FD03A 48F962B3C1D07EA5 DCAEB5F460219783	114	7F342609B58C1EDA 81B3C9F45A062D7E E3DFB0C94175286A 057A498C126EF3DB	119	754F1B3CD09E8A26 7A2EDB9014F56C38 EC213A498D60B7F5 F9D621C84053EB7A	120	7349DEC526A8BF01 4562B937CA1DF0E8 BE68013A4DF29C75 573CD16490B82EAF	116
E573864BFA0129DC 80E472B9FC531D6A BA6CD42E9057381F		6DA0924ECF3758B1 5C13F47DA62BE980 E1CD5679A3802F4B		703DC86519A4BF2E 96C53AB08EDF4217 942EBC8D70F6A351		C13BD52A8967E40F 9D2CB76810E4F35A FEC4D23B758619A0	

740815B9F6DCE23A	130	456EDC9B3A07182F	114	EF0CA7821694BD53	134	C35A41D2670EF98B	131
F46A2B5EC1D83970		D7C3E90BF518642A		36A80D2BE4F1597C		93FA81DC0E256B74	
B8321C4EFD9765A0		12CF348590E7AB6D		0A2CD651E8BF9473		BA3F476C95D20E81	
75B9306FA2D81E4C		93FCD156B087A42E		F198C246D3075ABE		8C324D07B96A15FE	
06B4738219FD5ECA	130	12C9EB83FAD56470	120	4C8135DBA26E70F9	126	E0BD7F695132AC48	117
F73821BD95CA046E		78AB0CFE514D6293		30D1E2768ABC94F5		4DF8C125A0EB9673	
CAEB3F906528D147		0814AE739F2CB5D6		35248FA7EC09B1D6		C6D1A39B28754F0E	
CBF26D31E795408A		10A2D3C5FB6948E7		B69C8E72A45FD031		04FC351D289EBA67	
9E04AC752B3F68D1	121	C568EF3B91A047D2	137	C321B0E67AF5D489	118	9CD063A5B4F27E18	123
698B1A30DF5E24C7		57B1A3CFE68D9402		FE6D7910A8B43C52		6CE09F143BD78A25	
456BC1DE78029F3A		F735A602CE14B8D9		E496CD518B32F70A		AB78DC5F6914203E	
B97485DC60EF231A		2908A34D57BFE6C1		A809ED621FBC3745		97F65D81342BA0CE	
C36B140DA895FE72	121	F4B172C869503EDA	118	D1A259E847063CBF	124	F01389D5A24BCE67	115
3C52904B1A7DF6E8		B6485F09C12E3DA7		6A34BE821C95F07D		257F6ED4BC83A910	
1CE6A9DF4208753B		F2EA9D506BC78341		2E4063B8F795A1CD		D386EA1C20957BF4	
9FC1764EBD0A3825		95067BAC3E148F2D		6C75DEF180293BA4		F9748B1DCA3E5620	
582D47EC16B30AF9	110	CA69DFB3E8542017	115	F9BE46715238ACD0	112	C8930AF4D752B1E6	132
2BA3FDC16E708945		AB415F0793CED862		2CAFED0763189B45		CD7B2EA56F039418	
E93B8652FD4A1C70		2A9ECF70DB814356		A297F1B06E3C854D		30F76D5C4A2E189B	
D1B78396054EFCA2		F359EA84670C12DB		C13680F574EBA9D2		B5C9F8D176023E4A	
3E96AFC871452D0B	123	F5320A17E94B8DC6	124	0A78E465C1D3F29B	129	EAC836742FB915D0	140
C573BF60A8E492D1		0F1725B43CDA698E		D8C15FB036274E9A		754A82BF93C06DE1	
6CB9A28D0415E37F		749B8FCE6A215D30		27EB3DC91645A08F		3C0F54DEB69A1872	
2AE93D8B5471F0C6		2E1C40B3ADF67859		1D57389C06FB2E4A		ADF657280391BC4E	
BA58074DF6C129E3	126	5A1F89B42C60DE37	111	20FE1CB4AD938756	118	347E89B5F0C6D2A1	109
B1C28AD03F96E457		906DF45231CE8B7A		4901FB635C2A8DE7		4CAB85160FED7392	
03CB24671EFD9A58		A4703195826BFEDC		3098EC1246BDF7A5		371B650D8CA2E9F4	
6B1E0328D759A4CF		1D06AF7359C4EB82		7C26D15F8E94A0B3		D94675F1EB0AC382	
E19B3D0F45A7C286	126	C83295B704DFAE16	130	56F914EAB73C820D	121	EA30F42C8967BD51	123
28DB741A936CFE05		5FBC9761A280D4E3		0CFA3E9B2857641D		74E69DA530CB28F1	
5723A1DBE06CF498		420E7AF5986BD3C1		3F67EA5C8194D0B2		7DA059623C4E18FB	
E8A294FDCB176350		B31D45AFE908C726		98F56C710EAD243B		C6E0FB94D73A2851	
0C6ED79F1B34A528	117	342018DF975ACE6B	117	97D8C06BF4E123A5	114	39FCB701485DE6A2	121
DB5148E69A0273FC		3BFA8149C6E07D52		46B0F13D7E89A2C5		CD13590A72684BEF	
80C1BEA256F374D9		7BDC6FEA81302945		B4FA0351D9E86C72		4BDEC9126A3F5708	
B49A607512FDCE83		BC52081467E3ADF9		910F754D8ACB62E3		68052C3D19B7FEA4	
7510C3AE498FB6D2	125	93B5170EA48D6FC2	111	40695372B1D8EAFC	118	02DCAF1546E93B78	133
2F5A196BDCE70384		3ABED05891274C6F		2E7613B48C09AFD5		94EB53D0C68A172F	
6315A89F274DC0BE		795E86ADC204B1F3		CE2F680A7934D5B1		E832A47B0C96F15D	
20AC8B156E3DF947		F7689E41235CB0AD		F132D94CB68E70A5		85FCBE7A692014D3	
E5724A80691BDF3C	120	FA8B72C03D49615E	105	DE629AC87B3045F1	119	1543C7AFB2089E6D	129
F3750AD91E2B6C84		0D82FA1B67E5394C		7C1980FD43265AEB		A067DE284953CF1B	
B03CFD6A74E89215		32C80A7EB496D51F		EB02D9814A3F75C6		B0A9D1C7E43528F6	
2974A5B3C18FD0E6		83BD2A670E4F51C9		D5C6B0138927AFE4		B402D8617E5ACF39	
DAB19F07352C46E8	129	8B729D651AEC40F3	136	8C40F165739BDA2E	119	4CD8290B17F3A56E	129
D5E9648071BC2F3A		17D0FE5689AB42C3		4EDA6892C035F7B1		96E75DA80FB23C14	
82B76DA0E593FC14		B738A19E5D0C4F26		0B1859F4CD32AE67		97FBE0C52D6483A1	
1BE40F9C2A76385D		DA047F6B3921EC58		9A6D483527FBE0C1		DA60C51824B9E7F3	
71E9FB52D304C86A	134	FC7B2054631ED9A8	109	AE72D8B60C451F93	114	D30425B1679ECA8F	122
E93587A4D20CF6B1		976CD5EA38F04B12		C514068AD3BF9E72		2915CD68FA47BE30	
0BAF1E62D84973C5		962840BA1DEC3F75		E05A6DB479FC8123		5B9C781E63A420DF	
C297B08FE365D1A4		D59F2781E6CB4A30		91CB5EDF2A603478		FE46A1C57BD83092	
C34A718E695DB02F	124	EF4C3A056812D7B9	120	54E0DCA2691BF837	115	65F0B3E1782CD94A	130
713D9F04A8E62BC5		4C6FD18B597302AE		89C24310F7A6BD5E		EC3B40ADF1287965	
4D0E8F6537A921BC		397B4DFC561208EA		AEC035641FBD7928		CE4B8F57962AD103	
329EC15DB68704AF		4261A503E8FB79CD		1A39756BC4ED08F2		3C9B74A86012FD5E	
CEA47B3D829F5601	121	1405FA23D98CB7E6	120	7CA6FEBD12439850	116	B6AEF9C138745D02	123
7039B8F4AE65D2C1		D64ECA235FB18097		2B9045761F8A3EDC		7D68A3E20CB5149F	
F1240EC73856A9DB		1E6058943AB7DFC2		C17069D5B8FE23A4		2ABC746380F5DE91	
CE42DA81397F065B		A3FBED1045296C87		541830D9AE67CF2B		F2403B9CE8D6175A	
BD972E4F0513A86C	128	5FC20E8BA6137D49	122	2FCBD135A7E96840	112	714B59EF8A6C30D2	117
48E561D39CFA270B		7FD21498EC0BA563		2A839E5D7140C6BF		9C4DB68F0537EA21	
CB0E75D1463F28A9		53C61290ADFB4E87		9F085D1C37EA4B26		E7D430892B61AFC5	
F60C82D351BA74E9		B9023F457AC86E1D		6054C2173EBDA9F8		40CD76EF2391AB85	
FED43890A276B1C5	126	BED547921AC8063F	112	046FCDBA5E713829	122	20B5ECAF3D468971	127
D9364A81BCE52F70		3F1E5B4D70CA9286		A21063FB4D857CE9		6EBCF04A385179D2	
4F1B6AD3C8E20759		AC14F52D067E38B9		048A96CBED21F573		E21083759C4B6DFA	
856D1BA03C7429EF		C348B76A2D91EF50		B3C219DAF7E54068		047BCFE528961DA3	
DA5E6B18F24079C3	120	34D96B5A107F2EC8	113	F7E862503C1DB49A	130	3201B467F9AEDC58	123
65DA032B87C1F9E4		D3C4758FB9210EA6		F1C532D4A86907BE		73A6B415C8FD20E9	
3187AB4F965C0E2D		DC8670A4B9E123F5		429B5A3DF60178CE		26731D9B5CA840FE	
B15F827C30DAE496		BAEFD029481653C7		64ECD89B7A5F3021		C5D60FB47A2189E3	
2A596147EDFB38C0	114	08DFB96214357CEA	120	90741EAB3C56DF82	143	AD5FB8C407213E69	112
163F0CD542BA78E9		96C28EA07BFD1453		91F72805CB4DE3A6		6B5DFAC12E983704	
D98F5B74A1E20C36		650A8731FBE94CD2		0782EF195A6D34CB		693B0C78EF254A1D	
9E52AF0186CD34B7		8A46E320B75D9CF1		A729C8ED0F561B43		5B2F9ADE0C637814	
BF6E87921D0A543C	114	2FD9B1E5874A036C	130	0DBA9CE54132687F	134	C0D46E9B21F358A7	103
4B607298DAF3E5C1		41E3DAFCB5927086		9A30DE48612FBC57		DE0561972B8C34FA	
63AFCBD52108E794		5C6ED17F23A4B098		91A4675D0CF32E8B		B870F5469A3DC2E1	
145E736C9D8FA20B		6E154B390A287DCF		D6C57E40A29B318F		4539CDAB827106FE	
D9A28E1F460C357B	121	AD527B06913C8F4E	117	7C3206189ABD4F5E	107	EC7862B135A4F9D0	128
268971AFC35E4B0D		AC0FB7E653498D12		8A6FE3D7419B0C52		2BAE734C8FD96105	
849EF125BDA63C07		75862409D1ACB3FE		92C3B76AFE10584D		FC29ED60BA781354	
FDAC7054BE392681		E6BDC7F942815A03		624FA987D50BC1E3		8BF276DC4A3E1905	
64D13AE05278FB9C	122	839E5BCFA62D1740	134	C17A64B90D8E5F32	119	6B508CEF213D479A	132
6E190F482C3DAB57		17C460AD58E3BF29		BA7F842CD39601E5		053FDB2417E9C68A	

23647B50D91E8FCA		7095C41FBE32DA68		624F9AE875BDC130		E83CFD2A6140B957	
F927D830E54BCA61		28695C703F4EAB1D		D3E6C507F28B41A9		BD32F456891AEC70	
40FB6DA97C85E321	115	6D8C7015AF9B342E	113	A1769DEF243CB058	125	8BE79623D50A14CF	122
D73B45EC198A2F06		8502A34167C9FBED		28A90ED1B67C3F45		09CB3624D7A81E5F	
F532E4107B98DA6C		13658B9FA47CE20D		1F39C0A482D6B57E		E897A4DFB032C156	
79D0FE5B8A632C14		A259ED7381C4F06B		140ACF8D325B69E7		0F9B36D7142AC8E5	
BA62370DF45E81C9	114	E9B7A15D2CF40836	122	A72ED38F94065C1B	119	70289FED3A65B4C1	131
7604F89CAD3E5B12		34BDFA71E5892C06		FE4789A2C16B53D0		93062CBE7F15DA48	
162A9703BDEF45C8		6BA09375281DC4EF		4097CF6E1285AD3B		B9A451F03DC7E826	
42C7EFA8D106B953		487FB569C203D1AE		1FC4AD0B53279E68		5A62DB1C3798F04E	
1FB48E369D57A20C	130	C74A59036FD8E2B1	119	5C8AB30E21647F9D	137	B897C46A3E52DF01	115
C1A260E379D854BF		6E8A0357FB19D2C4		0A4F923C5D867E1B		A32F0851B4C97ED6	
BA2F3D16058E794C		67D8A902BF415E3C		2F071A8E39B6DC54		312E685CBD0F9A47	
9CD12356E47AB0F8		50148F2ABD7E69C3		018EDB325FA69C74		928BCA0F754D13E6	
8BE5AC7362F091D4	123	1C39A405B7862FED	115	1B936E0ACD8F5742	105	42F37EDC56098B1A	124
3AB9C7FE8641502D		F698120DBA453CE7		3869F0142EBD7C5A		65BAF4E328D09C71	
E47038BD1A62F5C9		36BEF10C8A79542D		3D47589C2F61B0EA		F634C8DA15702E9B	
E90CD81BF23A5467		AE749C5621BFD380		9C20F6473EAB518D		082C149E6FA357BD	
BC408DFE967123A5	110	BA69D840E325C71F	124	3B1A62D5980E7C4F	124	859670F13AE2DC4B	99
C82943E07FAD65B1		1274389FD6E5BC0A		D70FE591A6C4283B		5F362E089D4BC71A	
A8C3E5BF7D296104		64A5F203B98DC1E7		8AE19C3F25760BD4		984ACFE675B310D2	
70BD2E916CF85A43		3E0B87964DF51CA2		64CDE85F30A17B92		EC38F4A56B7192D0	
A0D7F49E26C8351B	115	276CB045F8D391AE	121	D086375EB9AF1C42	123	1D09FE326BA8745C	124
E3CA290641F87D5B		B05E68312AF7D94C		137D9A2EB0F45C68		96B20C34EA185D7F	
F6097AE23CD81B45		C4B9E7365F2A801D		35FD0C64A178BE92		840AFE13D9B56C27	
498EBC71D6A320F5		628195FEA430D7CB		7095E2D61A83FC4B		10A3569B784FCE2D	
B6A9DC071254E38F	110	63AE4D7C81F905B2	123	8F07C6E9B42D5A31	109	6245907C8FDBEA13	126
3FE8AC7B41206D95		CDF401A36792E5B8		2EF03648ABCD9517		FE412CD6A359087B	
F62C0E39AD54B781		6AB05DF984E273C1		D68EF0B15349C2A7		89203546EF7DCBA1	
632BF0C14DAE9578		4FA65B8EC1D02397		97058E3641AB2DCF		C26A493E0F817DB5	
B9185CFE7026A43D	119	95A71FBEC348D620	122	8932B0E4CFA157D6	108	D5B39ECA2F147068	117
546AFED2901C8B37		9C1E385B74602AFD		D310AC74E9BF8256		D106C48FE2975B3A	
6FE0958A2B41D3C7		B369F1D2870A4CE5		4FD23BA0E81956C7		574C86DEA90123FB	
98201FA7BDE643C5		7B5E1492A0F38DC6		C68B315E7D4A209F		E095672AF3CDB841	
B56C0FEA49D78132	119	FB251CA7340E9D86	130	C80A79DB14EF5326	122	6FC4A879EB31D250	108
EFD7B458C1A96320		1A435C72D0FB9E86		02D573C8F96E14BA		C4A6F3B871DE2509	
8C76DBE01A935F42		D08BEA7659243FC1		20364C5EA9B7F18D		9FCDB65410EA3872	
C7F98EA125430D6B		6182FD93EA0547CB		C6F4792E10A5DB38		10F4B8C7E3296A5D	
0983CB51D4F6E27A	118	5AEFC68D9372041B	117	E51D3AB470F8926C	114	06E1A7C832BF9D45	110
4EF2B971C6A3D508		02B8AD6C397FE415		5E80AFD629174B3C		8CD52B73AE0F4916	
4CD2581FE9A03B76		8206DCBA9F7E3514		8E76F534A1B2C09D		57C0FB1A2D6489E3	
8B2E30975DFAC614		B32F60195ACD784E		09C651FA27E3B8D4		ED8B43AF05C27619	
3586F2ADE4719B0C	110	FE284516DA379B0C	122	7B3902C416A8D5FE	123	4F978312ABD0C5E6	116
731E2F6C5B904D8A		9FB18C7540EDA362		4DA78F2C03569BE1		BECF9D0317A86254	
08ED1A4F759C23B6		E4FC185207D6AB39		A614B9D70EC28F35		E3ACD42187B9F056	
D52B86E7F431A0C9		08DB261C4F5A973E		92685CBA4EF173D0		1FDA34BE896275C0	
1AEF9C7243B5D086	112	75B8DEAF09C13246	124	76EFD0135B2C948A	124	3D59BC72A684E01F	118
F196D83E0C4B27A5		7814A9320E6CBDF5		09BF27E3468A1CD5		EDB2365FA781C940	
49C75F63DA08BE12		763F409DAC82BE51		B7319650A82FCDE4		FA0E7CB135D82964	
058BA4C67F31E92D		310AB2F76C9E58D4		42B3EA0C7D6F8951		A1B73546CEF0D892	
B01EF876CA943D52	127	B2916AF043E5C7D8	121	D52B10AE3946F78C	118	8EFD73B9542A60C1	117
053DAE927FB81C46		E6B19340A72FC5D8		69D8CA014375BF2E		E3C762A59840BD1F	
93D0A15CEB284F76		53A9847C61D0BEF2		7A930214E56C8FDB		FC1867B30245E9AD	
3D902B46AEC8F715		408967FBDCEA5231		CB5F762E140A9D38		C5D36EA810247B9F	
6D98E1534B70CA2F	120	9AE146F580CD723B	117	64AD2E9CF1730B85	132	3D6B89E0517F24CA	120
0365EFB129478DCA		92DF680C345EB17A		54827EC3B01DA69F		5EF9DC7021463B8A	
DA90EF6B413C2758		EB6DF7180C4A3925		C45D062E1783B9FA		DBF624918037ACE5	
895EAF21D067B4C3		3D04E8F7251B69AC		1CEB629540738FDA		7D246EBAF153C809	
C29D10AB34E6875F	120	DA428E7C3B0F6951	117	AC415908236BED7F	122	B13F25D9C87E0A46	122
98F5CA7621B04D3E		C3587241FBE690AD		6A3C7B5192D4E80F		4D59386107EBCFA2	
DE52F198C60BA473		31CA6705D9BE8F42		E690BAF8D71235C4		3C06D2478B91E5AF	
9735028CE1F4B6AD		3764120CAF89E5DB		A801CE3B5F6479D2		5A348CB9E0FD7261	
FB69752031DEAC48	127	719CB485ED0F63A2	145	0DC792EB658F134A	114	AC4961F2E835BD70	130
BF904DC32AE71865		4156A2B8CED79F03		B734C1D8F09625EA		7CF134A2DE980B56	
850B3D1AC62F4E79		D728150ABE93FC64		DE1B70F5493A862C		476B3052C18D9EAF	
2063D1594FAE8C7B		496123FE7C05D8BA		1A98C6D2370B54FE		AEFBD23C14097658	
FC04E832B76AD519	134	A36B14D5EFC29087	119	F43C0A51B2697DE8	123	E8CB9402F7A156D3	122
6B1ECFDA07249538		ADB93487152EF6C0		C730A8EF1B49526D		CDB0E92147F85A63	
C50D91A23B87FE64		BC9D537EA1806F42		6ADE345BF8712C90		7D3A24B98065FCE1	
EF012DA97B6C8345		87A614FBE59C02D3		42B59C3A6E7F08D1		0FB286DA9431EC57	
27ABE6F1D38095C4	119	6E9F1C72AD48B305	122	C1405E8B3FA7269D	129	EB7C4302F61A598D	117
D9E1F0625C87BA34		6FD78EC9420A5B31		4F8B706DEC9125A3		EB2A15F809C673D4	
F5073D8A6CEB9421		853C219EBFDA6704		B81F0AE94C65D327		D0B5273CA6984FE1	
B1FC5A0263ED7948		7E1FDA85C239B460		3F5DB162C7E89A04		3F291B6E0A8754CD	
BA7685DE243F01C9	126	018B6C4A7FE9D235	120	85D6C34E179F2B0A	130	740EA8129DC35BF6	134
8F0CE7BD9624A513		95D64CFB38A2E170		DE281536B90ACF47		A9F6B05DCE147823	
AB6E1DC574238F90		572A6941D8B0E3CF		01BDE8763924FAC5		147CA60E9B83FD52	
AB9260FE435CD871		6A42E1D3F90578BC		E1DFA2B03496587C		7A013D98E4BFC652	
C528E4B3A1076FD9	118	67354AF08B92D1EC	116	503C4D9E1FAB8762	123	384DBF6271905ECA	124
3529A1E70FC4D68B		DAFB817530E46C92		913F0E4C6B7528AD		2D13FA60B5879CE4	
1B0DA268E5937CF4		3267DCB01AFE5984		3F64D21B590CE78A		15CA98E03F64BD72	
197E52D80A6F34CB		BDAF07542E83916C		53E0918BFC6274DA		84B76DC301F9E2A5	
6B84DE9AC571023F	130	8150CDB46E23FA97	127	1AC0FD5B98E63427	123	5F2B716094EC8A3D	137
F890235CEDBA1746		8630DEBA47C1925F		F74D051AC68E39B2		DB1946057A23FEC8	
A37C0415D9F268BE		63D7B4890E2A51FC		0386F94E25D1CBA7		57F063E2AB8D4C91	
2A6CE958BD13740F		6C310E5872ADFB49		2F1B5D9360A7E8C4		736A95FCDB42018E	

85406FAEDB2C3197	123	65D3AE2C7498BF10	126	E42CD19B5837A6F0	126	15DAC038742EFB96	120
E10C4D2AF569B387		B7EA1863942D5CF0		A19863FC57ED402B		4305AFD8E16CB927	
7CF9A103254BE86D		FE1465DC79B8A320		D2A3481B605F7EC9		C04B72FED6A18539	
267A1905EFBD438C		E6B0A51839DFC247		F1B75DEAC4893026		8021C6AD3B9FE457	
D82453A17E09C6BF	130	217EC56BAF3894D0	116	29C8D1F47306EAB5	116	D9A1CFE84B207563	120
A9D0B41C6F7E3852		25A370416EC8FDB9		0582AB3D76FEC914		C17FA90EB6D32548	
A1260EF984C75B3D		504B8E3F19AD76C2		1A38C627FB509E4D		A5C8061372EDB49F	
A51396F4BCED7802		8B70C1AFE362459D		51A0B39DE8F627C4		69DBC2FE7154830A	
D26AE37058CBF419	132	AB5CDE64019328F7	109	D0E47326B19CF5A8	119	F2D18AE37560B49C	120
90EC7D2F138645AB		94CE175D3FA8260B		C3D1869B4AE250F7		41AC79B23865F0DE	
FCB92E18574D6A30		5F89B13C6D0742EA		139FC8EBA26057D4		39B4FC518276DEA0	
7129FA0CE3856B4D		7B3FD825CA460E19		FC1957AE8460DB32		BE1F48902D67C35A	
6ED1A8B720954C3F	126	28D53E71A04BC9F6	116	4AC01B68E2F73D59	122	12C39F765AEB8D04	129
D9A150F42863ECB7		610CA872BF53D94E		0FBE198C634A5D72		64E07F3DBC2A5918	
3B01C87529EAD46F		B71853D9F62AC4E0		7BA2EC140F85D369		8241CBD5E3F097A6	
3F29E5DB84A6071C		13E89A0DFB576C24		D34B8561F0EC79A2		297AC065F1B38E4D	
C214DA0E35867FB9	126	2147E9F35CABD608	135	C8BF6904D1A3E527	113	51479AE2BC0D683F	116
6D19CF8E473502AB		0F9B2D8E735C164A		CE7A6D4325890BF1		15FDEC4B6892A370	
4CB1D3502EF87A69		F4C361BAE2709D58		7590ED4A86F2C3B1		DFA4E3769815B20C	
5A1ED8F63C497B02		5C12B73F864AE09D		913FCB560A8E27D4		83105AB96F2DE74C	
F7DE8CB10452639A	106	39FAEB6548C2D701	129	8B1DE706952CFA43	118	D5B069C78E2314FA	126
981F4B6C72A0D53E		EB32D90C1A84657F		0D35F497B621C8AE		74BEA60D25C839F1	
7FBC589ED34120A6		50E8F4D91C67BA23		E1AB87562CF340D9		98027F6DC1A45BE3	
BAE4F8156D9073C2		A5674C02F931EB8D		2E0ACB165FD78349		2A04C69EB17F853D	
A739D0EC41F6825B	117	C136B2FE07459D8A	112	EB5D6A12FC478093	120	806C9D51E4A2B7F3	122
B79FD0382C1EA465		15FA2B9EC047D836		320FD961E58A7BC4		7C53910B482EAD6F	
02DB695EFA4731C8		692F83DA01B57C4E		5D94F382C176AB0E		F8BA1E6D253479C0	
ED4BF25139860AC7		B1C9308F247AE56D		B67D03C28A5F41E9		F7380ED4A9C21B56	
7CB5D6F931A042E8	125	6E5714089C3ABD2F	118	DC3681B5AE74029F	124	3108769F4AEDC25B	117
E01C653874F9DB2A		608F194B72E35CDA		ECA682015D4937FB		A2B051D4FC396E87	
2E75A49D0368BFC1		90EC15B32F8746AD		E2DA0CF348B59761		26B5F981E3DCA470	
A570BCFED3841629		4C15BD83F0679E2A		81259EA73F640CBD		5A34F09867B21CDE	
15D803EB7A2F49C6	130	1F720B5E86CA34D9	122	8BFC764D3E19A520	108	E2A53CF7491B806D	137
AF14EC3D7082B596		8FA9D37E12CB5046		E8712A6F3D95C4B0		7F59461BE2830DCA	
1AE435BF6D29C087		DB368A0471FCE295		C42A9E530B8D6F71		1C09A83ED7BF6542	
3174F6E90ABD528C		7DE9F1634A208C5B		D9F274A05B13CE68		628D71EC4A95F3B0	
64705132C98BAEFD	117	734FE5A21BC968D0	120	39D6B1FE8A254C07	109	AED9F01C8472356B	113
13D0594C86B2A7FE		74B0FC8E936D1A25		60E3FCA4981D75B2		1340F8AEC62795DB	
D584B3F29C76EA10		F10B983C26D745EA		4FBDC28E63795A10		CE15436A8F7B0D29	
4E720B3A568F1CD9		38FB1A9DCE452670		8FB645C2903AE1D7		4F5783C2DE1A9B06	
4CF5290D7A8B316E	127	B013F892DC54EA67	117	150B948267FACE3D	131	DE6C2F07891B5A43	108
C0F195EB7A36482D		6A1749DB308FC5E2		2A96CF3081DBE475		BEAF07D85C419362	
5794A2E1D8FB60C3		E0FCB7568A239D41		C2F387051ADB469E		1653B89AEC407F2D	
945DFE6CA0B31278		C9AE713062F854BD		632C19FD08E75B4A		AF27E1698D0C53B4	
8AF742E650D91C3B	111	05FB3D16E74A89C2	137	D3C9F642B80E5A17	123	2A163D0F87BCE549	110
9B2658CD0314EF7A		654E07829CB1D3FA		C372D9B5E01F84A6		7208AD1F9ECB6354	
7CB26D1AF0E53894		C950B78FD164A3E2		B401276F8D3C5E9A		C894256A137EDBF0	
62D380EFC1A79B54		2109B6E58F4A7C3D		FCB546E9031A27D8		EF71BC2AD5904368	
25CE1A7BD603F849	122	2F41789B3560ECDA	124	76FC2AD345B891E0	120	0CDB782319AE5F46	126
AB419F2ED6C58307		7956102D8CFBA4E3		DC9BFE7482A63510		05C9861DEFAB2437	
7F50D16E2B948CA3		F4BC159AD32687E0		50DF9A82E1C6743B		B4A6EFC2D9831705	
2A059B437EDC8F16		8FB5619E7A0C423D		A25B8EC3F49701D6		C7E1D46A2F0859B3	
B1359A04FCE86D72	121	A7E3F021D58B9C64	125	2F7E5B9306CA48D1	115	E9D5A14C607F2B38	111
26A4D09F7E51B3C8		64C5EB208D17A93F		2A58039BC14FD67E		60FC9AB5731E284D	
18BAE426F0573DC9		9F8BEA6C7132D405		DBC5E096187A43F2		3E92FCA7B5614D80	
2F80D19B56CAE734		6E4809A7DFB3251C		8EB91A052F3D764C		8E0BF7936C4A251D	
752146CB93A8F0DE	113	C3715208F9AD4B6E	125	4819B72EA60C5D3F	126	BA32EC645FD17098	125
FE16A958C4207D3B		F6572A8EC49D3B10		3C91B840F56ED72A		A538E40C17B96F2D	
D2E0C518AB3496F7		50AB43E82F6D7C91		FD29BC173EA56480		1FACD29637580E4B	
590FACB1E4863D72		364FCE278D190B5A		8946B523DC01F7EA		CF19D4253E7680BA	
18FCBD4E976520A3	126	81E2AC9543D6BF70	110	D23869CA5B71FE40	126	AC109B7E8D56324F	120
93ADE7B481C506F2		2F8EC4395D7160BA		B4A209165ED38F7C		D26FAB50E49C8173	
3A1CB87F05D2E469		A10896DECF5237B4		6F0C312954ED8BA7		4F205386AE7DB91C	
6F52D73849EA0B1C		40CE7DB1839562FA		F6CDE5970183BA42		D60F3A5B1C9E2748	
A2041BF7DC683E95	122	91246B7DAECF0538	121	F6DB3C801E4279A5	116	519C8FBA074E6D32	133
9DA42F831E06B7C5		E09FBA128647D5C3		1AC0F9678D4BE523		B5A8D276E3901CF4	
95462C73EB1A80FD		8F40CDBE2576139A		3F91A84E2C6D57B0		9DA13C07EF25B468	
86514AB903ED2C7F		D2F8A6B1E73C0549		3687E90DA1C45F2B		CB4712A9FD865E30	
9A27DB84EF1063C5	116	32A7684F50B1DEC9	114	EC37480A592BFD61	109	A84761F35B20D9CE	117
94650E2C137ABFD8		F750A28413BEC96D		AB5410E3F72DC689		9CD4B21A53E0F687	
8A41B720D5ECF396		293B54C6FD0A18E7		20678E931DAFB45C		B3E6F2C0A871549D	
79F342056DA81ECB		0A17F69C3ED85B42		D024F58AB73C6E19		48DE2F710C9563AB	
B8A2103FE7965D4C	132	CF8AB9160435D72E	117	6D81EC023FB479A5	120	DE413F86BA7C9502	133
DB3FE76C2859A104		C0E12B9AD378456F		A4F20D593EC167B8		CBEA826540391F7D	
4701AE5FC63D28B9		28D6C9405B173EFA		0C1FA2485D73EB69		0DC53827A6E9FB41	
ADF2E64B031C5897		A8C76DB293E4F150		5F287ED6A93BC041		CF45392B86E1AD70	
DF95BE12087C43A6	122	5EFCB0642A97813D	119	290768BA5EDC34F1	115	49AECF0315D672B8	121
7EC08F9A54263D1B		9042DCA65F3B7E81		C7D6A4823B01F59E		64BD80AC571F293E	
8F563C1AEB0274D9		7EDF2516CA3409B8		93CF586D20BE4A71		264E5F1DC8A3B097	
BA0CE16827F4953D		F76BD98AC341E520		1E2C93854F6BAD07		1BFEA658D2903C47	
895CDA0461FB23E7	119	F165AE47C938DB02	123	453F7B91AE280CD6	112	62BA4C715E908F3D	111
0B53E47618DAC9F2		5E46F78193B2C0AD		AE489F217D60C3B5		3B9AEC81257604DF	
1CD098E76A254F3B		85CB9367AED4F012		F3710E25DA9BC846		50CD839146FA7B2E	
F831C7D0A24569BE		84156A9FE2DC70B3		ED2AC7385F9B0164		D7F8519EB63204CA	
589A6BD730CE2F41	125	E5F30C697B8241AD	123	B168703FCEA2D954	125	5E98CD016A3FB427	119
FCEDB69A47083512		128AFB094DC76E53		0B64A517C3DFE289		316E927CB58DF40A	

B693A48071FD2CE5 49B7E283CA15FD06 672EB8391DFC0A45	132	2483EDAC57916FB0 EC38179BF20564DA 8709A314DF265CEB	111	E9620F58C14A3DB7 23FDE48690C51AB7 095873ABF1EDC426	130	18AEFD623B54970C 3B96D0871AF4EC52 DE82407AF1C3B569	114
2E4530B67DF9AC81 609C5D72E4F38AB1 FBA31ED548729C06 3E0F7C4AB89D6215	122	48D52F6B9AC1E370 105E8F7B436D2AC9 79C6513DE824B0AF 6D1A39E4BC078F25	116	95D4B68A20CEF173 7FE0B291DA43658C 95C846EF1B2DA073 564B12098AF7CE3D	113	42F3E1087BD5A6C9 C41079853FAEBD26 28B0731ED4CA95F6 2CF94518ED7BA360	128
AB75FD2461930C8E B153C6D29F84E0A7 20A91EB743D8F6C5 9821B30AD5C4F6E7	127	F09814B7C25EAD63 3A8761EFC2D945B0 75CA6418DF039BE2 D026E839C1A7B5F4	135	F2BD0A398CE76145 3FE4D718CA96B025 AB2F174E95D806C3 7EDB2F45A9C80631	125	2E8CAD9615F437B0 8547FDA32B10CE69 593D2470186BEFCA 3E2164A90D85B7CF	120
9F0E65327A4D8B1C 4F732B1AEC6590D8 078E5AD2C4619F3B 978C14AB35EDF602	109	C2AD6951E08F437B A76098345CDBEF21 1D59FACE78630B42 7410ECD5F36BA298	95	FE82BA15734C69D0 012D947836F5ABEC 5BEF1AC27864903D 91A36B45F07E82CD	123	08C5712DE3F9BA64 56EC81A092F4B37D 743C8650FBE91DA2 3CDB84AE16F27590	114
74BC0F85291A63ED 681A7F5E43C9DB20 1365720BD4ECFA89 B0EC715A2683D4F9	124	1C53408AF976E2BD 0B26CF395E1A4D87 20ACEF38591D67B4 82F6E0AB143C57D9	124	BA4D6738C10F592E 8A2F4BE6305719CD C80AE174F62359BD 860CD2715AB394FE	127	7BC48AE9D20365F1 FC542E8A1BD03679 B0EA8F267451C39D C5A2F1B40369E78D	115
2E5C08B739DF1A64 E386DA7F02915BC4 09D682F1C4B573AE E2183947FCDB65A0	112	53CB7098D1A46FE2 3A2EFB0156798CD4 E34C6F29A501B7D8 74E19D6FA30C852B	119	127D3BF5496CAE80 3FC186B4A0ED7592 BD52079AFE164C38 897CE46D3512AB0F	114	74D13ABF8E259C06 04673E21ACB5D98F DA53B81FC2E67409 E357B816C29FD04A	118
D23CBA7F5098E146 61E74FA3B89025DC D1EB08F6537C2A94 A1C8E4BF6D023795	112	D86AE3F924C71B05 3078BA2154F9ECD6 35179426ACDEF08B 86C795FD2E34A1B0	122	70812A3B496DCEF5 89C62357BA4ED01F 841CEAB73265DF09 0386F4127B95ECAD	149	184F0639A7CED2B5 9D1C567F8ABE3402 26570FAE84CB193D 8D6F47B093A2EC51	111
46025BEDF739AC18 E3084A2D579BC61F 2EC9D43061F7A5B8 1A53D4607CE2BF89	116	AC57E01DB649F823 0CD8456A39BE12F7 DE9583A7B06142CF 9A20FCDBE4156837	117	2C4BF0D6871EA539 2C1D5684BE7390FA CEB954213A8F7D60 7BC5923A01FDE648	111	4A160CFB527389DE 84C05372EF16DB9A 0F58CB14DEA79632 23640EA9CD5B7F81	103
8A6049B5FC23ED71 C7A8123D065B9FE4 F0EBA21D86479C35 C93AB51F62D47E80	128	4B0DC285E1A3F769 5DBA7390248E6FC1 A13269F78D0CB45E 6C345A70F8D2EB91	115	DAB65FE402917C38 5A948B16D0CF732E DA84526E7B31C0F9 3FB08271C6AE495D	105	54CD723A9EF806B1 9F07B28C63E15DA4 13EA7D0246985CFB 8D64E0CF137AB925	106
7A54DB98F021EC36 BEDA30967FC14258 0AD43C918562BF7E A627E04F1BCD9835	130	4AC187D3E0925B6F 95C0742ED13A6B8F 182647F5B3CA9E0D 72BA51E30698DCF4	119	68F3B1D740CE259A F078E463B2C9A15D 89137CE04B5D2F6A 9085ECAB213D7F46	108	8FEA0B791253C46D 0F76E1B53AC4D982 E7823109A5FCD4B6 3D98140B5C67AEF2	111
39E05A6F4DC812B7 A94E60F537B1D8C2 E2F5C6741308A9DB 1D5AC9BFE2038467	121	896307ED12A4C5FB E3DCF57649821AB0 C6FE13A547892BD0 19E6435DB0AC782F	112	4D680159FACE27B3 2E954B78AF6CD301 6A584FD91E3C70B2 A7501C39BE2D648F	118	6A51239FD84ECB07 86410C359FE7AB2D 6ABDEC12370F8594 04BA6E92D8C5F317	121
DC0F763129BAE845 EF08CAD926517B43 E632F5C4908DAB71 5C7B93D0FE12A486	124	B493A18C62E05D7F 34D6E5F9B2087AC1 CF46798BD3150EA2 378D2640F9B5CEA1	123	D9A7F8B10C26453E 4A6EC87290B15F3D 78BF1E59D43A260C 83A6E017F5CB492D	129	784956A1E30BFD2C 183D046AFE257C9B 9C547BFED0236A81 92E4608F1CD7AB35	120
5AE79C0B81F2D643 F9632D4EA5B087C1 470F56DEACB93128 EB5A9C41F2D60783	120	6908E5F24A1D7B3C 63DB471F258A9CE0 EB3F6708249DCA15 FA3E2C8DB4075169	116	2CEB5397FD64081A 870F3D9A2CB4156E 23BFEC89174D065A B6F8C134D072AE95	120	F1AD5680E329CB47 81A694E2B50C3F7D 0364F89A1D5BEC72 7E5348AF9B1CD206	116
10AB873F529CD64E CF8159B3D06427AE A6950ECD47F328B1 9702361CAFD45BE8	115	2D65FEC4B9801A73 D9E170642BC3FA85 827640DCABF53E91 68E3A7D9045B2FC1	129	A2381950CB7DEF46 BD9F5743128C0A6E B032789AD645CF1E C4EF023B5AD87196	120	FEB2DA304195C786 05368B4FA712E9DC D02E1CB34F69A857 3D0752814CAF96EB	113
E32C681D9A475FB0 9D8B71CF0E256A43 FA4E065732C891BD 381C5DFA47620B9E	119	1C703B4F8A9DE625 C039AD4B681E572F 8CA5D7F0614E239B 30C96AF45B817D2E	129	DB432F18A9C06E75 7A854E310DC96B2F 7A249B0DF13E86C5 02614AB3978DEFC5	130	4A6BC8132057F9ED AFD9E856B132C470 B63091845DFAC72E 106E5B87D4CF29A3	126
94FC7E0218B65D3A 5A8B4601FEDC7239 7B654F13C802AE9D C2ABE30F9D685174	115	86AB354E7091CFD2 AEBC3647D0F58192 CDA2968B1FE34750 C5183D47F2E09BA6	114	48167FDC205EA93B 1740F582B3E96CAD D963C4EFBA102785 A4E32FD7B98061C5	114	C8D749051E36F2BA DA58E2B069C31F74 68F1AD9053724BCE C3A290E864FD7B15	120
82150E3D6AB9FC74 BE53A172CDF09684 DC7BE82F1A543096 A3985D6CBF0421E7	125	A1D73BE946C8F250 C697E0D4A8BF3251 9E06A4DBF52137C8 89BFD146237AC50E	127	871D0AC92F354E6B C27EDA318F0B6549 4309B1576DFA82CE 06D2A957F8C134EB	109	615DE4BFA0792C38 5C471063D2F8EBA9 C4A835F0B26197ED D2CA5B608417F9E3	130
A9C2D145076F38BE EF67B41D5AC03928 1B926D3FAEC58740 901F8C43B567D2AE	113	065AC8492E7B1D3F 923487AED56BCF01 EF9653BC078214DA 790FD8623AE15CB4	121	6ECD29B3584AF710 BF169C0E32874A5D 3A9FC48B52E0671D 69817D4BC523EF0A	112	E47D0AC986F23B15 A5084D32E6C17F9B F503249816AEBCD7 740E659A2CFD13B8	99
94B2ED6F183A70C5 A128C4FB6E503D79 8F25A149CB7306DE 7E06F825CBD134A9	122	0748CF952EADB361 2806FA973DC1EB54 DAFB906CE5432781 AE71F3925680C4DB	111	D8C61AE35B09F427 E7F5641C30B9A28D 87D341A265BFE09C 7A23ECF915B0846D	119	7F412CED903B86A5 591BEA64CD32F087 7D2C58F3091BE4A6 60958DE41AB2F73C	112
D20E379CBA615F48 25EBC346D7A80F19 1DCB65A8274E9F30 1FD6A94CE305728B	121	92FEC78430A15DB6 576B39420DCE18FA 2CBFA0174985E3D6 084AE162D9C7FB35	118	97583FEA6DB1C204 207B83E5194CDF6A DF6AB94E50C87213 621E43FC0B57AD89	116	5A3FC4B89DE10762 7C0415369AE28DFB BA0415D638CF927E 0E34D659A1C8F27B	101
F085DB214A639EC7 91D035EAF6CB8274 456DF0913E78CA2B 1DCB9563A2048E7F	126	0915FA3DE67824CB 45ACE0D3769BF218 F3C219A8DE750B64 894361DC7E0BA25F	114	7D98125ACE340B6F ADF930C784625B1E AC4502F7B863ED91 BC87F019E6A25D43	130	31B9E5A026C784DF ED68C1435907FB2A 215F3E09AB6D7C48 7214A03EBF869CD5	126
B9845ADC103F762E 7B06281E4FA93D5C 4F236DBC8E75A901		19B367FE2C48A5D0 DC0E39F8B14576A2 3E42F7951C086ABD		3A25147E6FCD09B8 785394BFEDC6A012 209FB6E84C513AD7		F7A3C6512D94E08B 1D27F95BEA6C8304 348BC0A12F695D7E	

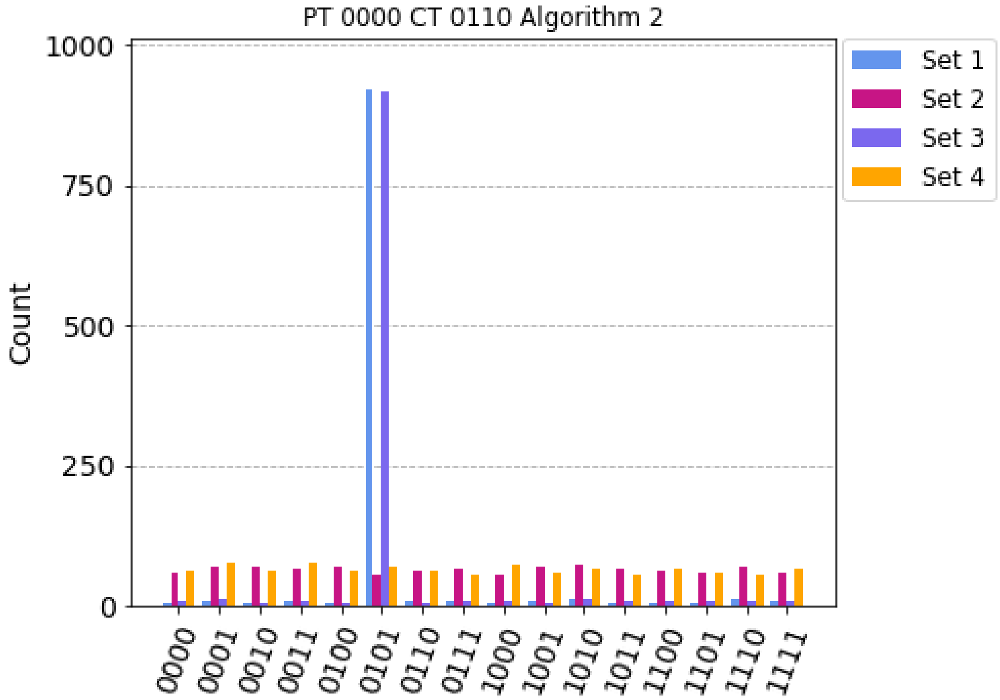
2E4F3C1596B78A0D	115	C29EA318B7D0645F	118	B96872E1A0D43F5C	132	846ABF5123DE70C9	130
3B957840C26E1DFA		519A7C6D40B8F3E2		D5940A812EC36FB7		7CE283B0615A4FD9	
30824CF6A9E517DB		65F7840C1392BAED		02A64F78139BECD5		CEAF86347291BD50	
B05A6F81CE47293D		70A5C4163D8FE2B9		849FD013E7B2AC56		B192DA476538CFE0	
B0AD1F95386C47E2	127	0C786BAD915342FE	123	6E830CB7F1A92D45	124	D21C30E5F7BA4896	130
567C3210BFAD89E4		6D3F59E10748AB2C		3A56B9F72DC1048E		F5CBA9E3061742D8	
A1EDFC0392485B76		CBA0D7298E6F5341		B7DAE5628F143C09		625F8C039DB7E4A1	
1407CA39BE5FD862		691A2E4D7C5B3F80		5962FD3A4CEB8701		29653D1E4FC8BA07	
8FD571032CE4A6B9	116	C3DF481A6027B95E	111	8A156B47C2EF930D	111	3EB751C26D9F0A48	121
45DE8B3012A76FC9		896FCB3D025A741E		0BE3927864FD51AC		B3F2671A0C4E598D	
B0D31AE7682F4C95		6BAE850D1274F39C		F6970CA8D213B4E5		0BED9C21457F36A8	
9B6AF854723ECD01		601FD782C9A45BE3		4F7C6ADE2950183B		6FB84215E73CA9D0	
432AF0185CED76B9	128	F3A0D8E1C2B79645	112	D3E54A09B126F87C	118	6FD3A50429CB1E87	129
B83A4269D0F71CE5		BE1D6C40738F25A9		43A80D2E6B571C9F		BFDCAE5974061823	
7C1F56829E4BA0D3		6F45D9A381C07B2E		B7AD513C09F48E62		1475BFEC092A8D36	
65F342C7A9BE0D18		4859B27A31E6FD0C		C472DE1869F3B05A		5DAE4719FB3C0682	
36A2814CE0B7DF95	122	EF6C32D7A15B8094	117	F764D3981BEC205A	136	1E73CA6902D84B5F	122
4A8D2713FBC5690E		5398CFDA641B720E		7BF2D815E09463AC		B6CE13072AD8945F	
F72958ACE016BD43		BDCE08F1562A3749		30DF279C641E8AB5		0B17C9D56FE2348A	
094156AB3ED2F7C8		29F304E85DBA7C16		76D9A48B13C52EF0		ED641F387952ABC0	
E94FBC2AD0683571	121	05D2F9317A864CEB	129	7CA0592EB186D34F	114	30D8E9162CBAF547	123
B5036EACD4817F29		5E03B9A476C182DF		625084CB7DAF319E		EBC2306F8D7A5149	
FE8AD930475CB162		BF8EA92D0163547C		ED941A27CF53086B		4A59BD628730E1FC	
26CE58A109FB74D3		5B0C89F14D72A3E6		12F38B5D46079ACE		4C25FB10963E87DA	
270BA59341F68DEC	134	42DA609B31E7C5F8	125	A0B8435C691FE2D7	121	ADF30712846C5BE9	126
9D4E80172F56B3CA		EF9837C4B20D1A65		720AD58391B6C4EF		E7BF36912845C0AD	
6D97CFEB5231A408		BF1E5A4680327DC9		C0712563BDEA498F		07F2B945CAD6E318	
73FAD2501E9864BC		69EB07413ADF825C		3E0A4D518C72F69B		C4B296085173DEAF	
B965D1C72F8E30A4	127	85E1F937BA402CD6	122	962370F18D45AECB	123	BACDF1476085E932	125
9741CFDA65B83E20		F48E9D7A620BC135		8F4EA573D901C2B6		D7A9E8F235B64C10	
F58316DA04B7E29C		36B870E512CF4D9A		7ED4569AB0FC8132		C0FE79643A152DB8	
312EDAC897450FB6		8F63C207DE9B4A15		6780512CA93DBF4E		BF019D256EA348C7	
81594F6A37EBD2C0	118	2F4C6AE70D9815B3	132	1284057EBA9CFD36	108	3AF46B82EC157D90	114
B9DF45C362A807E1		EBD3A26C9F175480		26379B0A8C5ED14F		8C479A126F3E0D5B	
2C1E5BA4687D90F3		58073CB14F69E2AD		83154B906AEDF2C7		4ACFE520B1D96837	
DCA539608BF741E2		A0D967B83F2CE415		732F904DAC8561EB		CE84A6213D5F97B0	
D51C36F0B29EA478	115	F8ADCB27591306E4	129	6A4EF5B39C7281D0	120	8FE31976BADC5420	112
84703BD65F9ACE12		6C1E83D50FB92A74		C562A70FE18DB439		1E964F735BAD8C02	
103479BE82FC5DA6		F1A8043ECD57B269		30E9C2F68715DB4A		0765183D29EABFC4	
9C3052AE17B684DF		4A59EF7B12DC6083		0F2689EB75CA3D14		5184DCF036B297AE	
728BCD39A6145FE0	132	BCD3960EA12587F4	105	89D65FAC402B13E7	111	2FE58A9C70614DB3	108
98C0D267FBEA5314		A37F4B9E861CD205		3C2570EFA1468B9D		671ED93F250C4BA8	
C76ABFE940D85132		E38691A5C72D04BF		E2801C54D693AFB7		39A05F24C1D8E6B7	
28AFB97D635CE410		6A7CFE1B9D382450		86A5EDFB29037C14		82D47EBC196A05F3	
2E73F08B4A561CD9	134	65C3D1B7A4298F0E	117	912F0DB54C376AE8	115	D7C3FE9A462B5108	125
4BE7350ADC2F6189		43DAF165097E2C8B		AFBD5E38917C4260		1A25BE497CD03F86	
5498BFA360D721EC		06E542A897FCBD31		F031846C9EB2AD57		A476E8FC90B5312D	
01A2658E9C7FB3D4		91A0DF75C63B4E28		91ED746083B5FCA2		3958CE4AB26D7F10	
0D6548A793EF1CB2	121	E27A51809F3DB46C	126	DCE2054A9BF17638	115	70F1523B9DEA48C6	120
C5D21340EF6B978A		8FE2B9513D0CA467		F160528BE3C97A4D		0E23ADF9B67185C4	
526EC0819AD3FB74		8F14652BC37E0D9A		5CB39128AD6F7E04		753042D1BF896EAC	
859AFC7D64023E1B		4BE8259CF7DA1063		F2C468A73DBE1095		DA71865EBC320F94	
C6E17940DABF5832	105	F02EA798BCD13654	117	6C07FDA132B485E9	122	6E1FC9405B827DA3	124
63B25471DEC8A90F		EF8A95CB462713D0		AF036ED174B9C528		51E0BD492CA6783F	
F4D832E0B75CA619		463D01CFE7A2B958		58A203E691CFDB74		E23DB15CF67A9084	
960BE15F4D827CA3		ADCBF19E25873460		4F013EC782DBA659		51A6D8E47023CB9F	
A0C9537216F4BDE8	117	04E7539CD61AFB28	99	BE28361790FDA4C5	124	1A98B07D4FE235C6	114
B9103675DAC2EF84		F0BD357129E6AC84		5C2AB13DF8749E06		8DB731A4E2F5960C	
28F5CA391D40B7E6		EF71598364CBD02A		DBA58410F7C3E296		7B493A8DEF2C0561	
1F748C60DE953AB2		C0896D15EFA473B2		A143D9F72E058CB6		914C85BF6A27E03D	
CA604823F59B71DE	125	94F28DC01E36B75A	128	D40CA3F6597BE182	121	BF054E7D92CA8163	114
27408BE39DA1F65C		FE684A1CD532097B		CFE7A561320B49D8		5BCF49E8D7A26103	
5ED2AB816094CF73		9527830B6CD1F4AE		9EABD73C610425F8		41A6DC5237FEB089	
497FE81BD2A3C065		8C71A594BFE632D0		8FECA4D359B67021		3DE17046A259CB8F	
A8506E7DBF91243C	116	FC5297BD64810EA3	128	6B29DAE048CF5713	106	D1954EF02B78A36C	118
42E67013BF9D5A8C		58219DAE340FBC76		FA7E294103B6DC85		B26845C901DEFA73	
ECB2F480D7A59163		FDEC5B869043A271		76B8D93EFC14A052		B920F8D367E154CA	
8D1B64237C9A50FE		A6154FD89E0327CB		ABC7F180629534ED		164B0A389E2CF57D	
A9EB6FC103524D87	113	69A4EB73C0F8D512	119	1CE532A4D76F89B0	112	3C74DFB8E51209A6	124
C1EDA472830B59F6		54EB0A13F98C26D7		FB5CD01A3649872E		0ED62A519BC83F74	
C2EA751683D490BF		F4A2CE307B16895D		3247B6E8DA5C0F19		E472B369DF80CA51	
981D6AB20C7F4E53		0E47695B1A83F2CD		F02938BAC56DE174		E6BAC92843D57F10	
7589C4BDA1230FE6	132	50B37F21C6D89A4E	125	97BD6CE1F3A58204	125	D87162FCE0A9B543	118
B9AFE653D102748C		8B12ED5397A40CF6		850DA127B9FE4C36		3A6FD452BCE90781	
854D3F67E01C9B2A		28EAD5410F679B3C		F84A6D0B17E5329C		6EB2541FA07983CD	
9D67FE435218AC0B		B0745E168F9D23CA		2137A0FC8EBD6549		360EBFD5A294781C	
A6043EC597FD821B	127	24ED1805CA6F397B	103	0E46A3F81C9B52D7	127	13450CBFD978E2A6	92
420EC9D81F57B6A3		5940CAFB1D27E386		E6C74F38B219A50D		7208D5163B49ACEF	
5341BF269DA07E8C		F8D25A0E19B34C67		DF2793A806EB514C		1C278AB5349DF06E	
07D28F51C436A9BE		6F3095B284E71CDA		E946D15CBA728F03		F302E4CA59D78B16	
EDC3F8192074B6A5	102	642E187CA9DB0F53	104	FEA361870B4295CD	113	8F5C4D21E3AB6709	124
AD1594B83CE207F6		682F9731C4EBA05D		2C78564EB0A9D31F		5810CEA67F39DB24	
FBD946EA87C12530		4AEC1F208796B35D		BF1243D0C96A785E		B1D5CF460879AE23	
2BED7A9610F4853C		6085CED2BF14739A		743A0158D26FEB9C		039C651AB4D27EF8	
1EDCF374A8B95620	116	B75C09DE64821F3A	122	230E8D174FBC65A9	116	8FDC590E64A2137B	129
CD9F2B3EA6817054		51BD867EACF29043		1EB82F43695A7C0D		6C2B5901EA473DF8	

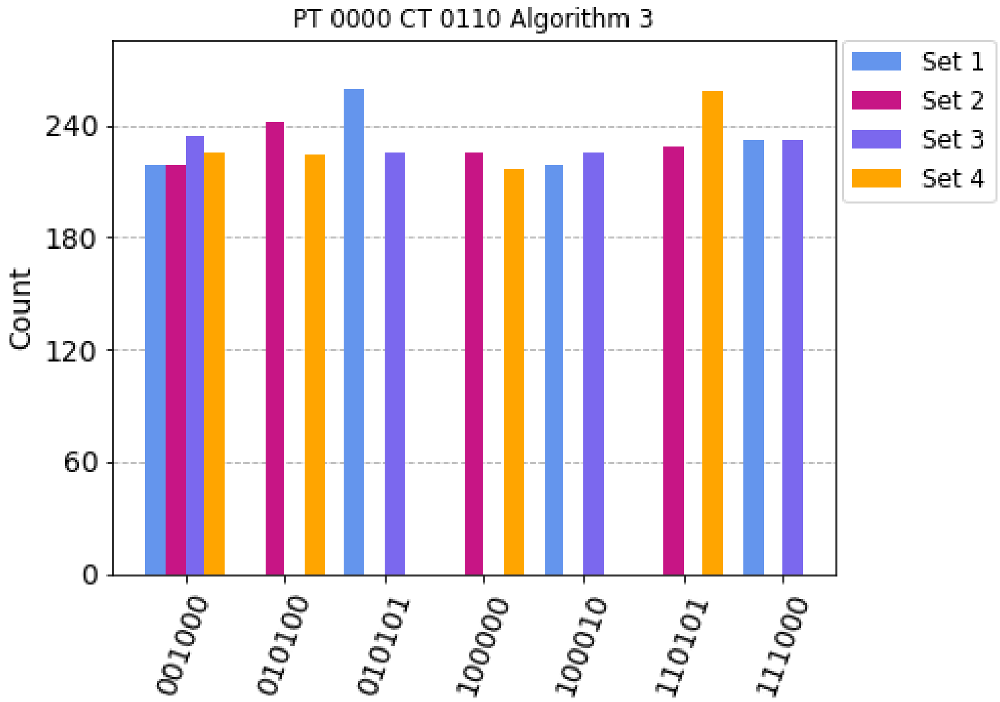
1862DF753E4BCA09 0FA3D5BE164872C9 49B102567CAFDE83	124	9B6EC5247A1F83D0 64257D3FC9ABE810 BD0389AE17F654C2	105	51E9F8B4630CDA27 E5DC3076A89B241F 9058AF46E1DB3C72	127	8CD2915BEF376A04 C7451AE38026DB9F 3902C4F658BD17EA	126
9348CE12075B6FDA 5B62CDAE891073F4 5F9A82B347C01E6D 3476E0D82C5F91AB	121	C2607EB894F3A5D1 A08C4DE967231BF5 0E2B76F5381D9A4C 50AF1247B3968ECD	115	C216B9A73F5ED084 7CFDBA2943805E61 6A1E0489F2C7D35B F9EAD80C236147B5	130	391E60B8FC745AD2 B8D731C069EAF425 F753D2C98140A6BE E0D2C65798FB431A	126
94A7F608EB31CD25 DE179A52CBF08634 845EBC0A9176DF23 02348A1BF9C675ED	113	1FA32C57DB0E6849 AC682E094BF573D1 294E18035AC7BF6D 9170CBD2A46538FE	113	F591D3BA0284E76C CB63D78EF24091A5 DB8C532076E4A91F 2E79601A48D53CBF	124	1C9B2AD87354F06E 3C164DE57F90A2B8 09E74CDBAF863512 FB0D239C7AE81546	126
D3C4A9F162B70E85 6FA9D2C80137EB54 4305FA128ED7CB96 4DCE705812BF369A	130	0EA18FD653C429B7 F1E9805A632D74BC D9A80F6C357B42E1 708C316A2F9B4D5E	127	7DC01283BAF4E695 36ACF01BD9E25487 0A5836F4CD1279EB 2605B8743AF9C1DE	117	0A93FE271D6C5B48 B30F8C7E691D45A2 61CF2B34D8E7A509 9265BEA478DF0C13	126
48CEFDA5B2791063 78AE19FB03DC5624 564A08DECB239F71 7EF30962DA14C8B5	120	45260D3ACB81E9F7 81A27453EBD69CF0 1A5F480E79C3B26D 7A5EC2B0318F64D9	110	2E56A49DCF170B83 6F12539EA48DC70B 3E7BC4859061AF2D C60BF5479D3A2E81	109	9F4B7513C2AD068E D5F3E48791C60A2B B61FD54709EC283A 78D56AB2F901C34E	119
9D7CAEB21804563F E74D165CF3B8902A 0C37DBFE1856A942 CA0E69F5B4713D28	133	1ED58B6932AF74C0 01D74C95E8B3A62F 13B7FDE0A596842C 78BCA2ED65F43901	121	9C27B35A0E1F8D64 E1A570DF4B26389C 062D5479CE8A3B1F 24FBEC5187A9D063	116	BD9E6537C8402AF1 75E219AFBD86C034 A67D80C4BE25F931 C503E6A78B2F914D	131
69E185D3A70CF42B C76023D985E1FB4A 4FE87C29A6013DB5 CDB8026E1F9734A5	116	BD14E5607ACF9283 354B0C8912D7EF6A 934BA1DCF2087E65 16B873ECFAD95420	120	0923DC1AE4576BF8 EF23AD479156BC80 C908172AF34B65ED EB3169D80CA5472F	118	E37C1AF54B89620D 4603BFEC2D859A17 30BE9C168D47A52F BF1A0C3745D29E68	127
A613BF8D72CE0549 78FBAD52C43169E0 043E19582DCA6FB7 760EC8235BF91AD4	125	F3C285BA791E04D6 56BF07438C9EAD12 0913EBF25D48A7C6 4FE9A87510DCB362	121	836A91FDE540C72B ED13C594708BA62F A80C931274E5FB6D C6B4FD3021A7985E	111	38BD0AC74921E5F6 A51C42E3D68B79F0 426A9BCD3E1570F8 3E627B98C51F04AD	123
546238F0DBC17E9A 78CBA25EF4069D13 DB3025E4CA61879F 821EBCA45D739F60	130	DFAC2341E8690B57 BACD06394758E21F 26E5AC89B37DF401 4908BD2E6A715C3F	118	356CF12E9B0AD874 732B8195AEDC406F 4E28D9F1AC30B675 485F1AE9BCD36270	110	AB096D7EF452831C 70DBA1954C26EF83 9E5F34B02A67D81C D96A7120B8CE4F35	112
E4DC270A536B1F98 471FB2CE9DA85603 6E5CD18B73A0924F 4357B9CEA1D6028F	122	920BA4EC7D568F31 35AECDF0296B7148 B42EC3150DAF8967 6E70891A43B2DCF5	112	6D8E342B57C901AF 325AB6019EF84CD7 08672EBAC1D9F543 830DC41F6A5B7E29	122	FD20736C5148AEB9 0AF156874CE2B39D 2DE608A794F3CB51 6E342AD07BCF9158	125
3B1FDA04C96E2785 D96540CA2BE8173F 6371A8B02F954DCE 821E7F46095B3DAC	126	96EB54A13D82FC07 A54C29F76B0381ED C65A1F3924E087BD 9A01E7D32456B8CF	122	5E3024CA6D8BF791 9A170D45E3B682CF FED2C8AB91765043 6C8547EDAFB29103	118	65420718ABD9EFC3 BC763DE9F2A05418 EC245738B9A6F1D0 AC86E1D2F05794B3	102
5CF16ADB3942078E AB38152970D4EF6C B913EC67F28A5D04 1A63EFDC870425B9	126	51B8AD207C364E9F 7501A28D43BE6F9C 0258B93D6F74AEC1 624018CD3EBF75A9	116	346CD751B8FA9E02 547F8A069E1D2C3B AC8F14D65297B30E 275F4DE3A9BC1806	126	E73A8C4102695FDB 6EC4BF2A50893D71 951A632E7C840FBD 1023F7DAB5984CE6	122
06E458B2CF13D9A7 F5E31A0D8697CB42 08D126CF7BAE9345 85293AC607DEBF14	117	2BC4A35F79618DE0 4E2BF801597C63AD 25FA698E47BDC310 7D92A8BE65C41F30	126	C0E5B736FD92814A 6E531F79DC8BA024 3BF4195CD82067EA C03F726E5BA918D4	115	4BCDF6701235E89A 4AD2BEC9380F7561 3241D07E8AF69B5C 29108E354BC7AFD6	126
AF9D7123850B6E4C 87F1EADC95B24360 07ED6341AC8F592B 74A36B59C2ED801F	112	3DB05CF62E814A79 6D3EBA1F8C240597 0ED16397C58B24AF ECF048A62B53D719	116	CB91D538E7A20F64 A217C6534D8EBF09 D14A58BF792C630E 58B214C790E6DFA3	150	4508EBCA7F3D2691 15EC4D6B0798A23F 8623DC0417EFB95A 52C6B4980EA3DF17	125
FBEA537DC6402819 BF0D569E8134A2C7 93526A7D14BFC8E0 3A6CB5908FED2174	109	9703FDE1C4825BA6 CD746E1A802F9B35 70524B316EAF9DC8 2913D5AEFB86C740	128	9CB1FA436E58D720 7492D18A05B3E6FC 7DB614CF9E8A5023 C58F71B49E30DA26	128	938E42705B6D1CFA 217950E3CFD46B8A 6EB12FA49C3D0785 2F501EB473A986DC	118
A4DC203B9F5E8671 76308D9CF1ABE452 F7E2351C80B4AD96 45CB0E1268AD93F7	133	8D5E0B6A71F9432C 26A984C1FD73E5B0 0C6853FBD942A17E A150B2FD4796C8E3	128	8627AE514F0D9BC3 7D32F61CAE9845B0 D328B714EF0C96A5 435027ABED91C8F6	126	49EA5638C170B2DF 0F2E817CB36D945A 137C896A402DE5FB 569417A8E0FCDB23	108
C061A792B5D83EF4 AC35710649EBDF82 EDF10328657BAC49 0DE7CB2384AF6159	126	A4ED89307FB52C16 9D5A8CF6403E7B21 528DB17A39C4FE06 F63825D7091BC4EA	126	3B145A86D729FCE0 D56B27C84FA0913E 6D1F2B3708EC9A45 7A0CF859D4EB2631	109	B29A486DE105C3F7 B594C6703E1AD2F8 9E8416FCB5D307A2 E4750263AD8FBC91	119
4A2F9B8013CD6E57 876B913F0CA25DE4 D5AE3984061B2CF7 E86D453A0C7B92F1	129	BD43E28A17560FC9 E3B05C97482FA6D1 64B80D3592AE1FC7 87F2B0659C1DEA43	114	3476C09FBE52AD81 16F742A9CB80DE35 2E8963A14B75DFC0 793CD215EF60AB84	119	31C65FDA08274EB9 2543ED0AC1F698B7 9D18B306F4A5C2E7 47625AC8E1B903DF	110
4567EA3F9C8D102B 26D8C5B9437EA0F1 1BC4E3D7F98A0625 53CB18AE9DF42067	117	E0D3894C5F1672AB DF25EB08A96437C1 D6FC304E81BA7529 DF61984CAE520B73	122	DF61E039B852A74C 301B9CA7EFD58264 6391CF54DE70A2B8 547198F3ED2BCA06	128	72341CF90EAD586B 802F759346BECD1A C03A291D75F68B4E 687BDCE5A9302F41	125
BA673DE25C01F948 EFB9463201D758CA 376149A0CD2EB5F8 09315426B87EDCFA	108	C3E4D728B9A16F05 8042BF36DEAC5917 659C420B3FA18D7E F8BC531D046A92E7	131	1ECD259BF63A4780 14C280D9E5FA3B76 62B5078EF4C31AD9 56C209AE3DF18B74	113	862B43F951E70DAC E5160CF794283DAB 3D1EA8027F5C49B6 A69B81EDF32C4570	120
59B6A0D41C2E78F3 35C8A90EDF71264B 92475C3BD6F0E8A1 F8CD536407AB1E92	115	654073BCF982DE1A A9413B0C7D2856FE 3E41AFD7C2806B95 231D0A948F65B7EC	120	657DEFA804C391B2 7EBC390421586FAD 354CB6FE207891DA D0AF6794B832C1E5	128	891A7EC4D306FB25 0AD37E814925BF6C 762F95DC81AB34E0 0B4C351F82A6E79D	119
36928A7D45CFEB01 2A90BD36E7C4185F 879AC4132E056FBD		F12587DC4A9EB306 CDE286547B0F91A3 7204EA9518F6D3CB		E0547FA2C83DB916 A910D2375EF84CB6 9E63D02B4C175FA8		06524DB1AFEC3897 348E1DC26BFA9507 763DB4F9E2C0815A	

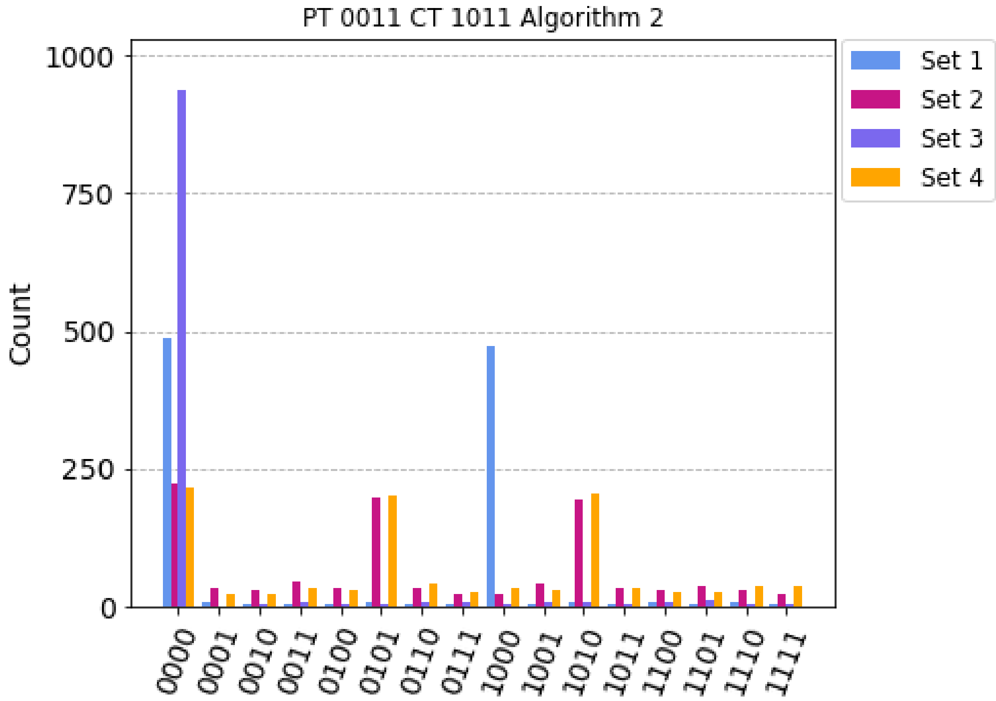
D3A415C867F92E0B	117	8CD73014A6E5B29F	120	FE07A3C5864D2B19	130	7B854ED3F2AC6019	118
FDCE561437B809A2		15790286BACDEF34		412B3780EAF5DC69		8D0F3C6472B91A5E	
BD9E1F37A804265C		1BC7F96308DE5A24		4B358EA20D9FC716		AF3E01596D247CB8	
F421D638ECA7B059		06A51E7D923CB4F8		590EA271D638B4FC		7214EC9BAFD86035	
E9036BDCF74A8152	109	C8F30179B5AED462	115	AEBF06C81539D247	111	2C4D30E6718A9BF5	110
6D73A915842FECB0		D1906F27485AC3EB		3CB08962DE51F47A		F9E65BA8071234CD	
EF1935CD6AB48720		F19584BAD2760E3C		AD92C60E745B183F		A49B53608CD1EF72	
243E60597A18CFDB		476B1C23F8095DAE		1268A75D09F4E3CB		FCA9E147B36D0528	
52A8DF1BE479603C	112	142360A5798EBDFC	126	8139DAF56E2047CB	115	3EF175D4069BC28A	112
6D89EAB3C410572F		40E78DAC15F296B3		6F39E874BAC52D01		5F769DEB83C0A124	
E6FC132AB0D97584		2AFD5C791064E83B		EF91563BA2CD7408		31D746EB5CF0892A	
1034E582F7D6B9AC		703182A6DCE4FB95		B691F35A27DCE804		FEB289D5A016347C	
B1963EADCF482057	121	28EA5063FC149DB7	119	D4630829B5E7AFC1	113	856419EA7C3FB02D	129
F73CB16A40D925E8		DAB09354FE167C82		9768CD1AFEB30254		4B7CDE95806A12F3	
C215E0439DB87F6A		94A257C18EF0DB36		C7BE43A0129F56D8		E68BC3F4A10275D9	
29D784C60E51F3AB		1470F96D38ACBE52		1FA34DB9E28650C7		04FA86D2C537E9B1	
AE6940573CB1DF82	121	E87A92B016FDC543	112	6917483EF2AB5D0C	114	E8FD9542B03A176C	116
8E3C60B1F2579DA4		FC81BAD02795E364		327DFA4058BE9C16		62BE3A04C978D51F	
47508DCAE6F1B329		182409D57A3CF6EB		9280CB14AE63F57D		4FD37A29B1EC5680	
8A4197C0DE2653BF		42FAC3675109BE8D		7A0E893546D2F1CB		BE2015C8A4963D7F	
61E08AD3C97F524B	113	B2308F4615EAD9C7	117	127E536DAB80C49F	110	61B27CD8E905F4A3	126
BF53A9E0274C6D18		EAF30781B49DC625		6234AE0FC5971BD8		7D05B362C1FE9A84	
402E953D6CAF178B		A96FED83B25170C4		B64D103F7EAC8592		3A5B26F7D01E9C84	
F9E3C8165D04A72B		0B7D8259F641AEC3		1F2B670E8A34CD59		6734AC92F8ED501B	
E5C24179AF036DB8	135	D7BF691A2E35408C	114	1AF28B634CD790E5	122	9FCD062BE3A84517	115
EBA0F27186CD4359		0EB9257A4D1F6C38		B109F27E586AC3D4		A73D08145C29EB6F	
1E74D85B0CA239F6		12FBC5D97E6A4308		46C1859B7A0E2DF3		FD0681E425BCA973	
F40C5791E6AB3D28		248F07C6DB3E1A59		B6EA74CF1D520398		C9E0D61F35A4278B	
A91D780256FCBE43	124	ED74AF1836259BC0	118	C7316AE0B94DF852	115	B2F6E381CD95A074	117
8FB1260D93AE745C		4F95DCE2716A830B		B1DEC495FA320867		67E40CB139D5A28F	
61709CDE8A35F2B4		69D58CA407F3BE12		25B46E378CFD019A		2613EFA904C875BD	
2B86AD03F15C749E		C691D530E8F74B2A		8B532F7E046C1DA9		820671AEB4D59C3F	
BF2647E9C1D8053A	116	C98241AB506FD37E	123	0B576CEFD9A24813	132	EA4B570CF3962D81	131
8C7FE36542DAB019		129A6CD3F058EB74		B51E69D4A270CF38		24810F95EADC7B36	
5D231F7A4096BCE8		4580E31672BAC9FD		6F7A0D9B5832C1E4		A4E2150DF7CB6389	
231F609DB78A5E4C		78D6FE9213540ABC		128E4B5D37FC9A06		3B0EDF91C768452A	
B9E305D64C8A2F17	129	237C4B91A5068DEF	120	F8AE913BD574602C	122	1EFC42358B60AD97	121
45CA1E36DF097B28		12D843AFC9076BE5		F38B5027D46AC1E9		5E6F37B8AD29140C	
973481F6205BDECA		E3F25BCAD1087469		7D340BECF5821A69		E6B38920A4DC1F75	
A52DBF46E18C7309		8B053DC14E92AF76		D3BA6710E85CF429		1EA2CB6D508749F3	
3E2851FCBD9670A4	127	91DAF2405CE6B873	126	EBDC28F35471A096	122	2C9D16E5734B8AF0	128
98E453B1DCF7A620		21974E0DAB3F658C		7124BE8A6F03D59C		02897CAEF6B4D315	
F9472ED053CAB168		32516BD9A04C8EF7		2B95A03D8C1E76F4		48AF0EB962C1537D	
98B32145CE67AD0F		B9E50A23CD1F6784		2CE743A8FD6519B0		034CBA2856EFD719	
AB0F849EDC617325	120	9A602E4D183F5CB7	115	90721FEDA4583B6C	120	EC4FB570216A98D3	120
DB1532FC490E76A8		152B076EF4D3C9A8		FE18CB92057A63D4		89B3F0A671245EDC	
ED98CB6A250147F3		0AC2571EBF49D836		86EF9D15307CA2B4		52EF0A7BC34869D1	
1B69F0C3A4E2D875		C0D4726AB31E59F8		0EC238FAB59D1746		0D68514A932FCBE7	
149AC87E6235FBD0	124	DE0738C2BFA91564	105	40736EFAC92B5D18	131	CB4F2073D96E185A	122
074B6EC9823DA15F		8A9E3F470C652D1B		F91C8625A074EB3D		E6908AF25D31CB47	
D529FCBE0A784163		3AB6E19C8D5407F2		BC82456F90E71DA3		92E10FB8D37C654A	
759DE4FCA0B38126		F16E3B94DA8C0572		8F9A7150C3B26DE4		FB2CED037586941A	
AE8C9625D0134FB7	133	20C1598743D6FABE	121	AB5839DFE024C617	123	D18A37BF46EC2095	120
25F40B93DE718C6A		837F05CEDA42619B		62B9F4A10DCE8537		681B904ADCF2E357	
86DAFC1420E359B7		176E3BF428C5DA09		E2CD954FB78013A6		C61E39F27BD5480A	
1DC63B20FA4798E5		7C81596AD4BF302E		B4C2F30D8795E16A		A984B57C062EF31D	
DEB375C8F209164A	116	D2AC650FE34971B8	131	8539C1D72A0B6F4E	133	BD928C13FE5A7604	121
64259F37AC80DEB1		F8D769A3B415E20C		01D97EF24CA6B583		D305B2C9A8E4F617	
4670C9BAD31E528F		5B6EC028D79FA413		EFA19560D73BC428		3D0A596E27C48FB1	
CF1394680BED72A5		B9FE1AC78364205D		CF0568A7BE139D42		8F749063CA2B5E1D	
467E582FBD091CA3	112	75891EDF4362BCA0	118	3E8C6F94251D07BA	110	A5B3F026491ED7C8	131
5E4067DCB398AF12		51D8FB2A4E76C039		09DFBC83E651472A		C5AB24803F716ED9	
54FE86B291D073AC		4671D9583BCF0EA2		CF129DB43E07A856		C479861BDA2F5E30	
3EFA048D275C91B6		72FAB8091C34D6E5		9CD17852AFE3046B		FDBE9523A68107C4	
621FAC7B83E549D0	128	5A2C6BF4D187E903	110	B2DC41F5A38790E6	128	0B4C2631F7D859AE	125
2D3B974CA08E651F		A1C936DB47E502F8		548F713A0B2CE69D		ABED741C03F65982	
74BDEF2C9A083165		639FA04B5E18D7C2		83FD2B1047C6A9E5		21CF73654D9A0BE8	
7D1C8AB62F95E430		04ED8C3A9F72B651		23B6E18C45A907DF		E2FAC759B81D4036	
91253CFB76D8E40A	122	E8A7B532D91CF604	131	CA2DB7801F4E5396	114	3C897B2FEA601D54	109
473E69D0AF8BC125		F9B6D08A7532C1E4		5DA7E021F96BC483		AB42D7C5613E8F09	
13BDFA2E87945C06		1293E6408B57FACD		4130F5E8B97CD2A6		F75E4962DCB138A0	
63B9F2017EC8A54D		9374A01DF2CE685B		91EC0F7B28456D3A		3F74BC69581E2AD0	
BD0369C42817EFA5	118	D90357E824CBA1F6	110	7E8D195B432CF6A0	122	42E78C9B013A56DF	128
F4A2CBD985E10763		9B8C3102E7A5F4D6		209B84F1CD37E5A6		C9A15B04786D32FE	
8A46073FB9E5D2C1		E6951247CDBA0F83		8015E2936ADCBF47		0D849E2567FB1C3A	
31482AEB95D76F0C		D01248EF9CAB7356		0B3FE9AD172468C5		3EADB5C72F068914	
C0DF9E82653147AB	131	EC9AF7281BD64305	106	1760F9E3AB5D42C8	111	871A05BF3EDC9264	127
A16B0725C49DE38F		2A54D1B80E9C76F3		8341D95E02ABC7F6		170F5329B684DACE	
8ADB670EFC952341		05FB284E61A3D7C9		C45E1603B7F8D9A2		FCB503E286194A7D	
4EAF20D7598BC613		381F4BC57AE9D620		167CB48EF5032A9D		92F518E0746AD3BC	
E865317AB04DFC29	122	8DA21C4F06539B7E	109	E5843B0A9FC71D62	123	092E5C1A476B38FD	105
95B0CD83AF641E72		8A01E9536CDB247F		6A543D18EC27F09B		065B43E791C8AFD2	
12F36085BEDC47A9		39F5871D460EC2BA		9ADC7F3E502816B4		45A7C3DB06F8E192	
914A5BDF7036CE82		BC2D8E653A4F1079		FC1BE0568A423D79		2F7B4C81D3E569A0	
927C18DBEF536A40	118	94258AF61DBE307C	118	309C7BA2D8F4E651	147	9A2F4E51D6B83C07	117
14703258BC9ADF6E		6D507491FAE38C2B		092BF5DAC8E43176		B5687E12F4AC39D0	

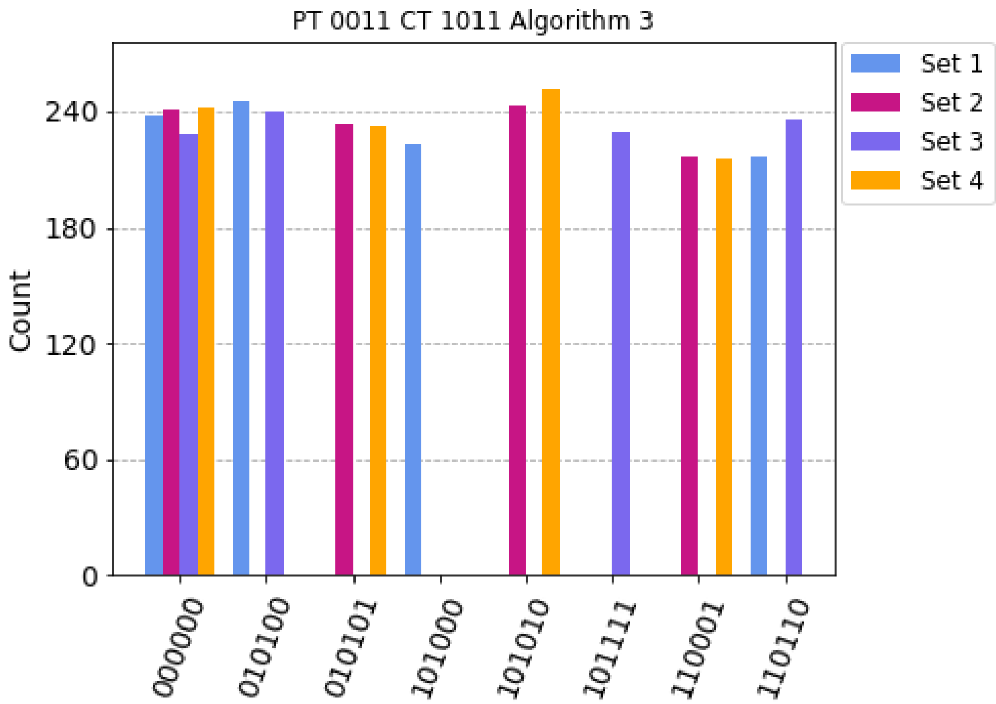
610D3FC54AE2B978 A4E829750CD31BF6 0389DF52BE14C7A6	114	5827D6E3AC4B1F09 7C54D3E9BF826A01 A901F5D78BC4E362	117	FAE194D52638B70C 2493CB687F0AD1E5 0E42AB8D7613FC59	114	F1759804EBD6CA32 78DF032C541A6EB9 125ADF83460E9C7B	117
18B74AC2D3E96F05 E7405268BF9CA3D1 7C84FBD9605123EA A1C6842BF3E9D705	108	FAC4E329BD710685 BDC23169E045AF87 4982D160F5BC3AE7 3DA8C7FB0164295E	127	83941F6CE0B5A27D A67FBE08429D3C51 1F2C8DBE34A60579 C7B69F58E203D4A1	111	B8A0C41DF567E932 72D46EA10C39F85B 40E159B8CD3F7A26 3FE6C7AD4250B891	115
249085EBF6CA31D7 8C71EF42509B3DA6 BD8172F59E360AC4 5F37A469E2D80C1B	121	31DE572CBF689A04 E249B7CA851FD603 F8CBD61E403529A7 9BA3687F5D4E2C01	111	57C834DBA10F926E 083CBA265471FE9D 587FD1690CBA34E2 073C1648DEAF5B29	116	9D7B602AFE154C83 1ADE08769B54C32F 7BDEC284A91036F5 17E9B0AC4F683D52	117

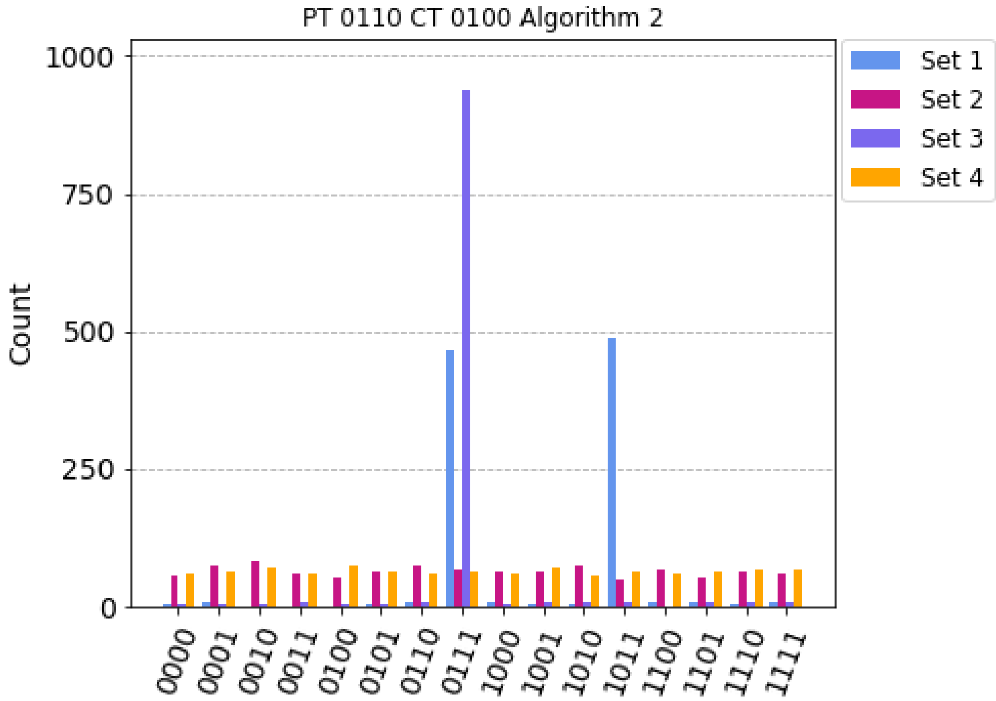
C Results of Using Grover's Algorithm to Perform a Known Plaintext Attack on Implementations of S-AES That Use a 16x4 S-Box

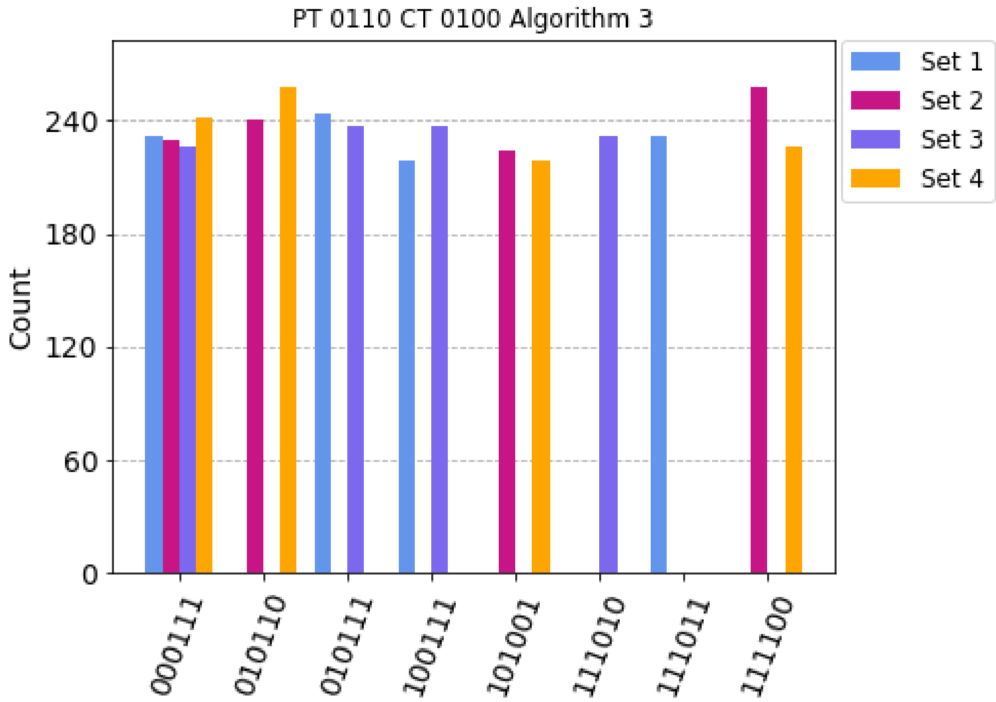





PT 0011 CT 1011 Algorithm 2
Count
1000
750
500
250
0
Set 1
Set 2
Set 3
Set 4
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111


PT 0011 CT 1011 Algorithm 3
Count
240
180
120
60
0
Set 1
Set 2
Set 3
Set 4
000000
010100
010101
101000
101010
101111
110001
110110


PT 0110 CT 0100 Algorithm 2
Count
1000
750
500
250
0
0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111
Set 1
Set 2
Set 3
Set 4


PT 0110 CT 0100 Algorithm 3
Count
240
180
120
60
0
000111
010110
010111
100111
101001
111010
111011
111100
Set 1
Set 2
Set 3
Set 4

D Statistical Analysis Results

Set 1

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.276	100%	0	93.33%	0.254	100%
Block Frequency	0.378	98.33%	0	98.33%	0.299	100%
Sums 1	0.672	100%	0	90.0%	0.437	98.33%
Sums 2	0.111	100%	0	88.33%	0.254	100%
Runs	0.006	95.0%	0.501	96.66%	0.773	98.33%
Longest Run	0.082	100%	0.276	95.0%	0.213	98.33%
Rank	0.091	96.66%	0	35.0%	0	78.33%
FFT	0.888	100%	0	0.0%	0	70.0%
Non-Overlapping	0.304	99.32%	0.445	98.36%	0.499	98.98%
Overlapping	0.035	100%	0.74	100%	0.804	100%
Universal	0.041	—	0.054	—	0.001	—
Entropy	0.005	98.33%	0	86.66%	0.976	98.33%
Excursions	—	100%	—	100%	—	98.61%
Excursion Variants	—	100%	—	96.28%	—	98.76%
Serial 1	0.054	98.33%	0.091	98.33%	0.637	100%
Serial 2	0.834	100%	0.706	100%	0.534	100%
Linear Complexity	0.324	98.33%	0.74	100%	0.862	100%
Average	0.273	99.01%	0.237	86.01%	0.436	96.12%
100% Pass Rate	9		4		7	

S-AES (Set 1)

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0	100%	0.324	100%	0.299	100%	0.082	100%
Block Frequency	0.178	93.33%	0.276	98.33%	0.016	96.66%	0.01	98.33%
Sums 1	0	100%	0.111	100%	0.001	100%	0.091	100%
Sums 2	0	100%	0.35	100%	0.01	100%	0.091	100%
Runs	0	100%	0.213	100%	0.773	100%	0.004	100%
Longest Run	0.324	98.33%	0.163	100%	0.706	100%	0.324	100%
Rank	0.437	100%	0.804	100%	0.195	98.33%	0.025	100%
FFT	0	16.66%	0	33.33%	0	20.0%	0	23.33%
Non-Overlapping	0.256	99.06%	0.342	99.06%	0.247	98.88%	0.269	99.07%
Overlapping	0.804	98.33%	0.028	91.66%	0.195	98.33%	0.135	100%
Universal	0.83	—	0.826	—	0.886	—	0.98	—
Entropy	0.407	100%	0	98.33%	0.02	100%	0.001	100%
Excursions	—	100%	—	98.21%	—	100%	0.35	98.86%
Excursion Variants	—	100%	—	100%	—	97.22%	0.46	100%
Serial 1	0.74	100%	0.834	100%	0.148	100%	0.135	100%
Serial 2	0.233	100%	0.672	100%	0.773	100%	0	100%
Linear Complexity	0.773	100%	0.602	98.33%	0.054	100%	0.407	100%
Average	0.332	94.10%	0.37	94.82%	0.288	94.33%	0.198	94.97%
100% Pass Rate	11		9		10		12	

Set 2

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.95	100%	0.067	96.66%	0.568	100%
Block Frequency	0.002	98.33%	0.437	98.33%	0.74	98.33%
Sums 1	0.031	100%	0	95.0%	0.163	100%
Sums 2	0.437	100%	0	96.66%	0.074	100%
Runs	0.378	96.66%	0.911	98.33%	0.122	100%
Longest Run	0.018	96.66%	0.568	100%	0.233	100%
Rank	0.378	100%	0	53.33%	0.044	86.66%
FFT	0.067	98.33%	0	0.0%	0	73.33%
Non-Overlapping	0.306	98.59%	0.529	98.82%	0.515	98.95%
Overlapping	0.004	98.33%	0.35	100%	0.437	96.66%
Universal	0.66	—	0.404	—	0.222	—
Entropy	0.534	100%	0.195	95.0%	0.95	98.33%
Excursions	—	100%	—	100%	0.382	98.86%
Excursion Variants	—	100%	—	100%	0.43	98.14%
Serial 1	0.003	96.66%	0.378	100%	0.773	100%
Serial 2	0.101	100%	0.276	98.33%	0.233	100%
Linear Complexity	0.195	100%	0.378	100%	0.834	100%
Average	0.271	98.97%	0.3	89.40%	0.395	96.82%
100% Pass Rate	9		6		8	

S-AES (Set 2)

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0	100%	0.111	100%	0.013	100%	0.163	100%
Block Frequency	0.178	93.33%	0.002	98.33%	0.111	96.66%	0.001	91.66%
Sums 1	0	100%	0.002	100%	0	100%	0.06	100%
Sums 2	0	100%	0.018	100%	0	100%	0.007	100%
Runs	0	100%	0.135	95.0%	0.054	100%	0.082	100%
Longest Run	0.324	98.33%	0.178	100%	0.672	98.33%	0.049	100%
Rank	0.437	100%	0.74	98.33%	0.773	98.33%	0.233	98.33%
FFT	0	16.66%	0	10.0%	0	41.66%	0	43.33%
Non-Overlapping	0.256	99.06%	0.269	99.2%	0.231	99.0%	0.251	99.03%
Overlapping	0.804	98.33%	0.602	98.33%	0.437	100%	0.049	100%
Universal	0.83	—	0.131	—	0.768	—	0.413	—
Entropy	0.407	100%	0.074	100%	0.035	100%	0.039	100%
Excursions	—	100%	0.364	98.75%	—	98.42%	0.231	99.1%
Excursion Variants	—	100%	0.398	99.44%	—	100%	0.204	100%
Serial 1	0.74	100%	0.001	98.33%	0.407	96.66%	0.031	100%
Serial 2	0.233	100%	0.469	100%	0.469	96.66%	0.254	100%
Linear Complexity	0.773	100%	0.148	98.33%	0.998	98.33%	0.804	98.33%
Average	0.332	94.10%	0.214	93.37%	0.331	95.25%	0.169	95.61%
100% Pass Rate	11		6		7		10	

Set 3

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.437	100%	0.035	90.0%	0.637	100%
Block Frequency	0.773	100%	0	98.33%	0.637	100%
Sums 1	0.74	100%	0.067	83.33%	0.016	100%
Sums 2	0.233	100%	0.006	88.33%	0.111	100%
Runs	0.299	100%	0.637	98.33%	0.178	100%
Longest Run	0.005	96.66%	0.773	100%	0.534	100%
Rank	0.602	100%	0	38.33%	0	71.66%
FFT	0.407	96.66%	0	0.0%	0	60.0%
Non-Overlapping	0.265	99.05%	0.443	98.22%	0.531	98.87%
Overlapping	0.213	100%	0.501	100%	0.148	100%
Universal	0.074	—	0.433	—	0.584	—
Entropy	0.001	95.0%	0	90.0%	0.324	96.66%
Excursions	—	100%	—	100%	0.532	97.72%
Excursion Variants	—	100%	—	100%	0.531	100%
Serial 1	0.049	100%	0.378	91.66%	0.276	100%
Serial 2	0.091	95.0%	0.178	95.0%	0.534	100%
Linear Complexity	0.299	95.0%	0.834	100%	0.932	96.66%
Average	0.299	98.58%	0.286	85.72%	0.383	95.09%
100% Pass Rate	10		5		10	

S-AES (Set 3)

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0	100%	0.111	100%	0.035	100%	0.254	100%
Block Frequency	0.804	93.33%	0.276	98.33%	0.054	98.33%	0	98.33%
Sums 1	0	100%	0.148	100%	0.067	100%	0.178	100%
Sums 2	0	100%	0.299	100%	0.009	100%	0.163	100%
Runs	0.101	100%	0.804	100%	0.002	98.33%	0.568	100%
Longest Run	0.534	96.66%	0.233	100%	0.672	100%	0.054	98.33%
Rank	0.602	100%	0.534	100%	0.122	100%	0.135	100%
FFT	0	20.0%	0	40.0%	0	45.0%	0	13.33%
Non-Overlapping	0.296	99.02%	0.343	99.05%	0.27	99.14%	0.285	99.13%
Overlapping	0.025	100%	0.254	95.0%	0.028	100%	0	100%
Universal	0.085	—	0.118	—	0.041	—	0.222	—
Entropy	0.039	100%	0	100%	0.932	100%	0.501	100%
Excursions	—	100%	—	98.21%	—	100%	—	100%
Excursion Variants	—	100%	—	100%	—	100%	—	99.38%
Serial 1	0.003	96.66%	0.074	96.66%	0.008	100%	0.407	100%
Serial 2	0	100%	0.049	100%	0.804	96.66%	0.407	100%
Linear Complexity	0.501	95.0%	0.911	100%	0.706	96.66%	0.862	100%
Average	0.199	93.79%	0.277	95.45%	0.25	95.88%	0.269	94.28%
100% Pass Rate	10		10		10		11	

Set 4

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.378	98.33%	0.111	95.0%	0.195	100%
Block Frequency	0.001	98.33%	0.254	98.33%	0.233	98.33%
Sums 1	0.276	96.66%	0	91.66%	0.091	100%
Sums 2	0.888	100%	0	91.66%	0.025	100%
Runs	0.254	100%	0.834	98.33%	0.324	100%
Longest Run	0	96.66%	0.74	100%	0.067	98.33%
Rank	0.122	100%	0	58.33%	0.091	93.33%
FFT	0.804	96.66%	0	0.0%	0	71.66%
Non-Overlapping	0.303	98.99%	0.486	98.72%	0.498	98.96%
Overlapping	0.06	100%	0.135	98.33%	0.991	98.33%
Universal	0.461	—	0.713	—	0.621	—
Entropy	0.35	98.33%	0.028	98.33%	0.005	100%
Excursions	—	93.75%	—	98.61%	—	96.87%
Excursion Variants	—	100%	—	96.28%	—	93.05%
Serial 1	0.005	100%	0.534	100%	0.378	100%
Serial 2	0.834	100%	0.888	100%	0.437	100%
Linear Complexity	0.148	100%	0.35	95.0%	0.602	100%
Average	0.326	98.60%	0.338	88.66%	0.304	96.80%
100% Pass Rate	8		3		8	

S-AES (Set 4)

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0	100%	0.005	100%	0.035	100%	0.276	100%
Block Frequency	0.804	93.33%	0	98.33%	0.501	100%	0.054	95.0%
Sums 1	0	100%	0	100%	0	100%	0.888	100%
Sums 2	0	100%	0	100%	0.004	100%	0.74	100%
Runs	0.101	100%	0.135	100%	0.122	100%	0.049	100%
Longest Run	0.534	96.66%	0.501	100%	0.602	98.33%	0	96.66%
Rank	0.602	100%	0.95	100%	0.028	98.33%	0.002	100%
FFT	0	20.0%	0	5.0%	0	55.00%	0	80.0%
Non-Overlapping	0.296	99.02%	0.259	99.09%	0.269	99.26%	0.32	98.92%
Overlapping	0.025	100%	0.378	100%	0.501	98.33%	0.01	100%
Universal	0.085	—	0.028	—	0.971	—	0.583	—
Entropy	0.039	100%	0.378	100%	0.932	100%	0.082	100%
Excursions	—	100%	0.546	100%	0.311	100%	—	92.85%
Excursion Variants	—	100%	0.23	100%	0.574	98.98%	—	98.41%
Serial 1	0.003	96.66%	0.023	100%	0.082	100%	0	100%
Serial 2	0	100%	0.101	100%	0.501	100%	0	100%
Linear Complexity	0.501	95.0%	0.378	95.0%	0.082	98.33%	0.469	96.66%
Average	0.199	93.79%	0.23	93.58%	0.324	96.66%	0.232	97.40%
100% Pass Rate	10		12		9		9	

Set 5

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.254	100%	0.009	91.66%	0.706	100%
Block Frequency	0.568	100%	0	91.66%	0.031	100%
Sums 1	0.299	100%	0	90.0%	0.437	100%
Sums 2	0.01	100%	0	86.66%	0.299	100%
Runs	0.011	100%	0.122	95.0%	0.834	98.33%
Longest Run	0.035	100%	0.254	95.0%	0.195	98.33%
Rank	0.74	98.33%	0	28.33%	0	73.33%
FFT	0.009	90.0%	0	0.0%	0	45.0%
Non-Overlapping	0.303	98.94%	0.462	98.59%	0.462	98.91%
Overlapping	0.602	96.66%	0.672	100%	0.534	98.33%
Universal	0.79	—	0.021	—	0.956	—
Entropy	0.011	100%	0.834	100%	0.888	100%
Excursions	—	94.64%	—	98.42%	—	97.91%
Excursion Variants	—	98.41%	—	100%	—	99.07%
Serial 1	0.082	100%	0.407	96.66%	0.888	100%
Serial 2	0.74	100%	0.568	100%	0.602	100%
Linear Complexity	0.163	96.66%	0.568	98.33%	0.74	100%
Average	0.308	98.35%	0.261	85.64%	0.505	94.32%
100% Pass Rate	9		4		8	

S-AES (Set 5)

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.074	100%	0	100%	0.378	100%	0.534	100%
Block Frequency	0.001	100%	0	100%	0.602	100%	0	96.66%
Sums 1	0.001	100%	0	100%	0.233	100%	0.672	100%
Sums 2	0.018	100%	0	100%	0.637	100%	0.637	100%
Runs	0.039	100%	0.534	100%	0.672	100%	0.233	100%
Longest Run	0.501	100%	0.672	100%	0.233	100%	0.254	100%
Rank	0.407	98.33%	0.862	96.66%	0.706	100%	0.672	98.33%
FFT	0	16.66%	0	21.66%	0	30.0%	0	8.33%
Non-Overlapping	0.303	99.15%	0.333	99.03%	0.314	99.14%	0.305	98.86%
Overlapping	0.74	98.33%	0.95	98.33%	0.932	100%	0.911	98.33%
Universal	0.53	—	0.3	—	0.338	—	0.898	—
Entropy	0.025	100%	0.001	100%	0.035	100%	0.501	100%
Excursions	0.361	100%	0.016	97.36%	—	100%	—	100%
Excursion Variants	0.293	100%	0.009	99.7%	—	100%	—	100%
Serial 1	0.862	96.66%	0.213	100%	0.469	100%	0	100%
Serial 2	0.834	100%	0.195	100%	0.407	100%	0.862	100%
Linear Complexity	0.911	98.33%	0.991	98.33%	0.672	100%	0.602	98.33%
Average	0.347	94.21%	0.299	94.44%	0.442	95.57%	0.472	93.67%
100% Pass Rate	10		9		14		10	

Set 6

	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.054	100%	0.378	96.66%	0.054	100%
Block Frequency	0.672	100%	0	100%	0.911	100%
Sums 1	0.031	100%	0.437	95.0%	0.378	100%
Sums 2	0.007	96.66%	0.135	95.0%	0.067	100%
Runs	0.706	100%	0.005	93.33%	0.862	100%
Longest Run	0.049	98.33%	0.672	98.33%	0.932	98.33%
Rank	0.082	100%	0	25.0%	0	68.33%
FFT	0.122	100%	0	0.0%	0	56.66%
Non-Overlapping	0.271	99.21%	0.522	98.79%	0.508	98.94%
Overlapping	0.054	100%	0.637	100%	0.299	100%
Universal	0.213	—	0.076	—	0.031	—
Entropy	0	96.66%	0.091	98.33%	0.074	98.33%
Excursions	—	100%	—	100%	—	98.21%
Excursion Variants	—	100%	—	93.05%	—	100%
Serial 1	0.074	100%	0.568	95.0%	0.501	100%
Serial 2	0.233	100%	0.932	96.66%	0.06	96.66%
Linear Complexity	0.276	98.33%	0.932	98.33%	0.324	98.33%
Average	0.19	99.32%	0.359	86.46%	0.333	94.61%
100% Pass Rate	11		3		8	

S-AES (Set 6)

	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.031	100%	0	100%	0.025	100%	0.011	100%
Block Frequency	0.054	95.0%	0	90.0%	0.003	100%	0.091	100%
Sums 1	0	100%	0	100%	0.003	100%	0.122	100%
Sums 2	0	100%	0	100%	0.005	100%	0	100%
Runs	0.06	100%	0.407	100%	0.163	100%	0.044	100%
Longest Run	0.049	95.0%	0.233	98.33%	0.091	100%	0.233	100%
Rank	0.888	100%	0.534	100%	0.773	100%	0.706	100%
FFT	0	0.0%	0	5.0%	0	25.0%	0	36.66%
Non-Overlapping	0.292	99.21%	0.295	99.03%	0.29	99.17%	0.331	99.13%
Overlapping	0.049	95.0%	0.672	100%	0.299	100%	0.195	100%
Universal	0	—	0.098	—	0.593	—	0.012	—
Entropy	0.254	100%	0.101	100%	0.049	98.33%	0.035	100%
Excursions	0.168	98.07%	—	100%	—	100%	—	100%
Excursion Variants	0.247	99.2%	—	100%	—	100%	—	98.88%
Serial 1	0.049	100%	0.016	100%	0.035	96.66%	0.101	100%
Serial 2	0.111	100%	0.178	96.66%	0.005	100%	0.74	100%
Linear Complexity	0.014	100%	0.324	100%	0.082	100%	0.706	100%
Average	0.133	92.59%	0.191	93.06%	0.161	94.94%	0.222	95.91%
100% Pass Rate	9		11		12		13	

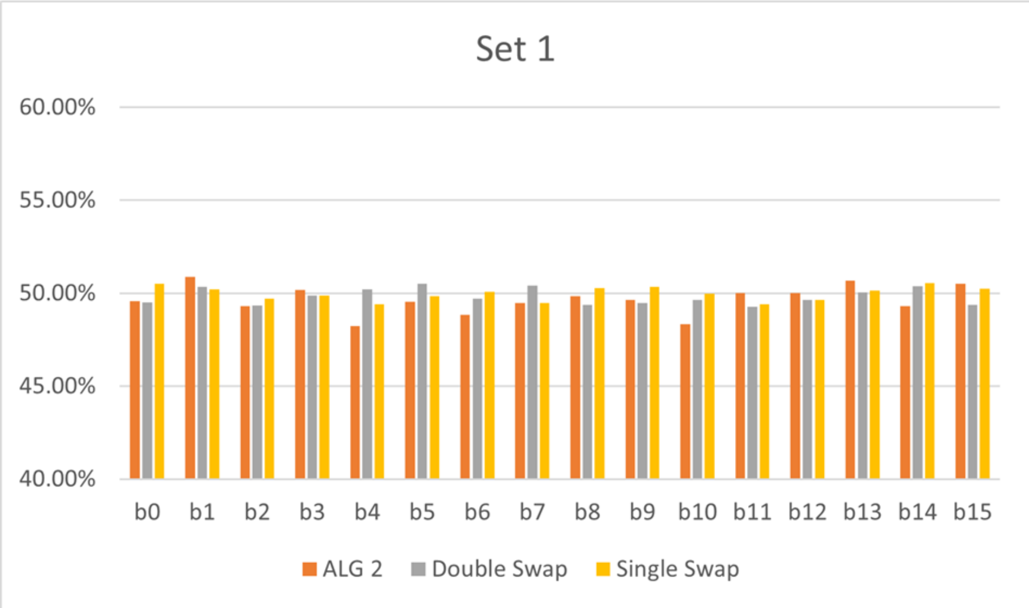
Set 7

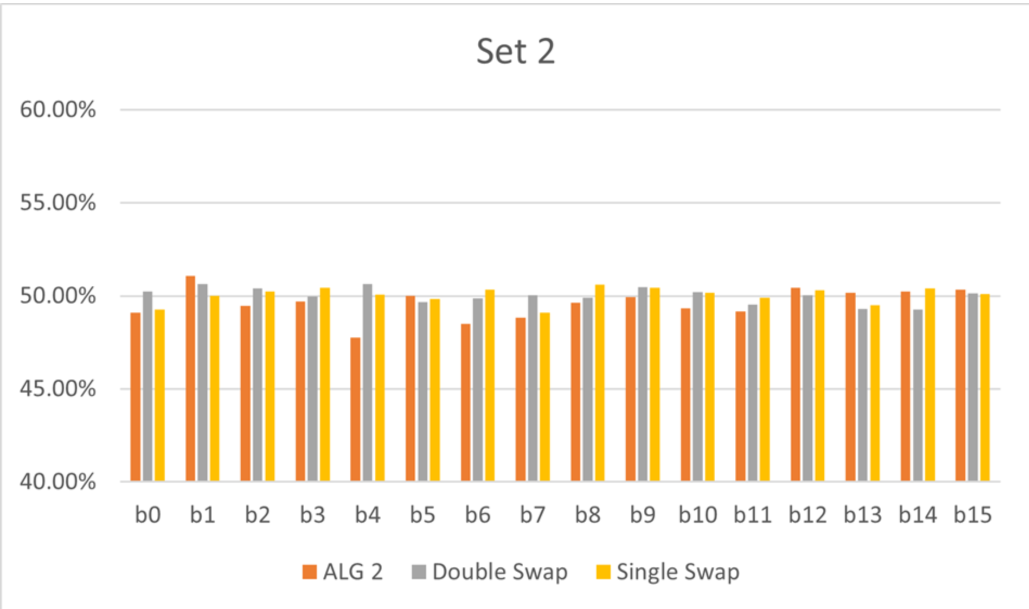
	ALG 2		Double Swap		Single Swap	
	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.74	98.33%	0.911	95.0%	0.706	98.33%
Block Frequency	0.082	100%	0	86.66%	0.195	98.33%
Sums 1	0.035	96.66%	0.008	93.33%	0.834	100%
Sums 2	0.74	96.66%	0.016	91.66%	0.602	100%
Runs	0.018	100%	0.834	98.33%	0.082	100%
Longest Run	0.178	98.33%	0.985	100%	0.602	100%
Rank	0.672	98.33%	0	31.66%	0	75.0%
FFT	0.534	98.33%	0	0.0%	0	73.33%
Non-Overlapping	0.313	99.0%	0.471	98.65%	0.469	98.98%
Overlapping	0.501	100%	0.35	96.66%	0.324	96.66%
Universal	0.279		0.937		0.224	
Entropy	0.122	100%	0.178	98.33%	0.804	100%
Excursions	—	100%	—	100%	—	100%
Excursion Variants	—	100%	—	100%	—	100%
Serial 1	0.023	98.33%	0.568	100%	0.35	100%
Serial 2	0.324	100%	0.862	100%	0.324	100%
Linear Complexity	0.407	100%	0.672	98.33%	0.233	100%
Average	0.331	98.99%	0.453	86.78%	0.383	96.28%
100% Pass Rate	8		5		10	

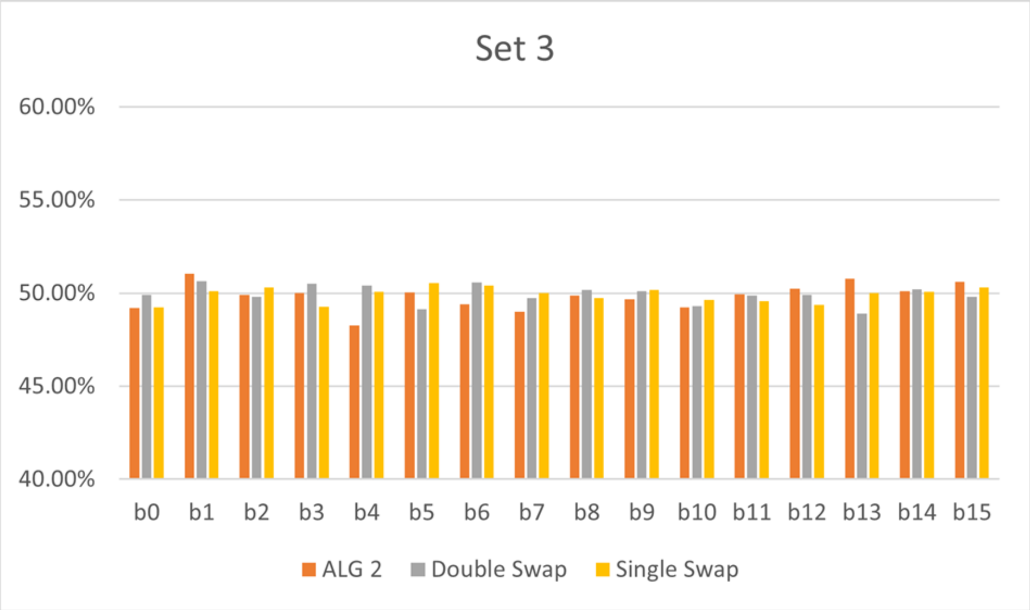
S-AES (Set 7)

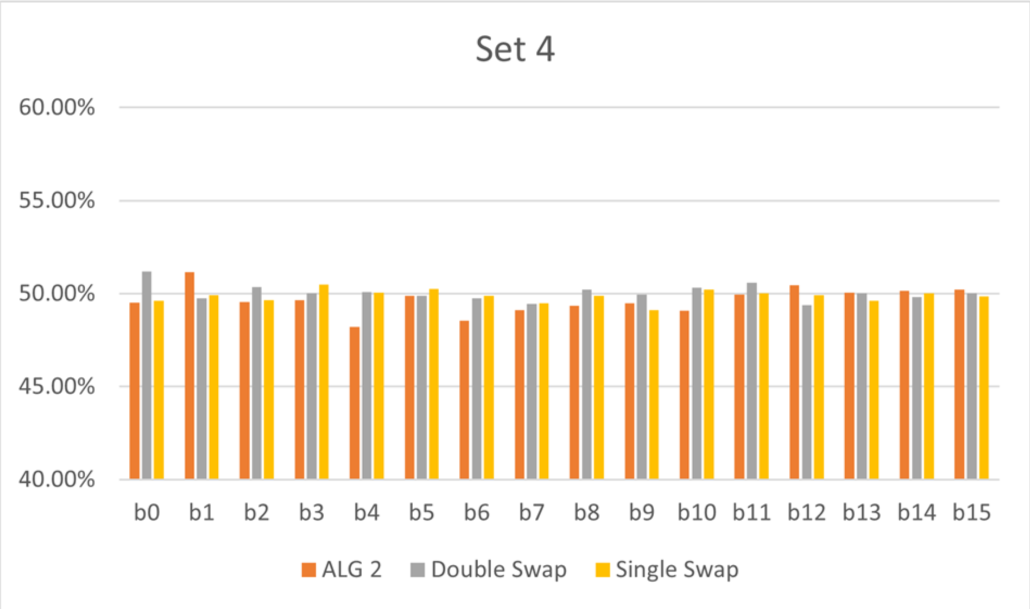
	S-Box 1		S-Box 2		S-Box 3		S-Box 4	
	P-val	Passed	P-val	Passed	P-val	Passed	P-val	Passed
Frequency	0.773	100%	0.018	100%	0.074	100%	0.082	100%
Block Frequency	0	93.33%	0.213	100%	0	98.33%	0.005	96.66%
Sums 1	0.834	100%	0	100%	0.067	100%	0.001	100%
Sums 2	0.862	100%	0.004	100%	0	100%	0.002	100%
Runs	0.007	100%	0.35	100%	0.018	100%	0.013	100%
Longest Run	0.195	100%	0.35	100%	0.534	100%	0.35	98.33%
Rank	0.213	100%	0.122	100%	0.008	100%	0.637	100%
FFT	0	11.66%	0	28.33%	0	13.33%	0	30.0%
Non-Overlapping	0.321	98.99%	0.312	98.98%	0.248	98.98%	0.297	99.22%
Overlapping	0.101	100%	0.163	100%	0.95	100%	0.378	95.0%
Universal	0.103	—	0.669	—	0.807	—	0.832	—
Entropy	0.013	100%	0	96.66%	0.002	100%	0.888	100%
Excursions	—	100%	0.337	98.86%	—	97.91%	0.558	98.95%
Excursion Variants	—	100%	0.427	100%	—	100%	0.478	99.53%
Serial 1	0	100%	0.002	100%	0.008	100%	0.35	100%
Serial 2	0.06	100%	0.568	100%	0.163	100%	0.195	100%
Linear Complexity	0.637	96.66%	0.706	100%	0.706	96.66%	0.637	100%
Average	0.275	93.78%	0.249	95.17%	0.239	94.07%	0.335	94.85%
100% Pass Rate	12		12		11		9	

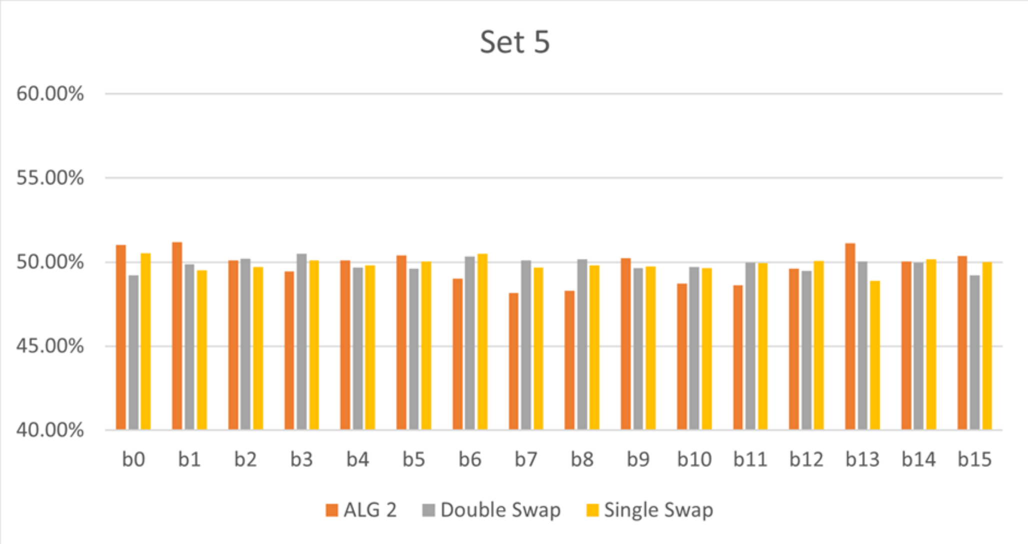
E Avalanche Criterion Analysis Results

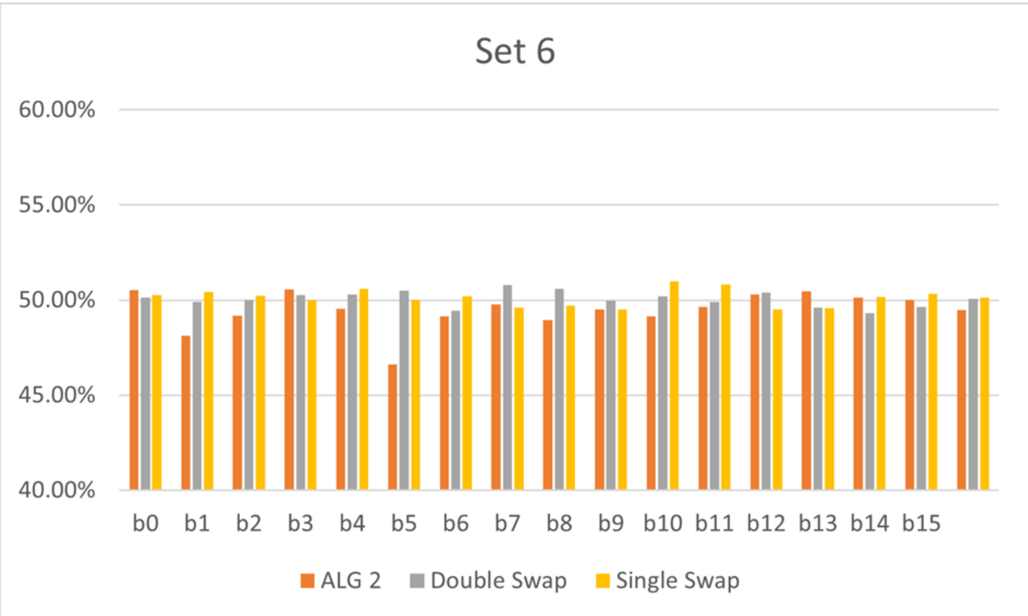


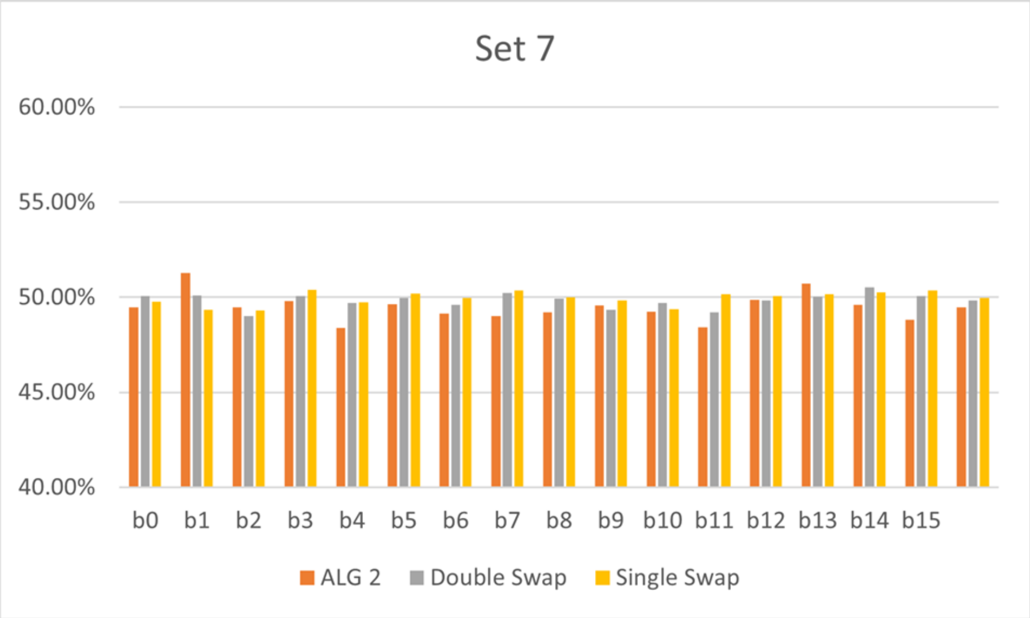


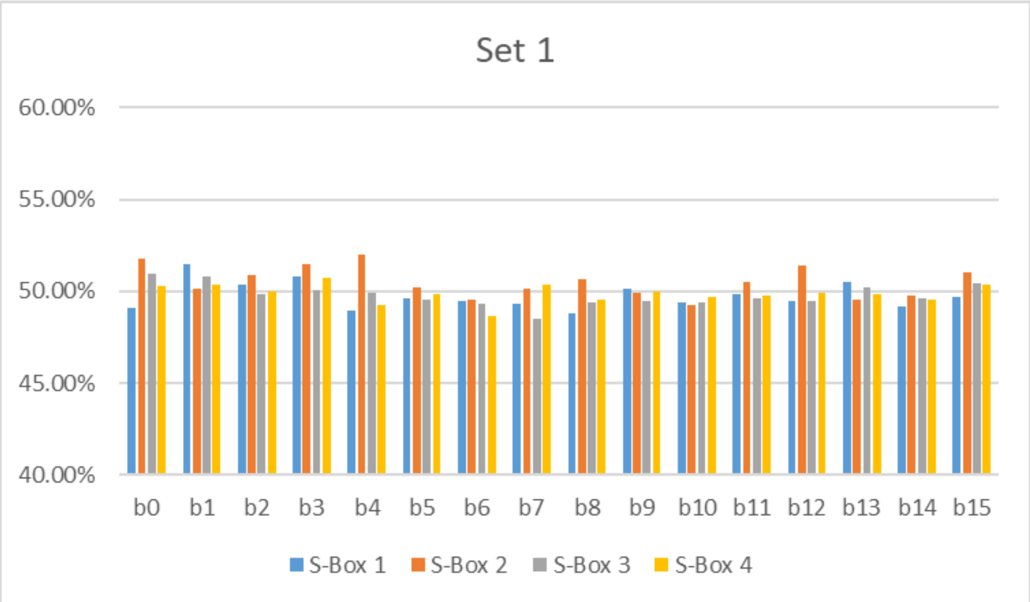

Set 3
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
ALG 2
Double Swap
Single Swap

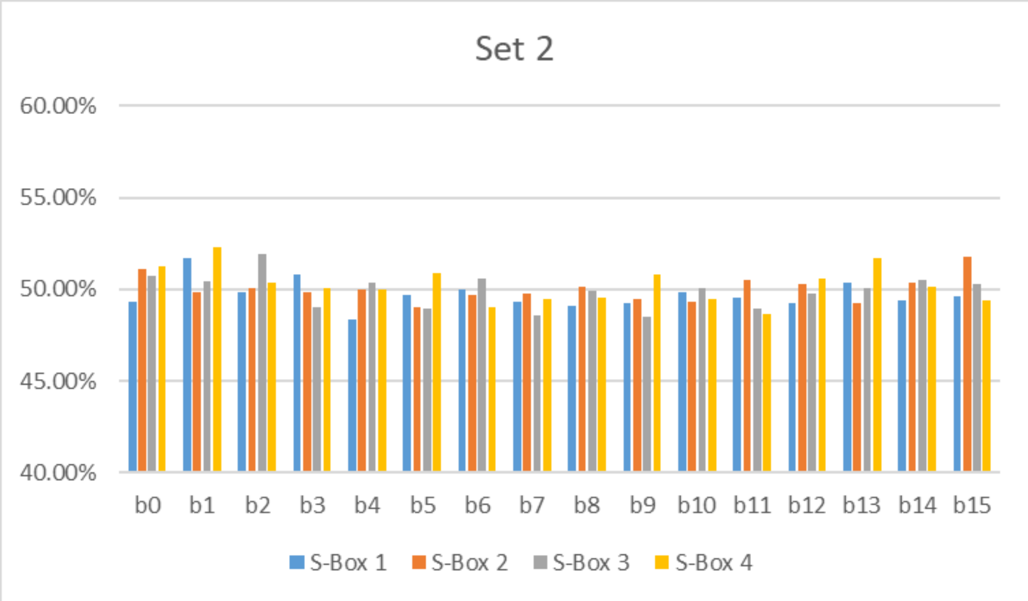

Set 4
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
ALG 2
Double Swap
Single Swap

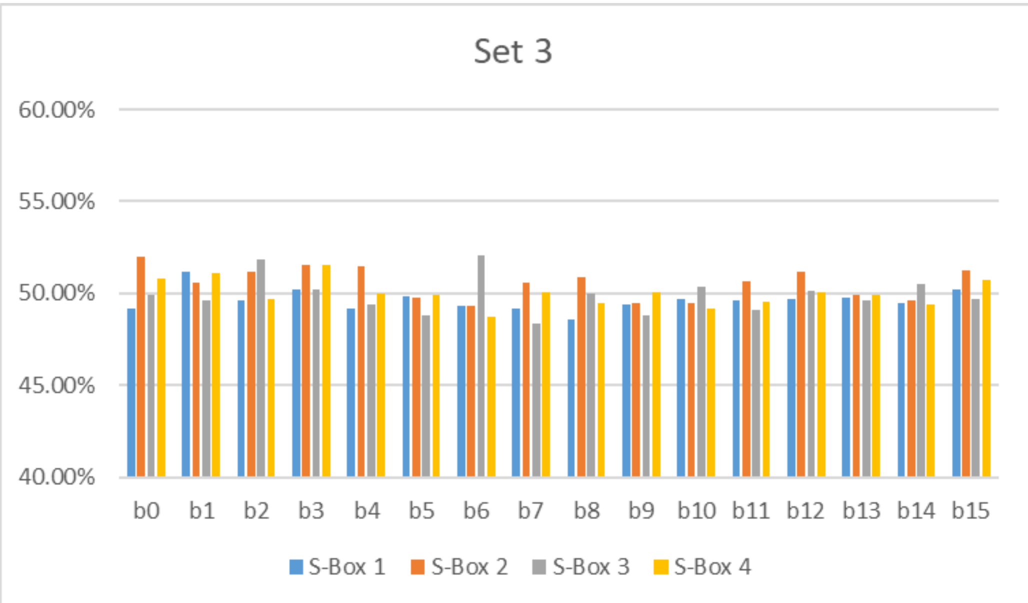

Set 5
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
ALG 2
Double Swap
Single Swap

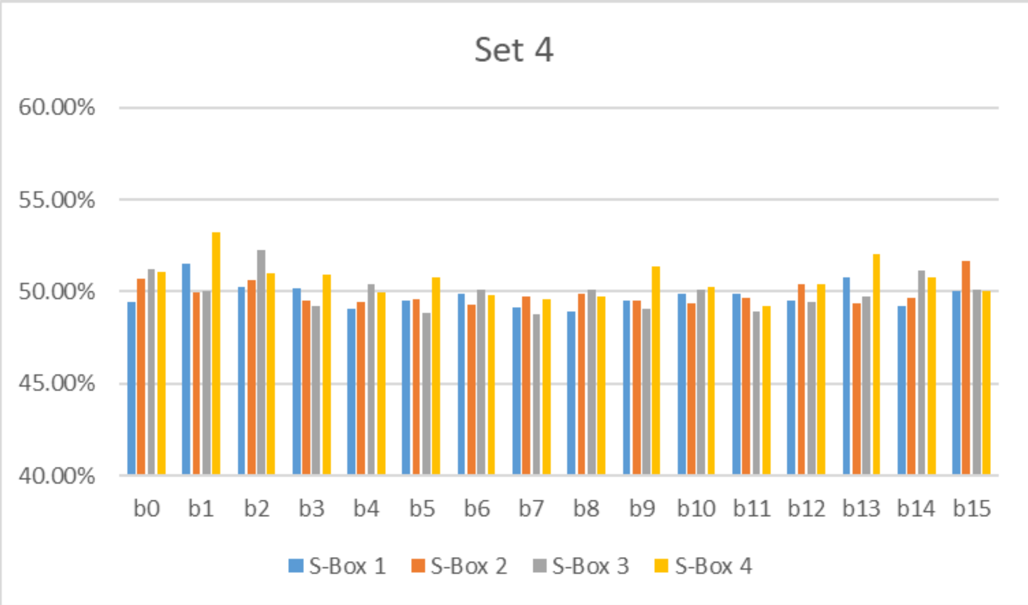

Set 6
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
ALG 2
Double Swap
Single Swap

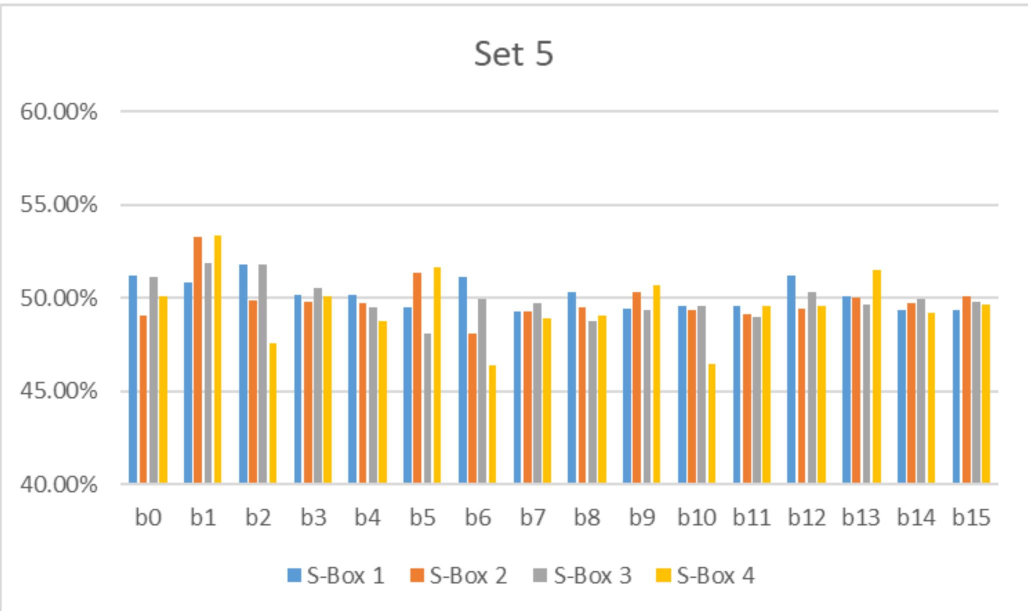

Set 7
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
ALG 2
Double Swap
Single Swap

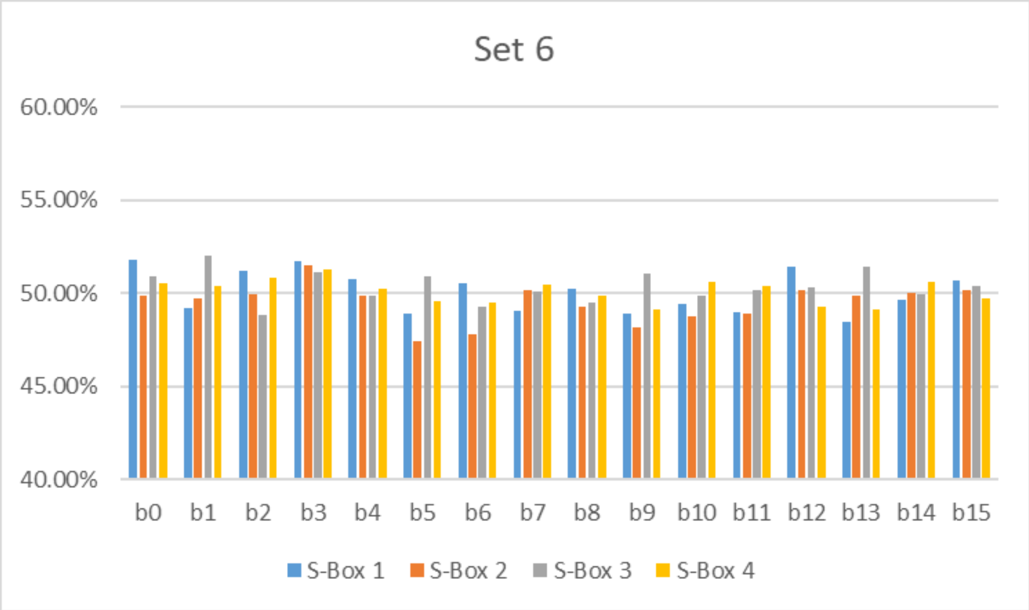

Set 1
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1
S-Box 2
S-Box 3
S-Box 4

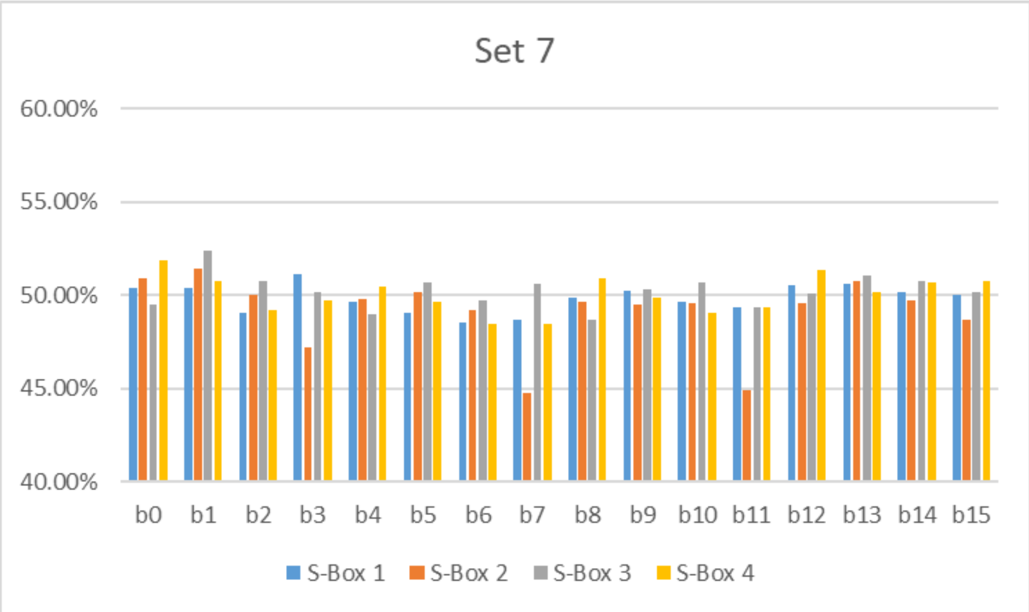

Set 2
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1 S-Box 2 S-Box 3 S-Box 4


Set 3
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1 S-Box 2 S-Box 3 S-Box 4


Set 4
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1 S-Box 2 S-Box 3 S-Box 4


Set 5
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1 S-Box 2 S-Box 3 S-Box 4


Set 6
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1 S-Box 2 S-Box 3 S-Box 4


Set 7
60.00%
55.00%
50.00%
45.00%
40.00%
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
S-Box 1 S-Box 2 S-Box 3 S-Box 4

F ANF of AES

$$
y_0 = x_0x_1x_2x_3x_4x_6x_7 \oplus x_0x_1x_2x_3x_4x_6 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_5x_7 \oplus
x_0x_1x_2x_3x_6x_7 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_3 \oplus x_0x_1x_2x_4x_5x_6x_7 \oplus x_0x_1x_2x_4x_5x_7 \oplus
x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4x_7 \oplus x_0x_1x_2x_5x_6x_7 \oplus x_0x_1x_2x_5x_7 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_7 \oplus
x_0x_1x_2x_6 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_3x_4x_6x_7 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_5x_6 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_6x_7 \oplus
x_0x_1x_4x_5x_6x_7 \oplus x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_6 \oplus
x_0x_1x_7 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus x_0x_2x_3x_4x_5x_6 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_6 \oplus
x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4x_6x_7 \oplus x_0x_2x_4x_7 \oplus
x_0x_2x_4 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5 \oplus x_0x_2x_6 \oplus x_0x_2x_7 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_5x_7 \oplus
x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_6x_7 \oplus x_0x_3x_5x_6 \oplus x_0x_3x_5 \oplus x_0x_3x_6 \oplus x_0x_4x_5x_6 \oplus
x_0x_4x_5x_7 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0x_6 \oplus x_0 \oplus x_1x_2x_3x_4x_6x_7 \oplus
x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5x_7 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_7 \oplus x_1x_2x_3 \oplus x_1x_2x_4x_5x_6x_7 \oplus
x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_6x_7 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4 \oplus x_1x_2x_5x_6x_7 \oplus x_1x_2x_6x_7 \oplus
x_1x_2x_6 \oplus x_1x_2 \oplus x_1x_3x_4x_5x_6x_7 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_6 \oplus x_1x_3x_4 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_7 \oplus
x_1x_3 \oplus x_1x_4x_5x_6 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_6 \oplus x_1x_4 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6 \oplus x_1x_6 \oplus x_2x_3x_4x_5x_6x_7 \oplus
x_2x_3x_4x_5x_6 \oplus x_2x_3x_4x_5x_7 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5 \oplus x_2x_3x_6x_7 \oplus x_2x_3x_7 \oplus x_2x_3 \oplus x_2x_4x_5x_6x_7 \oplus
x_2x_4x_5x_6 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_7 \oplus x_2x_4 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_2x_6 \oplus x_2x_7 \oplus x_2 \oplus
x_3x_4x_7 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_3 \oplus x_4x_5x_6 \oplus x_4x_6 \oplus x_4 \oplus x_5x_6x_7 \oplus x_5x_6 \oplus x_5x_7 \oplus
x_6x_7 \oplus 1
$$

$$
y_1 = x_0x_1x_2x_3x_4x_6x_7 \oplus x_0x_1x_2x_3x_4x_6 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_5x_6x_7 \oplus
x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_4x_5x_6x_7 \oplus x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_5 \oplus
x_0x_1x_2x_4x_6x_7 \oplus x_0x_1x_2x_4x_6 \oplus x_0x_1x_2x_4x_7 \oplus x_0x_1x_2x_5x_6x_7 \oplus x_0x_1x_2x_6x_7 \oplus x_0x_1x_2x_6 \oplus
x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_6 \oplus x_0x_1x_3x_4x_6x_7 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_4x_7 \oplus x_0x_1x_3x_4 \oplus
x_0x_1x_3x_5x_6 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_6x_7 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5 \oplus
x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_6 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5x_6 \oplus x_0x_2x_3x_4x_5x_7 \oplus
x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_7 \oplus x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5x_7 \oplus x_0x_2x_3x_6x_7 \oplus
x_0x_2x_3x_6 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_5x_6x_7 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_7 \oplus x_0x_2 \oplus
x_0x_3x_4x_5x_7 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_6x_7 \oplus x_0x_3 \oplus x_0x_4x_5x_6x_7 \oplus x_0x_4x_5x_6 \oplus
x_0x_4x_5x_7 \oplus x_0x_4x_5 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4 \oplus x_0x_5x_7 \oplus x_0x_6x_7 \oplus x_0x_7 \oplus x_0 \oplus
x_1x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5 \oplus
x_1x_2x_3 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_6x_7 \oplus x_1x_3x_4x_5x_6x_7 \oplus
x_1x_3x_4x_5x_6 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5x_7 \oplus
x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_3 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_7 \oplus x_1x_4 \oplus x_1x_5x_6 \oplus
x_1x_7 \oplus x_2x_3x_4x_5x_7 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_6x_7 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5 \oplus
x_2x_3x_6 \oplus x_2x_3 \oplus x_2x_4x_5x_6x_7 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_6x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_2x_6 \oplus x_2x_7 \oplus
x_3x_4x_5x_6 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_3x_7 \oplus
x_3 \oplus x_4x_5 \oplus x_4x_6 \oplus x_5x_6x_7 \oplus x_6 \oplus x_7 \oplus 1
$$

$$
y_2 = x_0x_1x_2x_3x_4x_5 \oplus x_0x_1x_2x_3x_4x_6x_7 \oplus x_0x_1x_2x_3x_4x_6 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4 \oplus
x_0x_1x_2x_3x_5x_6x_7 \oplus x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_4x_5x_6 \oplus
x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4x_7 \oplus x_0x_1x_2x_5x_7 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_7 \oplus
x_0x_1x_2x_7 \oplus x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_7 \oplus x_0x_1x_3x_4x_6x_7 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_4x_7 \oplus
x_0x_1x_3x_4 \oplus x_0x_1x_3x_5x_6x_7 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3x_6x_7 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3 \oplus
x_0x_1x_4x_5x_6x_7 \oplus x_0x_1x_4x_6x_7 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5 \oplus x_0x_1x_6 \oplus x_0x_1x_7 \oplus
x_0x_2x_3x_4x_5x_6x_7 \oplus x_0x_2x_3x_4x_5x_6 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_7 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5x_6x_7 \oplus
x_0x_2x_3x_5x_7 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5x_6x_7 \oplus x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_6 \oplus
x_0x_2x_4x_7 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_6x_7 \oplus x_0x_2x_5 \oplus x_0x_2x_7 \oplus x_0x_2 \oplus x_0x_3x_4x_5x_7 \oplus x_0x_3x_4x_6 \oplus
x_0x_3x_4x_7 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_6x_7 \oplus x_0x_3x_5x_6 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5 \oplus x_0x_3x_6 \oplus x_0x_3x_7 \oplus x_0x_3 \oplus
x_0x_4x_5x_6x_7 \oplus x_0x_4x_5 \oplus x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4 \oplus x_0x_5x_7 \oplus x_0x_5 \oplus x_0x_6x_7 \oplus x_0x_6 \oplus x_0x_7 \oplus x_0 \oplus
x_1x_2x_3x_4x_5x_6x_7 \oplus x_1x_2x_3x_4x_5x_7 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_4 \oplus
x_1x_2x_3x_5 \oplus x_1x_2x_3x_6x_7 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5x_7 \oplus x_1x_2x_4x_6x_7 \oplus x_1x_2x_4x_7 \oplus
$$

$x_1x_2x_4 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4x_5x_6 \oplus x_1x_3x_4x_6x_7 \oplus$
$x_1x_3x_4 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5x_7 \oplus x_1x_3x_5 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_7 \oplus x_1x_4x_5x_6x_7 \oplus x_1x_4x_5x_7 \oplus$
$x_1x_4x_5 \oplus x_1x_4x_7 \oplus x_1x_4 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_1 \oplus x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_6x_7 \oplus$
$x_2x_3x_4x_6 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5x_6x_7 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_6 \oplus x_2x_3x_7 \oplus x_2x_3 \oplus$
$x_2x_4x_5x_6 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_6x_7 \oplus x_2x_5x_6x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5x_6x_7 \oplus x_3x_4x_5x_6 \oplus$
$x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_4 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_6 \oplus x_4x_5x_6x_7 \oplus x_4x_6x_7 \oplus x_4x_7 \oplus x_5x_6 \oplus x_5 \oplus$
$x_6x_7 \oplus x_7$

$y_3 = x_0x_1x_2x_3x_4x_5x_6 \oplus x_0x_1x_2x_3x_4x_6 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_5x_6x_7 \oplus$
$x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5x_7 \oplus x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_3x_6x_7 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_3 \oplus$
$x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_6x_7 \oplus x_0x_1x_2x_4x_7 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5x_6 \oplus x_0x_1x_2x_5x_7 \oplus$
$x_0x_1x_2x_5 \oplus x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_7 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_4x_7 \oplus$
$x_0x_1x_3x_5x_6 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5x_7 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_7 \oplus$
$x_0x_1x_5x_6 \oplus x_0x_1x_5 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6 \oplus x_0x_1x_7 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus x_0x_2x_3x_4x_5 \oplus$
$x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5x_6 \oplus x_0x_2x_3x_5x_7 \oplus x_0x_2x_3x_6x_7 \oplus x_0x_2x_3x_7 \oplus$
$x_0x_2x_3 \oplus x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_6 \oplus x_0x_2x_4x_7 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_6x_7 \oplus$
$x_0x_2x_5x_6 \oplus x_0x_2x_6x_7 \oplus x_0x_2x_6 \oplus x_0x_2x_7 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_5x_7 \oplus x_0x_3x_4x_6x_7 \oplus$
$x_0x_3x_4x_6 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_6x_7 \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6 \oplus x_0x_3x_7 \oplus x_0x_3 \oplus x_0x_4x_5x_6x_7 \oplus$
$x_0x_4x_5x_6 \oplus x_0x_4x_5 \oplus x_0x_4x_6 \oplus x_0x_5x_6x_7 \oplus x_0x_7 \oplus x_0 \oplus x_1x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_4x_5x_7 \oplus$
$x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_7 \oplus x_1x_2x_3 \oplus$
$x_1x_2x_4x_5x_6x_7 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_5x_6x_7 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5 \oplus$
$x_1x_2x_6x_7 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_6x_7 \oplus x_1x_3x_4x_6 \oplus x_1x_3x_4x_7 \oplus$
$x_1x_3x_4 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5x_6 \oplus x_1x_4x_5x_6 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6 \oplus$
$x_1x_7 \oplus x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_5x_6 \oplus x_2x_3x_4x_5x_7 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \oplus$
$x_2x_3 \oplus x_2x_4x_5x_6x_7 \oplus x_2x_4x_5x_6 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_6x_7 \oplus x_2x_5x_7 \oplus x_3x_4x_5x_6x_7 \oplus$
$x_3x_4x_5x_6 \oplus x_3x_4x_6x_7 \oplus x_3x_4x_7 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6 \oplus x_3x_7 \oplus x_4x_5x_6x_7 \oplus$
$x_4x_5 \oplus x_4 \oplus x_5x_6x_7 \oplus x_5x_6 \oplus x_5x_7 \oplus x_6x_7 \oplus x_6 \oplus x_7$

$y_4 = x_0x_1x_2x_3x_4x_5x_7 \oplus x_0x_1x_2x_3x_4x_5 \oplus x_0x_1x_2x_3x_4x_6x_7 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4 \oplus$
$x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_4x_5x_6 \oplus x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_5x_7 \oplus$
$x_0x_1x_2x_6x_7 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_4x_5x_6 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3x_6x_7 \oplus$
$x_0x_1x_3x_6 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_5x_6 \oplus$
$x_0x_1x_5x_7 \oplus x_0x_1x_6x_7 \oplus x_0x_1 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_6 \oplus$
$x_0x_2x_3x_4 \oplus x_0x_2x_3x_5x_6 \oplus x_0x_2x_3x_5x_7 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_6x_7 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_6 \oplus$
$x_0x_3x_4x_5x_6x_7 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_6x_7 \oplus$
$x_0x_3x_5x_6 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5 \oplus x_0x_3x_6x_7 \oplus x_0x_4x_5x_6x_7 \oplus x_0x_4x_5x_6 \oplus x_0x_4x_5 \oplus x_0x_4x_6x_7 \oplus$
$x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4 \oplus x_0x_5 \oplus x_0x_6x_7 \oplus x_0x_6 \oplus x_0x_7 \oplus x_0 \oplus x_1x_2x_3x_4x_5x_6 \oplus x_1x_2x_3x_4x_5x_7 \oplus$
$x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5x_7 \oplus$
$x_1x_2x_3x_5 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5x_7 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4 \oplus x_1x_2x_5x_6x_7 \oplus x_1x_2x_5x_7 \oplus$
$x_1x_2x_6x_7 \oplus x_1x_3x_4x_5x_6 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5 \oplus$
$x_1x_4x_5x_6x_7 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_1x_5x_7 \oplus x_1x_5 \oplus x_1x_6x_7 \oplus x_1x_6 \oplus x_1 \oplus x_2x_3x_4x_5x_6 \oplus$
$x_2x_3x_4x_5x_7 \oplus x_2x_3x_4x_6x_7 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus$
$x_2x_3 \oplus x_2x_4x_5x_6x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5 \oplus x_2x_6x_7 \oplus x_2 \oplus x_3x_4x_5x_6x_7 \oplus$
$x_3x_4x_5x_7 \oplus x_3x_4x_5 \oplus x_3x_4x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_4x_7 \oplus x_3x_4 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus$
$x_3x_5 \oplus x_3x_6x_7 \oplus x_3x_7 \oplus x_3 \oplus x_4x_5x_7 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6 \oplus x_5x_6x_7 \oplus x_5x_7 \oplus x_5 \oplus x_6x_7$

$y_5 = x_0x_1x_2x_3x_4x_5 \oplus x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_5x_6x_7 \oplus x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5x_7 \oplus$
$x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_3 \oplus x_0x_1x_2x_4x_5x_6x_7 \oplus x_0x_1x_2x_4x_5x_6 \oplus$
$x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4x_6 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_7 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_4 \oplus$
$x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5x_7 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_6x_7 \oplus$
$x_0x_1x_4x_6 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_7 \oplus x_0x_1x_5 \oplus x_0x_1x_6 \oplus$
$x_0x_1x_7 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_7 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_5x_7 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3x_6x_7 \oplus$

$x_0x_2x_4x_5x_6x_7 \oplus x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4 \oplus x_0x_2x_6 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_5x_7 \oplus$
$x_0x_3x_4x_7 \oplus x_0x_3x_5 \oplus x_0x_3 \oplus x_0x_4x_5x_6x_7 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_7 \oplus x_0x_5x_6x_7 \oplus x_0x_5x_6 \oplus$
$x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_4x_7 \oplus x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6 \oplus$
$x_1x_2x_4x_5x_6x_7 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4x_5x_6 \oplus$
$x_1x_3x_4x_6x_7 \oplus x_1x_3x_4x_6 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5x_7 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus$
$x_1x_4x_5x_7 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_1x_5 \oplus x_1x_6x_7 \oplus x_1x_6 \oplus x_2x_3x_4x_5x_6 \oplus$
$x_2x_3x_4x_5 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_5x_6x_7 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_6 \oplus x_2x_3x_7 \oplus x_2x_4x_5x_6x_7 \oplus$
$x_2x_4x_5x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_4 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5x_6 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_5 \oplus$
$x_3x_4x_6x_7 \oplus x_3x_4 \oplus x_3x_5x_7 \oplus x_4x_5x_7 \oplus x_4x_6 \oplus x_4 \oplus x_5x_6x_7 \oplus x_5x_7 \oplus x_6 \oplus x_7 \oplus 1$

$y_6 = x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_4x_5x_6x_7 \oplus$
$x_0x_1x_2x_4x_5x_6 \oplus x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_6x_7 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_5x_6x_7 \oplus x_0x_1x_2x_5 \oplus$
$x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_6 \oplus x_0x_1x_3x_4x_5x_7 \oplus x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4x_6x_7 \oplus x_0x_1x_3x_4 \oplus$
$x_0x_1x_3x_5x_6x_7 \oplus x_0x_1x_3x_6x_7 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5x_7 \oplus x_0x_1x_4 \oplus$
$x_0x_1x_5 \oplus x_0x_1x_6x_7 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_5x_6 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus$
$x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_4x_6x_7 \oplus x_0x_2x_4x_6 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_6x_7 \oplus x_0x_2x_5x_7 \oplus$
$x_0x_2x_5 \oplus x_0x_2x_6 \oplus x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_5 \oplus x_0x_3x_6 \oplus x_0x_4x_5x_6x_7 \oplus$
$x_0x_4x_5 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4 \oplus x_0x_5x_6 \oplus x_0x_5x_7 \oplus x_0x_5 \oplus x_0x_7 \oplus x_1x_2x_3x_4x_5 \oplus$
$x_1x_2x_3x_4x_7 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5x_7 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5 \oplus$
$x_1x_2x_4x_7 \oplus x_1x_2x_5x_6x_7 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4x_5x_6x_7 \oplus x_1x_3x_4x_5x_6 \oplus$
$x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_6 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5x_7 \oplus x_1x_3x_6 \oplus x_1x_3 \oplus x_1x_4x_5x_6x_7 \oplus$
$x_1x_4x_5x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_6x_7 \oplus x_1x_7 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_6x_7 \oplus$
$x_2x_3x_4x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_5x_6x_7 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_7 \oplus x_2x_3 \oplus x_2x_4x_6 \oplus$
$x_2x_4x_7 \oplus x_3x_4x_5x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_5x_7 \oplus x_3x_5 \oplus x_3x_6x_7 \oplus x_3x_7 \oplus x_3 \oplus x_4x_5x_6x_7 \oplus x_4x_5x_6 \oplus$
$x_4x_6 \oplus x_5x_6x_7 \oplus x_5x_7 \oplus x_5 \oplus x_6 \oplus 1$

$y_7 = x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_6x_7 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3 \oplus x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_6 \oplus$
$x_0x_1x_2x_4 \oplus x_0x_1x_2x_5x_7 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_7 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_7 \oplus$
$x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4x_6x_7 \oplus x_0x_1x_3x_4x_7 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5x_6x_7 \oplus x_0x_1x_3x_6 \oplus$
$x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5x_7 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_5 \oplus x_0x_1x_6 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus$
$x_0x_2x_3x_4x_5x_6 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_6 \oplus x_0x_2x_3x_4x_7 \oplus$
$x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5x_6x_7 \oplus x_0x_2x_4x_6 \oplus$
$x_0x_2x_4x_7 \oplus x_0x_2x_5 \oplus x_0x_2x_7 \oplus x_0x_2 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus$
$x_0x_3x_5x_6x_7 \oplus x_0x_3x_5x_6 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5 \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6 \oplus x_0x_3x_7 \oplus x_0x_4x_5 \oplus$
$x_0x_4x_6x_7 \oplus x_0x_5x_6 \oplus x_0x_6x_7 \oplus x_0x_6 \oplus x_0x_7 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_7 \oplus$
$x_1x_2x_3 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6x_7 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_5x_6x_7 \oplus x_1x_2x_6 \oplus x_1x_2 \oplus$
$x_1x_3x_4x_5x_6x_7 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_6 \oplus x_1x_4x_5x_6x_7 \oplus$
$x_1x_4x_5x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_7 \oplus x_1x_5x_6x_7 \oplus x_1x_7 \oplus x_2x_3x_4x_5x_6 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_5 \oplus$
$x_2x_4x_6x_7 \oplus x_2x_4x_6 \oplus x_2x_4 \oplus x_2x_5x_6x_7 \oplus x_2x_5x_6 \oplus x_2x_6x_7 \oplus x_2x_6 \oplus x_2 \oplus x_3x_4x_5x_6x_7 \oplus$
$x_3x_4x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_5x_7 \oplus x_3x_5 \oplus x_4x_5x_6x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_4x_6 \oplus$
$x_4 \oplus x_5x_7 \oplus x_5 \oplus x_7$

References

[1] Lawrence Bassham, Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Stefan Leigh, M Levenson, M Vangel, Nathanael Heckert, and D Banks. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010-09-16 2010.

[2] William J. Buchanan, Shancang Li, and Rameez Asif. Lightweight cryptography methods. *Journal of Cyber Security Technology*, 1(3-4):187–201, 2017.

[3] Chris Christensen. Monoalphabetic substitution ciphers (mascs). https://www.nku.edu/~christensen/1901%20cscmat%20483%20section%201%20introduction%20and%20MASCs.pdf, 2019.

[4] Thomas Häner and Mathias Soeken. The multiplicative complexity of interval checking. *IACR Cryptol. ePrint Arch.*, page 91, 2022.

[5] Kyung-Bae Jang, Gyeong-Ju Song, Hyun-Ji Kim, and Hwa-Jeong Seo. Grover on simplified aes. In *2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, pages 1–4, 2021.

[6] Kyungbae Jang, Gyeongju Song, Hyunjun Kim, Hyeokdong Kwon, Hyunji Kim, and Hwajeong Seo. Efficient implementation of present and gift on quantum computers. *Applied Sciences*, 11(11), 2021.

[7] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing implementations of lightweight building blocks. *IACR Transactions on Symmetric Cryptology*, 2017(4):130–168, Dec. 2017.

[8] Mohammad Ayoub Khan, Mohammad Tabrez Quasim, Norah Saleh Alghamdi, and Mohammad Yahiya Khan. A secure framework for authentication and encryption using improved ecc for iot-based medical sensor data. *IEEE Access*, 8:52018–52027, 2020.

[9] Ilan Komargodski, Moni Naor, and Eylon Yogev. Collision resistant hashing for paranoids: Dealing with multiple collisions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 162–194, Cham, 2018. Springer International Publishing.

[10] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. Energy and area costs of lightweight cryptographic algorithms for authenticated encryption in WSN. *Security and Communication Networks*, 2018:14, 2018.

[11] Ryan Morrison. Post-quantum cryptography algorithm used by aws cracked "in about an hour", Aug 2022.

[12] Yusuf Moosa Motara and Barry Irwin. SHA-1 and the strict avalanche criterion. In Hein S. Venter, Marianne Loock, Marijke Coetzee, Mariki M. Eloff, and Jan H. P. Eloff, editors, *2016 Information Security for South Africa, ISSA 2016, Johannesburg, South Africa, August 17-18, 2016*, pages 35–40. IEEE, 2016.

[13] Mohammad A. Musa, Edward F. Schaefer, and Stephen Wedig. A simplified aes algorithm and its linear and differential cryptanalyses. *Cryptologia*, 27(2):148–177, 2003.

[14] Kaisa Nyberg. Statistical and linear independence of binary random variables. *IACR Cryptol. ePrint Arch.*, page 432, 2017.

[15] Sudheesh K. Rajput and Naveen K. Nishchal. Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem. *Optics Communications*, 309:231–235, 2013.

[16] Stefan Scheel, Jiannis Pachos, E. A. Hinds, and Peter L. Knight. Quantum gates and decoherence, 2004.

[17] Mister Serge and Adams Carlisle. Practical s-box design. 03 1997.

[18] Juan Soto and Lawrence Bassham. Randomness testing of the advanced encryption standard finalist candidates, 2000-04-01 00:04:00 2000.

[19] IonQ Staff. Unveiling IonQ Forte: The First Software-Configurable Quantum Computer — ionq.com. https://ionq.com/posts/may-17-2022-ionq-forte, 2022. [Accessed 23-Feb-2023].

[20] The Qiskit Team. Grover's algorithm, Nov 2022.

[21] Okamura Toshihiko. Lightweight cryptography applicable to various iot devices. *NEC*, 12(1), 2017.

[22] Lionel Sujay Vailshery. IoT connected devices worldwide 2019-2030 | Statista — statista.com. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, 2022. [Accessed 23-Feb-2023].

[23] David Wagner, Nicholas Weaver, Peyrin Kao, Fuzail Shakir, Andrew Law, and Nicholas Ngai. Symmetric-key cryptography. In *Computer Security*, chapter 6. Berkely, 2023.