IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2025, No. 1, pp. 586–631. DOI:10.46586/tches.v2025.i1.586-631

A Framework for Generating S-Box Circuits with Boyer–Peralta Algorithm-Based Heuristics, and Its Applications to AES, SNOW3G, and Saturnin

Yongjin Jeon*[1], Seungjun Baek*[1], Giyoon Kim[1], and Jongsung Kim[1,2](✉)

[1] Department of Financial Information Security, Kookmin University, Republic of Korea
{idealtop18,hellosj3,gi0412,jskim}@kookmin.ac.kr
[2] Department of Information Security, Cryptology, and Mathematics, Kookmin University, Republic of Korea

Abstract. In many lightweight cryptography applications, low area and latency are required for efficient implementation. The gate count in the cipher and the circuit depth must be low to minimize these two metrics. Many optimization strategies have been developed for the linear layer, led by the Boyer–Peralta (BP) algorithm. The Advanced Encryption Standard (AES) has been a focus of extensive research in this area. However, while the linear layer uses only XOR gates, the S-box, which is an essential nonlinear component in symmetric cryptography, uses various gate types, making optimization challenging, particularly as the bit size increases.

In this paper, we propose a new framework for a heuristic search to optimize the circuit depth or XOR gate count of S-box circuits. Existing S-box circuit optimization studies have divided the nonlinear and linear layers of the S-box, optimizing each separately, but limitations still exist in optimizing large S-box circuits. To extend the optimization target from individual internal components to the entire S-box circuit, we extract the XOR information of each node in the target circuit and reconstruct the nodes based on nonlinear gates. Next, we extend the BP algorithm-based heuristics to address nonlinear gates and incorporate this into the framework. It is noteworthy that the effects of our framework occur while maintaining the AND gate count and AND depth without any increase.

To demonstrate the effectiveness of the proposed framework, we apply it to the AES, SNOW3G, and Saturnin S-box circuits. Our results include depth improvements by about 40% and 11% compared to the existing AES S-box [BP10] and Saturnin super S-box [CDL+20] circuits, respectively. We implement a new circuit for the SNOW3G S-box, which has not previously been developed, and apply our framework to reduce its depth. We expect the proposed framework to contribute to the design and implementation of various symmetric-key cryptography solutions.

Keywords: Lightweight cryptography · S-box · Low-latency implementation · Circuit depth · Gate count · AES · SNOW3G · Saturnin

1 Introduction

With the development of communication technology and small-device manufacturing technology, encryption is required in many resource-constrained environments, such as the Internet of Things and radio-frequency identification. The National Institute of Standards and Technology (NIST) recognized this problem and decided to standardize Ascon, which was selected for lightweight cryptography standardization [oSN23]. In this context, many

*These authors contributed equally to this work.

Received: 2024-07-15 Accepted: 2024-09-15 Published: 2024-12-09

lightweight cryptographic algorithms have also been developed [SLH24, ABD+23, BDD+23, BLMR19, ARS+15]. Lightweight ciphers developed for Internet of Things environments can enhance the performance of new devices but may not maintain compatibility with existing devices. Environments that use traditional cryptography are unlikely to adapt quickly, and commonly employed cryptosystems, such as `AES` [DR02], continue to secure various devices. Therefore, research should focus on making existing cryptographic systems more lightweight to reduce costs in configuring network environments with lightweight devices.

When implementing a cryptographic algorithm, low area and latency are critical for many applications. The gate equivalent is a measure of area, effectively approximating the complexity of digital electronic circuits. Reducing the gate count of a circuit directly reduces the number of gate equivalents. From another perspective, many applications require low-latency, including automobiles, robots, and mission-critical computational applications. Recently, the importance of low latency has gained more attention because it influences the throughput of encryption and decryption and plays a critical role in the efficiency of ciphers. The depth of a circuit measures the latency of the implemented circuit. Therefore, when designing an efficient cryptographic algorithm, a low gate count and circuit depth must be considered.

The S-box is the most critical component creating confusion in symmetric-key cryptography. The S-box constitutes a significant load in cryptographic implementations; thus, efficiently implementing it is crucial. However, optimizing circuits that include nonlinear gates is challenging, and several tools have contributed to overcoming this difficulty, such as the LIGHTER [JPST17], PEIGEN [BGLS19], and SAT solver-based tools [Sto16, ZH23], graph based A* search tools [JBK24], and others. Some tools can optimize the number of nonlinear gates, aiding in efficient side-channel analysis countermeasures, but this optimization is challenging for large S-boxes of at least 8 bits. This limitation is compared to heuristic searches optimizing 32-bit matrices [LXZZ21, SFX23] in terms of bit size because S-box circuits involve many operation types (i.e., gates) and require more careful consideration of the order of operations. For example, for three bit values $a, b, c \in \mathbb{F}_2$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ holds, but $(a \cdot b) \oplus c \neq a \cdot (b \oplus c)$; hence, the value varies depending on the order of operations.

The `AES` S-box, a representative large S-box, is defined by a combination of the inverse operation and affine function over the finite field $GF(2^8)$. As $GF(2^8)$ is a field extension of $GF(2^4)$, it can be decomposed into a combination of multiplication and inverse operations over $GF(2^4)$. Moreover, $GF(2^4)$ is also a field extension of $GF(2^2)$, and can be decomposed into a combination of multiplications and inverse operations over $GF(2^2)$. The operations over $GF(2^2)$ are performed at the bit level, translating these operations directly into gates. The efficiency of the circuit depends on how the field is decomposed based on the selected basis. The normal, polynomial, and mixed bases [Can05, SMTM01, NNT+10] are well known, and redundant representations also exist such as polynomial ring representation [Dro98] and the redundantly represented basis [NNI12]. The overall process of transforming the `AES` S-box into the mentioned bases in $GF(2^8)$, and then reverting it, can be expressed as a multiplication of linear matrices. This matrix is combined with the affine function applied after the inverse operation in $GF(2^8)$, and the combined linear layer is optimized using a heuristic algorithm. However, the optimization of parts excluding the linear layer still requires improvement.

In this context, developing a tool for the overall optimization of large S-box circuits benefits efficient circuit implementation. The most challenging aspect of overall optimization is considering the combination and sequence of gates, and the `AES` S-box is a representative example. The existing literature on constructing an `AES` S-box circuit typically separates the entire S-box circuit into small S-boxes and linear layers, optimizing the linear layers without considering the small S-box. However, if small S-boxes and linear layers can be

integrated and optimized, a metric element may be amortized between the two layers, but no such research has been conducted so far.

Contributions. This paper proposes a new framework for a heuristic search to optimize the circuit depth or XOR gate count while maintaining the AND gate count and the AND depth of S-box circuits, applying this framework to the `AES`, `SNOW3G`, and `Saturnin` S-boxes. The contributions of this work are two-fold, summarized as follows:

1. First, this study proposes a framework optimizing the depth or XOR gate count while maintaining the AND gate count and the AND depth of the S-box circuit. Research on optimizing S-box circuits has primarily employed mathematical automation tools, such as SAT solvers [Sto16, BMD+20, ZH23] or pathfinding algorithms by graphing the circuit [JPST17, BGLS19, JBK24]. Because these methods are based on a thorough investigation, they tend to become more difficult as the size of the S-box or the number of operations increases. For large S-boxes, such as the `AES` S-box, the approach of optimizing the small S-boxes and linear layers separately before combining them has been widely adopted. However, the proposed framework extracts information from each node of the target circuit and reconstructs them based on nonlinear gates. Adopting a new approach that uses Boyar–Peralta (BP) algorithm-based heuristics to integrate and optimize the small S-boxes and linear layers can amortize the optimization process and offer possibilities for further optimization. We redefine the commonly used concepts of *distance* and *Dist* in BP algorithm-based heuristics. Based on this, we extend the heuristics to address nonlinear gates not presented in the linear layer. For higher performance, we also apply various circuit modification techniques, such as switching AND and OR gates. The proposed approach can manage 8-bit `AES` [DR02], `SNOW3G` [BHNS10] S-box circuits, and the 16-bit `Saturnin` [CDL+20] S-box circuit, all of which are difficult to manage with existing tools. Figure 1 illustrates how the proposed framework optimizes the circuit in terms of depth.

2. To demonstrate the effectiveness of the proposed framework, we incorporate the random-normal-BP (RNBP) and BP with a depth limit (BPD) algorithms (BP algorithm-based heuristics) into the framework and apply them to the `AES` [BP10, BP12], `SNOW3G` [BHNS10], and `Saturnin` S-box [CDL+20] circuits. To conduct extensive experiments on `AES` S-box circuits, we find four new `AES` S-box circuits using the method from [JBK24], based on the circuits in [BP10, BP12]. By applying our framework to those six circuits, we discover several improved `AES` S-box circuits in terms of depth and XOR gate count. It is worth noting that we identify a circuit that reduces the depth from 27 to 24, compared to the best circuit in [mt16] with an AND gate count of 32, surprisingly reducing the AND depth from 6 to 5 as well. In addition, for the circuit discovered by Calik [mt16], we reduce the depth from 27 to 26, while maintaining the AND gate count of 32, XOR gate count of 81, and AND depth of 6. For the same AND gate count and the AND depth, we also lower the depth to 18, using, at most, 12 more XOR gates. We also obtain an `AES` S-box circuit with AND depths of 4 and total gate depth of 15, representing an approximately 7% improvement in depth. This result is the best in terms of depth among the existing `AES` S-box circuits with the lowest AND depth. From another perspective, we obtain a circuit with a reduction in the XOR gate count from 94 to 81, a 14% improvement, although the depth increased. In summary, when applied to `AES` S-box circuits, the proposed framework reduced the depth by up to 11 or the XOR gate count by up to 47, representing about 40% and 32% improvements, respectively. For the `SNOW3G` S-box and `Saturnin` super S-box, the depth is reduced by about 25% and 11%, from 50 to 35 and from 28 to 25, respectively.

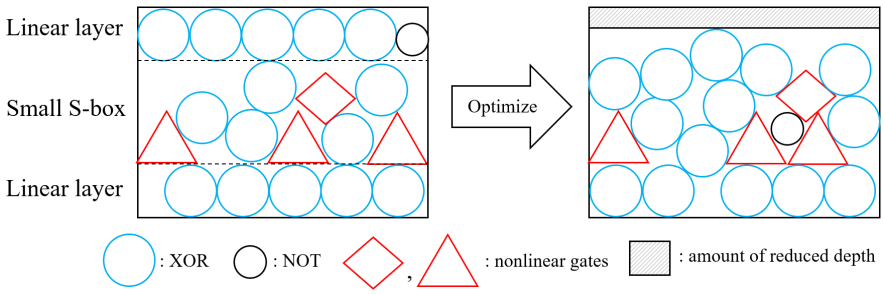

Figure 1: Our framework for optimization of the circuit depth of a large S-box

Organization. Section 2 introduces the notation and BP algorithm-based heuristics (i.e., the RNBP and BPD algorithms). Next, Section 3 presents the proposed framework, divided into pre-processing, optimization, and post-processing stages, demonstrating how the RNBP and BPD algorithms are incorporated into the framework as examples during the optimization steps. Section 4 investigates new circuits against `AES` and `SNOW3G` S-boxes for experiments with the proposed framework, and presenting the optimization results for various `AES` and `SNOW3G` S-box circuits and the `Saturnin` super S-box circuit. Section 5 explains how the proposed framework shifts the paradigm in the field of S-box circuit optimization. Finally, Section 6 concludes the paper.

Software and Experimental Results. Our code can be found at https://github.com/lemontrr/Extended-BP-Framework. The code can be easily applied to optimize other S-boxes if the circuits are provided.

2 Preliminaries

In this section, we introduce the notation in this paper and describe the BP, RNBP, and BPD algorithms.

2.1 Notation

The $\mathbb{F}_2$ is a finite field with the set $\{0,1\}$ equipped with multiplication $\cdot$ and addition $\oplus$ operations, and $\mathbb{F}_2^n$ is an n-dimensional vector space over $\mathbb{F}_2$. A gate is a function from $\mathbb{F}_2^*$ to $\mathbb{F}_2$, and depending on the value of $*$, it is a $*$-fanin gate. The 1-fanin gates include $BUFFER$ and NOT, whereas the 2-fanin gates include AND, OR, $NAND$, NOR, XOR, and $XNOR$. The definitions of these gates for $a, b \in \mathbb{F}_2$ are as follows:

$$\begin{array}{lll} BUFFER(a) = a; & NOT(a) = a \oplus 1; & \\ AND(a,b) = a \cdot b; & OR(a,b) = (a \oplus 1) \cdot (b \oplus 1) \oplus 1; & XOR(a,b) = a \oplus b; \\ NAND(a,b) = a \cdot b \oplus 1; & NOR(a,b) = (a \oplus 1) \cdot (b \oplus 1); & XNOR(a,b) = a \oplus b \oplus 1. \end{array}$$

Among these gates, AND, OR, $NAND$, and NOR are nonlinear gates, and the rest are linear. All nonlinear gates in this paper are 2-fanin gates. Composing appropriate linear gates at the inputs and outputs can generate operations with different inputs and the same output or modify the nonlinear gates into other nonlinear gates. Section 3.2 describes this property in detail.

The gate inputs and outputs, called nodes, must be stored to implement the gate. The use of a single gate implies a relationship in which one or two nodes are input into the gate and one node is output. The gate is defined as G, the input nodes as v (resp. v, v'), and the output node as w. Thus we define this relationship as $(w : G, \{v\})$ (resp.

$(w : G, \{v, v'\}))$. For example, when a NOT gate is used, it is written as $(w : NOT, \{v\})$, meaning $w = v \oplus 1$, and when an AND gate is used, it is written as $(w : AND, \{v, v'\})$ and indicates that $w = v \cdot v'$. A circuit is represented as a sequence of relationships and is defined below.

Definition 1. *The number of gates used in a circuit is c, where $G_0, \cdots, G_{c-1}$ are gates, and $w_0, \cdots, w_{c-1}$ represent the output nodes of each gate. For each i, V_i denotes the set of input nodes for G_i. If $x_0, \cdots, x_{n-1}$ denote the input nodes of the entire circuit, and $y_0, \cdots, y_{m-1}$ represent the output nodes of the circuit, then $i_j (< c)$ exists, such that $y_j = w_{i_j}$ for all $j < m$. Then, circuit $\mathcal{C}$ is defined as a list of tuples, as follows:*

$$\mathcal{C} = [(w_0 : G_0, V_0), (w_1 : G_1, V_1), \cdots, (w_{c-1} : G_{c-1}, V_{c-1}),$$
$$(y_0 : BUFFER, \{w_{i_0}\}), (y_1 : BUFFER, \{w_{i_1}\}), \cdots, (y_{m-1} : BUFFER, \{w_{i_{m-1}}\})],$$

where $v \in \{x_0, x_1, \cdots, x_{n-1}\} \cup \{w_j | j < i\}$ for all $v \in V_i$ $(0 \leq i < c)$, and the output nodes $w_0, \cdots, w_{c-1}$ of the gates are all distinct nodes.

The number of input and output nodes, n and m, respectively, are the input and output size of the circuit. When expressing the number of times a specific gate is used in a circuit, the gate is prefixed with #. For example, #XOR is the number of XOR gates in the circuit.

The depths of the nodes are defined inductively and depend on the circuit. Depth refers to the total time required to run a circuit (i.e., the length of the longest path involved in computing an output). The depth of a node w in the circuit is denoted as $\mathcal{D}(w)$. The input and output sizes of circuit $\mathcal{C}$ are n and m, respectively, and the *max* function takes an arbitrary number of inputs and returns the largest value among them. Then, the depth is formally defined with the following properties:

- For $i < n$, $\mathcal{D}(x_i) = 0$.
- For any nodes v and w, if $(w : BUFFER, v) \in \mathcal{C}$, then $\mathcal{D}(w) = \mathcal{D}(v)$.
- For any nodes v and w, if $(w : NOT, v) \in \mathcal{C}$, then $\mathcal{D}(w) = \mathcal{D}(v) + 1$.
- For any nodes v_0, v_1, and w and the 2-fanin gate G, if $(w : G, v_0, v_1) \in \mathcal{C}$, then $\mathcal{D}(w) = max\,(\mathcal{D}(v_0), \mathcal{D}(v_1)) + 1$.

The depth of $\mathcal{C}$ is defined as $\max\,(\mathcal{D}(y_0), \cdots, \mathcal{D}(y_{m-1}))$.

2.2 BP Algorithm and Its Variants

Boyar and Peralta argued that the linear layer can be represented as a matrix, and optimizing its XOR gate count is NP-hard, necessitating the development of heuristic algorithms [BP10]. To address this problem, they proposed the heuristic BP algorithm to reduce the XOR gate count. The BP algorithm has many variants, with aims falling into two categories: minimizing the XOR gate count or minimizing the XOR gate count with a depth limit. In this section, we introduce the BP, RNBP, and BPD algorithms.

BP and RNBP: Minimizing the XOR Gate Count. The BP algorithm starts by initializing S (called the base) as the set of input nodes $x_0, x_1, \cdots, x_{n-1}$ for a circuit with input and output sizes of n and m, respectively. Then, the algorithm repeatedly selects a pair of nodes from the base, runs XOR on them, and stores the results in the base. When all output nodes $y_0, \cdots, y_{m-1}$ (called targets) are included in the base, the algorithm terminates and outputs the constructed circuit up to that point. To select node pairs wisely, we calculated the distance, measuring how far each target is from the base (i.e., the

minimum number of additional XOR operations needed to implement the target). The distance δ is defined below for base S and each target y_i:

$$\delta(S, y_i) = \min \left\{ d \mid \exists v_0, \cdots, v_{d-1} \in S \text{ such that } y_i = \bigoplus_{j=0}^{d-1} v_j, \text{ for } d \leq |S| \right\}.$$

The distances for each target are calculated based on the above definition, and the distance vector $Dist$ is formed from these distances:

$$Dist = [\delta(S, y_0), \delta(S, y_1), \cdots, \delta(S, y_{m-1})]$$

The BP algorithm selects node pairs by making them compete against each other. For each node pair (v_i, v_i'), the selection strategy is as follows:

1. The pair that minimizes the sum of the elements in the new Dist created by $S \cup \{v_i \oplus v_i'\}$ wins.

2. The pair that maximizes the Euclidean norm of the new Dist created by $S \cup \{v_i \oplus v_i'\}$ wins.

The Euclidean norm of $Dist$ is defined as $\sqrt{\sum_{i=0}^{m-1} \delta(S, y_i)^2}$. Pairs first compete using Strategy 1, and if a tie occurs, they compete using Strategy 2. The pair is randomly chosen if a tie also occurs using the second strategy.

If a specific target is implemented with a single XOR operation, no method is more efficient than that operation, expressed as a distance of 1 to the target. Thus, pairs whose distance changes from 1 to 0 are selected first without competition. This strategy is called a *pre-emptive strategy*.

In the BP algorithm, two notable improvements exist without significant changes to the strategy. The first improvement concerns the timing of triggering the pre-emptive strategy. The traditional BP algorithm determines whether a pair qualifies for the pre-emptive strategy while pairs are competing. If a pair qualifies, it is selected, but unnecessary competition occurs until that point. Reyhani et al. [RTA18] proposed that pairs suitable for the pre-emptive strategy can be identified as soon as the distance decreases from 2 to 1; thus, these pairs are selected without further competition. This improvement reduces the computational effort spent on unnecessary competition.

The second improvement is the equalization of selection probabilities for tied pairs. The BP algorithm compares the pair against newly examined pairs, discarding the losing pair and selecting the winning pair. A random selection to break the tie is also made during this process, increasing the final selection probability for later pairs. If the tied pairs are investigated in the order $(v_0, v_0'), (v_1, v_1'), (v_2, v_2')$, and (v_3, v_3'), the probability of each pair being selected is $1/8, 1/8, 1/4$, and $1/2$, respectively. Tan and Peyrin [TP20] improved the algorithm by collecting all pairs resulting in ties from Strategies 1 and 2, making a uniformly random selection among them. This algorithm is called RNBP.

BPD: Minimizing the XOR Gate Count with a Depth Limit. Li et al. [LSL+19] proposed the BPD algorithm, which reduces XOR gates under a limited depth for low-latency implementation. This algorithm is based on the BP algorithm and adds a feature to limit the depth required to implement the target. They first proposed the following theorem to obtain the minimum depth to implement an expression solely comprising XOR operations.

Theorem 1. *[LSL+19] Let $S = \{v_0, v_1, \cdots, v_n\}$ be a set of nodes with $\mathcal{D}(v_i) = d_i$, then the lower bound of the depth of the circuit implementing $z = v_0 \oplus \cdots \oplus v_n$ is $\lceil log_2 \sum_{i=0}^{n-1} 2^{d_i} \rceil$.*

Based on Theorem 1, the H-distance δ_H is defined to limit the depth in the BPD algorithm. In addition, δ_H represents the additional XOR gate count to implement the target without exceeding the depth H. If the implementation is infeasible, it outputs ∞:

$$\delta_H(S, y_i) = \min\left(\left\{ d \mid \exists v_0, \cdots, v_{d-1} \in S \text{ s.t. } y_i = \bigoplus_{j=0}^{d-1} v_j \text{ and } \left\lceil \log_2 \left(\sum_{j=0}^{n-1} 2^{\mathcal{D}(v_j)} \right) \right\rceil \leq H \text{ for } d \leq |S| \right\} \cup \{\infty\}\right).$$

The BPD algorithm uses δ_H to construct $Dist$ and selects node pairs by following the strategy of the BP algorithm, where pairs exceeding the depth H are excluded from the selection. Additionally, the depths of all variables in the base are stored in Δ and used to determine whether the depth exceeds a certain threshold. For an appropriate c, when $S = \{v_0, v_1, \cdots, v_{c-1}\}$, Δ is defined as follows:

$$\Delta = [\mathcal{D}(v_0), \mathcal{D}(v_1), \cdots, \mathcal{D}(v_{c-1})].$$

3 Generating S-Box Circuits with BP-based Heuristics

In this section, we introduce a new framework for heuristic search aimed at optimizing the circuit depth or XOR gate count in S-box circuits while preserving the AND gate count and AND depth. To achieve this aim, we described the three steps that constitute the proposed framework and explained the process of incorporating BP-based heuristics, such as the RNBP and BPD algorithms.

3.1 Overview of the Framework

The framework is divided into three steps: a pre-processing step that transforms the circuit, an optimizing step that employs embedded tools, and a post-processing step that manages NOT gates. Figure 2 illustrates the overall structure.

Pre-processing Step. The pre-processing step extracts the XOR information from the target circuit so that the framework can operate in the optimizing step, which manages circuits with nonlinear gates. Next, the circuit is transformed into multiple forms $\mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_{p-1}$ where p denotes the number of transformed circuits. This process allows the optimizing step to process the circuit with various configurations. Specifically, we employed equivalent circuits to convert the XOR information and perform multiple optimizing steps. This strategy relies on the fact that the BP-based heuristic has demonstrated improved performance through simple matrix transformations (row and column transformations) [BFI19, BFI21].

Finally, the NOT operations are removed from the XOR information and stored separately. An additional node representing the constant 1 must be considered to address the NOT operations. In Figure 2, $\mathcal{C}_i^*$ represents $\mathcal{C}_i$ with the NOT operation removed for $i < p$. Although NOT gates typically have less load than other gates, the extended BP-based heuristic treats the node with a constant of 1, the same as any other node. Experimentally, adding the NOT gates later is effective. Therefore, the NOT gate is removed in advance, and the node in which the NOT gate was used is recorded and added during the post-processing step.

Optimizing Step. The optimizing step requires a heuristic for optimizing the linear layer (extended BP-based heuristics) and extends the BP-based heuristic. Simple modifications eliminate errors and enable the heuristic to manage nonlinear gates, which the original

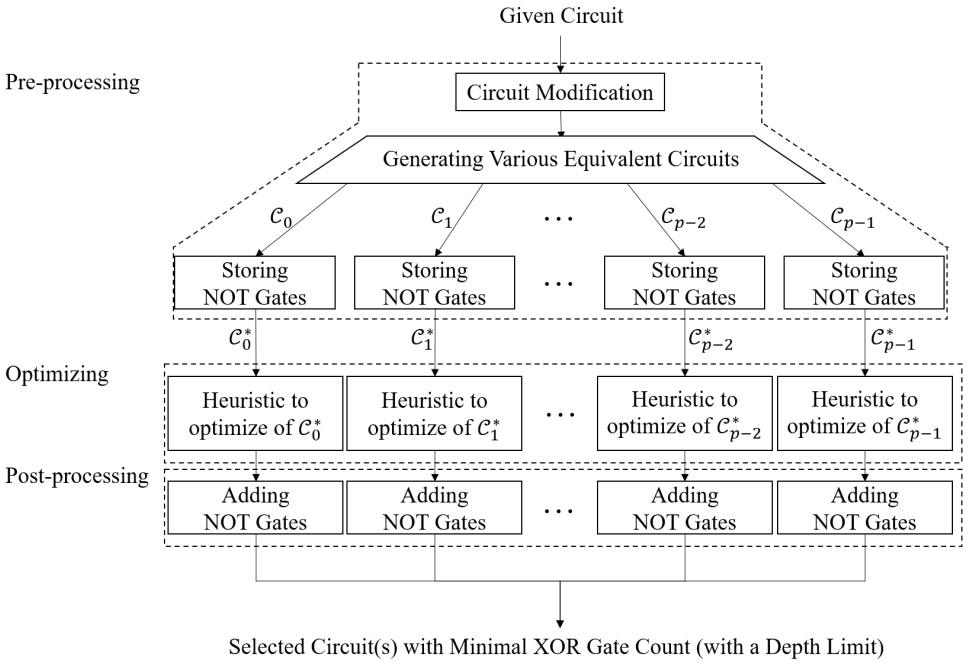

Figure 2: New framework for a heuristic search to optimize the circuit depth or XOR gate count

BP-based heuristic could not manage. However, the existing strategy does not perform well with circuits with nonlinear gates; therefore, further adjustments are required. Several methods are described to modify the algorithm by incorporating the RNBP and BPD algorithms.

Post-processing Step. The post-processing step adds the NOT gates stored during the pre-processing step. The nodes with removed NOT gates are located and added back. If possible, we combined them with existing XOR operations to form XNOR gates.

3.2 Pre-processing the S-Box Circuit

Related literature has explained the input-output XOR relationship of the linear layer through matrix representation. However, we deal with circuits that include nonlinear gates, and explaining the input-output relationships of such circuits via matrix representation is challenging. We took a different approach to addressing this problem by extracting the information of each node in the target circuit and reconstructing the nodes based on the nonlinear gates.

The inputs and outputs of a circuit containing nonlinear gates are $x_0, \cdots, x_{n-1}$ and $y_0, \cdots, y_{m-1}$, respectively. The number of nonlinear gates is k, and the input-output nodes of the i-th nonlinear gate are r_{2i}, r_{2i+1}, and g_i. The framework extracts the XOR information used to form $r_0, \cdots, r_{2k-1}, y_0, \cdots, y_{m-1}$.

For $i > 0$, each g_i cannot be used to construct $g_0, \cdots, g_{i-1}$; hence, r_{2i} and r_{2i+1} comprise the XOR of a constant of 1, $x_0, \cdots, x_{n-1}$, and $g_0, \cdots, g_{i-1}$, where r_0 and r_1 comprise the XOR of a constant of 1 and the input nodes. The output nodes comprise the XOR of a constant of 1, $x_0, \cdots, x_{n-1}$, and $g_0, \cdots, g_{k-1}$. For better performance, the information of the running XOR with a constant of 1 is stored separately and applied in the post-processing step.

We took the software-optimized implementation of the 4-bit `GIFT` [BPP+17] S-box as an example to illustrate the new representation method. In Section 2.1, circuits are formally defined; however, they are presented as equations for readability. In Table 1, the circuit on the left is the original circuit, whereas the rewritten circuit on the right contains information extracted according to the proposed method. The circuit on the right includes XOR information and nonlinear gates to aid in understanding.

Table 1: Extraction of the XOR information from the `GIFT` S-box circuit

Original circuit			Extraction of XOR information and nonlinear gates			
No.	Gate		No.	Gate	No.	Gate
1	$x_1 = x_1 \oplus AND(x_0, x_2)$		1	$r_0 = x_0$	9	$g_2 = OR(r_4, r_5)$
2	$t = x_0 \oplus AND(x_1, x_3)$		2	$r_1 = x_2$	10	$r_6 = x_0 \oplus g_1$
3	$x_2 = x_2 \oplus OR(t, x_1)$		3	$g_0 = AND(r_0, r_1)$	11	$r_7 = x_1 \oplus x_2 \oplus x_3 \oplus g_0 \oplus g_2$
4	$x_0 = x_3 \oplus x_2$	➔	4	$r_2 = x_1 \oplus g_0$	12	$g_3 = AND(r_6, r_7)$
5	$x_1 = x_1 \oplus x_0$		5	$r_3 = x_3$	13	$y_0 = x_2 \oplus x_3 \oplus g_2$
6	$x_0 = x_0 \oplus 1$		6	$g_1 = AND(r_2, r_3)$	14	$y_1 = x_1 \oplus x_2 \oplus x_3 \oplus g_0 \oplus g_2$
7	$x_2 = x_2 \oplus AND(t, x_1)$		7	$r_4 = x_0 \oplus g_1$	15	$y_2 = x_2 \oplus g_2 \oplus g_3$
8	$x_3 = t$		8	$r_5 = x_1 \oplus g_0$	16	$y_3 = x_0 \oplus g_1$
			Nodes where NOT gate is used : y_0			

We obtained more diverse results by creating various configurations, slightly modifying the circuit without adding nonlinear gates and changing the AND depth. The primary modifications apply the properties of AND and OR gates.

Modifications of Input Bits of AND and OR Gates. Property 1 is easily verified to hold for AND gates.

Property 1. *For input nodes r_{2i} and r_{2i+1} and output node g_i of the i-th nonlinear gate, if $g_i = AND(r_{2i}, r_{2i+1})$, then*

$$\begin{aligned} g_i = AND(r_{2i}, r_{2i+1}) &= r_{2i} \cdot r_{2i+1} \\ &= r_{2i} \cdot (r_{2i} \oplus r_{2i+1}) \oplus r_{2i} = AND(r_{2i}, r_{2i} \oplus r_{2i+1}) \oplus r_{2i} \\ &= r_{2i+1} \cdot (r_{2i} \oplus r_{2i+1}) \oplus r_{2i+1} = AND(r_{2i+1}, r_{2i} \oplus r_{2i+1}) \oplus r_{2i+1}. \end{aligned}$$

The above property allows the circuit to be modified by adding additional XOR operations to the inputs and outputs of the AND gate. Applying the two substitutions below, which use the above property, can achieve two additional modifications:

- $g_i \to g_i \oplus r_{2i}$ and $r_{2i+1} \to r_{2i} \oplus r_{2i+1}$ in XOR information.
- $g_i \to g_i \oplus r_{2i+1}$ and $r_{2i} \to r_{2i} \oplus r_{2i+1}$ in XOR information.

At first, this transformation appears to require an additional XOR gate, but depending on the target XOR information, it can reduce the number of XOR gates. For example, for a given target y, let $y = AND(v, v \oplus v') \oplus v$. The above modification simplifies to $y = AND(v, v')$, reducing the number of XOR gates by two.

Similarly, we can derive Property 2 for OR gates.

Property 2. *For input nodes r_{2i} and r_{2i+1} and output node g_i of the i-th nonlinear gate, if $g_i = OR(r_{2i}, r_{2i+1})$, then*

$$\begin{aligned} g_i = OR(r_{2i}, r_{2i+1}) &= (r_{2i} \oplus 1) \cdot (r_{2i+1} \oplus 1) \oplus 1 \\ &= (r_{2i} \oplus 1) \cdot (r_{2i} \oplus r_{i+1} \oplus 1) \oplus 1 = OR(r_{2i}, r_{2i} \oplus r_{2i+1}) \\ &= (r_{2i+1} \oplus 1) \cdot (r_{2i} \oplus r_{2i+1} \oplus 1) \oplus 1 = OR(r_{2i+1}, r_{2i} \oplus r_{2i+1}). \end{aligned}$$

Then, two more transformations can be attained through the following two substitutions based on Property 2:

- $r_{2i+1} \to r_{2i} \oplus r_{2i+1}$ in XOR information.
- $r_{2i} \to r_{2i} \oplus r_{2i+1}$ in XOR information.

Transformations Between AND and OR Gates. The AND and OR gates can also be converted to each other using an additional XOR operation, leading to Property 3.

Property 3. *For input nodes r_{2i} and r_{2i+1} and output node g_i of the i-th nonlinear gate, if $g_i = AND(r_{2i}, r_{2i+1})$, then*

$$\begin{aligned} g_i = AND(r_{2i}, r_{2i+1}) = r_{2i} \cdot r_{2i+1} &= (r_{2i} \oplus 1) \cdot (r_{2i+1} \oplus 1) \oplus 1 \oplus r_{2i} \oplus r_{2i+1} \\ &= OR(r_{2i}, r_{2i+1}) \oplus r_{2i} \oplus r_{2i+1}. \end{aligned}$$

Then, two more transformations can be obtained via the following two substitutions based on Property 3:

- $g_i \to g_i \oplus r_{2i} \oplus r_{2i+1}$ in XOR information and $g_i = AND(r_{2i}, r_{2i+1}) \to g_i = OR(r_{2i}, r_{2i+1})$.
- $g_i \to g_i \oplus r_{2i} \oplus r_{2i+1}$ in XOR information and $g_i = OR(r_{2i}, r_{2i+1}) \to g_i = AND(r_{2i}, r_{2i+1})$.

For input nodes r_{2i} and r_{2i+1} and output node g_i of the i-th nonlinear gate, NAND and NOR gates can also be converted to other nonlinear gates using Properties 1, 2, and 3, and vice versa.

How to Select Transformations for Nonlinear Gates. When many nonlinear gates exist, attempting to optimize all possible forms of transformed circuits is infeasible. The initial circuit form influences the proposed heuristic algorithms; hence, we selected the transformation for each nonlinear gate that results in the greatest reduction of XOR gates. If transformations have equal rankings, we choose one at random or select both to increase the number of possibilities. This process is repeated until no more transformations reduce the number of XOR gates. Once this is accomplished, we proceed with the optimizing step using the resulting circuits.

3.3 Incorporating Extended BP-based Heuristics into the Framework

In this section, we extend the RNBP and BPD algorithms to address nonlinear gates by applying a new pre-emptive strategy similar to that in Section 2.2. Then, the algorithms are incorporated into the proposed framework. In the framework, the RNBP algorithm optimizes the XOR gate count, whereas the BPD algorithm optimizes the XOR gate count with the depth limited to H. If $H = \infty$ in the BPD algorithm, it becomes the same as the RNBP algorithm.

Extending BP-based Heuristics to Address Nonlinear Gates. The difficulty in directly applying the RNBP and BPD algorithms to S-box circuit optimization is that targets cannot be created using only XOR gates. In circuits with nonlinear gates, BP-based heuristics terminate and output $\perp$ without generating nonlinear gates. Our framework solves this problem by adding the input nodes of nonlinear gates to the set of targets and by adding the output node of that gate to base S if two inputs of a nonlinear gate are implemented. The input nodes of the i-th nonlinear gate are r_{2i} and r_{2i+1}, and let the output node is g_i. If r_{2i} and r_{2i+1} are implemented, g_i can be computed in a single operation; thus, it is implemented immediately. That is, if r_{2i} and r_{2i+1} belong to S, g_i is added to S, and this process is a *new pre-emptive strategy*. In this way, as the output nodes of nonlinear gates are added to S, the targets can be gradually implemented.

Recall that the BP-based heuristics are discussed in Section 2.2. For a circuit using k nonlinear gates, the extended algorithm and original algorithm are collectively provided in Algorithm 1. The black text indicates generalized BP-based heuristics, whereas the red text indicates extensions for the complete application in our framework.

Algorithm 1 Extended BP/RNBP algorithm-based heuristic (**eBP/eRNBP**)

Input: input size n, target nodes (output of a circuit) $y_0, \cdots, y_{m-1}$, number of nonlinear gates k, nonlinear gates $G_0, \cdots, G_{k-1}$
Output: optimized circuit $\mathcal{C}$

```
Y ← {r_0, ··· , r_{2k−1}, y_0, ··· , y_{m−1}}
S ← {x_0, ··· , x_{n−1}}
C ← [ ]
Dist ←update_Dist(S, Y)
while Y ⊄ S do
  W ← {w | w = v ⊕ v' such that w ∉ S for v, v' ∈ S}
  if W = ∅ then
    return ⊥
  if g_i ∉ S and r_{2i}, r_{2i+1} ∈ S for any i then
    (w : G, {v, v'}) ← (g_i : G_i, {r_{2i}, r_{2i+1}})        ▷ new pre-emptive strategy
  else
    (w : G, {v, v'}) ← T(W, S, Y, Dist)                       ▷ w = v ⊕ v' for v, v' ∈ S and G = XOR
  S ← S ∪ {w}
  append (w : G, {v, v'}) to C
  Dist ←update_Dist(S, Y)
return C
```

In this study, S represents the base, and Y denotes the set of targets. The function update_Dist recalculates the distances in $Dist$. Strategy $\mathcal{T}$ is applied for the competition between pairs, and for three nodes w, v, and v' satisfying $w = v \oplus v'$, the function outputs the tuple $(w : XOR, \{v, v'\})$. An XOR gate is assigned to G, and the tuple is appended to $\mathcal{C}$. In addition, (v, v') represents the node pair selected via strategy $\mathcal{T}$, and the strategies explained in Section 2.2 are examples of this strategy. These strategies work to select the node pairs that bring the algorithm closer to the goal, using all values of W, S, Y, and $data$ that the algorithm can manage.

Incorporating the RNBP Algorithm. The distance δ defined in Section 2.2 is changed to output ∞ because it may be impossible to implement the target due to a nonlinear gate. For all targets y_i, the new distance $\delta^*(S, y_i)$ is defined as follows:

$$\delta^*(S, y_i) = \min\left(\left\{d \mid \exists v_0, \cdots, v_{d-1} \in S \text{ such that } y_i = \bigoplus_{j=0}^{d-1} v_j, \text{ for } d \leq |S|\right\} \cup \{\infty\}\right).$$

This adjustment ensures that the update_Dist function works without errors. Strategy $\mathcal{T}$ adopted the strategies of the RNBP algorithms as described in Section 2.2. We applied the Euclidean norm of $Dist$ and the sum of the elements of $Dist$ in the selection strategy. If ∞ is included in $Dist$, both cases output ∞, which does not cause errors but does not significantly influence pair selection. In such cases, the RNBP algorithm is forced to make random choices, deviating from the goal of an efficient circuit. To optimize, we adjust $Dist$ by excluding values that output ∞. Our framework incorporating the RNBP algorithm conforms to Algorithm 1 and we call this **eRNBP**.

Incorporating the BPD Algorithm. The BPD algorithm takes an input S-box circuit, sets a threshold for a certain depth, and outputs a circuit with a minimized XOR gate count, without exceeding the depth threshold. The update_Dist_and_Δ function calculates $Dist$ and Δ and outputs $Dist, \Delta$, and H, using S and Y in its calculations. H is a fixed value and can therefore be defined within the algorithm. H is the final depth of the circuit (excluding NOT gates), and we use Theorem 1 to determine the minimum value of H to consider its possible range. The XOR information for $r_0, \cdots, r_{2k-1}, y_0, \cdots, y_{m-1}$ is known from Section 3.2; therefore, the minimum depth required to construct each node can be obtained if the depths of $g_0, g_1, \cdots, g_{k-1}$ are known. According to the definition of depth, for each i,

$$\mathcal{D}(g_i) = \max(\mathcal{D}(r_{2i}, r_{2i+1})) + 1. \tag{1}$$

Furthermore, each g_i is not used to construct $r_0, \cdots, r_{2i-1}$. Thus, Theorem 1 and Equation (1) can determine the minimum depth for each node in the order of r_0, r_1, g_0, r_2, r_3, g_1, $\cdots$, r_{2k-2}, r_{2k-1}, g_{k-1}, y_0, y_1, $\cdots$, y_{m-1}. The minimum depth of the entire circuit is $max(\mathcal{D}(y_0), \cdots, \mathcal{D}(y_{m-1}))$, which is considered the minimum value of H.

The distance used in the BPD algorithm is set to H, the maximum depth that any target can have, but this cannot be done for the new targets (inputs of nonlinear gates). Because these are values in the middle of the circuit, when H is reached, the final depth of the circuit can exceed H. Therefore, we set a maximum depth for all targets. We calculated the minimum depths of the targets using Theorem 1 and increased the depths so that the final depth of the circuit does not exceed H. The function calculate_depth_limit_each_target describes this process, and the output of this function, H_Y, is a function that outputs the maximum depth that the target can reach when a target is input. For all targets y_i, the new distance $\delta^*_H(S, y_i)$ is defined as follows:

$$\delta^*_H(S, y_i) = \min\left(\left\{ d \mid \exists v_0, \cdots, v_{d-1} \in S \text{ s.t. } y_i = \bigoplus_{j=0}^{d-1} v_j \text{ and } \left\lceil \log_2 \left(\sum_{j=0}^{n-1} 2^{\mathcal{D}(v_j)} \right) \right\rceil \leq H_Y(y_i) \text{ for } d \leq |S| \right\} \cup \{\infty\}\right).$$

In incorporating the BPD algorithm, $Dist$ is defined well, and by definition, Δ does not include noninteger values (e.g., ∞). However, the BPD algorithm also uses the Euclidean norm of $Dist$ and the sum of the elements of $Dist$ in the selection strategy; thus, it can still lead to the problem of distances potentially being ∞. As with the incorporating of the RNBP algorithm, $Dist$ is constructed excluding ∞. During the investigation, the depth limit H was manually set according to Theorem 1 starting from the lower bound of the depth. Therefore, if the circuit with H as the lower bound is generated, it can be considered optimized from the perspective of depth. Our framework incorporating the BPD algorithm conforms to Algorithm 2.

The most time-consuming part of the algorithm is applying strategy $\mathcal{T}$ to all elements in W; thus, reducing the size of W increases the speed of the algorithm. In each iteration, the algorithm calculates the $Dist$ caused by elements in W to apply strategy $\mathcal{T}$, and in the next iteration, it recalculates $Dist$ for elements that were not selected. To improve the algorithm's performance, we can consider removing elements whose $Dist$ does not change in the next iteration. By investigating only a portion of W, the speed improves, but the algorithm output may not be optimal.

Comparison of eRNBP and eBPD. The eBPD determines whether the depth of the two input nodes of an AND gate exceeds a threshold when triggering a new pre-emptive strategy, whereas eRNBP does not. Accordingly, eRNBP minimizes only the XOR gate count of the given S-box circuit, and its depth cannot be manually controlled. However, eBPD sets the input depth as a threshold and minimizes the XOR gate count without exceeding this threshold. Among the two methods, eBPD produced better overall results, as provided in Section 4.

Algorithm 2 Extended BPD algorithm based heuristic (**eBPD**)

Input: input size n, depth limit H, target nodes (output of a circuit) $y_0, \cdots, y_{m-1}$, number of nonlinear gates k, nonlinear gates $G_0, \cdots, G_{k-1}$
Output: optimized circuit $\mathcal{C}$

```
Y ← {r_0, ··· , r_{2k−1}, y_0, ··· , y_{m−1}}
S ← {x_0, ··· , x_{n−1}}
C ← [ ]
H_Y ←calculate_depth_limit_each_target(Y, H)
Dist, Δ ←update_Dist_and_Δ(S, Y, H)
while Y ⊄ S do
  W ← {w | w = v ⊕ v' such that w ∉ S for v, v' ∈ S}
  if W = ∅ then
    return ⊥
  if g_i ∉ S and r_{2i}, r_{2i+1} ∈ S for any i then
    if D(r_{2i}) ≤ H_Y(r_{2i}) and D(r_{2i+1}) ≤ H_Y(r_{2i+1}) then
      (w : G, {v, v'}) ← (g_i : G_i, {r_{2i}, r_{2i+1}})      ▷ new pre-emptive strategy
  else
    (w : G, {v, v'}) ← T(W, S, Y, Dist, Δ, H)      ▷ w = v ⊕ v' for v, v' ∈ S and G = XOR
  S ← S ∪ {w}
  append (w : G, {v, v'}) to C
  Dist, Δ ←update_Dist_and_Δ(S, Y, H)
return C
```

4 Applications to AES, SNOW3G, and Saturnin S-Box Circuits

We applied the proposed framework to the AES, SNOW3G, and Saturnin S-boxes to evaluate its effectiveness. In particular, we searched for new circuits that are competitive in terms of the AND gate count and the AND depth to perform various experiments on the AES S-box. Specifically, we conducted a new investigation on a polynomial basis representation of the $GF(2^8)$ inverse. In the case of the SNOW3G S-box, the circuit had not previously been proposed and is newly implemented in this work. Finally, we optimized the competitive circuits for the AES, SNOW3G, and Saturnin S-boxes, including our proposed circuits, for either the circuit depth or XOR gate count. These S-boxes share the common feature of being structural combinations of small S-boxes; hence, they are suitable for applying our framework.

4.1 Generating New AES S-box Circuits

The AES S-box circuits by Boyar and Peralta [BP10, BP12] were generated using tower field construction. Since it is shown in [BP10] that constructing $GF(2^8)$ inverter based on tower field construction is optimal from a cost perspective, it is reasonable to use circuits based on the approach. We applied the tool from [JBK24] to the two circuits proposed in [BP10, BP12], modifying only the multiplicative inverter over $GF(2^4)$. The tool outputs only a single result, but we modified the tool to output all possible circuits. Similar to the approach in [BP12], where the AND gate count was increased to reduce the depth, we modified the tool to output circuits that slightly increase the AND gate count while reducing the depth.

Using the strategy described above, we found several new AES S-box circuits that show performance improvements in one or two of the five metrics. In concrete, for each of the circuits in [BP10] and [BP12], we applied two types of multiplicative inverters, resulting in a total of four AES S-box circuits (see Table 2). These circuits have AND depths of 5 and 4, using 32 and 33 AND gates, respectively. Compared to the original ones, our results reduce either the AND depth or the AND gate count by up to 2. The new circuits for [BP10] and [BP12] are presented in Listings 1 and 2, and in Listings 3 and 4 in Appendix B, respectively.

4.2 Generating New SNOW3G S-box Circuit

We newly implemented the 8-bit S-box S_Q [For06], used to operate $S2$ in SNOW3G. This S-box comprises the function $g_{49} : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ defined as $g_{49}(x) \oplus 0\text{x}25$. The function g_{49}, known as the Dickson polynomial, is defined as follows:

$$g_{49}(t) = t + t^9 + t^{13} + t^{15} + t^{33} + t^{41} + t^{45} + t^{47} + t^{49}.$$

g_{49} satisfies $g_{49} = g_7(g_7(t))$, where g_7 is another Dickson polynomial [BHNS10], defined as follows:

$$g_7(t) = t + t^5 + t^7.$$

By implementing g_7 and composing it with itself, we can implement g_{49}.

Since t^7 is constructed as the product of t^2 and t^5, we implemented the operations in the order of t^2, t^5, t^7, and $t + t^5 + t^7$. We performed the implementation using the finite field extension. Specifically, $GF(2^8)$ is treated as a field constructed with $x^2 + Ax + B$ for $A, B \in GF(2^4)$, where W is the root of $x^2 + Ax + B$, and α, β are elements of $GF(2^4)$.

Computing t^2. Let $t = \alpha W + \beta$. Then, t^2 is calculated as follows:

$$t^2 = (\alpha W + \beta)^2 = \alpha^2 W^2 + \beta^2 = \alpha^2 AW + \alpha^2 B + \beta^2.$$

Since t^2 consists of squaring and scalar multiplication operations over $GF(2^4)$, by Theorem 2, it is a linear operation.

Computing t^5. Let $t = \alpha W + \beta$. Squaring t^2 to obtain t^4 yields the following:

$$t^4 = (\alpha^2 AW + \alpha^2 B + \beta^2)^2 = \alpha^4 A^2 W^2 + \alpha^4 B^2 + \beta^4 = \alpha^4 A^3 W + \alpha^4 A^2 B + \alpha^4 B^2 + \beta^4.$$

As $t^5 = t \times t^4$, it can be obtained as follows:

$$\begin{aligned} t^5 &= (\alpha W + \beta)(\alpha^4 A^3 W + \alpha^4 A^2 B + \alpha^4 B^2 + \beta^4) \\ &= \alpha^5 A^3 W^2 + (\alpha^5 A^2 B + \alpha^5 B^2 + \alpha\beta^4 + \alpha^4 \beta A^3) W + \alpha^4 \beta A^2 B + \alpha^4 \beta B^2 + \beta^5 \\ &= (\alpha^5 A^4 + \alpha^5 A^2 B + \alpha^5 B^2 + \alpha\beta^4 + \alpha^4 \beta A^3) W + \alpha^5 A^3 B + \alpha^4 \beta A^2 B + \alpha^4 \beta B^2 + \beta^5 \end{aligned}$$

If we set $A = 1$, t^5 is expressed as follows:

$$\begin{aligned} t^5 &= (\alpha^5 + \alpha^5 B + \alpha^5 B^2 + \alpha\beta^4 + \alpha^4 \beta) W + \alpha^5 B + \alpha^4 \beta B + \alpha^4 \beta B^2 + \beta^5 \\ &= \left((\alpha + \beta)^5 + (B + B^2)\alpha^5 + \beta^5\right) W + \alpha^5 B + (B + B^2)\alpha^4 \beta + \beta^5 \end{aligned}$$

According to the above expression, implementing t^5 requires constant multiplication over $GF(2^4)$ and the implementation of α^4, where α^4 is calculated through two squaring operations. These two operations are implemented as linear operations by Theorem 2.

Theorem 2. *Squaring and multiplying by a constant over $GF(2^4)$ are linear operations.*

Proof. The proof of this theorem is given in Appendix A. □

Thus, by computing α^5, β^5, $(\alpha + \beta)^5$, and $\alpha^4\beta$, we can determine t^5 via linear operations.

- Using the tool from [JBK24], we obtained a circuit for computing the fifth power over $GF(2^4)$ using 3 AND gates. Thus, we used 3 AND gates each to compute α^5, β^5, and $(\alpha + \beta)^5$.
- According to Theorem 2, computing α^4 is a linear operation. Since $\alpha^4\beta$ can be implemented as multiplication in $GF(2^4)$, we used the method from [PFR98] to implement it with 9 AND gates.

We computed t^5 using 18 AND gates and additional linear operations.

Computing t^7. The multiplication of elements $\alpha W + \beta$ and $\alpha' W + \beta'$ proceeds as follows:

$$\begin{aligned}(\alpha W + \beta)(\alpha' W + \beta') &= \alpha\alpha' W^2 + (\alpha\beta' + \alpha'\beta)W + \beta\beta' \\ &= (\alpha\alpha' A + \alpha\beta' + \alpha'\beta)W + \alpha\alpha' B + \beta\beta'.\end{aligned}$$

When $A = 1$, the equation expands as follows:

$$\begin{aligned}(\alpha W + \beta)(\alpha' W + \beta') &= (\alpha\alpha' + \alpha\beta' + \alpha'\beta)W + \alpha\alpha' B + \beta\beta' \\ &= \left((\alpha + \beta)(\alpha' + \beta') + \beta\beta'\right) W + \alpha\alpha' B + \beta\beta'.\end{aligned}$$

Thus, t^7 can be implemented using three multiplications over $GF(2^4)$ for $\alpha\alpha'$, $\beta\beta'$, and $(\alpha + \beta)(\alpha' + \beta')$, along with linear operation. Each multiplication was implemented using the method from [PFR98], requiring a total of 27 AND gates.

Computing $t + t^5 + t^7$. 18 AND gates were used to implement t^5, and 27 AND gates were used to implement t^7. Therefore, 45 AND gates were used in total to implement g_7.

Constructing g_{49}. Due to the complexity of the circuit structure, we optimized S_Q by dividing it into first and second halves. As g_{49} comprises of g_7 and its composite, we divided it into the first g_7 and last g_7, applied the above computational process to each, and combined the two results. This approach allowed us to implement S_Q with a depth of 34 and an AND depth of 4, using 90 AND gates and 366 XOR gates (Listing 20 in Appendix B). The total number of gates proposed in [BHNS10] is 498, while our result improves upon this, reducing the count to 456.

4.3 Results for `AES`, `SNOW3G`, and `Saturnin` S-Box Circuits

Due to the difficulty of calculating all transformations presented in the pre-processing step, we adopted the search strategy discussed in Section 3.2. Our experiments focused on the `AES` S-box circuit from [BP10] and its improved circuit [mt16], the one from [BP12] and its improved circuit [BFP+17], and two new circuits discussed in Section 4.1. The circuits proposed in [BP10] and [mt16] have the same XOR information, and the circuits proposed in [BP12] and [BFP+17] also share the same XOR information. Therefore, only the circuits proposed in [BP10] and [BP12] must be considered to obtain results for analyzing the four targets. Additionally, we explored the `SNOW3G` S-box circuit [For06] (discussed in Section 4.2) and the `Saturnin` super S-box circuit [CDL+20]. All circuits we found are presented in Appendix B, and Table 2 summarizes the results. All results were investigated by increasing the depth threshold starting from the lower bound according to Theorem 1 ([LSL+19]); thus, Listings 10, 14, 15, 17, 18, 19, and 22 have optimized depths.

It is worth noting that we identified the best 24-depth implementation of the `AES` circuit among circuits with an AND gate count of 32 and an AND depth of 5 (Listing 11), which is based on the newly generated circuit (Listing 1). The circuit reduces the depth and the AND depth by 3 and 1, respectively, compared to the circuit in [mt16]. We also obtained the 26-depth implementation of the `AES` S-box circuit (Listing 5), which was the best among the circuits with an AND gate count of 32 and an AND depth of 6. Based on the circuit in [mt16], the depth was reduced to as low as 18 using 12 additional XOR gates at most. Another one is the `AES` S-box circuit with a depth of 15 (Listing 17) using 100 XOR gates, improving on the previous minimum depth of 16 for an `AES` S-box with an AND gate count of 34 and an AND depth of 4. To the best of our knowledge, the `AES` S-box circuit with a depth of 15, using 34 AND gates, represents the best result in this category in terms of depth. For the `SNOW3G` S-box circuit, the depth was reduced from 34 to 24 (Listing 21). Additionally, for the `Saturnin` super S-box circuit, the depth was reduced from 28 to 25 (Listing 22). These results demonstrate the effectiveness of our framework.

Based on our experiments, the BPD algorithm yielded better overall results compared to the RNBP algorithm in the proposed framework. For the `AES` S-box circuit in [BP10], we found an implementation with an XOR gate count of 81 using eRNBP, increasing the depth from 28 to 34. In contrast, using eBPD, we found an implementation with the same XOR gate count 81 but with a depth reduced from 28 to 26 (Listing 5). For the `Saturnin` super S-box, the results from eRNBP were worse, and only eBPD offered better results in terms of depth.

For the `AES` S-box circuits, the results based on eBPD tend to involve a trade-off between the depth and number of linear gates. As the depth decreases, the increase in XOR gate count is

Table 2: Comparison of results for `AES`, `SNOW3G`, and `Saturnin`

S-box	D	AD	#NL	#L	#(gate)	Algorithm	Reference
`AES` S-box	28	6	32	83	115	BP + ad-hoc	[BP10]
	27	6	32	81	113	ad-hoc	[mt16]
	26	6	32	81	113	eBPD	Sect. 4.3 (Listing 5)
	23	6	32	82	114	eBPD	Sect. 4.3 (Listing 6)
	22	6	32	85	117	eBPD	Sect. 4.3 (Listing 7)
	21	6	32	90	122	eBPD	Sect. 4.3 (Listing 8)
	20	6	32	92	124	eBPD	Sect. 4.3 (Listing 9)
	18†	6	32	93	125	eBPD	Sect. 4.3 (Listing 10)
	25	5	32	85	117	ad-hoc	Sect. 4.1 (Listing 1)
	24	5	32	**81**	**113**	eBPD	Sect. 4.3 (Listing 11)
	23	5	32	**83**	**115**	eBPD	Sect. 4.3 (Listing 12)
	22	5	32	84	116	eBPD	Sect. 4.3 (Listing 13)
	17†	5	32	97	129	eBPD	Sect. 4.3 (Listing 14)
	23	4	33	85	118	ad-hoc	Sect. 4.1 (Listing 2)
	16†	4	33	104	137	eBPD	Sect. 4.3 (Listing 15)
	16	4	34	94	128	ad-hoc	[BP12]
	16	4	34	91	125	ad-hoc	[BFP+17]
	28	4	34	**81**	**115**	eRNBP	Sect. 4.3 (Listing 16)
	15†	4	34	100	134	eBPD	Sect. 4.3 (Listing 17)
	18	5	32	96	128	ad-hoc	Sect. 4.1 (Listing 3)
	17†	5	32	**93**	**125**	eBPD	Sect. 4.3 (Listing 18)
	17	4	33	96	129	ad-hoc	Sect. 4.1 (Listing 4)
	16†	4	33	101	134	eBPD	Sect. 4.3 (Listing 19)
	15	5	54	107	161	ad-hoc	[UHS+15]
	17	5	50	79	129	ad-hoc	[RTA18]
	21	5	50	69	119	ad-hoc	[RTA18]
`SNOW3G` S-box	34	4	90	366	456	ad-hoc	Sect. 4.2 (Listing 20)
	24	4	90	533	623	eBPD	Sect. 4.2 (Listing 21)
`Saturnin` S-box	28	12	48	86	134	ad-hoc	[CDL+20]
	25†	12	48	143	191	eBPD	Sect. 4.3 (Listing 22)

- D: depth / AD: AND depth / #NL: the number of nonlinear gates / #L: the number of linear gates
- †Optimized depth for each circuit

relatively small, which can facilitate selecting the appropriate circuit depending on the application environment.

5 Discussion: Paradigm Shift in S-Box Circuit Optimization

Optimization techniques for S-box circuits are categorized based on the target size. Various tools and techniques for optimally implementing small-sized S-box circuits work particularly well for 4-bit sizes. These tools primarily operate by inputting an S-box table. Although the proposed framework requires more information than just an S-box table because it requires an S-box circuit as input, this disadvantage can be overcome by integrating this technique with other tools.

In contrast, optimizing large-sized S-box circuits is challenging. Several mathematical techniques are applied using a divide-and-conquer approach for mathematically constructed S-boxes. This paradigm leaves room for further optimization because the divided parts do not interfere with each other. The proposed framework can manage an 8-bit `AES` S-box and advances this paradigm.

Small S-box Circuits. The measures considered for constructing circuits for small S-boxes are the MC, bitslice gate complexity (BGC), gate complexity (GC), depth, and AND depth. Table 3

compares the designed tool with existing tools for implementing circuits of S-boxes. The search methods of the existing tools are divided into two categories: using SAT solvers or constructing graphs and applying pathfinding logic. Both methods are based on exhaustive searches, which tend to become significantly more difficult as the size of the S-box or the number of required operators increases.

The SAT solver-based tool presented in [Sto16] can optimize the MC, BGC, GC, and depth. The paper demonstrates a method for optimizing multiple measures by optimizing one measure before optimizing the others. Zhang and Huang [ZH23] found significant performance improvements by changing the expression format of the equations in [Sto16]. Bilgin et al. [BMD+20] introduced a tool based on the work in [Sto16] to optimize the MC and AND depth of 4-bit S-boxes. They also proposed an analysis of some large S-boxes and employed additional tools to optimize of internal affine layers.

LIGHTER [JPST17] is a circuit generation tool for 4-bit S-boxes, which constructs a graph where function values are vertices and gates are edges, performing a breadth-first search (BFS) integrated with MITM to determine the circuit. LIGHTER has the advantage of allowing the customization of the gate costs used in GC calculations and enabling the calculation of BGC. PEIGEN [BGLS19] improves the performance of [JPST17] via technical upgrades and can calculate depth but can hardly handle S-boxes larger than a 5-bit size. Jeon et al. [JBK24] proposed a novel approach that constructs a different type of graph and performs an A* search to determine the S-box circuit. This tool determines circuits using the minimum number of AND gates and can construct circuits for 5-bit and some 6-bit S-boxes.

The three tools in [BMD+20], [JPST17], and [JBK24] can reduce the MC and AND depth but cannot simultaneously optimize depth. Incorporating the proposed framework into circuits with reduced MC and AND depth can determine S-boxes with low depth. This framework with [JBK24], which manages sizes up to 6 bits, maximizes performance.

Table 3: Comparison of the existing tools for generating efficient S-box circuits

Tools	Base technique	Target measure	Input type	Applicability to `AES` S-box
[Sto16]	SAT solver	MC, BGC, GC, depth	S-box table	No
[JPST17]	Graph based BFS with MITM	BGC, GC	S-box table	No
[BGLS19]	Graph based BFS with MITM	MC, BGC, GC, depth	S-box table	No
[BMD+20]	SAT solver	MC, AND depth	S-box table	No
[ZH23]	SAT solver	MC, BGC, GC, depth	S-box table	No
[JBK24]	Graph based A* search	MC	S-box table	No
Ours	**eRNBP, eBPD**	**#XOR, depth**	**S-box circuit**	Yes

MC : multiplicative complexity / BGC : bitslice gate complexity / GC : gate complexity

Large S-box Circuits. Until now, tools could not directly manage the circuit of an 8-bit S-box. For instance, the `AES` S-box circuit often requires a divide-and-conquer approach, where it is mathematically decomposed, and smaller S-boxes and linear layers are optimized separately. Additional methods, such as tower field extension or Fermat's little theorem, are often used to structure the S-box, allowing for partial implementation but making it challenging to directly optimize the entire circuit. However, our tool integrates and optimizes small S-boxes and linear layers using BP-based heuristics, amortizing the optimization process and offering possibilities for further optimization. As demonstrated by the improvements in Section 4, our tool can efficiently manage 8-bit `AES` and `SNOW3G` S-boxes, and 16-bit `Saturnin` super S-box circuits. Figure 3 illustrates our proposed paradigm, where the process of optimizing linear gates (in the blue box) refers to our framework.

Advantages of the New Paradigm. Our paradigm, like the previous one, offers more efficient circuits by optimizing circuits for small S-boxes in the larger S-box. However, in the previous paradigm, although linear layers and small S-boxes could each be individually optimized well, the interactions at their connection points were not considered. Our paradigm rewrites the inputs of the nonlinear and linear gates in the circuit, allowing for the interactions between layers to be considered. With this approach, various cost metrics can be reduced, the most notable being

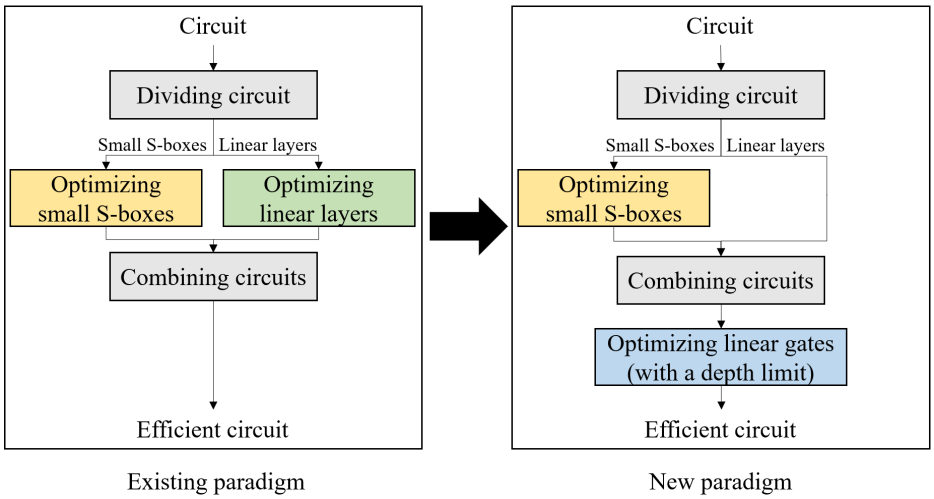

Figure 3: New paradigm to find efficient circuits for large S-boxes

the depth and XOR gate count. Regarding depth, the interaction between layers can potentially reduce the depth at the connection points, as more gates can be processed at a single depth. When two layers are considered together, there can be instances where XOR gates are used consecutively. In such cases, these two gates can be removed, offering an opportunity to reduce the XOR gate count. Optimizing the depth and identifying shared operations across layers can improve the latency and area.

6 Conclusion and Future Work

In this paper, we proposed a new framework for a heuristic search to optimize the circuit depth or XOR gate count of S-box circuits without increasing the AND gate count and the AND depth. We expanded the method from an individual component optimization to a comprehensive optimization by extracting and reconstructing XOR information for each node based on the nonlinear gates. Considering the RNBP and BPD algorithms, we also extended the BP algorithm-based heuristics to manage the nonlinear gates, incorporating these into the framework. Thus, we acquired several results for the `AES`, `SNOW3G`, and `Saturnin` S-box circuits.

The following research is of interest for future work:

- The algorithm incorporating BPD sometimes implements a node representing the same value twice, which is inefficient; hence, eliminating this problem could improve performance.
- To improve performance, we removed ∞ from *Dist*. Thus, targets with a distance of ∞ were excluded from consideration when selecting a node pair for a new XOR operation. We can calculate the distance by excluding the unrealized nonlinear gates from the XOR information of the corresponding target to account partially for the excluded targets. This approach is expected to yield more efficient results.
- In addition to the RNBP and BPD algorithms considered in the current framework, other BP algorithm-based heuristics can be incorporated, and it would be interesting to analyze their results.

Acknowledgments

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2024-RS-2022-00164800) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation).

References

[ABD+23] Roberto Avanzi, Subhadeep Banik, Orr Dunkelman, Maria Eichlseder, Shibam Ghosh, Marcel Nageler, and Francesco Regazzoni. The qarmav2 family of tweakable block ciphers. *IACR Transactions on Symmetric Cryptology*, 2023(3):25–73, 2023.

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 430–454. Springer, 2015.

[BDD+23] Yanis Belkheyar, Joan Daemen, Christoph Dobraunig, Santosh Ghosh, and Shahram Rasoolzadeh. Bipbip: A low-latency tweakable block cipher with small dimensions. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(1):326–368, 2023.

[BFI19] Subhadeep Banik, Yuki Funabiki, and Takanori Isobe. More results on shortest linear programs. In Nuttapong Attrapadung and Takeshi Yagi, editors, *Advances in Information and Computer Security - 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, August 28-30, 2019, Proceedings*, volume 11689 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2019.

[BFI21] Subhadeep Banik, Yuki Funabiki, and Takanori Isobe. Further results on efficient implementations of block cipher linear layers. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 104-A(1):213–225, 2021.

[BFP+17] Joan Boyar, Magnus Gausdal Find, Rene Peralta, et al. Low-depth low-size circuits for cryptographic applications. In *Proc. 2nd Int. Workshop Boolean Functions Their Appl.-BFA*, 2017.

[BGLS19] Zhenzhen Bao, Jian Guo, San Ling, and Yu Sasaki. PEIGEN - a platform for evaluation, implementation, and generation of s-boxes. *IACR Transactions on Symmetric Cryptology*, 2019(1):330–394, 2019.

[BHNS10] Billy Bob Brumley, Risto M. Hakala, Kaisa Nyberg, and Sampo Sovio. Consecutive s-box lookups: A timing attack on SNOW 3g. In Miguel Soriano, Sihan Qing, and Javier López, editors, *Information and Communications Security - 12th International Conference, ICICS 2010, Barcelona, Spain, December 15-17, 2010. Proceedings*, volume 6476 of *Lecture Notes in Computer Science*, pages 171–185. Springer, 2010.

[BLMR19] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Transactions on Symmetric Cryptology*, 2019(1):5–45, 2019.

[BMD+20] Begül Bilgin, Lauren De Meyer, Sébastien Duval, Itamar Levi, and François-Xavier Standaert. Low AND depth and efficient inverses: a guide on s-boxes for low-latency masking. *IACR Transactions on Symmetric Cryptology*, 2020(1):144–184, 2020.

[BP10] Joan Boyar and René Peralta. A new combinational logic minimization technique with applications to cryptology. In Paola Festa, editor, *Experimental Algorithms, 9th International Symposium, SEA 2010, Ischia Island, Naples, Italy, May 20-22, 2010. Proceedings*, volume 6049 of *Lecture Notes in Computer Science*, pages 178–189. Springer, 2010.

[BP12] Joan Boyar and René Peralta. A small depth-16 circuit for the AES s-box. In Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou, editors, *Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 287–298. Springer, 2012.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware*

and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer, 2017.

[Can05] David Canright. A very compact s-box for AES. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 441–455. Springer, 2005.

[CDL+20] Anne Canteaut, Sébastien Duval, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Thomas Pornin, and André Schrottenloher. Saturnin: a suite of lightweight symmetric algorithms for post-quantum security. *IACR Transactions on Symmetric Cryptology*, 2020(S1):160–207, 2020.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[Dro98] Germain Drolet. A new representation of elements of finite fields gf(2^{m}) yielding small complexity arithmetic circuits. *IEEE Transactions on Computers*, 47(9):938–946, 1998.

[For06] 3GPP Task Force. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification. Technical Report Version 1.1, 3GPP, 2006.

[JBK24] Yongjin Jeon, Seungjun Baek, and Jongsung Kim. Towards finding s-box circuits with optimal multiplicative complexity. *IEEE Transactions on Computers*, 73(8):2036–2050, 2024.

[JPST17] 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, 2017.

[LSL+19] Shun Li, Siwei Sun, Chaoyun Li, Zihao Wei, and Lei Hu. Constructing low-latency involutory MDS matrices with lightweight circuits. *IACR Transactions on Symmetric Cryptology*, 2019(1):84–117, 2019.

[LXZZ21] Da Lin, Zejun Xiang, Xiangyong Zeng, and Shasha Zhang. A framework to optimize implementations of matrices. In Kenneth G. Paterson, editor, *Topics in Cryptology - CT-RSA 2021 - Cryptographers' Track at the RSA Conference 2021, Virtual Event, May 17-20, 2021, Proceedings*, volume 12704 of *Lecture Notes in Computer Science*, pages 609–632. Springer, 2021.

[mt16] CMT: Circuit minimization team. Circuit minimization work, 2016. last accessed on: 20th September, 2024.

[NNI12] Kenta Nekado, Yasuyuki Nogami, and Kengo Iokibe. Very short critical path implementation of AES with direct logic gates. In Goichiro Hanaoka and Toshihiro Yamauchi, editors, *Advances in Information and Computer Security - 7th International Workshop on Security, IWSEC 2012, Fukuoka, Japan, November 7-9, 2012. Proceedings*, volume 7631 of *Lecture Notes in Computer Science*, pages 51–68. Springer, 2012.

[NNT+10] Yasuyuki Nogami, Kenta Nekado, Tetsumi Toyota, Naoto Hongo, and Yoshitaka Morikawa. Mixed bases for efficient inversion in \mathbb $F((2^2)^2)$ and conversion matrices of subbytes of AES. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 234–247. Springer, 2010.

[oSN23] National Institute of Standards and Technology (NIST). Lightweight cryptography: Nist selects ascon. https://csrc.nist.gov/news/2023/lightweight-cryptography-nist-selects-ascon, 2023. Accessed: 15.06.2024.

[PFR98] Christof Paar, Peter Fleischmann, and Peter Roelse. Efficient multiplier architectures for galois fields GF(2 $^{4\mathrm{n}}$). *IEEE Trans. Computers*, 47(2):162–170, 1998.

[RTA18] Arash Reyhani-Masoleh, Mostafa M. I. Taha, and Doaa Ashmawy. Smashing the implementation records of AES s-box. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(2):298–336, 2018.

[SFX23] Haotian Shi, Xiutao Feng, and Shengyuan Xu. A framework with improved heuristics to optimize low-latency implementations of linear layers. *IACR Transactions on Symmetric Cryptology*, 2023(4):489–510, 2023.

[SLH24] Qingling Song, Lang Li, and Xiantong Huang. LELBC: A low energy lightweight block cipher for smart agriculture. *Internet Things*, 25:101022, 2024.

[SMTM01] Akashi Satoh, Sumio Morioka, Kohji Takano, and Seiji Munetoh. A compact rijndael hardware architecture with s-box optimization. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 239–254. Springer, 2001.

[Sto16] Ko Stoffelen. Optimizing s-box implementations for several criteria using SAT solvers. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 140–160. Springer, 2016.

[TP20] Quan Quan Tan and Thomas Peyrin. Improved heuristics for short linear programs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(1):203–230, 2020.

[UHS+15] Rei Ueno, Naofumi Homma, Yukihiro Sugawara, Yasuyuki Nogami, and Takafumi Aoki. Highly efficient gf(2^8) inversion circuit based on redundant GF arithmetic and its application to AES design. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, volume 9293 of *Lecture Notes in Computer Science*, pages 63–80. Springer, 2015.

[ZH23] Fuxin Zhang and Zhenyu Huang. Optimizing s-box implementations using SAT solvers: Revisited. *IACR Cryptology ePrint Archive*, page 1721, 2023.

A Proof of Theorem 2

We treat $GF(2^8)$ as a field constructed with $x^2 + Ax + B$ for $A, B \in GF(2^4)$, and consider the irreducible polynomial used in $GF(2^4)$ as $x^4 + C_3x^3 + C_2x^2 + C_1x + C_0$. If z is a root of this polynomial, the elements of $GF(2^4)$ is represented as $\gamma_3z^3 + \gamma_2z^2 + \gamma_1z + \gamma_0$. The squaring of this element can be calculated as follows:

$$\begin{aligned}(\gamma_3z^3 + \gamma_2z^2 + \gamma_1z + \gamma_0)^2 = &((C_3 + C_1)\gamma_3 + C_3\gamma_2)z^3 \\ &+ ((C_3C_2 + C_3C_1 + C_2 + C_0)\gamma_3 + C_2\gamma_2 + \gamma_1)z^2 \\ &+ ((C_3C_1 + C_3C_0 + C_2C_1)\gamma_3 + C_1\gamma_2)z \\ &+ ((C_3C_0 + C_2C_0)\gamma_3 + C_0\gamma_2).\end{aligned}$$

Thus, once the polynomial is determined, this calculation can be implemented using only XOR gates.

The constant A is also an element of $GF(2^4)$; hence, it can be represented as $A_3z^3 + A_2z^2 +$

$A_1z + A_0$. The multiplication of A with $\gamma_3z^3 + \gamma_2z^2 + \gamma_1z + \gamma_0$ is as follows:

$$\begin{aligned}
&A(\gamma_3z^3 + \gamma_2z^2 + \gamma_1z + \gamma_0)\\
&= ((A_3C_3 + A_3C_1 + A_2C_3 + A_2C_2 + A_1C_3 + A_0)\gamma_3 + (A_3C_3 + A_3C_2 + A_2C_3 + A_1)\gamma_2\\
&\qquad + (A_3C_3 + A_3 + A_2)\gamma_1)z^3\\
&\quad + (A_3C_3C_2 + A_3C_3C_1 + A_3C_2 + A_3C_0 + A_2C_3C_2 + A_2C_1 + A_1C_2)\gamma_3\\
&\qquad + (A_3C_3C_2 + A_3C_1 + A_2C_2 + A_0)\gamma_2 + (A_3C_2 + A_1)\gamma_1 + A_2\gamma_0)z^2\\
&\quad + (A_3C_3C_1 + A_3C_3C_0 + A_3C_2C_1 + A_2C_3C_1 + A_2C_0 + A_1C_1)\gamma_3\\
&\qquad + (A_3C_3C_1 + A_3C_0 + A_2C_1)\gamma_2 + (A_3C_1 + A_0)\gamma_1 + A_1\gamma_0)z\\
&\quad + (A_3C_3C_0 + A_3C_2C_0 + A_2C_3C_0 + A_1C_0)\gamma_3 + (A_3C_3C_0 + A_2C_0)\gamma_2 + A_3C_0\gamma_1 + A_0\gamma_0).
\end{aligned}$$

Thus, once the polynomial and constant A are determined, this calculation can be implemented using only XOR gates. The calculation of multiplying constant B can also be implemented using only XOR gates.

B New S-box Circuits of AES, SNOW3G and Saturnin

This section presents the discovered AES, SNOW3G, and Saturnin S-box circuits. For all i and j, x_i and y_i are the input and output nodes of the circuit, respectively, and t_j is a temporary node. r_{2i} and r_{2i+1} are the input nodes of the i-th nonlinear gate, and g_i is output node of the gate. XOR and $XNOR$ are expressed using $\oplus$ and constant 1, and nonlinear gates are expressed as the gate function such as AND, OR.

Listing 1: New AES S-box circuit (D: 25, AD: 5, #NL: 32, #L: 85, #(gate): 117)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
1	$t_0 = x_4 \oplus x_2$	7	$g_7 = AND(t_0, t_{18})$	15	$g_{11} = AND(t_{34}, t_{39})$	19	$t_{58} = g_{23} \oplus g_{24}$
1	$t_1 = x_7 \oplus x_1$	7	$t_{21} = t_1 \oplus t_{20}$	15	$g_{13} = AND(t_{36}, t_{42})$	19	$t_{59} = g_{16} \oplus g_{26}$
1	$t_2 = x_7 \oplus x_4$	7	$t_{22} = x_7 \oplus t_{20}$	15	$g_{16} = AND(t_{45}, x_0)$	19	$t_{62} = g_{14} \oplus g_{17}$
1	$t_3 = x_7 \oplus x_2$	7	$t_{23} = g_1 \oplus g_0$	15	$g_{19} = AND(t_{49}, t_{17})$	19	$t_{65} = g_{26} \oplus t_{57}$
1	$t_4 = x_6 \oplus x_5$	7	$t_{28} = g_8 \oplus g_6$	15	$g_{25} = AND(t_{45}, t_6)$	20	$t_{55} = g_{29} \oplus g_{30}$
2	$t_5 = t_4 \oplus x_0$	8	$t_{25} = g_4 \oplus g_3$	15	$g_{28} = AND(t_{49}, t_8)$	20	$t_{61} = g_{21} \oplus g_{22}$
2	$t_7 = t_1 \oplus t_0$	8	$t_{26} = g_5 \oplus g_3$	15	$t_{51} = t_{49} \oplus t_{45}$	20	$t_{63} = g_{20} \oplus g_{21}$
3	$t_6 = t_5 \oplus x_4$	8	$t_{27} = g_7 \oplus g_6$	16	$g_{20} = AND(t_{51}, t_{16})$	20	$t_{64} = g_{30} \oplus g_{31}$
3	$t_8 = t_5 \oplus x_7$	8	$t_{30} = t_{24} \oplus t_{28}$	16	$g_{29} = AND(t_{51}, t_2)$	20	$t_{66} = t_{59} \oplus t_{62}$
3	$t_9 = t_5 \oplus x_1$	9	$t_{29} = t_{23} \oplus t_{27}$	16	$t_{44} = g_{13} \oplus t_{43}$	21	$t_{67} = g_{18} \oplus t_{55}$
3	$t_{11} = x_3 \oplus t_7$	9	$t_{31} = t_{25} \oplus t_{27}$	16	$t_{48} = g_{11} \oplus t_{47}$	21	$t_{68} = g_{17} \oplus t_{63}$
4	$g_2 = AND(t_6, x_0)$	9	$t_{32} = t_{26} \oplus t_{28}$	16	$t_{60} = g_{16} \oplus g_{19}$	21	$t_{69} = t_{55} \oplus t_{66}$
4	$g_4 = AND(t_9, t_5)$	9	$t_{34} = t_{30} \oplus t_{19}$	17	$g_{15} = AND(t_{44}, t_{14})$	21	$t_{70} = g_{28} \oplus t_{66}$
4	$t_{10} = t_9 \oplus t_3$	10	$t_{33} = t_{29} \oplus t_{13}$	17	$g_{18} = AND(t_{48}, t_5)$	22	$t_{71} = t_{61} \oplus t_{67}$
4	$t_{12} = t_{11} \oplus x_2$	10	$t_{35} = t_{31} \oplus t_{21}$	17	$g_{24} = AND(t_{44}, t_{10})$	22	$t_{72} = t_{58} \oplus t_{67}$
4	$t_{13} = t_{11} \oplus x_6$	10	$t_{36} = t_{32} \oplus t_{22}$	17	$g_{27} = AND(t_{48}, t_9)$	22	$t_{73} = g_{18} \oplus t_{68}$
5	$g_0 = AND(t_7, t_{12})$	11	$g_9 = AND(t_{33}, t_{35})$	17	$t_{50} = t_{48} \oplus t_{44}$	22	$\boldsymbol{y_0 = t_{69} \oplus t_{57} \oplus 1}$
5	$t_{14} = t_{12} \oplus x_0$	11	$t_{37} = t_{33} \oplus t_{34}$	17	$t_{52} = t_{49} \oplus t_{48}$	23	$t_{74} = t_{70} \oplus t_{71}$
5	$t_{15} = t_{12} \oplus t_4$	11	$t_{40} = t_{35} \oplus t_{36}$	17	$t_{53} = t_{45} \oplus t_{44}$	23	$t_{75} = g_{15} \oplus t_{72}$
5	$t_{16} = t_{13} \oplus t_2$	11	$t_{46} = t_{34} \oplus t_{33}$	18	$g_{14} = AND(t_{53}, t_{12})$	23	$\boldsymbol{y_1 = t_{71} \oplus t_{65} \oplus 1}$
6	$g_1 = AND(t_{10}, t_{14})$	12	$t_{38} = t_{36} \oplus g_9$	18	$g_{17} = AND(t_{52}, t_{20})$	23	$\boldsymbol{y_7 = t_{68} \oplus t_{72}}$
6	$g_6 = AND(t_2, t_{16})$	12	$t_{41} = t_{34} \oplus g_9$	18	$g_{22} = AND(t_{50}, t_{15})$	24	$t_{76} = t_{73} \oplus t_{74}$
6	$g_8 = AND(t_3, t_{15})$	13	$g_{10} = AND(t_{37}, t_{38})$	18	$g_{23} = AND(t_{53}, t_7)$	24	$\boldsymbol{y_2 = t_{56} \oplus t_{74}}$
6	$t_{17} = x_0 \oplus t_{16}$	13	$g_{12} = AND(t_{40}, t_{41})$	18	$g_{26} = AND(t_{52}, t_1)$	24	$\boldsymbol{y_3 = t_{60} \oplus t_{75}}$
6	$t_{18} = t_{15} \oplus t_{16}$	14	$t_{39} = g_9 \oplus g_{10}$	18	$g_{31} = AND(t_{50}, t_3)$	24	$\boldsymbol{y_4 = t_{62} \oplus t_{75}}$
6	$t_{19} = t_{15} \oplus t_3$	14	$t_{42} = g_9 \oplus g_{12}$	18	$t_{54} = t_{51} \oplus t_{50}$	25	$\boldsymbol{y_5 = t_{76} \oplus t_{64} \oplus 1}$
6	$t_{20} = t_4 \oplus t_{16}$	14	$t_{43} = t_{40} \oplus g_{12}$	18	$t_{56} = g_{24} \oplus g_{25}$	25	$\boldsymbol{y_6 = y_4 \oplus t_{73} \oplus 1}$
6	$t_{24} = g_2 \oplus g_0$	14	$t_{45} = t_{36} \oplus g_{12}$	18	$t_{57} = g_{19} \oplus g_{27}$		
7	$g_3 = AND(t_1, t_{20})$	14	$t_{47} = t_{46} \oplus g_{10}$	19	$g_{21} = AND(t_{54}, t_{18})$		
7	$g_5 = AND(t_8, t_{17})$	14	$t_{49} = t_{34} \oplus g_{10}$	19	$g_{30} = AND(t_{54}, t_0)$		

Listing 2: New AES S-box circuit (D: 23, AD: 4, #NL: 33, #L: 85, #(gate): 118)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
1	$t_0 = x_4 \oplus x_2$	7	$g_7 = AND(t_0, t_{18})$	13	$g_{14} = AND(t_{35}, t_{42})$	17	$g_{31} = AND(t_{54}, t_0)$
1	$t_1 = x_7 \oplus x_1$	7	$t_{21} = t_1 \oplus t_{20}$	14	$t_{44} = g_{14} \oplus t_{43}$	17	$t_{58} = g_{24} \oplus g_{25}$
1	$t_2 = x_7 \oplus x_4$	7	$t_{22} = x_7 \oplus t_{20}$	14	$t_{45} = t_{36} \oplus g_{11}$	17	$t_{59} = g_{17} \oplus g_{27}$
1	$t_3 = x_7 \oplus x_2$	7	$t_{23} = g_1 \oplus g_0$	14	$t_{48} = g_{13} \oplus t_{47}$	17	$t_{62} = g_{15} \oplus g_{18}$
1	$t_4 = x_6 \oplus x_5$	7	$t_{28} = g_8 \oplus g_6$	14	$t_{49} = t_{34} \oplus g_{10}$	17	$t_{65} = g_{27} \oplus t_{57}$
2	$t_5 = t_4 \oplus x_0$	8	$t_{25} = g_4 \oplus g_3$	15	$g_{16} = AND(t_{44}, t_{14})$	18	$t_{55} = g_{30} \oplus g_{31}$
2	$t_7 = t_1 \oplus t_0$	8	$t_{26} = g_5 \oplus g_3$	15	$g_{17} = AND(t_{45}, x_0)$	18	$t_{61} = g_{22} \oplus g_{23}$
3	$t_6 = t_5 \oplus x_4$	8	$t_{27} = g_7 \oplus g_6$	15	$g_{19} = AND(t_{48}, t_5)$	18	$t_{63} = g_{21} \oplus g_{22}$
3	$t_8 = t_5 \oplus x_7$	8	$t_{30} = t_{24} \oplus t_{28}$	15	$g_{20} = AND(t_{49}, t_{17})$	18	$t_{64} = g_{31} \oplus g_{32}$
3	$t_9 = t_5 \oplus x_1$	9	$t_{29} = t_{23} \oplus t_{27}$	15	$g_{25} = AND(t_{44}, t_{10})$	18	$t_{66} = t_{59} \oplus t_{62}$
3	$t_{11} = x_3 \oplus t_7$	9	$t_{31} = t_{25} \oplus t_{27}$	15	$g_{26} = AND(t_{45}, t_6)$	19	$t_{67} = g_{19} \oplus t_{55}$
4	$g_2 = AND(t_6, x_0)$	9	$t_{32} = t_{26} \oplus t_{28}$	15	$g_{28} = AND(t_{48}, t_9)$	19	$t_{68} = g_{18} \oplus t_{63}$
4	$g_4 = AND(t_9, t_5)$	9	$t_{34} = t_{30} \oplus t_{19}$	15	$g_{29} = AND(t_{49}, t_8)$	19	$t_{69} = t_{55} \oplus t_{66}$
4	$t_{10} = t_9 \oplus t_3$	10	$t_{33} = t_{29} \oplus t_{13}$	15	$t_{50} = t_{48} \oplus t_{44}$	19	$t_{70} = g_{29} \oplus t_{66}$
4	$t_{12} = t_{11} \oplus x_2$	10	$t_{35} = t_{31} \oplus t_{21}$	15	$t_{51} = t_{49} \oplus t_{45}$	20	$t_{71} = t_{61} \oplus t_{67}$
4	$t_{13} = t_{11} \oplus x_6$	10	$t_{36} = t_{32} \oplus t_{22}$	15	$t_{52} = t_{49} \oplus t_{48}$	20	$t_{72} = t_{58} \oplus t_{67}$
5	$g_0 = AND(t_7, t_{12})$	11	$g_9 = AND(t_{33}, t_{35})$	15	$t_{53} = t_{45} \oplus t_{44}$	20	$t_{73} = g_{19} \oplus t_{68}$
5	$t_{14} = t_{12} \oplus x_0$	11	$g_{12} = AND(t_{34}, t_{36})$	16	$g_{15} = AND(t_{53}, t_{12})$	20	$\boldsymbol{y_0 = t_{69} \oplus t_{57} \oplus 1}$
5	$t_{15} = t_{12} \oplus t_4$	11	$t_{37} = t_{33} \oplus t_{34}$	16	$g_{18} = AND(t_{52}, t_{20})$	21	$t_{74} = t_{70} \oplus t_{71}$
5	$t_{16} = t_{13} \oplus t_2$	11	$t_{39} = t_{35} \oplus t_{36}$	16	$g_{21} = AND(t_{51}, t_{16})$	21	$t_{75} = g_{16} \oplus t_{72}$
6	$g_1 = AND(t_{10}, t_{14})$	11	$t_{46} = t_{34} \oplus t_{33}$	16	$g_{23} = AND(t_{50}, t_{15})$	21	$\boldsymbol{y_1 = t_{71} \oplus t_{65} \oplus 1}$
6	$g_6 = AND(t_2, t_{16})$	12	$t_{38} = t_{36} \oplus g_9$	16	$g_{24} = AND(t_{53}, t_7)$	21	$\boldsymbol{y_7 = t_{68} \oplus t_{72}}$
6	$g_8 = AND(t_3, t_{15})$	12	$t_{40} = t_{34} \oplus g_9$	16	$g_{27} = AND(t_{52}, t_1)$	22	$t_{76} = t_{73} \oplus t_{74}$
6	$t_{17} = x_0 \oplus t_{16}$	12	$t_{41} = t_{36} \oplus g_{12}$	16	$g_{30} = AND(t_{51}, t_2)$	22	$\boldsymbol{y_2 = t_{56} \oplus t_{74}}$
6	$t_{18} = t_{15} \oplus t_{16}$	12	$t_{42} = t_{34} \oplus g_{12}$	16	$g_{32} = AND(t_{50}, t_3)$	22	$\boldsymbol{y_3 = t_{60} \oplus t_{75}}$
6	$t_{19} = t_{15} \oplus t_3$	12	$t_{43} = g_9 \oplus t_{39}$	16	$t_{54} = t_{51} \oplus t_{50}$	22	$\boldsymbol{y_4 = t_{62} \oplus t_{75}}$
6	$t_{20} = t_4 \oplus t_{16}$	12	$t_{47} = g_9 \oplus t_{46}$	16	$t_{56} = g_{25} \oplus g_{26}$	23	$\boldsymbol{y_5 = t_{76} \oplus t_{64} \oplus 1}$
6	$t_{24} = g_2 \oplus g_0$	13	$g_{10} = AND(t_{37}, t_{38})$	16	$t_{57} = g_{20} \oplus g_{28}$	23	$\boldsymbol{y_6 = y_4 \oplus t_{73} \oplus 1}$
7	$g_3 = AND(t_1, t_{20})$	13	$g_{11} = AND(t_{39}, t_{40})$	16	$t_{60} = g_{17} \oplus g_{20}$		
7	$g_5 = AND(t_8, t_{17})$	13	$g_{13} = AND(t_{33}, t_{41})$	17	$g_{22} = AND(t_{54}, t_{18})$		

Listing 3: New AES S-box circuit (D: 18, AD: 5, #NL: 32, #L: 96, #(gate): 128)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
1	$t_0 = x_7 \oplus x_4$	4	$g_5 = AND(t_{19}, t_{16})$	11	$g_{13} = AND(t_{40}, t_{46})$	15	$t_{62} = g_{22} \oplus g_{26}$
1	$t_1 = x_7 \oplus x_2$	4	$g_8 = AND(t_1, t_9)$	11	$g_{16} = AND(t_{50}, x_0)$	15	$t_{63} = g_{17} \oplus g_{29}$
1	$t_2 = x_7 \oplus x_1$	4	$t_{23} = t_1 \oplus t_9$	11	$g_{19} = AND(t_{47}, t_{16})$	15	$t_{73} = g_{23} \oplus t_{59}$
1	$t_3 = x_4 \oplus x_2$	4	$t_{24} = t_{19} \oplus t_{16}$	11	$g_{25} = AND(t_{50}, t_{18})$	15	$t_{75} = g_{25} \oplus t_{59}$
1	$t_4 = x_3 \oplus x_1$	4	$t_{27} = t_{13} \oplus g_0$	11	$g_{28} = AND(t_{47}, t_{19})$	15	$t_{76} = g_{26} \oplus t_{66}$
1	$t_6 = x_6 \oplus x_5$	4	$t_{28} = g_2 \oplus g_0$	11	$t_{54} = t_{47} \oplus t_{50}$	16	$t_{58} = g_{29} \oplus g_{30}$
1	$t_{10} = x_6 \oplus x_2$	4	$t_{29} = t_{25} \oplus g_3$	12	$g_{20} = AND(t_{54}, t_{14})$	16	$t_{64} = g_{30} \oplus t_{63}$
1	$t_{11} = x_5 \oplus x_2$	4	$t_{31} = g_7 \oplus g_6$	12	$g_{29} = AND(t_{54}, t_0)$	16	$t_{65} = g_{14} \oplus t_{61}$
1	$t_{17} = x_4 \oplus x_0$	5	$t_{30} = g_5 \oplus g_3$	12	$t_{49} = g_{11} \oplus t_{48}$	16	$t_{67} = g_{20} \oplus g_{21}$
1	$t_{20} = x_1 \oplus x_0$	5	$t_{32} = g_8 \oplus g_6$	12	$t_{52} = g_{13} \oplus t_{51}$	16	$t_{68} = g_{21} \oplus t_{62}$
2	$t_5 = t_0 \oplus t_4$	5	$t_{33} = t_{27} \oplus g_1$	12	$t_{70} = g_{16} \oplus g_{19}$	16	$t_{69} = g_{28} \oplus t_{60}$
2	$t_8 = x_0 \oplus t_6$	5	$t_{34} = t_{28} \oplus t_{23}$	13	$g_{15} = AND(t_{52}, t_7)$	16	$t_{77} = g_{31} \oplus t_{62}$
2	$t_{12} = t_2 \oplus t_3$	5	$t_{35} = t_{29} \oplus g_4$	13	$g_{18} = AND(t_{49}, t_8)$	16	$t_{80} = t_{61} \oplus t_{70}$
2	$t_{14} = t_4 \oplus t_{10}$	6	$t_{36} = t_{30} \oplus t_{32}$	13	$g_{24} = AND(t_{52}, t_{22})$	16	$t_{81} = t_{76} \oplus t_{60}$
2	$t_{15} = t_4 \oplus t_{11}$	6	$t_{37} = t_{33} \oplus t_{31}$	13	$g_{27} = AND(t_{49}, t_{21})$	17	$t_{71} = g_{18} \oplus t_{58}$
2	$t_{18} = t_6 \oplus t_{17}$	6	$t_{38} = t_{34} \oplus t_{32}$	13	$t_{53} = t_{49} \oplus t_{52}$	17	$t_{74} = g_{24} \oplus t_{58}$
2	$t_{21} = t_6 \oplus t_{20}$	6	$t_{39} = t_{35} \oplus t_{31}$	13	$t_{55} = t_{47} \oplus t_{49}$	17	$t_{78} = t_{58} \oplus t_{59}$
2	$t_{26} = t_0 \oplus t_{11}$	7	$g_9 = AND(t_{37}, t_{39})$	13	$t_{56} = t_{50} \oplus t_{52}$	17	$t_{79} = t_{59} \oplus t_{65}$
3	$g_0 = AND(t_{12}, t_5)$	7	$t_{40} = t_{36} \oplus t_{24}$	13	$t_{72} = g_{20} \oplus g_{29}$	17	$t_{82} = t_{73} \oplus t_{67}$
3	$g_2 = AND(t_{18}, x_0)$	7	$t_{41} = t_{37} \oplus t_{38}$	14	$g_{14} = AND(t_{56}, t_5)$	17	$t_{83} = t_{64} \oplus t_{68}$
3	$g_3 = AND(t_2, t_{15})$	8	$t_{42} = t_{40} \oplus g_9$	14	$g_{17} = AND(t_{55}, t_{15})$	17	$t_{84} = t_{65} \oplus t_{67}$
3	$g_4 = AND(t_{21}, t_8)$	8	$t_{44} = t_{39} \oplus t_{40}$	14	$g_{22} = AND(t_{53}, t_9)$	17	$t_{85} = t_{66} \oplus t_{68}$
3	$g_6 = AND(t_0, t_{14})$	8	$t_{45} = t_{38} \oplus g_9$	14	$g_{23} = AND(t_{56}, t_{12})$	17	$t_{86} = t_{69} \oplus t_{72}$
3	$g_7 = AND(t_3, t_{26})$	9	$g_{10} = AND(t_{41}, t_{42})$	14	$g_{26} = AND(t_{55}, t_2)$	17	$t_{87} = t_{69} \oplus t_{75}$
3	$t_7 = x_0 \oplus t_5$	9	$g_{12} = AND(t_{44}, t_{45})$	14	$g_{31} = AND(t_{53}, t_1)$	17	$\boldsymbol{y_0 = t_{81} \oplus t_{64} \oplus 1}$
3	$t_9 = t_5 \oplus t_6$	10	$t_{43} = g_9 \oplus g_{10}$	14	$t_{57} = t_{54} \oplus t_{53}$	18	$\boldsymbol{y_1 = t_{85} \oplus t_{71} \oplus 1}$
3	$t_{13} = t_5 \oplus t_{10}$	10	$t_{46} = g_9 \oplus g_{12}$	14	$t_{59} = g_{18} \oplus g_{24}$	18	$\boldsymbol{y_2 = t_{83} \oplus t_{87}}$
3	$t_{16} = t_8 \oplus t_{15}$	10	$t_{47} = t_{38} \oplus g_{10}$	14	$t_{66} = g_{19} \oplus g_{27}$	18	$\boldsymbol{y_3 = t_{78} \oplus t_{80}}$
3	$t_{19} = t_0 \oplus t_{18}$	10	$t_{48} = t_{41} \oplus g_{10}$	15	$g_{21} = AND(t_{57}, t_{26})$	18	$\boldsymbol{y_4 = t_{64} \oplus t_{79}}$
3	$t_{22} = t_1 \oplus t_{21}$	10	$t_{50} = t_{40} \oplus g_{12}$	15	$g_{30} = AND(t_{57}, t_3)$	18	$\boldsymbol{y_5 = t_{86} \oplus t_{77} \oplus 1}$
3	$t_{25} = t_2 \oplus t_{15}$	10	$t_{51} = t_{44} \oplus g_{12}$	15	$t_{60} = g_{14} \oplus g_{16}$	18	$\boldsymbol{y_6 = t_{84} \oplus t_{74} \oplus 1}$
4	$g_1 = AND(t_{22}, t_7)$	11	$g_{11} = AND(t_{38}, t_{43})$	15	$t_{61} = g_{15} \oplus g_{23}$	18	$\boldsymbol{y_7 = t_{64} \oplus t_{82}}$

Listing 4: New `AES` S-box circuit (D: 17, AD: 4, #NL: 33, #L: 96, #(gate): 129)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
1	$t_0 = x_7 \oplus x_4$	4	$g_8 = AND(t_1, t_9)$	11	$g_{17} = AND(t_{50}, x_0)$	14	$t_{73} = g_{24} \oplus t_{59}$
1	$t_1 = x_7 \oplus x_2$	4	$t_{23} = t_1 \oplus t_9$	11	$g_{20} = AND(t_{47}, t_{16})$	14	$t_{75} = g_{26} \oplus t_{59}$
1	$t_2 = x_7 \oplus x_1$	4	$t_{24} = t_{19} \oplus t_{16}$	11	$g_{26} = AND(t_{50}, t_{18})$	14	$t_{76} = g_{27} \oplus t_{66}$
1	$t_3 = x_4 \oplus x_2$	4	$t_{27} = t_{13} \oplus g_0$	11	$g_{29} = AND(t_{47}, t_{19})$	15	$t_{58} = g_{30} \oplus g_{31}$
1	$t_4 = x_3 \oplus x_1$	4	$t_{28} = g_2 \oplus g_0$	11	$t_{49} = g_{13} \oplus t_{48}$	15	$t_{64} = g_{31} \oplus t_{63}$
1	$t_6 = x_6 \oplus x_5$	4	$t_{29} = t_{25} \oplus g_3$	11	$t_{52} = g_{14} \oplus t_{51}$	15	$t_{65} = g_{15} \oplus t_{61}$
1	$t_{10} = x_6 \oplus x_2$	4	$t_{31} = g_7 \oplus g_6$	11	$t_{54} = t_{47} \oplus t_{50}$	15	$t_{67} = g_{21} \oplus g_{22}$
1	$t_{11} = x_5 \oplus x_2$	5	$t_{30} = g_5 \oplus g_3$	12	$g_{16} = AND(t_{52}, t_7)$	15	$t_{68} = g_{22} \oplus t_{62}$
1	$t_{17} = x_4 \oplus x_0$	5	$t_{32} = g_8 \oplus g_6$	12	$g_{19} = AND(t_{49}, t_8)$	15	$t_{69} = g_{29} \oplus t_{60}$
1	$t_{20} = x_1 \oplus x_0$	5	$t_{33} = t_{27} \oplus g_1$	12	$g_{21} = AND(t_{54}, t_{14})$	15	$t_{77} = g_{32} \oplus t_{62}$
2	$t_5 = t_0 \oplus t_4$	5	$t_{34} = t_{28} \oplus t_{23}$	12	$g_{25} = AND(t_{52}, t_{22})$	15	$t_{80} = t_{61} \oplus t_{70}$
2	$t_8 = x_0 \oplus t_6$	5	$t_{35} = t_{29} \oplus g_4$	12	$g_{28} = AND(t_{49}, t_{21})$	15	$t_{81} = t_{76} \oplus t_{60}$
2	$t_{12} = t_2 \oplus t_3$	6	$t_{36} = t_{30} \oplus t_{32}$	12	$g_{30} = AND(t_{54}, t_0)$	16	$t_{71} = g_{19} \oplus t_{58}$
2	$t_{14} = t_4 \oplus t_{10}$	6	$t_{37} = t_{33} \oplus t_{31}$	12	$t_{53} = t_{49} \oplus t_{52}$	16	$t_{74} = g_{25} \oplus t_{58}$
2	$t_{15} = t_4 \oplus t_{11}$	6	$t_{38} = t_{34} \oplus t_{32}$	12	$t_{55} = t_{47} \oplus t_{49}$	16	$t_{78} = t_{58} \oplus t_{59}$
2	$t_{18} = t_6 \oplus t_{17}$	6	$t_{39} = t_{35} \oplus t_{31}$	12	$t_{56} = t_{50} \oplus t_{52}$	16	$t_{79} = t_{59} \oplus t_{65}$
2	$t_{21} = t_6 \oplus t_{20}$	7	$g_9 = AND(t_{37}, t_{39})$	12	$t_{70} = g_{17} \oplus g_{20}$	16	$t_{82} = t_{73} \oplus t_{67}$
2	$t_{26} = t_0 \oplus t_{11}$	7	$t_{40} = t_{36} \oplus t_{24}$	13	$g_{15} = AND(t_{56}, t_5)$	16	$t_{83} = t_{64} \oplus t_{68}$
3	$g_0 = AND(t_{12}, t_5)$	7	$t_{41} = t_{37} \oplus t_{38}$	13	$g_{18} = AND(t_{55}, t_{15})$	16	$t_{84} = t_{65} \oplus t_{67}$
3	$g_2 = AND(t_{18}, x_0)$	8	$g_{12} = AND(t_{38}, t_{40})$	13	$g_{23} = AND(t_{53}, t_9)$	16	$t_{85} = t_{66} \oplus t_{68}$
3	$g_3 = AND(t_2, t_{15})$	8	$t_{42} = t_{40} \oplus g_9$	13	$g_{24} = AND(t_{56}, t_{12})$	16	$t_{86} = t_{69} \oplus t_{72}$
3	$g_4 = AND(t_{21}, t_8)$	8	$t_{43} = t_{39} \oplus t_{40}$	13	$g_{27} = AND(t_{55}, t_2)$	16	$t_{87} = t_{69} \oplus t_{75}$
3	$g_6 = AND(t_0, t_{14})$	8	$t_{44} = t_{38} \oplus g_9$	13	$g_{32} = AND(t_{53}, t_1)$	16	$\boldsymbol{y_0 = t_{81} \oplus t_{64} \oplus 1}$
3	$g_7 = AND(t_3, t_{26})$	8	$t_{48} = g_9 \oplus t_{41}$	13	$t_{57} = t_{54} \oplus t_{53}$	17	$\boldsymbol{y_1 = t_{85} \oplus t_{71} \oplus 1}$
3	$t_7 = x_0 \oplus t_5$	9	$g_{10} = AND(t_{41}, t_{42})$	13	$t_{59} = g_{19} \oplus g_{25}$	17	$\boldsymbol{y_2 = t_{83} \oplus t_{87}}$
3	$t_9 = t_5 \oplus t_6$	9	$g_{11} = AND(t_{43}, t_{44})$	13	$t_{66} = g_{20} \oplus g_{28}$	17	$\boldsymbol{y_3 = t_{78} \oplus t_{80}}$
3	$t_{13} = t_5 \oplus t_{10}$	9	$t_{45} = t_{40} \oplus g_{12}$	13	$t_{72} = g_{21} \oplus g_{30}$	17	$\boldsymbol{y_4 = t_{64} \oplus t_{79}}$
3	$t_{16} = t_8 \oplus t_{15}$	9	$t_{46} = t_{38} \oplus g_{12}$	14	$g_{22} = AND(t_{57}, t_{26})$	17	$\boldsymbol{y_5 = t_{86} \oplus t_{77} \oplus 1}$
3	$t_{19} = t_0 \oplus t_{18}$	9	$t_{51} = g_9 \oplus t_{43}$	14	$g_{31} = AND(t_{57}, t_3)$	17	$\boldsymbol{y_6 = t_{84} \oplus t_{74} \oplus 1}$
3	$t_{22} = t_1 \oplus t_{21}$	10	$g_{13} = AND(t_{37}, t_{45})$	14	$t_{60} = g_{15} \oplus g_{17}$	17	$\boldsymbol{y_7 = t_{64} \oplus t_{82}}$
3	$t_{25} = t_2 \oplus t_{15}$	10	$g_{14} = AND(t_{39}, t_{46})$	14	$t_{61} = g_{16} \oplus g_{24}$		
4	$g_1 = AND(t_{22}, t_7)$	10	$t_{47} = t_{38} \oplus g_{10}$	14	$t_{62} = g_{23} \oplus g_{27}$		
4	$g_5 = AND(t_{19}, t_{16})$	10	$t_{50} = t_{40} \oplus g_{11}$	14	$t_{63} = g_{18} \oplus g_{30}$		

Listing 5: New AES S-box circuit (D: 26, AD: 6, #NL: 32, #L: 81, #(gate): 113)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	5	$g_0 = AND(r_0, r_1)$	13	$g_{11} = AND(r_{22}, r_{23})$	20	$g_{22} = AND(r_{44}, r_{45})$
0	$r_{33} = x_0$	5	$g_3 = AND(r_6, r_7)$	14	$t_{40} = g_9 \oplus g_{11}$	20	$g_{26} = AND(r_{52}, r_{53})$
1	$t_0 = x_1 \oplus x_7$	5	$t_7 = x_0 \oplus t_6$	14	$t_{41} = g_{10} \oplus t_{38}$	20	$g_{31} = AND(r_{62}, r_{63})$
1	$t_1 = x_4 \oplus x_7$	5	$t_{14} = t_6 \oplus t_8$	14	$t_{44} = t_{30} \oplus g_{11}$	20	$t_{49} = t_{43} \oplus t_{47}$
1	$t_2 = x_2 \oplus x_4$	5	$t_{17} = t_9 \oplus t_{16}$	14	$r_{25} = t_{40}$	20	$t_{60} = g_{18} \oplus t_{57}$
1	$t_4 = x_2 \oplus x_7$	5	$t_{18} = t_8 \oplus t_{16}$	14	$r_{26} = t_{41}$	20	$r_{42} = t_{49}$
1	$t_8 = x_5 \oplus x_6$	5	$t_{21} = g_4 \oplus g_7$	14	$r_{32} = t_{44}$	20	$r_{60} = t_{49}$
1	$r_6 = t_0$	5	$r_3 = t_7$	14	$r_{38} = t_{41}$	21	$g_{21} = AND(r_{42}, r_{43})$
1	$r_{12} = t_1$	5	$r_{11} = t_{17}$	14	$r_{50} = t_{44}$	21	$g_{30} = AND(r_{60}, r_{61})$
1	$r_{14} = t_2$	5	$r_{13} = t_{18}$	14	$r_{56} = t_{41}$	21	$t_{55} = g_{18} \oplus g_{17}$
1	$r_{16} = t_4$	5	$r_{17} = t_{14}$	15	$g_{12} = AND(r_{24}, r_{25})$	21	$t_{64} = g_{16} \oplus g_{22}$
1	$r_{53} = t_0$	5	$r_{31} = t_7$	15	$g_{16} = AND(r_{32}, r_{33})$	22	$t_{51} = g_{29} \oplus g_{30}$
1	$r_{59} = t_1$	5	$r_{39} = t_{17}$	15	$g_{19} = AND(r_{38}, r_{39})$	22	$t_{56} = g_{20} \oplus g_{21}$
1	$r_{61} = t_2$	5	$r_{41} = t_{18}$	15	$g_{25} = AND(r_{50}, r_{51})$	22	$t_{62} = g_{14} \oplus t_{55}$
1	$r_{63} = t_4$	5	$r_{45} = t_{14}$	15	$g_{28} = AND(r_{56}, r_{57})$	22	$t_{67} = g_{21} \oplus t_{64}$
2	$t_3 = t_0 \oplus t_2$	6	$g_1 = AND(r_2, r_3)$	15	$t_{48} = t_{41} \oplus t_{44}$	23	$t_{52} = g_{23} \oplus t_{51}$
2	$t_9 = x_0 \oplus t_8$	6	$g_5 = AND(r_{10}, r_{11})$	15	$r_{40} = t_{48}$	23	$t_{58} = g_{26} \oplus t_{51}$
2	$t_{15} = x_5 \oplus t_1$	6	$g_6 = AND(r_{12}, r_{13})$	15	$r_{58} = t_{48}$	23	$t_{69} = g_{14} \oplus t_{56}$
2	$r_0 = t_3$	6	$g_8 = AND(r_{16}, r_{17})$	16	$g_{20} = AND(r_{40}, r_{41})$	23	$t_{71} = g_{28} \oplus t_{67}$
2	$r_9 = t_9$	7	$t_{20} = g_8 \oplus g_5$	16	$g_{29} = AND(r_{58}, r_{59})$	24	$t_{53} = g_{24} \oplus t_{52}$
2	$r_{37} = t_9$	7	$t_{22} = t_{16} \oplus g_6$	16	$t_{42} = t_{34} \oplus g_{12}$	24	$t_{59} = g_{27} \oplus t_{58}$
2	$r_{47} = t_3$	7	$t_{24} = g_1 \oplus t_{15}$	16	$t_{43} = t_{27} \oplus g_{12}$	24	$t_{72} = t_{58} \oplus t_{71}$
3	$t_5 = x_3 \oplus t_3$	7	$t_{35} = g_2 \oplus g_8$	16	$t_{57} = g_{19} \oplus g_{16}$	24	$t_{78} = g_{30} \oplus t_{69}$
3	$t_{10} = x_4 \oplus t_9$	8	$t_{23} = g_3 \oplus t_{22}$	16	$r_{27} = t_{42}$	25	$t_{54} = g_{15} \oplus t_{53}$
3	$t_{12} = x_1 \oplus t_9$	8	$t_{25} = g_7 \oplus t_{24}$	16	$r_{28} = t_{43}$	25	$t_{65} = t_{59} \oplus t_{60}$
3	$t_{13} = x_7 \oplus t_9$	8	$t_{28} = x_1 \oplus t_{20}$	16	$r_{46} = t_{43}$	25	$t_{73} = t_{53} \oplus t_{55}$
3	$t_{19} = x_2 \oplus t_{15}$	8	$t_{31} = g_0 \oplus t_{22}$	17	$g_{13} = AND(r_{26}, r_{27})$	25	$t_{75} = t_{62} \oplus t_{72}$
3	$r_4 = t_{10}$	8	$t_{36} = x_4 \oplus t_{35}$	17	$g_{14} = AND(r_{28}, r_{29})$	25	$t_{79} = g_{31} \oplus t_{78}$
3	$r_8 = t_{12}$	9	$t_{26} = t_0 \oplus t_{23}$	17	$g_{23} = AND(r_{46}, r_{47})$	26	$t_{61} = t_{54} \oplus t_{60}$
3	$r_{10} = t_{13}$	9	$t_{29} = t_{21} \oplus t_{28}$	17	$t_{45} = t_{43} \oplus t_{44}$	26	$t_{63} = t_{54} \oplus t_{62}$
3	$r_{15} = t_{19}$	9	$t_{32} = x_6 \oplus t_{31}$	17	$r_{30} = t_{45}$	26	$t_{66} = t_{62} \oplus t_{65} \oplus 1$
3	$r_{43} = t_{19}$	9	$t_{37} = t_{25} \oplus t_{36}$	17	$r_{48} = t_{45}$	26	$t_{68} = t_{65} \oplus t_{67} \oplus 1$
3	$r_{51} = t_{10}$	9	$r_{20} = t_{37}$	18	$g_{15} = AND(r_{30}, r_{31})$	26	$t_{70} = t_{54} \oplus t_{69} \oplus 1$
3	$r_{55} = t_{12}$	9	$r_{23} = t_{29}$	18	$g_{24} = AND(r_{48}, r_{49})$	26	$t_{74} = t_{56} \oplus t_{73}$
3	$r_{57} = t_{13}$	10	$t_{27} = t_{21} \oplus t_{26}$	18	$t_{46} = t_{37} \oplus g_{13}$	26	$t_{77} = t_{75} \oplus t_{76}$
4	$g_2 = AND(r_4, r_5)$	10	$t_{30} = t_{26} \oplus t_{28}$	18	$r_{36} = t_{46}$	26	$t_{80} = t_{72} \oplus t_{79} \oplus 1$
4	$g_4 = AND(r_8, r_9)$	10	$t_{33} = t_{25} \oplus t_{32}$	18	$r_{54} = t_{46}$	26	$\boldsymbol{y_0 = t_{66}}$
4	$g_7 = AND(r_{14}, r_{15})$	10	$t_{38} = t_{32} \oplus t_{36}$	19	$g_{18} = AND(r_{36}, r_{37})$	26	$\boldsymbol{y_1 = t_{68}}$
4	$t_6 = x_2 \oplus t_5$	10	$r_{18} = t_{33}$	19	$g_{27} = AND(r_{54}, r_{55})$	26	$\boldsymbol{y_2 = t_{77}}$
4	$t_{11} = t_3 \oplus t_{10}$	10	$r_{19} = t_{27}$	19	$t_{47} = t_{41} \oplus t_{46}$	26	$\boldsymbol{y_3 = t_{61}}$
4	$t_{16} = t_5 \oplus t_{15}$	10	$r_{24} = t_{30}$	19	$t_{50} = t_{45} \oplus t_{46}$	26	$\boldsymbol{y_4 = t_{63}}$
4	$r_1 = t_6$	11	$g_9 = AND(r_{18}, r_{19})$	19	$t_{76} = g_{25} \oplus g_{24}$	26	$\boldsymbol{y_5 = t_{80}}$
4	$r_2 = t_{11}$	12	$t_{34} = t_{30} \oplus g_9$	19	$r_{34} = t_{47}$	26	$\boldsymbol{y_6 = t_{70}}$
4	$r_7 = t_{16}$	12	$t_{39} = g_9 \oplus t_{38}$	19	$r_{44} = t_{50}$	26	$\boldsymbol{y_7 = t_{74}}$
4	$r_{29} = t_6$	12	$r_{21} = t_{34}$	19	$r_{52} = t_{47}$		
4	$r_{35} = t_{16}$	12	$r_{22} = t_{39}$	19	$r_{62} = t_{50}$		
4	$r_{49} = t_{11}$	13	$g_{10} = AND(r_{20}, r_{21})$	20	$g_{17} = AND(r_{34}, r_{35})$		

Listing 6: New AES S-box circuit (D: 23, AD: 6, #NL: 32, #L: 82, #(gate): 114)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{13} = t_{18}$	11	$g_{11} = AND(r_{22}, r_{23})$	18	$g_{17} = AND(r_{34}, r_{35})$
0	$r_{33} = x_0$	3	$r_{17} = t_{14}$	12	$t_{40} = g_9 \oplus g_{11}$	18	$g_{22} = AND(r_{44}, r_{45})$
1	$t_0 = x_1 \oplus x_7$	3	$r_{31} = t_7$	12	$t_{41} = g_{10} \oplus t_{38}$	18	$g_{26} = AND(r_{52}, r_{53})$
1	$t_1 = x_4 \oplus x_7$	3	$r_{39} = t_{17}$	12	$t_{44} = t_{27} \oplus g_{11}$	18	$g_{31} = AND(r_{62}, r_{63})$
1	$t_2 = x_2 \oplus x_4$	3	$r_{41} = t_{18}$	12	$r_{25} = t_{40}$	18	$t_{49} = t_{43} \oplus t_{47}$
1	$t_4 = x_2 \oplus x_7$	3	$r_{45} = t_{14}$	12	$r_{26} = t_{41}$	18	$t_{62} = g_{18} \oplus t_{57}$
1	$t_5 = x_1 \oplus x_3$	3	$r_{51} = t_{10}$	12	$r_{32} = t_{44}$	18	$r_{42} = t_{49}$
1	$t_8 = x_5 \oplus x_6$	3	$r_{55} = t_{12}$	12	$r_{38} = t_{41}$	18	$r_{60} = t_{49}$
1	$t_{15} = x_2 \oplus x_5$	3	$r_{57} = t_{13}$	12	$r_{50} = t_{44}$	19	$g_{21} = AND(r_{42}, r_{43})$
1	$r_6 = t_0$	4	$g_2 = AND(r_4, r_5)$	12	$r_{56} = t_{41}$	19	$g_{30} = AND(r_{60}, r_{61})$
1	$r_{12} = t_1$	4	$g_4 = AND(r_8, r_9)$	13	$g_{12} = AND(r_{24}, r_{25})$	19	$t_{56} = g_{18} \oplus g_{17}$
1	$r_{14} = t_2$	4	$g_5 = AND(r_{10}, r_{11})$	13	$g_{16} = AND(r_{32}, r_{33})$	19	$t_{64} = g_{16} \oplus g_{22}$
1	$r_{16} = t_4$	4	$g_6 = AND(r_{12}, r_{13})$	13	$g_{19} = AND(r_{38}, r_{39})$	19	$t_{70} = g_{28} \oplus g_{26}$
1	$r_{53} = t_0$	4	$g_8 = AND(r_{16}, r_{17})$	13	$g_{25} = AND(r_{50}, r_{51})$	20	$t_{51} = g_{29} \oplus g_{30}$
1	$r_{59} = t_1$	4	$t_{11} = t_3 \oplus t_{10}$	13	$g_{28} = AND(r_{56}, r_{57})$	20	$t_{55} = g_{20} \oplus g_{21}$
1	$r_{61} = t_2$	4	$t_{24} = t_{15} \oplus g_7$	13	$t_{48} = t_{41} \oplus t_{44}$	20	$t_{60} = g_{14} \oplus t_{56}$
1	$r_{63} = t_4$	4	$r_2 = t_{11}$	13	$r_{40} = t_{48}$	20	$t_{65} = g_{21} \oplus t_{64}$
2	$t_3 = t_0 \oplus t_2$	4	$r_{49} = t_{11}$	13	$r_{58} = t_{48}$	21	$t_{53} = t_{51} \oplus t_{52}$
2	$t_6 = t_1 \oplus t_5$	5	$g_1 = AND(r_2, r_3)$	14	$g_{20} = AND(r_{40}, r_{41})$	21	$t_{58} = g_{27} \oplus t_{51}$
2	$t_9 = x_0 \oplus t_8$	5	$t_{20} = g_4 \oplus g_7$	14	$g_{29} = AND(r_{58}, r_{59})$	21	$t_{66} = g_{14} \oplus t_{55}$
2	$t_{16} = t_5 \oplus t_{15}$	5	$t_{21} = g_8 \oplus g_5$	14	$t_{42} = t_{37} \oplus g_{12}$	21	$t_{71} = t_{65} \oplus t_{70}$
2	$t_{19} = t_1 \oplus t_{15}$	5	$t_{22} = g_3 \oplus g_6$	14	$t_{43} = t_{29} \oplus g_{12}$	21	$t_{72} = t_{60} \oplus t_{62}$
2	$r_0 = t_3$	5	$t_{31} = t_4 \oplus g_8$	14	$t_{57} = g_{19} \oplus g_{16}$	21	$t_{74} = t_{62} \oplus t_{65}$
2	$r_1 = t_6$	5	$t_{35} = g_0 \oplus g_6$	14	$r_{27} = t_{42}$	22	$t_{54} = g_{15} \oplus t_{53}$
2	$r_7 = t_{16}$	6	$t_{23} = t_{16} \oplus t_{22}$	14	$r_{28} = t_{43}$	22	$t_{59} = g_{26} \oplus t_{58}$
2	$r_9 = t_9$	6	$t_{25} = g_1 \oplus t_{24}$	14	$r_{46} = t_{43}$	22	$t_{68} = t_{53} \oplus t_{60}$
2	$r_{15} = t_{19}$	6	$t_{28} = x_1 \oplus t_{20}$	15	$g_{13} = AND(r_{26}, r_{27})$	22	$t_{76} = g_{29} \oplus t_{66}$
2	$r_{29} = t_6$	6	$t_{32} = g_2 \oplus t_{31}$	15	$g_{14} = AND(r_{28}, r_{29})$	22	$t_{77} = g_{31} \oplus t_{71}$
2	$r_{35} = t_{16}$	7	$t_{26} = x_7 \oplus t_{23}$	15	$g_{23} = AND(r_{46}, r_{47})$	22	$t_{80} = t_{71} \oplus t_{79}$
2	$r_{37} = t_9$	7	$t_{30} = t_{21} \oplus t_{28}$	15	$t_{45} = t_{43} \oplus t_{44}$	23	$t_{61} = t_{54} \oplus t_{60}$
2	$r_{43} = t_{19}$	7	$t_{33} = t_{25} \oplus t_{32}$	15	$r_{30} = t_{45}$	23	$t_{63} = t_{54} \oplus t_{62}$
2	$r_{47} = t_3$	7	$t_{34} = t_{14} \oplus t_{25}$	15	$r_{48} = t_{45}$	23	$t_{67} = t_{54} \oplus t_{66} \oplus 1$
3	$g_0 = AND(r_0, r_1)$	7	$r_{20} = t_{33}$	16	$g_{15} = AND(r_{30}, r_{31})$	23	$t_{69} = t_{66} \oplus t_{68}$
3	$g_3 = AND(r_6, r_7)$	7	$r_{23} = t_{30}$	16	$g_{24} = AND(r_{48}, r_{49})$	23	$t_{73} = t_{59} \oplus t_{72} \oplus 1$
3	$g_7 = AND(r_{14}, r_{15})$	8	$t_{27} = t_{21} \oplus t_{26}$	16	$t_{46} = t_{33} \oplus g_{13}$	23	$t_{75} = t_{59} \oplus t_{74} \oplus 1$
3	$t_7 = x_0 \oplus t_6$	8	$t_{29} = t_{26} \oplus t_{28}$	16	$t_{79} = g_{23} \oplus g_{25}$	23	$t_{78} = t_{76} \oplus t_{77} \oplus 1$
3	$t_{10} = x_4 \oplus t_9$	8	$t_{36} = t_{34} \oplus t_{35}$	16	$r_{36} = t_{46}$	23	$t_{81} = t_{68} \oplus t_{80}$
3	$t_{12} = x_1 \oplus t_9$	8	$r_{18} = t_{36}$	16	$r_{54} = t_{46}$	23	$\boldsymbol{y_0 = t_{73}}$
3	$t_{13} = x_7 \oplus t_9$	8	$r_{19} = t_{29}$	17	$g_{18} = AND(r_{36}, r_{37})$	23	$\boldsymbol{y_1 = t_{75}}$
3	$t_{14} = t_6 \oplus t_8$	8	$r_{24} = t_{27}$	17	$g_{27} = AND(r_{54}, r_{55})$	23	$\boldsymbol{y_2 = t_{81}}$
3	$t_{17} = t_9 \oplus t_{16}$	9	$g_9 = AND(r_{18}, r_{19})$	17	$t_{47} = t_{41} \oplus t_{46}$	23	$\boldsymbol{y_3 = t_{63}}$
3	$t_{18} = t_8 \oplus t_{16}$	9	$t_{38} = t_{33} \oplus t_{36}$	17	$t_{50} = t_{45} \oplus t_{46}$	23	$\boldsymbol{y_4 = t_{61}}$
3	$r_3 = t_7$	10	$t_{37} = t_{27} \oplus g_9$	17	$t_{52} = g_{23} \oplus g_{24}$	23	$\boldsymbol{y_5 = t_{78}}$
3	$r_4 = t_{10}$	10	$t_{39} = g_9 \oplus t_{38}$	17	$r_{34} = t_{47}$	23	$\boldsymbol{y_6 = t_{67}}$
3	$r_8 = t_{12}$	10	$r_{21} = t_{37}$	17	$r_{44} = t_{50}$	23	$\boldsymbol{y_7 = t_{69}}$
3	$r_{10} = t_{13}$	10	$r_{22} = t_{39}$	17	$r_{52} = t_{47}$		
3	$r_{11} = t_{17}$	11	$g_{10} = AND(r_{20}, r_{21})$	17	$r_{62} = t_{50}$		

Listing 7: New AES S-box circuit (D: 22, AD: 6, #NL: 32, #L: 85, #(gate): 117)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{17} = t_{14}$	11	$t_{41} = g_{10} \oplus t_{38}$	17	$t_{49} = t_{43} \oplus t_{47}$
0	$r_{33} = x_0$	3	$r_{31} = t_7$	11	$t_{44} = t_{29} \oplus g_{11}$	17	$t_{54} = g_{15} \oplus g_{18}$
1	$t_0 = x_1 \oplus x_7$	3	$r_{39} = t_{17}$	11	$r_{25} = t_{40}$	17	$r_{42} = t_{49}$
1	$t_1 = x_4 \oplus x_7$	3	$r_{41} = t_{18}$	11	$r_{26} = t_{41}$	17	$r_{60} = t_{49}$
1	$t_2 = x_2 \oplus x_4$	3	$r_{45} = t_{14}$	11	$r_{32} = t_{44}$	18	$g_{21} = AND(r_{42}, r_{43})$
1	$t_4 = x_2 \oplus x_7$	3	$r_{51} = t_{10}$	11	$r_{38} = t_{41}$	18	$g_{30} = AND(r_{60}, r_{61})$
1	$t_5 = x_1 \oplus x_3$	3	$r_{55} = t_{12}$	11	$r_{50} = t_{44}$	18	$t_{56} = g_{14} \oplus g_{17}$
1	$t_8 = x_5 \oplus x_6$	3	$r_{57} = t_{13}$	11	$r_{56} = t_{41}$	18	$t_{62} = t_{54} \oplus t_{57}$
1	$t_{15} = x_2 \oplus x_5$	4	$g_2 = AND(r_4, r_5)$	12	$g_{12} = AND(r_{24}, r_{25})$	18	$t_{71} = g_{18} \oplus g_{22}$
1	$r_6 = t_0$	4	$g_4 = AND(r_8, r_9)$	12	$g_{16} = AND(r_{32}, r_{33})$	18	$t_{75} = g_{28} \oplus g_{26}$
1	$r_{12} = t_1$	4	$g_5 = AND(r_{10}, r_{11})$	12	$g_{19} = AND(r_{38}, r_{39})$	19	$t_{51} = g_{29} \oplus g_{30}$
1	$r_{14} = t_2$	4	$g_6 = AND(r_{12}, r_{13})$	12	$g_{25} = AND(r_{50}, r_{51})$	19	$t_{55} = g_{20} \oplus g_{21}$
1	$r_{16} = t_4$	4	$g_8 = AND(r_{16}, r_{17})$	12	$g_{28} = AND(r_{56}, r_{57})$	19	$t_{60} = t_{56} \oplus t_{57}$
1	$r_{53} = t_0$	4	$t_{11} = t_3 \oplus t_{10}$	12	$t_{48} = t_{41} \oplus t_{44}$	19	$t_{64} = t_{54} \oplus t_{56}$
1	$r_{59} = t_1$	4	$t_{22} = t_{16} \oplus g_3$	12	$r_{40} = t_{48}$	19	$t_{72} = g_{21} \oplus t_{71}$
1	$r_{61} = t_2$	4	$t_{24} = t_{15} \oplus g_7$	12	$r_{58} = t_{48}$	19	$t_{81} = g_{31} \oplus t_{62}$
1	$r_{63} = t_4$	4	$t_{31} = g_0 \oplus t_{14}$	13	$g_{20} = AND(r_{40}, r_{41})$	20	$t_{52} = g_{23} \oplus t_{51}$
2	$t_3 = t_0 \oplus t_2$	4	$r_2 = t_{11}$	13	$g_{29} = AND(r_{58}, r_{59})$	20	$t_{58} = g_{27} \oplus t_{51}$
2	$t_6 = t_1 \oplus t_5$	4	$r_{49} = t_{11}$	13	$t_{42} = t_{34} \oplus g_{12}$	20	$t_{67} = t_{55} \oplus t_{66}$
2	$t_9 = x_0 \oplus t_8$	5	$g_1 = AND(r_2, r_3)$	13	$t_{43} = t_{27} \oplus g_{12}$	20	$t_{73} = g_{19} \oplus t_{72}$
2	$t_{16} = t_5 \oplus t_{15}$	5	$t_{20} = g_8 \oplus g_5$	13	$t_{57} = g_{19} \oplus g_{16}$	20	$t_{77} = g_{24} \oplus t_{51}$
2	$t_{19} = t_1 \oplus t_{15}$	5	$t_{21} = g_4 \oplus g_7$	13	$r_{27} = t_{42}$	20	$t_{78} = g_{25} \oplus t_{60}$
2	$r_0 = t_3$	5	$t_{23} = g_6 \oplus t_{22}$	13	$r_{28} = t_{43}$	20	$t_{82} = g_{29} \oplus t_{81}$
2	$r_1 = t_6$	5	$t_{32} = g_6 \oplus t_{31}$	13	$r_{46} = t_{43}$	21	$t_{53} = g_{24} \oplus t_{52}$
2	$r_7 = t_{16}$	5	$t_{35} = t_4 \oplus g_8$	14	$g_{13} = AND(r_{26}, r_{27})$	21	$t_{59} = g_{26} \oplus t_{58}$
2	$r_9 = t_9$	6	$t_{25} = g_1 \oplus t_{24}$	14	$g_{14} = AND(r_{28}, r_{29})$	21	$t_{69} = t_{64} \oplus t_{67}$
2	$r_{15} = t_{19}$	6	$t_{26} = t_{21} \oplus t_{23}$	14	$g_{23} = AND(r_{46}, r_{47})$	21	$t_{76} = t_{73} \oplus t_{75}$
2	$r_{29} = t_6$	6	$t_{28} = x_7 \oplus t_{23}$	14	$t_{45} = t_{43} \oplus t_{44}$	21	$t_{79} = t_{77} \oplus t_{78}$
2	$r_{35} = t_{16}$	6	$t_{36} = g_2 \oplus t_{35}$	14	$r_{30} = t_{45}$	21	$t_{83} = t_{67} \oplus t_{82}$
2	$r_{37} = t_9$	7	$t_{27} = t_0 \oplus t_{26}$	14	$r_{48} = t_{45}$	22	$t_{61} = t_{59} \oplus t_{60} \oplus 1$
2	$r_{43} = t_{19}$	7	$t_{29} = t_{20} \oplus t_{28}$	15	$g_{15} = AND(r_{30}, r_{31})$	22	$t_{63} = t_{53} \oplus t_{62}$
2	$r_{47} = t_3$	7	$t_{33} = t_{25} \oplus t_{32}$	15	$g_{24} = AND(r_{48}, r_{49})$	22	$t_{65} = t_{53} \oplus t_{64}$
3	$g_0 = AND(r_0, r_1)$	7	$t_{37} = t_{25} \oplus t_{36}$	15	$t_{46} = t_{37} \oplus g_{13}$	22	$t_{68} = t_{53} \oplus t_{67} \oplus 1$
3	$g_3 = AND(r_6, r_7)$	7	$t_{38} = t_{32} \oplus t_{36}$	15	$r_{36} = t_{46}$	22	$t_{70} = t_{53} \oplus t_{69}$
3	$g_7 = AND(r_{14}, r_{15})$	7	$r_{18} = t_{33}$	15	$r_{54} = t_{46}$	22	$t_{74} = t_{59} \oplus t_{73} \oplus 1$
3	$t_7 = x_0 \oplus t_6$	7	$r_{19} = t_{27}$	16	$g_{18} = AND(r_{36}, r_{37})$	22	$t_{80} = t_{76} \oplus t_{79}$
3	$t_{10} = x_4 \oplus t_9$	7	$r_{20} = t_{37}$	16	$g_{27} = AND(r_{54}, r_{55})$	22	$t_{84} = t_{76} \oplus t_{83} \oplus 1$
3	$t_{12} = x_1 \oplus t_9$	7	$r_{24} = t_{29}$	16	$t_{47} = t_{41} \oplus t_{46}$	22	$\boldsymbol{y_0 = t_{61}}$
3	$t_{13} = x_7 \oplus t_9$	8	$g_9 = AND(r_{18}, r_{19})$	16	$t_{50} = t_{45} \oplus t_{46}$	22	$\boldsymbol{y_1 = t_{74}}$
3	$t_{14} = t_6 \oplus t_8$	8	$t_{30} = t_{27} \oplus t_{29}$	16	$t_{66} = g_{14} \oplus g_{15}$	22	$\boldsymbol{y_2 = t_{80}}$
3	$t_{17} = t_9 \oplus t_{16}$	8	$r_{23} = t_{30}$	16	$r_{34} = t_{47}$	22	$\boldsymbol{y_3 = t_{63}}$
3	$t_{18} = t_8 \oplus t_{16}$	9	$t_{34} = t_{29} \oplus g_9$	16	$r_{44} = t_{50}$	22	$\boldsymbol{y_4 = t_{65}}$
3	$r_3 = t_7$	9	$t_{39} = g_9 \oplus t_{38}$	16	$r_{52} = t_{47}$	22	$\boldsymbol{y_5 = t_{84}}$
3	$r_4 = t_{10}$	9	$r_{21} = t_{34}$	16	$r_{62} = t_{50}$	22	$\boldsymbol{y_6 = t_{68}}$
3	$r_8 = t_{12}$	9	$r_{22} = t_{39}$	17	$g_{17} = AND(r_{34}, r_{35})$	22	$\boldsymbol{y_7 = t_{70}}$
3	$r_{10} = t_{13}$	10	$g_{10} = AND(r_{20}, r_{21})$	17	$g_{22} = AND(r_{44}, r_{45})$		
3	$r_{11} = t_{17}$	10	$g_{11} = AND(r_{22}, r_{23})$	17	$g_{26} = AND(r_{52}, r_{53})$		
3	$r_{13} = t_{18}$	11	$t_{40} = g_9 \oplus g_{11}$	17	$g_{31} = AND(r_{62}, r_{63})$		

Listing 8: New AES S-box circuit (D: 21, AD: 6, #NL: 32, #L: 90, #(gate): 122)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	4	$g_0 = AND(r_0, r_1)$	12	$t_{43} = g_{10} \oplus t_{40}$	17	$r_{60} = t_{53}$
0	$r_{33} = x_0$	4	$g_2 = AND(r_4, r_5)$	12	$t_{46} = t_{26} \oplus g_{11}$	17	$r_{62} = t_{51}$
1	$t_0 = x_1 \oplus x_7$	4	$g_4 = AND(r_8, r_9)$	12	$r_{25} = t_{42}$	18	$g_{17} = AND(r_{34}, r_{35})$
1	$t_1 = x_4 \oplus x_7$	4	$g_5 = AND(r_{10}, r_{11})$	12	$r_{26} = t_{43}$	18	$g_{21} = AND(r_{42}, r_{43})$
1	$t_2 = x_2 \oplus x_4$	4	$g_6 = AND(r_{12}, r_{13})$	12	$r_{32} = t_{46}$	18	$g_{22} = AND(r_{44}, r_{45})$
1	$t_4 = x_2 \oplus x_7$	4	$g_7 = AND(r_{14}, r_{15})$	12	$r_{38} = t_{43}$	18	$g_{26} = AND(r_{52}, r_{53})$
1	$t_5 = x_5 \oplus x_6$	4	$t_8 = t_3 \oplus t_7$	12	$r_{50} = t_{46}$	18	$g_{30} = AND(r_{60}, r_{61})$
1	$t_{11} = x_2 \oplus x_3$	4	$t_{13} = x_0 \oplus t_{12}$	12	$r_{56} = t_{43}$	18	$g_{31} = AND(r_{62}, r_{63})$
1	$t_{15} = x_1 \oplus x_5$	4	$t_{14} = t_5 \oplus t_{12}$	13	$g_{12} = AND(r_{24}, r_{25})$	18	$t_{60} = g_{19} \oplus g_{18}$
1	$t_{31} = x_5 \oplus x_7$	4	$t_{34} = t_1 \oplus t_{18}$	13	$g_{16} = AND(r_{32}, r_{33})$	18	$t_{80} = g_{20} \oplus t_{76}$
1	$r_6 = t_0$	4	$r_2 = t_8$	13	$g_{19} = AND(r_{38}, r_{39})$	18	$t_{86} = t_{76} \oplus t_{85}$
1	$r_{12} = t_1$	4	$r_3 = t_{13}$	13	$g_{25} = AND(r_{50}, r_{51})$	19	$t_{54} = g_{29} \oplus g_{30}$
1	$r_{14} = t_2$	4	$r_{17} = t_{14}$	13	$g_{28} = AND(r_{56}, r_{57})$	19	$t_{58} = g_{18} \oplus g_{17}$
1	$r_{16} = t_4$	4	$r_{31} = t_{13}$	13	$t_{50} = t_{43} \oplus t_{46}$	19	$t_{59} = g_{20} \oplus g_{21}$
1	$r_{53} = t_0$	4	$r_{45} = t_{14}$	13	$r_{40} = t_{50}$	19	$t_{61} = g_{16} \oplus t_{60}$
1	$r_{59} = t_1$	4	$r_{49} = t_8$	13	$r_{58} = t_{50}$	19	$t_{62} = g_{26} \oplus g_{22}$
1	$r_{61} = t_2$	5	$g_1 = AND(r_2, r_3)$	14	$g_{20} = AND(r_{40}, r_{41})$	19	$t_{72} = g_{27} \oplus t_{60}$
1	$r_{63} = t_4$	5	$g_8 = AND(r_{16}, r_{17})$	14	$g_{29} = AND(r_{58}, r_{59})$	19	$t_{77} = g_{26} \oplus t_{75}$
2	$t_3 = t_0 \oplus t_2$	5	$t_{21} = g_3 \oplus g_6$	14	$t_{44} = t_{39} \oplus g_{12}$	19	$t_{81} = g_{31} \oplus t_{80}$
2	$t_6 = x_0 \oplus t_5$	5	$t_{23} = g_4 \oplus g_7$	14	$t_{45} = t_{28} \oplus g_{12}$	19	$t_{87} = g_{21} \oplus t_{86}$
2	$t_{16} = t_{11} \oplus t_{15}$	5	$t_{35} = g_6 \oplus g_7$	14	$r_{27} = t_{44}$	20	$t_{56} = t_{54} \oplus t_{55}$
2	$r_0 = t_3$	6	$t_{20} = g_8 \oplus g_7$	14	$r_{28} = t_{45}$	20	$t_{63} = t_{57} \oplus t_{58}$
2	$r_7 = t_{16}$	6	$t_{22} = t_{16} \oplus t_{21}$	14	$r_{46} = t_{45}$	20	$t_{65} = t_{58} \oplus t_{59}$
2	$r_9 = t_6$	6	$t_{24} = g_8 \oplus g_5$	15	$g_{13} = AND(r_{26}, r_{27})$	20	$t_{67} = t_{57} \oplus t_{59}$
2	$r_{35} = t_{16}$	6	$t_{27} = t_0 \oplus t_{23}$	15	$g_{14} = AND(r_{28}, r_{29})$	20	$t_{69} = g_{15} \oplus t_{61}$
2	$r_{37} = t_6$	6	$t_{30} = g_2 \oplus g_1$	15	$g_{23} = AND(r_{46}, r_{47})$	20	$t_{71} = g_{21} \oplus t_{62}$
2	$r_{47} = t_3$	6	$t_{36} = g_1 \oplus t_{34}$	15	$t_{47} = t_{45} \oplus t_{46}$	20	$t_{73} = t_{54} \oplus t_{72}$
3	$g_3 = AND(r_6, r_7)$	7	$t_{25} = x_7 \oplus t_{24}$	15	$t_{52} = t_{43} \oplus t_{45}$	20	$t_{78} = t_{58} \oplus t_{77}$
3	$t_7 = x_4 \oplus t_6$	7	$t_{28} = t_{22} \oplus t_{27}$	15	$r_{30} = t_{47}$	20	$t_{82} = g_{29} \oplus t_{62}$
3	$t_9 = x_1 \oplus t_6$	7	$t_{32} = t_{20} \oplus t_{30}$	15	$r_{48} = t_{47}$	20	$t_{84} = t_{58} \oplus t_{62}$
3	$t_{10} = x_7 \oplus t_6$	7	$t_{37} = t_{35} \oplus t_{36}$	16	$g_{15} = AND(r_{30}, r_{31})$	20	$t_{88} = t_{54} \oplus t_{87}$
3	$t_{12} = t_3 \oplus t_{11}$	7	$r_{19} = t_{28}$	16	$g_{24} = AND(r_{48}, r_{49})$	21	$t_{64} = t_{56} \oplus t_{63}$
3	$t_{17} = t_6 \oplus t_{16}$	8	$t_{26} = t_{22} \oplus t_{25}$	16	$t_{48} = t_{33} \oplus g_{13}$	21	$t_{66} = t_{56} \oplus t_{65}$
3	$t_{18} = t_5 \oplus t_{16}$	8	$t_{29} = t_{25} \oplus t_{27}$	16	$t_{75} = g_{14} \oplus g_{16}$	21	$t_{68} = t_{56} \oplus t_{67} \oplus 1$
3	$t_{19} = t_3 \oplus t_{15}$	8	$t_{33} = t_{31} \oplus t_{32}$	16	$r_{36} = t_{48}$	21	$t_{70} = t_{56} \oplus t_{69}$
3	$r_1 = t_{12}$	8	$t_{38} = g_0 \oplus t_{37}$	16	$r_{54} = t_{48}$	21	$t_{74} = t_{71} \oplus t_{73} \oplus 1$
3	$r_4 = t_7$	8	$r_{18} = t_{38}$	17	$g_{18} = AND(r_{36}, r_{37})$	21	$t_{79} = t_{73} \oplus t_{78} \oplus 1$
3	$r_8 = t_9$	8	$r_{20} = t_{33}$	17	$g_{27} = AND(r_{54}, r_{55})$	21	$t_{83} = t_{81} \oplus t_{82} \oplus 1$
3	$r_{10} = t_{10}$	8	$r_{23} = t_{29}$	17	$t_{49} = t_{43} \oplus t_{48}$	21	$t_{89} = t_{84} \oplus t_{88}$
3	$r_{11} = t_{17}$	8	$r_{24} = t_{26}$	17	$t_{51} = t_{47} \oplus t_{48}$	21	$\boldsymbol{y_0 = t_{79}}$
3	$r_{13} = t_{18}$	9	$g_9 = AND(r_{18}, r_{19})$	17	$t_{53} = t_{48} \oplus t_{52}$	21	$\boldsymbol{y_1 = t_{74}}$
3	$r_{15} = t_{19}$	9	$t_{40} = t_{33} \oplus t_{38}$	17	$t_{55} = g_{23} \oplus g_{24}$	21	$\boldsymbol{y_2 = t_{89}}$
3	$r_{29} = t_{12}$	10	$t_{39} = t_{26} \oplus g_9$	17	$t_{57} = g_{14} \oplus g_{15}$	21	$\boldsymbol{y_3 = t_{70}}$
3	$r_{39} = t_{17}$	10	$t_{41} = g_9 \oplus t_{40}$	17	$t_{76} = g_{28} \oplus t_{75}$	21	$\boldsymbol{y_4 = t_{64}}$
3	$r_{41} = t_{18}$	10	$r_{21} = t_{39}$	17	$t_{85} = g_{25} \oplus g_{24}$	21	$\boldsymbol{y_5 = t_{83}}$
3	$r_{43} = t_{19}$	10	$r_{22} = t_{41}$	17	$r_{34} = t_{49}$	21	$\boldsymbol{y_6 = t_{68}}$
3	$r_{51} = t_7$	11	$g_{10} = AND(r_{20}, r_{21})$	17	$r_{42} = t_{53}$	21	$\boldsymbol{y_7 = t_{66}}$
3	$r_{55} = t_9$	11	$g_{11} = AND(r_{22}, r_{23})$	17	$r_{44} = t_{51}$		
3	$r_{57} = t_{10}$	12	$t_{42} = g_9 \oplus g_{11}$	17	$r_{52} = t_{49}$		

Listing 9: New `AES` S-box circuit (D: 20, AD: 6, #NL: 32, #L: 92, #(gate): 124)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	4	$r_3 = t_7$	12	$t_{45} = t_{31} \oplus g_{11}$	16	$r_{54} = t_{46}$
0	$r_{33} = x_0$	4	$r_7 = t_{16}$	12	$t_{48} = t_{34} \oplus g_{10}$	16	$r_{60} = t_{51}$
1	$t_0 = x_1 \oplus x_7$	4	$r_{13} = t_{18}$	12	$t_{52} = t_{30} \oplus g_{11}$	16	$r_{62} = t_{58}$
1	$t_1 = x_4 \oplus x_7$	4	$r_{17} = t_{14}$	12	$r_{25} = t_{41}$	17	$g_{17} = AND(r_{34}, r_{35})$
1	$t_2 = x_2 \oplus x_4$	4	$r_{31} = t_7$	12	$r_{26} = t_{42}$	17	$g_{18} = AND(r_{36}, r_{37})$
1	$t_4 = x_2 \oplus x_7$	4	$r_{35} = t_{16}$	12	$r_{32} = t_{45}$	17	$g_{21} = AND(r_{42}, r_{43})$
1	$t_8 = x_5 \oplus x_6$	4	$r_{41} = t_{18}$	12	$r_{38} = t_{42}$	17	$g_{22} = AND(r_{44}, r_{45})$
1	$t_{19} = x_4 \oplus x_5$	4	$r_{45} = t_{14}$	12	$r_{50} = t_{45}$	17	$g_{26} = AND(r_{52}, r_{53})$
1	$r_6 = t_0$	4	$r_{49} = t_{11}$	12	$r_{56} = t_{42}$	17	$g_{27} = AND(r_{54}, r_{55})$
1	$r_{12} = t_1$	5	$g_1 = AND(r_2, r_3)$	13	$g_{12} = AND(r_{24}, r_{25})$	17	$g_{30} = AND(r_{60}, r_{61})$
1	$r_{14} = t_2$	5	$g_3 = AND(r_6, r_7)$	13	$g_{16} = AND(r_{32}, r_{33})$	17	$g_{31} = AND(r_{62}, r_{63})$
1	$r_{16} = t_4$	5	$g_6 = AND(r_{12}, r_{13})$	13	$g_{19} = AND(r_{38}, r_{39})$	17	$t_{81} = g_{29} \oplus t_{65}$
1	$r_{53} = t_0$	5	$g_8 = AND(r_{16}, r_{17})$	13	$g_{25} = AND(r_{50}, r_{51})$	18	$t_{54} = g_{29} \oplus g_{30}$
1	$r_{59} = t_1$	5	$t_{17} = t_9 \oplus t_{16}$	13	$g_{28} = AND(r_{56}, r_{57})$	18	$t_{59} = g_{20} \oplus g_{21}$
1	$r_{61} = t_2$	5	$t_{21} = g_4 \oplus g_7$	13	$t_{47} = t_{42} \oplus t_{45}$	18	$t_{61} = g_{18} \oplus g_{17}$
1	$r_{63} = t_4$	5	$t_{32} = g_0 \oplus t_8$	13	$r_{40} = t_{47}$	18	$t_{62} = g_{19} \oplus g_{18}$
2	$t_3 = t_0 \oplus t_2$	5	$r_{11} = t_{17}$	13	$r_{58} = t_{47}$	18	$t_{63} = g_{27} \oplus g_{26}$
2	$t_5 = x_3 \oplus t_1$	5	$r_{39} = t_{17}$	14	$g_{20} = AND(r_{40}, r_{41})$	18	$t_{72} = g_{17} \oplus t_{65}$
2	$t_9 = x_0 \oplus t_8$	6	$g_5 = AND(r_{10}, r_{11})$	14	$g_{29} = AND(r_{58}, r_{59})$	18	$t_{78} = g_{21} \oplus g_{22}$
2	$t_{20} = t_4 \oplus t_{19}$	6	$t_{23} = t_{16} \oplus g_6$	14	$t_{43} = t_{35} \oplus g_{12}$	18	$t_{82} = g_{26} \oplus t_{81}$
2	$r_0 = t_3$	6	$t_{25} = g_1 \oplus g_7$	14	$t_{44} = t_{28} \oplus g_{12}$	18	$t_{84} = g_{28} \oplus g_{31}$
2	$r_9 = t_9$	6	$t_{27} = t_0 \oplus t_{21}$	14	$t_{53} = g_{12} \oplus t_{52}$	18	$t_{89} = g_{30} \oplus t_{88}$
2	$r_{15} = t_{20}$	6	$t_{36} = g_2 \oplus g_8$	14	$t_{87} = g_{28} \oplus g_{25}$	19	$t_{56} = t_{54} \oplus t_{55}$
2	$r_{37} = t_9$	7	$t_{22} = g_8 \oplus g_5$	14	$r_{27} = t_{43}$	19	$t_{64} = t_{54} \oplus t_{63}$
2	$r_{43} = t_{20}$	7	$t_{24} = g_3 \oplus t_{23}$	14	$r_{28} = t_{44}$	19	$t_{66} = t_{59} \oplus t_{61}$
2	$r_{47} = t_3$	7	$t_{26} = t_1 \oplus t_{25}$	14	$r_{30} = t_{53}$	19	$t_{68} = t_{60} \oplus t_{61}$
3	$g_7 = AND(r_{14}, r_{15})$	7	$t_{33} = t_{23} \oplus t_{32}$	14	$r_{46} = t_{44}$	19	$t_{70} = t_{59} \oplus t_{60}$
3	$t_6 = x_1 \oplus t_5$	7	$t_{37} = t_{19} \oplus t_{36}$	14	$r_{48} = t_{53}$	19	$t_{73} = g_{19} \oplus t_{72}$
3	$t_{10} = x_4 \oplus t_9$	8	$t_{28} = t_{24} \oplus t_{27}$	15	$g_{13} = AND(r_{26}, r_{27})$	19	$t_{76} = t_{62} \oplus t_{75}$
3	$t_{12} = x_1 \oplus t_9$	8	$t_{29} = x_7 \oplus t_{22}$	15	$g_{14} = AND(r_{28}, r_{29})$	19	$t_{79} = t_{62} \oplus t_{78}$
3	$t_{13} = x_7 \oplus t_9$	8	$t_{34} = t_{26} \oplus t_{33}$	15	$g_{15} = AND(r_{30}, r_{31})$	19	$t_{83} = t_{78} \oplus t_{82}$
3	$t_{15} = t_3 \oplus t_5$	8	$t_{38} = t_{26} \oplus t_{37}$	15	$g_{23} = AND(r_{46}, r_{47})$	19	$t_{85} = t_{59} \oplus t_{84}$
3	$r_1 = t_6$	8	$t_{39} = t_{33} \oplus t_{37}$	15	$g_{24} = AND(r_{48}, r_{49})$	19	$t_{90} = t_{61} \oplus t_{89}$
3	$r_4 = t_{10}$	8	$r_{18} = t_{34}$	15	$t_{50} = t_{44} \oplus t_{48}$	20	$t_{67} = t_{56} \oplus t_{66}$
3	$r_8 = t_{12}$	8	$r_{19} = t_{28}$	15	$t_{57} = t_{38} \oplus t_{53}$	20	$t_{69} = t_{56} \oplus t_{68}$
3	$r_{10} = t_{13}$	8	$r_{20} = t_{38}$	16	$t_{46} = t_{38} \oplus g_{13}$	20	$t_{71} = t_{56} \oplus t_{70} \oplus 1$
3	$r_{29} = t_6$	9	$g_9 = AND(r_{18}, r_{19})$	16	$t_{49} = g_{13} \oplus t_{48}$	20	$t_{74} = t_{64} \oplus t_{73} \oplus 1$
3	$r_{51} = t_{10}$	9	$t_{30} = t_{27} \oplus t_{29}$	16	$t_{51} = g_{13} \oplus t_{50}$	20	$t_{77} = t_{56} \oplus t_{76}$
3	$r_{55} = t_{12}$	9	$t_{31} = t_{24} \oplus t_{29}$	16	$t_{55} = g_{23} \oplus g_{24}$	20	$t_{80} = t_{64} \oplus t_{79} \oplus 1$
3	$r_{57} = t_{13}$	9	$r_{23} = t_{30}$	16	$t_{58} = g_{13} \oplus t_{57}$	20	$t_{86} = t_{83} \oplus t_{85} \oplus 1$
4	$g_0 = AND(r_0, r_1)$	9	$r_{24} = t_{31}$	16	$t_{60} = g_{14} \oplus g_{15}$	20	$t_{91} = t_{83} \oplus t_{90}$
4	$g_2 = AND(r_4, r_5)$	10	$t_{35} = t_{31} \oplus g_9$	16	$t_{65} = g_{14} \oplus g_{16}$	20	$\boldsymbol{y_0 = t_{74}}$
4	$g_4 = AND(r_8, r_9)$	10	$t_{40} = g_9 \oplus t_{39}$	16	$t_{75} = g_{16} \oplus g_{15}$	20	$\boldsymbol{y_1 = t_{80}}$
4	$t_7 = x_0 \oplus t_6$	10	$r_{21} = t_{35}$	16	$t_{88} = g_{24} \oplus t_{87}$	20	$\boldsymbol{y_2 = t_{91}}$
4	$t_{11} = t_3 \oplus t_{10}$	10	$r_{22} = t_{40}$	16	$r_{34} = t_{49}$	20	$\boldsymbol{y_3 = t_{77}}$
4	$t_{14} = t_6 \oplus t_8$	11	$g_{10} = AND(r_{20}, r_{21})$	16	$r_{36} = t_{46}$	20	$\boldsymbol{y_4 = t_{69}}$
4	$t_{16} = x_5 \oplus t_{15}$	11	$g_{11} = AND(r_{22}, r_{23})$	16	$r_{42} = t_{51}$	20	$\boldsymbol{y_5 = t_{86}}$
4	$t_{18} = x_6 \oplus t_{15}$	12	$t_{41} = g_9 \oplus g_{11}$	16	$r_{44} = t_{58}$	20	$\boldsymbol{y_6 = t_{71}}$
4	$r_2 = t_{11}$	12	$t_{42} = g_{10} \oplus t_{39}$	16	$r_{52} = t_{49}$	20	$\boldsymbol{y_7 = t_{67}}$

Listing 10: New `AES` S-box circuit (D: 18, AD: 6, #NL: 32, #L: 93, #(gate): 125)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$t_{21} = t_4 \oplus t_{20}$	10	$r_{25} = t_{42}$	14	$r_{62} = t_{59}$
0	$r_{33} = x_0$	3	$r_2 = t_{21}$	10	$r_{32} = t_{46}$	15	$g_{17} = AND(r_{34}, r_{35})$
1	$t_0 = x_1 \oplus x_7$	3	$r_3 = t_{11}$	10	$r_{50} = t_{46}$	15	$g_{18} = AND(r_{36}, r_{37})$
1	$t_1 = x_4 \oplus x_7$	3	$r_4 = t_7$	11	$g_{12} = AND(r_{24}, r_{25})$	15	$g_{21} = AND(r_{42}, r_{43})$
1	$t_2 = x_2 \oplus x_4$	3	$r_{10} = t_8$	11	$g_{16} = AND(r_{32}, r_{33})$	15	$g_{22} = AND(r_{44}, r_{45})$
1	$t_4 = x_2 \oplus x_7$	3	$r_{11} = t_{15}$	11	$g_{25} = AND(r_{50}, r_{51})$	15	$g_{26} = AND(r_{52}, r_{53})$
1	$t_5 = x_5 \oplus x_6$	3	$r_{17} = t_{12}$	11	$t_{43} = g_{10} \oplus t_{40}$	15	$g_{27} = AND(r_{54}, r_{55})$
1	$t_9 = x_1 \oplus x_3$	3	$r_{31} = t_{11}$	11	$t_{49} = t_{38} \oplus g_{10}$	15	$g_{30} = AND(r_{60}, r_{61})$
1	$t_{13} = x_2 \oplus x_5$	3	$r_{39} = t_{15}$	11	$r_{26} = t_{43}$	15	$g_{31} = AND(r_{62}, r_{63})$
1	$t_{17} = x_2 \oplus x_6$	3	$r_{45} = t_{12}$	11	$r_{38} = t_{43}$	15	$t_{79} = g_{19} \oplus t_{66}$
1	$t_{19} = x_0 \oplus x_1$	3	$r_{49} = t_{21}$	11	$r_{56} = t_{43}$	15	$t_{89} = t_{66} \oplus t_{88}$
1	$r_6 = t_0$	3	$r_{51} = t_7$	12	$g_{19} = AND(r_{38}, r_{39})$	16	$t_{55} = g_{29} \oplus g_{30}$
1	$r_{12} = t_1$	3	$r_{57} = t_8$	12	$g_{28} = AND(r_{56}, r_{57})$	16	$t_{60} = g_{20} \oplus g_{21}$
1	$r_{14} = t_2$	4	$g_1 = AND(r_2, r_3)$	12	$t_{44} = t_{39} \oplus g_{12}$	16	$t_{61} = g_{18} \oplus g_{17}$
1	$r_{16} = t_4$	4	$g_2 = AND(r_4, r_5)$	12	$t_{45} = t_{31} \oplus g_{12}$	16	$t_{63} = g_{19} \oplus g_{18}$
1	$r_{53} = t_0$	4	$g_5 = AND(r_{10}, r_{11})$	12	$t_{48} = t_{43} \oplus t_{46}$	16	$t_{64} = g_{27} \oplus g_{26}$
1	$r_{59} = t_1$	4	$g_8 = AND(r_{16}, r_{17})$	12	$t_{54} = g_{12} \oplus t_{53}$	16	$t_{76} = g_{21} \oplus g_{22}$
1	$r_{61} = t_2$	4	$t_{23} = g_7 \oplus g_4$	12	$r_{27} = t_{44}$	16	$t_{80} = g_{17} \oplus t_{79}$
1	$r_{63} = t_4$	4	$t_{24} = g_3 \oplus g_6$	12	$r_{28} = t_{45}$	16	$t_{83} = g_{26} \oplus t_{82}$
2	$t_3 = t_0 \oplus t_2$	4	$t_{26} = t_{13} \oplus g_7$	12	$r_{30} = t_{54}$	16	$t_{85} = g_{31} \oplus t_{66}$
2	$t_6 = x_0 \oplus t_5$	4	$t_{36} = g_0 \oplus t_{12}$	12	$r_{40} = t_{48}$	16	$t_{90} = g_{30} \oplus t_{89}$
2	$t_{10} = t_1 \oplus t_9$	5	$t_{22} = g_8 \oplus g_5$	12	$r_{46} = t_{45}$	17	$t_{57} = t_{55} \oplus t_{56}$
2	$t_{14} = t_9 \oplus t_{13}$	5	$t_{25} = t_{14} \oplus t_{24}$	12	$r_{48} = t_{54}$	17	$t_{65} = t_{55} \oplus t_{64}$
2	$t_{16} = t_1 \oplus t_{13}$	5	$t_{27} = g_1 \oplus t_{26}$	12	$r_{58} = t_{48}$	17	$t_{67} = t_{60} \oplus t_{62}$
2	$t_{18} = t_9 \oplus t_{17}$	5	$t_{30} = t_0 \oplus t_{23}$	13	$g_{13} = AND(r_{26}, r_{27})$	17	$t_{69} = t_{61} \oplus t_{62}$
2	$t_{20} = t_5 \oplus t_{19}$	5	$t_{33} = t_4 \oplus g_8$	13	$g_{14} = AND(r_{28}, r_{29})$	17	$t_{71} = t_{60} \oplus t_{61}$
2	$r_0 = t_3$	5	$t_{37} = g_6 \oplus t_{36}$	13	$g_{15} = AND(r_{30}, r_{31})$	17	$t_{74} = t_{63} \oplus t_{73}$
2	$r_1 = t_{10}$	6	$t_{28} = t_{22} \oplus t_{23}$	13	$g_{20} = AND(r_{40}, r_{41})$	17	$t_{77} = t_{63} \oplus t_{76}$
2	$r_7 = t_{14}$	6	$t_{31} = t_{25} \oplus t_{30}$	13	$g_{23} = AND(r_{46}, r_{47})$	17	$t_{84} = t_{76} \oplus t_{83}$
2	$r_8 = t_{20}$	6	$t_{34} = g_2 \oplus t_{33}$	13	$g_{24} = AND(r_{48}, r_{49})$	17	$t_{86} = t_{60} \oplus t_{85}$
2	$r_9 = t_6$	6	$t_{38} = t_{27} \oplus t_{37}$	13	$g_{29} = AND(r_{58}, r_{59})$	17	$t_{91} = t_{61} \oplus t_{90}$
2	$r_{13} = t_{18}$	6	$r_{18} = t_{38}$	13	$t_{51} = t_{45} \oplus t_{49}$	18	$t_{68} = t_{57} \oplus t_{67} \oplus 1$
2	$r_{15} = t_{16}$	6	$r_{19} = t_{31}$	13	$t_{58} = t_{35} \oplus t_{54}$	18	$t_{70} = t_{57} \oplus t_{69}$
2	$r_{29} = t_{10}$	7	$g_9 = AND(r_{18}, r_{19})$	14	$t_{47} = t_{35} \oplus g_{13}$	18	$t_{72} = t_{57} \oplus t_{71}$
2	$r_{35} = t_{14}$	7	$t_{29} = x_1 \oplus t_{28}$	14	$t_{50} = g_{13} \oplus t_{49}$	18	$t_{75} = t_{57} \oplus t_{74}$
2	$r_{37} = t_6$	7	$t_{35} = t_{27} \oplus t_{34}$	14	$t_{52} = g_{13} \oplus t_{51}$	18	$t_{78} = t_{65} \oplus t_{77} \oplus 1$
2	$r_{41} = t_{18}$	7	$t_{40} = t_{34} \oplus t_{37}$	14	$t_{56} = g_{23} \oplus g_{24}$	18	$t_{81} = t_{65} \oplus t_{80} \oplus 1$
2	$r_{43} = t_{16}$	7	$r_{20} = t_{35}$	14	$t_{59} = g_{13} \oplus t_{58}$	18	$t_{87} = t_{84} \oplus t_{86} \oplus 1$
2	$r_{47} = t_3$	7	$r_{23} = t_{29}$	14	$t_{62} = g_{14} \oplus g_{15}$	18	$t_{92} = t_{84} \oplus t_{91}$
2	$r_{55} = t_{20}$	8	$t_{32} = t_{29} \oplus t_{31}$	14	$t_{66} = g_{14} \oplus g_{16}$	18	$\boldsymbol{y_0 = t_{81}}$
3	$g_0 = AND(r_0, r_1)$	8	$t_{41} = g_9 \oplus t_{40}$	14	$t_{73} = g_{16} \oplus g_{15}$	18	$\boldsymbol{y_1 = t_{78}}$
3	$g_3 = AND(r_6, r_7)$	8	$r_{22} = t_{41}$	14	$t_{82} = g_{28} \oplus g_{29}$	18	$\boldsymbol{y_2 = t_{92}}$
3	$g_4 = AND(r_8, r_9)$	8	$r_{24} = t_{32}$	14	$t_{88} = g_{25} \oplus g_{24}$	18	$\boldsymbol{y_3 = t_{75}}$
3	$g_6 = AND(r_{12}, r_{13})$	9	$g_{11} = AND(r_{22}, r_{23})$	14	$r_{34} = t_{50}$	18	$\boldsymbol{y_4 = t_{70}}$
3	$g_7 = AND(r_{14}, r_{15})$	9	$t_{39} = t_{32} \oplus g_9$	14	$r_{36} = t_{47}$	18	$\boldsymbol{y_5 = t_{87}}$
3	$t_7 = x_4 \oplus t_6$	9	$r_{21} = t_{39}$	14	$r_{42} = t_{52}$	18	$\boldsymbol{y_6 = t_{68}}$
3	$t_8 = x_7 \oplus t_6$	10	$g_{10} = AND(r_{20}, r_{21})$	14	$r_{44} = t_{59}$	18	$\boldsymbol{y_7 = t_{72}}$
3	$t_{11} = x_0 \oplus t_{10}$	10	$t_{42} = g_9 \oplus g_{11}$	14	$r_{52} = t_{50}$		
3	$t_{12} = t_5 \oplus t_{10}$	10	$t_{46} = t_{32} \oplus g_{11}$	14	$r_{54} = t_{47}$		
3	$t_{15} = t_6 \oplus t_{14}$	10	$t_{53} = t_{29} \oplus g_{11}$	14	$r_{60} = t_{52}$		

Listing 11: New AES S-box circuit (D: 24, AD: 5, #NL: 32, #L: 81, #(gate): 113)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{13} = t_{18}$	11	$g_{10} = AND(r_{20}, r_{21})$	16	$g_{30} = AND(r_{60}, r_{61})$
0	$r_{33} = x_0$	3	$r_{17} = t_{14}$	11	$g_{12} = AND(r_{24}, r_{25})$	16	$t_{50} = t_{44} \oplus t_{47}$
1	$t_0 = x_1 \oplus x_7$	3	$r_{31} = t_7$	12	$t_{40} = g_9 \oplus g_{10}$	16	$t_{69} = g_{14} \oplus g_{20}$
1	$t_1 = x_4 \oplus x_7$	3	$r_{39} = t_{17}$	12	$t_{41} = g_9 \oplus g_{12}$	16	$r_{44} = t_{50}$
1	$t_2 = x_2 \oplus x_4$	3	$r_{41} = t_{18}$	12	$t_{43} = g_{12} \oplus t_{38}$	16	$r_{62} = t_{50}$
1	$t_4 = x_2 \oplus x_7$	3	$r_{45} = t_{14}$	12	$t_{46} = t_{28} \oplus g_{10}$	17	$g_{22} = AND(r_{44}, r_{45})$
1	$t_5 = x_1 \oplus x_3$	3	$r_{51} = t_{10}$	12	$r_{23} = t_{40}$	17	$g_{31} = AND(r_{62}, r_{63})$
1	$t_8 = x_5 \oplus x_6$	3	$r_{55} = t_{12}$	12	$r_{27} = t_{41}$	17	$t_{51} = g_{29} \oplus g_{30}$
1	$t_{15} = x_2 \oplus x_5$	3	$r_{57} = t_{13}$	12	$r_{32} = t_{43}$	17	$t_{52} = g_{23} \oplus g_{24}$
1	$r_6 = t_0$	4	$g_2 = AND(r_4, r_5)$	12	$r_{38} = t_{46}$	17	$t_{58} = g_{20} \oplus g_{21}$
1	$r_{12} = t_1$	4	$g_4 = AND(r_8, r_9)$	12	$r_{50} = t_{43}$	18	$t_{53} = t_{51} \oplus t_{52}$
1	$r_{14} = t_2$	4	$g_5 = AND(r_{10}, r_{11})$	12	$r_{56} = t_{46}$	18	$t_{61} = g_{26} \oplus t_{51}$
1	$r_{16} = t_4$	4	$g_6 = AND(r_{12}, r_{13})$	13	$g_{11} = AND(r_{22}, r_{23})$	18	$t_{65} = g_{16} \oplus g_{22}$
1	$r_{53} = t_0$	4	$g_8 = AND(r_{16}, r_{17})$	13	$g_{13} = AND(r_{26}, r_{27})$	18	$t_{73} = g_{15} \oplus t_{58}$
1	$r_{59} = t_1$	4	$t_{11} = t_3 \oplus t_{10}$	13	$g_{16} = AND(r_{32}, r_{33})$	19	$t_{54} = g_{15} \oplus t_{53}$
1	$r_{61} = t_2$	4	$t_{29} = t_{15} \oplus g_7$	13	$g_{19} = AND(r_{38}, r_{39})$	19	$t_{62} = g_{27} \oplus t_{61}$
1	$r_{63} = t_4$	4	$r_2 = t_{11}$	13	$g_{25} = AND(r_{50}, r_{51})$	19	$t_{71} = g_{28} \oplus t_{61}$
2	$t_3 = t_0 \oplus t_2$	4	$r_{49} = t_{11}$	13	$g_{28} = AND(r_{56}, r_{57})$	20	$t_{55} = g_{18} \oplus t_{54}$
2	$t_6 = t_1 \oplus t_5$	5	$g_1 = AND(r_2, r_3)$	13	$t_{48} = t_{43} \oplus t_{46}$	20	$t_{66} = g_{21} \oplus t_{54}$
2	$t_9 = x_0 \oplus t_8$	5	$t_{20} = g_4 \oplus g_7$	13	$r_{40} = t_{48}$	21	$t_{56} = g_{17} \oplus t_{55}$
2	$t_{16} = t_5 \oplus t_{15}$	5	$t_{21} = g_8 \oplus g_5$	13	$r_{58} = t_{48}$	21	$t_{59} = g_{19} \oplus t_{55}$
2	$t_{19} = t_1 \oplus t_{15}$	5	$t_{22} = t_{16} \oplus g_6$	14	$g_{20} = AND(r_{40}, r_{41})$	21	$t_{67} = t_{65} \oplus t_{66}$
2	$r_0 = t_3$	5	$t_{24} = t_4 \oplus g_2$	14	$g_{29} = AND(r_{58}, r_{59})$	21	$t_{70} = t_{66} \oplus t_{69} \oplus 1$
2	$r_1 = t_6$	5	$t_{26} = t_{14} \oplus g_6$	14	$t_{42} = t_{34} \oplus g_{13}$	21	$\boldsymbol{y_6 = t_{70}}$
2	$r_7 = t_{16}$	6	$t_{23} = g_3 \oplus t_{22}$	14	$t_{45} = t_{31} \oplus g_{11}$	22	$t_{57} = g_{14} \oplus t_{56}$
2	$r_9 = t_9$	6	$t_{25} = g_8 \oplus t_{24}$	14	$r_{28} = t_{42}$	22	$t_{60} = g_{16} \oplus t_{59}$
2	$r_{15} = t_{19}$	6	$t_{27} = g_0 \oplus t_{26}$	14	$r_{34} = t_{45}$	22	$t_{72} = t_{67} \oplus t_{71}$
2	$r_{29} = t_6$	6	$t_{30} = g_1 \oplus t_{29}$	14	$r_{46} = t_{42}$	22	$t_{74} = t_{56} \oplus t_{73}$
2	$r_{35} = t_{16}$	6	$t_{36} = x_1 \oplus t_{21}$	14	$r_{52} = t_{45}$	22	$t_{75} = g_{31} \oplus t_{70} \oplus 1$
2	$r_{37} = t_9$	7	$t_{28} = t_{25} \oplus t_{27}$	15	$g_{14} = AND(r_{28}, r_{29})$	22	$\boldsymbol{y_3 = t_{60}}$
2	$r_{43} = t_{19}$	7	$t_{31} = t_{27} \oplus t_{30}$	15	$g_{17} = AND(r_{34}, r_{35})$	22	$\boldsymbol{y_4 = t_{57}}$
2	$r_{47} = t_3$	7	$t_{32} = t_{25} \oplus t_{30}$	15	$g_{23} = AND(r_{46}, r_{47})$	22	$\boldsymbol{y_7 = t_{74}}$
3	$g_0 = AND(r_0, r_1)$	7	$t_{33} = t_0 \oplus t_{23}$	15	$g_{26} = AND(r_{52}, r_{53})$	23	$t_{63} = t_{60} \oplus t_{62}$
3	$g_3 = AND(r_6, r_7)$	7	$t_{37} = t_{20} \oplus t_{36}$	15	$t_{44} = t_{42} \oplus t_{43}$	23	$t_{76} = g_{30} \oplus t_{75}$
3	$g_7 = AND(r_{14}, r_{15})$	7	$r_{18} = t_{31}$	15	$t_{47} = t_{45} \oplus t_{46}$	23	$t_{78} = g_{25} \oplus t_{72}$
3	$t_7 = x_0 \oplus t_6$	7	$r_{20} = t_{32}$	15	$t_{49} = t_{42} \oplus t_{45}$	23	$t_{79} = g_{24} \oplus t_{57}$
3	$t_{10} = x_4 \oplus t_9$	7	$r_{22} = t_{28}$	15	$r_{30} = t_{44}$	24	$t_{64} = t_{57} \oplus t_{63} \oplus 1$
3	$t_{12} = x_1 \oplus t_9$	7	$r_{24} = t_{37}$	15	$r_{36} = t_{47}$	24	$t_{68} = t_{63} \oplus t_{67} \oplus 1$
3	$t_{13} = x_7 \oplus t_9$	8	$t_{34} = t_{20} \oplus t_{33}$	15	$r_{42} = t_{49}$	24	$t_{77} = t_{72} \oplus t_{76} \oplus 1$
3	$t_{14} = t_6 \oplus t_8$	8	$t_{38} = t_{33} \oplus t_{36}$	15	$r_{48} = t_{44}$	24	$t_{80} = t_{78} \oplus t_{79}$
3	$t_{17} = t_9 \oplus t_{16}$	8	$r_{19} = t_{34}$	15	$r_{54} = t_{47}$	24	$\boldsymbol{y_0 = t_{64}}$
3	$t_{18} = t_8 \oplus t_{16}$	8	$r_{26} = t_{38}$	15	$r_{60} = t_{49}$	24	$\boldsymbol{y_1 = t_{68}}$
3	$r_3 = t_7$	9	$g_9 = AND(r_{18}, r_{19})$	16	$g_{15} = AND(r_{30}, r_{31})$	24	$\boldsymbol{y_2 = t_{80}}$
3	$r_4 = t_{10}$	10	$t_{35} = t_{28} \oplus g_9$	16	$g_{18} = AND(r_{36}, r_{37})$	24	$\boldsymbol{y_5 = t_{77}}$
3	$r_8 = t_{12}$	10	$t_{39} = g_9 \oplus t_{38}$	16	$g_{21} = AND(r_{42}, r_{43})$		
3	$r_{10} = t_{13}$	10	$r_{21} = t_{39}$	16	$g_{24} = AND(r_{48}, r_{49})$		
3	$r_{11} = t_{17}$	10	$r_{25} = t_{35}$	16	$g_{27} = AND(r_{54}, r_{55})$		

Listing 12: New `AES` S-box circuit (D: 23, AD: 5, #NL: 32, #L: 83, #(gate): 115)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	4	$t_{13} = x_0 \oplus t_{12}$	12	$r_{25} = t_{41}$	18	$g_{27} = AND(r_{54}, r_{55})$
0	$r_{33} = x_0$	4	$t_{14} = t_5 \oplus t_{12}$	13	$g_{10} = AND(r_{20}, r_{21})$	18	$g_{30} = AND(r_{60}, r_{61})$
1	$t_0 = x_1 \oplus x_7$	4	$t_{17} = t_6 \oplus t_{16}$	13	$g_{12} = AND(r_{24}, r_{25})$	18	$t_{51} = t_{45} \oplus t_{48}$
1	$t_1 = x_4 \oplus x_7$	4	$t_{19} = t_{12} \oplus t_{16}$	14	$t_{40} = g_9 \oplus g_{10}$	18	$r_{44} = t_{51}$
1	$t_2 = x_2 \oplus x_4$	4	$r_2 = t_8$	14	$t_{42} = g_9 \oplus g_{12}$	18	$r_{62} = t_{51}$
1	$t_4 = x_2 \oplus x_7$	4	$r_3 = t_{13}$	14	$t_{44} = t_{28} \oplus g_{12}$	19	$g_{22} = AND(r_{44}, r_{45})$
1	$t_5 = x_5 \oplus x_6$	4	$r_{11} = t_{17}$	14	$t_{47} = t_{37} \oplus g_{10}$	19	$g_{31} = AND(r_{62}, r_{63})$
1	$t_{11} = x_2 \oplus x_3$	4	$r_{15} = t_{19}$	14	$r_{23} = t_{40}$	19	$t_{52} = g_{29} \oplus g_{30}$
1	$r_6 = t_0$	4	$r_{17} = t_{14}$	14	$r_{27} = t_{42}$	19	$t_{56} = g_{20} \oplus g_{21}$
1	$r_{12} = t_1$	4	$r_{31} = t_{13}$	14	$r_{32} = t_{44}$	19	$t_{57} = g_{17} \oplus g_{18}$
1	$r_{14} = t_2$	4	$r_{39} = t_{17}$	14	$r_{38} = t_{47}$	19	$t_{58} = g_{19} \oplus g_{18}$
1	$r_{16} = t_4$	4	$r_{43} = t_{19}$	14	$r_{50} = t_{44}$	20	$t_{53} = g_{24} \oplus t_{52}$
1	$r_{53} = t_0$	4	$r_{45} = t_{14}$	14	$r_{56} = t_{47}$	20	$t_{59} = g_{16} \oplus t_{58}$
1	$r_{59} = t_1$	4	$r_{49} = t_8$	15	$g_{11} = AND(r_{22}, r_{23})$	20	$t_{61} = g_{14} \oplus t_{57}$
1	$r_{61} = t_2$	5	$g_1 = AND(r_2, r_3)$	15	$g_{13} = AND(r_{26}, r_{27})$	20	$t_{63} = g_{26} \oplus g_{22}$
1	$r_{63} = t_4$	5	$g_5 = AND(r_{10}, r_{11})$	15	$g_{16} = AND(r_{32}, r_{33})$	20	$t_{64} = g_{27} \oplus t_{52}$
2	$t_3 = t_0 \oplus t_2$	5	$g_7 = AND(r_{14}, r_{15})$	15	$g_{19} = AND(r_{38}, r_{39})$	20	$t_{66} = g_{14} \oplus t_{56}$
2	$t_6 = x_0 \oplus t_5$	5	$g_8 = AND(r_{16}, r_{17})$	15	$g_{25} = AND(r_{50}, r_{51})$	20	$t_{76} = g_{29} \oplus g_{31}$
2	$t_{15} = x_1 \oplus t_{11}$	5	$t_{22} = g_3 \oplus g_6$	15	$g_{28} = AND(r_{56}, r_{57})$	21	$t_{54} = g_{23} \oplus t_{53}$
2	$r_0 = t_3$	5	$t_{24} = g_0 \oplus g_6$	15	$t_{49} = t_{44} \oplus t_{47}$	21	$t_{65} = g_{21} \oplus t_{63}$
2	$r_9 = t_6$	6	$t_{20} = g_8 \oplus g_5$	15	$r_{40} = t_{49}$	21	$t_{69} = t_{59} \oplus t_{64}$
2	$r_{37} = t_6$	6	$t_{21} = g_4 \oplus g_7$	15	$r_{58} = t_{49}$	21	$t_{75} = g_{28} \oplus t_{66}$
2	$r_{47} = t_3$	6	$t_{23} = t_{16} \oplus t_{22}$	16	$g_{20} = AND(r_{40}, r_{41})$	21	$t_{79} = g_{28} \oplus t_{53}$
3	$t_7 = x_4 \oplus t_6$	6	$t_{25} = g_2 \oplus g_8$	16	$g_{29} = AND(r_{58}, r_{59})$	21	$t_{80} = g_{25} \oplus t_{61}$
3	$t_9 = x_1 \oplus t_6$	6	$t_{26} = g_1 \oplus g_7$	16	$t_{43} = t_{30} \oplus g_{13}$	22	$t_{55} = g_{15} \oplus t_{54}$
3	$t_{10} = x_7 \oplus t_6$	6	$t_{32} = t_{18} \oplus t_{24}$	16	$t_{46} = t_{38} \oplus g_{11}$	22	$t_{68} = g_{16} \oplus t_{65}$
3	$t_{12} = t_3 \oplus t_{11}$	7	$t_{27} = x_7 \oplus t_{23}$	16	$r_{28} = t_{43}$	22	$t_{71} = t_{54} \oplus t_{61}$
3	$t_{16} = x_5 \oplus t_{15}$	7	$t_{29} = x_1 \oplus t_{21}$	16	$r_{34} = t_{46}$	22	$t_{73} = t_{61} \oplus t_{69}$
3	$t_{18} = x_6 \oplus t_{15}$	7	$t_{33} = t_{19} \oplus t_{25}$	16	$r_{46} = t_{43}$	22	$t_{77} = t_{75} \oplus t_{76}$
3	$r_1 = t_{12}$	8	$t_{28} = t_{20} \oplus t_{27}$	16	$r_{52} = t_{46}$	22	$t_{81} = t_{79} \oplus t_{80}$
3	$r_4 = t_7$	8	$t_{30} = t_{27} \oplus t_{29}$	17	$g_{14} = AND(r_{28}, r_{29})$	23	$t_{60} = t_{55} \oplus t_{59}$
3	$r_7 = t_{16}$	8	$t_{31} = t_{20} \oplus t_{29}$	17	$g_{17} = AND(r_{34}, r_{35})$	23	$t_{62} = t_{55} \oplus t_{61}$
3	$r_8 = t_9$	8	$t_{34} = t_{26} \oplus t_{33}$	17	$g_{23} = AND(r_{46}, r_{47})$	23	$t_{67} = t_{55} \oplus t_{66} \oplus 1$
3	$r_{10} = t_{10}$	8	$t_{36} = t_{32} \oplus t_{33}$	17	$g_{26} = AND(r_{52}, r_{53})$	23	$t_{70} = t_{68} \oplus t_{69} \oplus 1$
3	$r_{13} = t_{18}$	8	$r_{19} = t_{30}$	17	$t_{45} = t_{43} \oplus t_{44}$	23	$t_{72} = t_{66} \oplus t_{71}$
3	$r_{29} = t_{12}$	8	$r_{24} = t_{31}$	17	$t_{48} = t_{46} \oplus t_{47}$	23	$t_{74} = g_{26} \oplus t_{73} \oplus 1$
3	$r_{35} = t_{16}$	8	$r_{26} = t_{28}$	17	$t_{50} = t_{43} \oplus t_{46}$	23	$t_{78} = t_{68} \oplus t_{77} \oplus 1$
3	$r_{41} = t_{18}$	9	$t_{35} = t_2 \oplus t_{34}$	17	$r_{30} = t_{45}$	23	$t_{82} = t_{68} \oplus t_{81}$
3	$r_{51} = t_7$	9	$t_{37} = t_4 \oplus t_{36}$	17	$r_{36} = t_{48}$	23	$\boldsymbol{y_0 = t_{74}}$
3	$r_{55} = t_9$	9	$r_{20} = t_{35}$	17	$r_{42} = t_{50}$	23	$\boldsymbol{y_1 = t_{70}}$
3	$r_{57} = t_{10}$	9	$r_{22} = t_{37}$	17	$r_{48} = t_{45}$	23	$\boldsymbol{y_2 = t_{82}}$
4	$g_0 = AND(r_0, r_1)$	10	$t_{38} = t_{35} \oplus t_{37}$	17	$r_{54} = t_{48}$	23	$\boldsymbol{y_3 = t_{60}}$
4	$g_2 = AND(r_4, r_5)$	10	$r_{18} = t_{38}$	17	$r_{60} = t_{50}$	23	$\boldsymbol{y_4 = t_{62}}$
4	$g_3 = AND(r_6, r_7)$	11	$g_9 = AND(r_{18}, r_{19})$	18	$g_{15} = AND(r_{30}, r_{31})$	23	$\boldsymbol{y_5 = t_{78}}$
4	$g_4 = AND(r_8, r_9)$	12	$t_{39} = t_{28} \oplus g_9$	18	$g_{18} = AND(r_{36}, r_{37})$	23	$\boldsymbol{y_6 = t_{67}}$
4	$g_6 = AND(r_{12}, r_{13})$	12	$t_{41} = t_{37} \oplus g_9$	18	$g_{21} = AND(r_{42}, r_{43})$	23	$\boldsymbol{y_7 = t_{72}}$
4	$t_8 = t_3 \oplus t_7$	12	$r_{21} = t_{39}$	18	$g_{24} = AND(r_{48}, r_{49})$		

Listing 13: New AES S-box circuit (D: 22, AD: 5, #NL: 32, #L: 84, #(gate): 116)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	4	$t_{11} = t_3 \oplus t_{10}$	10	$r_{25} = t_{41}$	16	$g_{24} = AND(r_{48}, r_{49})$
0	$r_{33} = x_0$	4	$t_{14} = t_6 \oplus t_8$	11	$g_{10} = AND(r_{20}, r_{21})$	16	$g_{27} = AND(r_{54}, r_{55})$
1	$t_0 = x_1 \oplus x_7$	4	$t_{17} = t_9 \oplus t_{16}$	11	$g_{12} = AND(r_{24}, r_{25})$	16	$g_{30} = AND(r_{60}, r_{61})$
1	$t_1 = x_4 \oplus x_7$	4	$t_{18} = t_8 \oplus t_{16}$	12	$t_{40} = g_9 \oplus g_{10}$	16	$t_{51} = t_{45} \oplus t_{48}$
1	$t_2 = x_2 \oplus x_4$	4	$r_2 = t_{11}$	12	$t_{42} = g_9 \oplus g_{12}$	16	$t_{69} = g_{14} \oplus g_{26}$
1	$t_4 = x_2 \oplus x_7$	4	$r_3 = t_7$	12	$t_{44} = t_{31} \oplus g_{12}$	16	$t_{81} = g_{23} \oplus g_{25}$
1	$t_8 = x_5 \oplus x_6$	4	$r_{11} = t_{17}$	12	$t_{47} = t_{35} \oplus g_{10}$	16	$r_{44} = t_{51}$
1	$r_6 = t_0$	4	$r_{13} = t_{18}$	12	$r_{23} = t_{40}$	16	$r_{62} = t_{51}$
1	$r_{12} = t_1$	4	$r_{17} = t_{14}$	12	$r_{27} = t_{42}$	17	$g_{22} = AND(r_{44}, r_{45})$
1	$r_{14} = t_2$	4	$r_{31} = t_7$	12	$r_{32} = t_{44}$	17	$g_{31} = AND(r_{62}, r_{63})$
1	$r_{16} = t_4$	4	$r_{39} = t_{17}$	12	$r_{38} = t_{47}$	17	$t_{52} = g_{29} \oplus g_{30}$
1	$r_{53} = t_0$	4	$r_{41} = t_{18}$	12	$r_{50} = t_{44}$	17	$t_{53} = g_{23} \oplus g_{24}$
1	$r_{59} = t_1$	4	$r_{45} = t_{14}$	12	$r_{56} = t_{47}$	17	$t_{59} = g_{20} \oplus g_{21}$
1	$r_{61} = t_2$	4	$r_{49} = t_{11}$	13	$g_{11} = AND(r_{22}, r_{23})$	18	$t_{54} = t_{52} \oplus t_{53}$
1	$r_{63} = t_4$	5	$g_1 = AND(r_2, r_3)$	13	$g_{13} = AND(r_{26}, r_{27})$	18	$t_{62} = g_{27} \oplus t_{52}$
2	$t_3 = t_0 \oplus t_2$	5	$g_5 = AND(r_{10}, r_{11})$	13	$g_{16} = AND(r_{32}, r_{33})$	18	$t_{64} = g_{17} \oplus t_{59}$
2	$t_5 = x_3 \oplus t_0$	5	$g_6 = AND(r_{12}, r_{13})$	13	$g_{19} = AND(r_{38}, r_{39})$	18	$t_{66} = g_{18} \oplus t_{59}$
2	$t_9 = x_0 \oplus t_8$	5	$g_8 = AND(r_{16}, r_{17})$	13	$g_{25} = AND(r_{50}, r_{51})$	18	$t_{68} = g_{20} \oplus g_{22}$
2	$t_{15} = x_5 \oplus t_4$	5	$t_{20} = g_4 \oplus g_7$	13	$g_{28} = AND(r_{56}, r_{57})$	18	$t_{73} = g_{29} \oplus g_{31}$
2	$r_0 = t_3$	5	$t_{22} = t_{16} \oplus g_3$	13	$t_{49} = t_{44} \oplus t_{47}$	19	$t_{55} = g_{18} \oplus t_{54}$
2	$r_9 = t_9$	6	$t_{21} = g_8 \oplus g_5$	13	$r_{40} = t_{49}$	19	$t_{63} = g_{26} \oplus t_{62}$
2	$r_{37} = t_9$	6	$t_{23} = g_6 \oplus t_{22}$	13	$r_{58} = t_{49}$	19	$t_{70} = t_{68} \oplus t_{69}$
2	$r_{47} = t_3$	6	$t_{24} = g_0 \oplus g_6$	14	$g_{20} = AND(r_{40}, r_{41})$	19	$t_{75} = g_{17} \oplus t_{62}$
3	$t_6 = x_4 \oplus t_5$	6	$t_{25} = g_1 \oplus g_7$	14	$g_{29} = AND(r_{58}, r_{59})$	19	$t_{78} = t_{66} \oplus t_{68}$
3	$t_{10} = x_4 \oplus t_9$	6	$t_{26} = g_2 \oplus g_8$	14	$t_{43} = t_{28} \oplus g_{13}$	20	$t_{56} = g_{15} \oplus t_{55}$
3	$t_{12} = x_1 \oplus t_9$	6	$t_{27} = t_0 \oplus t_{20}$	14	$t_{46} = t_{37} \oplus g_{11}$	20	$t_{65} = t_{55} \oplus t_{64}$
3	$t_{13} = x_7 \oplus t_9$	7	$t_{28} = t_{23} \oplus t_{27}$	14	$t_{60} = g_{16} \oplus g_{19}$	20	$t_{71} = g_{16} \oplus t_{70}$
3	$t_{16} = t_5 \oplus t_{15}$	7	$t_{29} = x_7 \oplus t_{21}$	14	$r_{28} = t_{43}$	20	$t_{76} = t_{69} \oplus t_{75}$
3	$t_{19} = x_4 \oplus t_{15}$	7	$t_{32} = t_{19} \oplus t_{26}$	14	$r_{34} = t_{46}$	20	$t_{79} = g_{19} \oplus t_{63}$
3	$r_1 = t_6$	7	$t_{33} = t_{18} \oplus t_{24}$	14	$r_{46} = t_{43}$	20	$\boldsymbol{y_7 = t_{65}}$
3	$r_4 = t_{10}$	7	$t_{36} = t_1 \oplus t_{25}$	14	$r_{52} = t_{46}$	21	$t_{57} = g_{14} \oplus t_{56}$
3	$r_7 = t_{16}$	7	$r_{19} = t_{28}$	15	$g_{14} = AND(r_{28}, r_{29})$	21	$t_{61} = t_{56} \oplus t_{60}$
3	$r_8 = t_{12}$	8	$t_{30} = t_{27} \oplus t_{29}$	15	$g_{17} = AND(r_{34}, r_{35})$	21	$t_{72} = g_{28} \oplus t_{71}$
3	$r_{10} = t_{13}$	8	$t_{31} = t_{23} \oplus t_{29}$	15	$g_{23} = AND(r_{46}, r_{47})$	21	$t_{77} = t_{60} \oplus t_{76} \oplus 1$
3	$r_{15} = t_{19}$	8	$t_{34} = t_{32} \oplus t_{33}$	15	$g_{26} = AND(r_{52}, r_{53})$	21	$t_{80} = t_{78} \oplus t_{79} \oplus 1$
3	$r_{29} = t_6$	8	$t_{37} = t_{33} \oplus t_{36}$	15	$t_{45} = t_{43} \oplus t_{44}$	21	$t_{82} = t_{65} \oplus t_{81}$
3	$r_{35} = t_{16}$	8	$r_{18} = t_{37}$	15	$t_{48} = t_{46} \oplus t_{47}$	21	$\boldsymbol{y_0 = t_{77}}$
3	$r_{43} = t_{19}$	8	$r_{24} = t_{30}$	15	$t_{50} = t_{43} \oplus t_{46}$	21	$\boldsymbol{y_1 = t_{80}}$
3	$r_{51} = t_{10}$	8	$r_{26} = t_{31}$	15	$r_{30} = t_{45}$	21	$\boldsymbol{y_3 = t_{61}}$
3	$r_{55} = t_{12}$	9	$g_9 = AND(r_{18}, r_{19})$	15	$r_{36} = t_{48}$	22	$t_{58} = g_{17} \oplus t_{57}$
3	$r_{57} = t_{13}$	9	$t_{35} = t_4 \oplus t_{34}$	15	$r_{42} = t_{50}$	22	$t_{67} = t_{57} \oplus t_{66} \oplus 1$
4	$g_0 = AND(r_0, r_1)$	9	$r_{22} = t_{35}$	15	$r_{48} = t_{45}$	22	$t_{74} = t_{72} \oplus t_{73} \oplus 1$
4	$g_2 = AND(r_4, r_5)$	10	$t_{38} = t_{35} \oplus t_{37}$	15	$r_{54} = t_{48}$	22	$t_{83} = t_{72} \oplus t_{82}$
4	$g_3 = AND(r_6, r_7)$	10	$t_{39} = t_{31} \oplus g_9$	15	$r_{60} = t_{50}$	22	$\boldsymbol{y_2 = t_{83}}$
4	$g_4 = AND(r_8, r_9)$	10	$t_{41} = t_{35} \oplus g_9$	16	$g_{15} = AND(r_{30}, r_{31})$	22	$\boldsymbol{y_4 = t_{58}}$
4	$g_7 = AND(r_{14}, r_{15})$	10	$r_{20} = t_{38}$	16	$g_{18} = AND(r_{36}, r_{37})$	22	$\boldsymbol{y_5 = t_{74}}$
4	$t_7 = x_0 \oplus t_6$	10	$r_{21} = t_{39}$	16	$g_{21} = AND(r_{42}, r_{43})$	22	$\boldsymbol{y_6 = t_{67}}$

Listing 14: New AES S-box circuit (D: 17, AD: 5, #NL: 32, #L: 97, #(gate): 129)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$t_{17} = t_6 \oplus t_{16}$	10	$t_{47} = t_{38} \oplus g_{12}$	14	$g_{24} = AND(r_{48}, r_{49})$
0	$r_{33} = x_0$	3	$t_{21} = t_{10} \oplus t_{20}$	10	$t_{50} = t_{32} \oplus g_{10}$	14	$g_{30} = AND(r_{60}, r_{61})$
1	$t_0 = x_1 \oplus x_7$	3	$r_2 = t_{17}$	10	$t_{53} = t_{36} \oplus g_{10}$	14	$g_{31} = AND(r_{62}, r_{63})$
1	$t_1 = x_4 \oplus x_7$	3	$r_3 = t_{11}$	10	$t_{58} = t_{43} \oplus g_{12}$	14	$t_{63} = g_{17} \oplus g_{18}$
1	$t_2 = x_2 \oplus x_4$	3	$r_4 = t_7$	10	$r_{23} = t_{42}$	14	$t_{65} = g_{26} \oplus g_{27}$
1	$t_4 = x_2 \oplus x_7$	3	$r_{10} = t_8$	10	$r_{27} = t_{45}$	14	$t_{73} = g_{14} \oplus t_{64}$
1	$t_5 = x_0 \oplus x_6$	3	$r_{11} = t_{14}$	10	$r_{32} = t_{47}$	14	$t_{85} = g_{26} \oplus g_{28}$
1	$t_9 = x_1 \oplus x_3$	3	$r_{17} = t_{21}$	10	$r_{38} = t_{50}$	14	$t_{90} = g_{14} \oplus t_{89}$
1	$t_{12} = x_2 \oplus x_5$	3	$r_{31} = t_{11}$	10	$r_{50} = t_{47}$	15	$t_{55} = g_{29} \oplus g_{30}$
1	$t_{18} = x_1 \oplus x_5$	3	$r_{39} = t_{14}$	10	$r_{56} = t_{50}$	15	$t_{56} = g_{23} \oplus g_{24}$
1	$t_{20} = x_5 \oplus x_6$	3	$r_{45} = t_{21}$	11	$g_{11} = AND(r_{22}, r_{23})$	15	$t_{61} = g_{20} \oplus g_{21}$
1	$t_{22} = x_2 \oplus x_6$	3	$r_{49} = t_{17}$	11	$g_{13} = AND(r_{26}, r_{27})$	15	$t_{62} = g_{14} \oplus g_{15}$
1	$r_6 = t_0$	3	$r_{51} = t_7$	11	$g_{16} = AND(r_{32}, r_{33})$	15	$t_{74} = g_{19} \oplus g_{22}$
1	$r_{12} = t_1$	3	$r_{57} = t_8$	11	$g_{19} = AND(r_{38}, r_{39})$	15	$t_{75} = g_{17} \oplus t_{73}$
1	$r_{14} = t_2$	4	$g_1 = AND(r_2, r_3)$	11	$g_{25} = AND(r_{50}, r_{51})$	15	$t_{77} = g_{21} \oplus g_{18}$
1	$r_{16} = t_4$	4	$g_2 = AND(r_4, r_5)$	11	$g_{28} = AND(r_{56}, r_{57})$	15	$t_{80} = g_{15} \oplus t_{64}$
1	$r_{53} = t_0$	4	$g_5 = AND(r_{10}, r_{11})$	11	$t_{51} = t_{47} \oplus t_{50}$	15	$t_{83} = g_{29} \oplus g_{31}$
1	$r_{59} = t_1$	4	$g_8 = AND(r_{16}, r_{17})$	11	$r_{40} = t_{51}$	15	$t_{86} = t_{73} \oplus t_{85}$
1	$r_{61} = t_2$	4	$t_{24} = g_7 \oplus g_4$	11	$r_{58} = t_{51}$	15	$t_{91} = g_{22} \oplus t_{85}$
1	$r_{63} = t_4$	4	$t_{26} = t_{13} \oplus g_3$	12	$g_{20} = AND(r_{40}, r_{41})$	15	$t_{92} = g_{24} \oplus t_{63}$
2	$t_3 = t_0 \oplus t_2$	4	$t_{28} = g_0 \oplus g_6$	12	$g_{29} = AND(r_{58}, r_{59})$	15	$t_{94} = g_{21} \oplus t_{90}$
2	$t_6 = x_5 \oplus t_5$	4	$t_{33} = t_{12} \oplus g_7$	12	$t_{46} = t_{40} \oplus g_{13}$	16	$t_{57} = t_{55} \oplus t_{56}$
2	$t_{10} = t_1 \oplus t_9$	5	$t_{25} = g_5 \oplus g_8$	12	$t_{49} = t_{35} \oplus g_{11}$	16	$t_{66} = t_{55} \oplus t_{65}$
2	$t_{13} = t_9 \oplus t_{12}$	5	$t_{27} = g_6 \oplus t_{26}$	12	$t_{54} = g_{11} \oplus t_{53}$	16	$t_{67} = t_{62} \oplus t_{63}$
2	$t_{15} = t_1 \oplus t_{12}$	5	$t_{29} = t_{21} \oplus t_{28}$	12	$t_{59} = g_{13} \oplus t_{58}$	16	$t_{69} = t_{61} \oplus t_{62}$
2	$t_{16} = x_1 \oplus t_4$	5	$t_{30} = t_4 \oplus g_2$	12	$t_{64} = g_{16} \oplus g_{19}$	16	$t_{71} = t_{61} \oplus t_{63}$
2	$t_{19} = t_5 \oplus t_{18}$	5	$t_{34} = g_1 \oplus t_{33}$	12	$t_{89} = g_{16} \oplus g_{25}$	16	$t_{78} = t_{74} \oplus t_{77}$
2	$t_{23} = t_9 \oplus t_{22}$	5	$t_{39} = t_0 \oplus t_{24}$	12	$r_{28} = t_{46}$	16	$t_{81} = g_{18} \oplus t_{80}$
2	$r_0 = t_3$	6	$t_{31} = g_8 \oplus t_{30}$	12	$r_{34} = t_{49}$	16	$t_{84} = g_{20} \oplus t_{83}$
2	$r_1 = t_{10}$	6	$t_{35} = t_{29} \oplus t_{34}$	12	$r_{36} = t_{54}$	16	$t_{87} = t_{74} \oplus t_{86}$
2	$r_7 = t_{13}$	6	$t_{37} = x_7 \oplus t_{25}$	12	$r_{46} = t_{46}$	16	$t_{93} = t_{55} \oplus t_{92}$
2	$r_8 = t_{19}$	6	$t_{40} = t_{27} \oplus t_{39}$	12	$r_{52} = t_{49}$	16	$t_{95} = t_{91} \oplus t_{94}$
2	$r_9 = t_6$	6	$r_{18} = t_{35}$	12	$r_{54} = t_{54}$	17	$t_{68} = t_{57} \oplus t_{67}$
2	$r_{13} = t_{23}$	6	$r_{19} = t_{40}$	13	$g_{14} = AND(r_{28}, r_{29})$	17	$t_{70} = t_{57} \oplus t_{69} \oplus 1$
2	$r_{15} = t_{15}$	7	$g_9 = AND(r_{18}, r_{19})$	13	$g_{17} = AND(r_{34}, r_{35})$	17	$t_{72} = t_{57} \oplus t_{71}$
2	$r_{29} = t_{10}$	7	$t_{32} = t_{29} \oplus t_{31}$	13	$g_{18} = AND(r_{36}, r_{37})$	17	$t_{76} = t_{66} \oplus t_{75} \oplus 1$
2	$r_{35} = t_{13}$	7	$t_{36} = t_{31} \oplus t_{34}$	13	$g_{23} = AND(r_{46}, r_{47})$	17	$t_{79} = t_{66} \oplus t_{78} \oplus 1$
2	$r_{37} = t_6$	7	$t_{38} = t_{27} \oplus t_{37}$	13	$g_{26} = AND(r_{52}, r_{53})$	17	$t_{82} = t_{57} \oplus t_{81}$
2	$r_{41} = t_{23}$	7	$t_{43} = t_{37} \oplus t_{39}$	13	$g_{27} = AND(r_{54}, r_{55})$	17	$t_{88} = t_{84} \oplus t_{87} \oplus 1$
2	$r_{43} = t_{15}$	7	$r_{20} = t_{36}$	13	$t_{52} = t_{46} \oplus t_{49}$	17	$t_{96} = t_{93} \oplus t_{95}$
2	$r_{47} = t_3$	7	$r_{22} = t_{32}$	13	$t_{48} = t_{46} \oplus t_{47}$	17	$\boldsymbol{y_0 = t_{76}}$
2	$r_{55} = t_{19}$	7	$r_{24} = t_{43}$	13	$t_{60} = t_{54} \oplus t_{59}$	17	$\boldsymbol{y_1 = t_{79}}$
3	$g_0 = AND(r_0, r_1)$	7	$r_{26} = t_{38}$	13	$r_{30} = t_{59}$	17	$\boldsymbol{y_2 = t_{96}}$
3	$g_3 = AND(r_6, r_7)$	8	$t_{41} = t_{38} \oplus g_9$	13	$r_{42} = t_{52}$	17	$\boldsymbol{y_3 = t_{82}}$
3	$g_4 = AND(r_8, r_9)$	8	$t_{44} = t_{32} \oplus g_9$	13	$r_{44} = t_{60}$	17	$\boldsymbol{y_4 = t_{68}}$
3	$g_6 = AND(r_{12}, r_{13})$	8	$r_{21} = t_{41}$	13	$r_{48} = t_{59}$	17	$\boldsymbol{y_5 = t_{88}}$
3	$g_7 = AND(r_{14}, r_{15})$	8	$r_{25} = t_{44}$	13	$r_{60} = t_{52}$	17	$\boldsymbol{y_6 = t_{70}}$
3	$t_7 = x_4 \oplus t_6$	9	$g_{10} = AND(r_{20}, r_{21})$	13	$r_{62} = t_{60}$	17	$\boldsymbol{y_7 = t_{72}}$
3	$t_8 = x_7 \oplus t_6$	9	$g_{12} = AND(r_{24}, r_{25})$	14	$g_{15} = AND(r_{30}, r_{31})$		
3	$t_{11} = x_0 \oplus t_{10}$	10	$t_{42} = g_9 \oplus g_{10}$	14	$g_{21} = AND(r_{42}, r_{43})$		
3	$t_{14} = t_6 \oplus t_{13}$	10	$t_{45} = g_9 \oplus g_{12}$	14	$g_{22} = AND(r_{44}, r_{45})$		

Listing 15: New `AES` S-box circuit (D: 16, AD: 4, #NL: 33, #L: 104, #(gate): 137)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{53} = t_{10}$	9	$g_{13} = AND(r_{26}, r_{27})$	12	$r_{62} = t_{66}$
0	$r_{35} = x_0$	3	$r_{57} = t_{12}$	9	$g_{14} = AND(r_{28}, r_{29})$	13	$g_{15} = AND(r_{30}, r_{31})$
1	$t_0 = x_1 \oplus x_7$	3	$r_{59} = t_{13}$	9	$t_{36} = g_9 \oplus t_{35}$	13	$g_{21} = AND(r_{42}, r_{43})$
1	$t_1 = x_4 \oplus x_7$	4	$g_0 = AND(r_0, r_1)$	9	$t_{43} = g_9 \oplus t_{51}$	13	$g_{22} = AND(r_{44}, r_{45})$
1	$t_2 = x_2 \oplus x_4$	4	$g_2 = AND(r_4, r_5)$	9	$t_{60} = t_{30} \oplus g_9$	13	$g_{24} = AND(r_{48}, r_{49})$
1	$t_4 = x_2 \oplus x_7$	4	$g_4 = AND(r_8, r_9)$	9	$t_{63} = t_{26} \oplus g_9$	13	$g_{30} = AND(r_{60}, r_{61})$
1	$t_5 = x_2 \oplus x_3$	4	$g_5 = AND(r_{10}, r_{11})$	9	$r_{21} = t_{36}$	13	$g_{31} = AND(r_{62}, r_{63})$
1	$t_8 = x_5 \oplus x_6$	4	$g_7 = AND(r_{14}, r_{15})$	9	$r_{23} = t_{43}$	13	$t_{69} = g_{25} \oplus g_{19}$
1	$t_{14} = x_1 \oplus x_5$	4	$g_8 = AND(r_{16}, r_{17})$	10	$g_{10} = AND(r_{20}, r_{21})$	13	$t_{71} = g_{17} \oplus g_{20}$
1	$t_{20} = x_1 \oplus x_6$	4	$t_7 = x_0 \oplus t_6$	10	$g_{11} = AND(r_{22}, r_{23})$	13	$t_{75} = g_{23} \oplus g_{27}$
1	$t_{47} = x_4 \oplus x_6$	4	$t_{11} = t_3 \oplus t_{10}$	10	$t_{54} = t_{37} \oplus g_{14}$	13	$t_{86} = g_{20} \oplus g_{19}$
1	$r_6 = t_0$	4	$t_{23} = t_{15} \oplus g_3$	10	$t_{57} = t_{41} \oplus g_{13}$	13	$t_{88} = g_{17} \oplus g_{29}$
1	$r_{12} = t_1$	4	$t_{33} = x_7 \oplus g_6$	10	$t_{61} = g_{13} \oplus t_{60}$	13	$t_{96} = g_{16} \oplus g_{25}$
1	$r_{14} = t_2$	4	$t_{49} = g_6 \oplus t_{48}$	10	$t_{64} = g_{14} \oplus t_{63}$	13	$t_{100} = g_{26} \oplus g_{18}$
1	$r_{16} = t_4$	4	$r_2 = t_{11}$	11	$t_{44} = t_{35} \oplus g_{11}$	14	$t_{67} = g_{30} \oplus g_{31}$
1	$r_{55} = t_0$	4	$r_3 = t_7$	11	$t_{45} = g_{10} \oplus t_{51}$	14	$t_{70} = g_{16} \oplus t_{69}$
1	$r_{61} = t_1$	4	$r_{33} = t_7$	11	$t_{55} = g_9 \oplus t_{54}$	14	$t_{72} = g_{15} \oplus g_{18}$
1	$r_{63} = t_2$	4	$r_{51} = t_{11}$	11	$t_{58} = g_9 \oplus t_{57}$	14	$t_{73} = g_{21} \oplus g_{22}$
1	$r_{65} = t_4$	5	$g_1 = AND(r_2, r_3)$	11	$t_{59} = t_{54} \oplus t_{57}$	14	$t_{80} = g_{18} \oplus t_{69}$
2	$t_3 = t_0 \oplus t_2$	5	$t_{22} = g_7 \oplus g_6$	11	$t_{62} = g_{10} \oplus t_{61}$	14	$t_{83} = g_{27} \oplus t_{71}$
2	$t_9 = x_0 \oplus t_8$	5	$t_{25} = g_4 \oplus t_{23}$	11	$t_{65} = g_{11} \oplus t_{64}$	14	$t_{87} = g_{22} \oplus t_{75}$
2	$t_{15} = t_5 \oplus t_{14}$	5	$t_{28} = g_0 \oplus t_{21}$	11	$r_{32} = t_{55}$	14	$t_{89} = g_{15} \oplus t_{88}$
2	$t_{18} = t_5 \oplus t_8$	5	$t_{31} = g_5 \oplus g_8$	11	$r_{34} = t_{44}$	14	$t_{93} = g_{30} \oplus g_{32}$
2	$t_{21} = t_5 \oplus t_{20}$	5	$t_{32} = g_2 \oplus g_8$	11	$r_{36} = t_{62}$	14	$t_{97} = g_{15} \oplus t_{96}$
2	$r_0 = t_3$	5	$t_{34} = t_{23} \oplus t_{33}$	11	$r_{38} = t_{58}$	14	$t_{101} = t_{69} \oplus t_{100}$
2	$r_7 = t_{15}$	5	$t_{38} = x_5 \oplus t_{33}$	11	$r_{40} = t_{45}$	15	$t_{68} = g_{24} \oplus t_{67}$
2	$r_9 = t_9$	5	$t_{50} = g_0 \oplus t_{49}$	11	$r_{46} = t_{59}$	15	$t_{74} = g_{28} \oplus t_{67}$
2	$r_{13} = t_{21}$	6	$t_{24} = t_0 \oplus t_{22}$	11	$r_{50} = t_{55}$	15	$t_{76} = t_{70} \oplus t_{72}$
2	$r_{37} = t_{15}$	6	$t_{27} = t_1 \oplus t_{22}$	11	$r_{52} = t_{44}$	15	$t_{78} = t_{70} \oplus t_{71}$
2	$r_{39} = t_9$	6	$t_{29} = g_1 \oplus t_{28}$	11	$r_{54} = t_{62}$	15	$t_{81} = t_{73} \oplus t_{80}$
2	$r_{43} = t_{21}$	6	$t_{35} = t_{31} \oplus t_{34}$	11	$r_{56} = t_{58}$	15	$t_{84} = t_{72} \oplus t_{83}$
2	$r_{49} = t_3$	6	$t_{39} = t_{32} \oplus t_{38}$	11	$r_{58} = t_{45}$	15	$t_{90} = t_{87} \oplus t_{89}$
3	$g_3 = AND(r_6, r_7)$	6	$t_{40} = g_1 \oplus t_{22}$	11	$r_{64} = t_{59}$	15	$t_{91} = t_{86} \oplus t_{87}$
3	$g_6 = AND(r_{12}, r_{13})$	6	$t_{51} = t_{32} \oplus t_{50}$	12	$g_{16} = AND(r_{32}, r_{33})$	15	$t_{94} = t_{73} \oplus t_{93}$
3	$t_6 = t_3 \oplus t_5$	6	$r_{24} = t_{51}$	12	$g_{17} = AND(r_{34}, r_{35})$	15	$t_{98} = t_{73} \oplus t_{97}$
3	$t_{10} = x_4 \oplus t_9$	6	$r_{25} = t_{35}$	12	$g_{18} = AND(r_{36}, r_{37})$	15	$t_{102} = t_{67} \oplus t_{101}$
3	$t_{12} = x_1 \oplus t_9$	7	$g_{12} = AND(r_{24}, r_{25})$	12	$g_{19} = AND(r_{38}, r_{39})$	16	$t_{77} = t_{68} \oplus t_{76}$
3	$t_{13} = x_7 \oplus t_9$	7	$t_{26} = t_{24} \oplus t_{25}$	12	$g_{20} = AND(r_{40}, r_{41})$	16	$t_{79} = t_{68} \oplus t_{78}$
3	$t_{16} = t_9 \oplus t_{15}$	7	$t_{30} = t_{27} \oplus t_{29}$	12	$g_{23} = AND(r_{46}, r_{47})$	16	$t_{82} = t_{68} \oplus t_{81}$
3	$t_{17} = t_3 \oplus t_{14}$	7	$t_{41} = t_{39} \oplus t_{40}$	12	$g_{25} = AND(r_{50}, r_{51})$	16	$t_{85} = t_{74} \oplus t_{84} \oplus 1$
3	$t_{19} = t_3 \oplus t_{18}$	7	$r_{18} = t_{30}$	12	$g_{26} = AND(r_{52}, r_{53})$	16	$t_{92} = t_{74} \oplus t_{91} \oplus 1$
3	$t_{48} = t_{15} \oplus t_{47}$	7	$r_{19} = t_{26}$	12	$g_{27} = AND(r_{54}, r_{55})$	16	$t_{95} = t_{90} \oplus t_{94} \oplus 1$
3	$r_1 = t_6$	7	$r_{20} = t_{41}$	12	$g_{28} = AND(r_{56}, r_{57})$	16	$t_{99} = t_{68} \oplus t_{98} \oplus 1$
3	$r_4 = t_{10}$	7	$r_{26} = t_{30}$	12	$g_{29} = AND(r_{58}, r_{59})$	16	$t_{103} = t_{90} \oplus t_{102}$
3	$r_8 = t_{12}$	7	$r_{28} = t_{26}$	12	$g_{32} = AND(r_{64}, r_{65})$	16	$\boldsymbol{y_0 = t_{85}}$
3	$r_{10} = t_{13}$	8	$g_9 = AND(r_{18}, r_{19})$	12	$t_{46} = t_{44} \oplus t_{45}$	16	$\boldsymbol{y_1 = t_{92}}$
3	$r_{11} = t_{16}$	8	$t_{37} = t_{26} \oplus t_{35}$	12	$t_{56} = t_{44} \oplus t_{55}$	16	$\boldsymbol{y_2 = t_{103}}$
3	$r_{15} = t_{17}$	8	$t_{42} = t_{30} \oplus t_{41}$	12	$t_{66} = t_{62} \oplus t_{65}$	16	$\boldsymbol{y_3 = t_{79}}$
3	$r_{17} = t_{19}$	8	$t_{52} = t_{35} \oplus g_{12}$	12	$r_{30} = t_{65}$	16	$\boldsymbol{y_4 = t_{77}}$
3	$r_{31} = t_6$	8	$t_{53} = t_{51} \oplus g_{12}$	12	$r_{42} = t_{46}$	16	$\boldsymbol{y_5 = t_{95}}$
3	$r_{41} = t_{16}$	8	$r_{22} = t_{37}$	12	$r_{44} = t_{66}$	16	$\boldsymbol{y_6 = t_{99}}$
3	$r_{45} = t_{17}$	8	$r_{27} = t_{52}$	12	$r_{48} = t_{65}$	16	$\boldsymbol{y_7 = t_{82}}$
3	$r_{47} = t_{19}$	8	$r_{29} = t_{53}$	12	$r_{60} = t_{46}$		

Listing 16: New AES S-box circuit (D: 28, AD: 4, #NL: 34, #L: 81, #(gate): 115)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{17} = t_{14}$	10	$r_{27} = g_{12}$	15	$g_{22} = AND(r_{44}, r_{45})$
0	$r_{37} = x_0$	3	$r_{35} = t_7$	10	$r_{31} = g_{14}$	15	$g_{25} = AND(r_{50}, r_{51})$
1	$t_0 = x_1 \oplus x_7$	3	$r_{43} = t_{17}$	11	$g_{13} = AND(r_{26}, r_{27})$	15	$g_{28} = AND(r_{56}, r_{57})$
1	$t_1 = x_4 \oplus x_7$	3	$r_{45} = t_{18}$	11	$g_{15} = AND(r_{30}, r_{31})$	15	$g_{31} = AND(r_{62}, r_{63})$
1	$t_2 = x_2 \oplus x_4$	3	$r_{49} = t_{14}$	11	$t_{37} = t_{29} \oplus g_9$	15	$t_{49} = t_{45} \oplus t_{48}$
1	$t_4 = x_2 \oplus x_7$	3	$r_{55} = t_{10}$	11	$t_{39} = g_9 \oplus t_{38}$	15	$r_{46} = t_{49}$
1	$t_5 = x_1 \oplus x_3$	3	$r_{59} = t_{12}$	11	$r_{20} = t_{39}$	15	$r_{64} = t_{49}$
1	$t_8 = x_5 \oplus x_6$	3	$r_{61} = t_{13}$	11	$r_{22} = t_{37}$	16	$g_{23} = AND(r_{46}, r_{47})$
1	$t_{15} = x_2 \oplus x_5$	4	$g_2 = AND(r_4, r_5)$	12	$g_{10} = AND(r_{20}, r_{21})$	16	$g_{32} = AND(r_{64}, r_{65})$
1	$r_6 = t_0$	4	$g_4 = AND(r_8, r_9)$	12	$g_{11} = AND(r_{22}, r_{23})$	16	$t_{53} = g_{26} \oplus g_{25}$
1	$r_{12} = t_1$	4	$g_5 = AND(r_{10}, r_{11})$	12	$t_{43} = t_{34} \oplus g_{15}$	16	$t_{61} = g_{29} \oplus g_{28}$
1	$r_{14} = t_2$	4	$g_6 = AND(r_{12}, r_{13})$	12	$t_{46} = t_{25} \oplus g_{13}$	16	$t_{73} = g_{30} \oplus g_{28}$
1	$r_{16} = t_4$	4	$g_8 = AND(r_{16}, r_{17})$	13	$t_{40} = g_{11} \oplus t_{38}$	16	$t_{76} = g_{31} \oplus g_{33}$
1	$r_{57} = t_0$	4	$t_{11} = t_3 \oplus t_{10}$	13	$t_{41} = t_{29} \oplus g_{10}$	17	$t_{51} = g_{31} \oplus g_{32}$
1	$r_{63} = t_1$	4	$r_2 = t_{11}$	13	$t_{44} = g_9 \oplus t_{43}$	17	$t_{58} = g_{22} \oplus g_{23}$
1	$r_{65} = t_2$	4	$r_{53} = t_{11}$	13	$t_{47} = g_9 \oplus t_{46}$	18	$t_{52} = g_{20} \oplus t_{51}$
1	$r_{67} = t_4$	5	$g_1 = AND(r_2, r_3)$	13	$t_{50} = t_{43} \oplus t_{46}$	18	$t_{66} = t_{51} \oplus t_{61}$
2	$t_3 = t_0 \oplus t_2$	5	$t_{20} = g_8 \oplus g_7$	13	$r_{34} = t_{44}$	19	$t_{54} = t_{52} \oplus t_{53}$
2	$t_6 = t_1 \oplus t_5$	5	$t_{22} = g_6 \oplus g_7$	13	$r_{36} = t_{40}$	20	$t_{55} = g_{17} \oplus t_{54}$
2	$t_9 = x_0 \oplus t_8$	5	$t_{33} = x_1 \oplus g_4$	13	$r_{40} = t_{47}$	20	$t_{62} = g_{19} \oplus t_{54}$
2	$t_{16} = t_5 \oplus t_{15}$	6	$t_{21} = g_1 \oplus t_{15}$	13	$r_{42} = t_{41}$	21	$t_{56} = g_{16} \oplus t_{55}$
2	$t_{19} = t_1 \oplus t_{15}$	6	$t_{23} = t_4 \oplus t_{20}$	13	$r_{48} = t_{50}$	21	$t_{59} = g_{18} \oplus t_{55}$
2	$r_0 = t_3$	6	$t_{26} = g_0 \oplus t_{22}$	13	$r_{52} = t_{44}$	21	$t_{63} = t_{58} \oplus t_{62}$
2	$r_1 = t_6$	6	$t_{30} = g_5 \oplus t_{20}$	13	$r_{54} = t_{40}$	21	$\boldsymbol{y_7 = t_{63}}$
2	$r_7 = t_{16}$	6	$t_{31} = g_3 \oplus t_{22}$	13	$r_{58} = t_{47}$	22	$t_{57} = g_{19} \oplus t_{56}$
2	$r_9 = t_9$	7	$t_{24} = g_2 \oplus t_{23}$	13	$r_{60} = t_{41}$	22	$t_{60} = g_{21} \oplus t_{59}$
2	$r_{15} = t_{19}$	7	$t_{27} = t_{14} \oplus t_{26}$	13	$r_{66} = t_{50}$	22	$t_{64} = g_{20} \oplus t_{56}$
2	$r_{33} = t_6$	7	$t_{32} = t_{16} \oplus t_{31}$	14	$g_{17} = AND(r_{34}, r_{35})$	22	$t_{69} = g_{24} \oplus t_{59}$
2	$r_{39} = t_{16}$	7	$t_{34} = t_{30} \oplus t_{33}$	14	$g_{18} = AND(r_{36}, r_{37})$	22	$\boldsymbol{y_3 = t_{60}}$
2	$r_{41} = t_9$	7	$r_{23} = t_{34}$	14	$g_{20} = AND(r_{40}, r_{41})$	22	$\boldsymbol{y_4 = t_{57}}$
2	$r_{47} = t_{19}$	7	$r_{30} = t_{34}$	14	$g_{21} = AND(r_{42}, r_{43})$	23	$t_{65} = t_{58} \oplus t_{64} \oplus 1$
2	$r_{51} = t_3$	8	$t_{25} = t_{21} \oplus t_{24}$	14	$g_{24} = AND(r_{48}, r_{49})$	23	$t_{67} = t_{60} \oplus t_{66}$
3	$g_0 = AND(r_0, r_1)$	8	$t_{28} = t_{21} \oplus t_{27}$	14	$g_{26} = AND(r_{52}, r_{53})$	23	$t_{70} = g_{23} \oplus t_{69}$
3	$g_3 = AND(r_6, r_7)$	8	$t_{29} = t_{24} \oplus t_{27}$	14	$g_{27} = AND(r_{54}, r_{55})$	23	$\boldsymbol{y_6 = t_{65}}$
3	$g_7 = AND(r_{14}, r_{15})$	8	$t_{35} = x_7 \oplus t_{32}$	14	$g_{29} = AND(r_{58}, r_{59})$	24	$t_{68} = t_{57} \oplus t_{67} \oplus 1$
3	$t_7 = x_0 \oplus t_6$	8	$r_{19} = t_{28}$	14	$g_{30} = AND(r_{60}, r_{61})$	24	$t_{71} = g_{20} \oplus t_{70}$
3	$t_{10} = x_4 \oplus t_9$	8	$r_{21} = t_{25}$	14	$g_{33} = AND(r_{66}, r_{67})$	24	$t_{74} = t_{65} \oplus t_{73} \oplus 1$
3	$t_{12} = x_1 \oplus t_9$	8	$r_{24} = t_{28}$	14	$t_{42} = t_{40} \oplus t_{41}$	24	$\boldsymbol{y_0 = t_{68}}$
3	$t_{13} = x_7 \oplus t_9$	8	$r_{26} = t_{25}$	14	$t_{45} = t_{40} \oplus t_{44}$	25	$t_{72} = t_{67} \oplus t_{71} \oplus 1$
3	$t_{14} = t_6 \oplus t_8$	8	$r_{28} = t_{29}$	14	$t_{48} = t_{41} \oplus t_{47}$	25	$t_{75} = t_{71} \oplus t_{74}$
3	$t_{17} = t_9 \oplus t_{16}$	9	$t_{36} = t_{33} \oplus t_{35}$	14	$r_{32} = t_{45}$	25	$\boldsymbol{y_1 = t_{72}}$
3	$t_{18} = t_8 \oplus t_{16}$	9	$t_{38} = t_{30} \oplus t_{35}$	14	$r_{38} = t_{48}$	26	$t_{77} = t_{75} \oplus t_{76} \oplus 1$
3	$r_3 = t_7$	9	$r_{18} = t_{36}$	14	$r_{44} = t_{42}$	26	$t_{78} = g_{25} \oplus t_{75}$
3	$r_4 = t_{10}$	9	$r_{25} = t_{38}$	14	$r_{50} = t_{45}$	26	$\boldsymbol{y_5 = t_{77}}$
3	$r_8 = t_{12}$	9	$r_{29} = t_{36}$	14	$r_{56} = t_{48}$	27	$t_{79} = g_{27} \oplus t_{78}$
3	$r_{10} = t_{13}$	10	$g_9 = AND(r_{18}, r_{19})$	14	$r_{62} = t_{42}$	28	$t_{80} = t_{63} \oplus t_{79}$
3	$r_{11} = t_{17}$	10	$g_{12} = AND(r_{24}, r_{25})$	15	$g_{16} = AND(r_{32}, r_{33})$	28	$\boldsymbol{y_2 = t_{80}}$
3	$r_{13} = t_{18}$	10	$g_{14} = AND(r_{28}, r_{29})$	15	$g_{19} = AND(r_{38}, r_{39})$		

Listing 17: New AES S-box circuit (D: 15, AD: 4, #NL: 34, #L: 100, #(gate): 134)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{11} = t_{16}$	8	$t_{45} = t_{24} \oplus g_9$	11	$r_{64} = t_{63}$
0	$r_{37} = x_0$	3	$r_{17} = t_{13}$	8	$t_{53} = t_{24} \oplus t_{34}$	12	$g_{16} = AND(r_{32}, r_{33})$
1	$t_0 = x_1 \oplus x_7$	3	$r_{35} = t_{12}$	8	$t_{56} = t_{31} \oplus g_9$	12	$g_{22} = AND(r_{44}, r_{45})$
1	$t_1 = x_4 \oplus x_7$	3	$r_{43} = t_{16}$	8	$r_{20} = t_{41}$	12	$g_{23} = AND(r_{46}, r_{47})$
1	$t_2 = x_2 \oplus x_4$	3	$r_{49} = t_{13}$	8	$r_{22} = t_{39}$	12	$g_{25} = AND(r_{50}, r_{51})$
1	$t_4 = x_2 \oplus x_7$	3	$r_{53} = t_{26}$	8	$r_{31} = g_{14}$	12	$g_{31} = AND(r_{62}, r_{63})$
1	$t_5 = x_5 \oplus x_6$	3	$r_{55} = t_7$	9	$g_{10} = AND(r_{20}, r_{21})$	12	$g_{32} = AND(r_{64}, r_{65})$
1	$t_{10} = x_1 \oplus x_3$	3	$r_{59} = t_8$	9	$g_{11} = AND(r_{22}, r_{23})$	12	$t_{69} = g_{20} \oplus g_{19}$
1	$t_{14} = x_2 \oplus x_5$	3	$r_{61} = t_9$	9	$g_{15} = AND(r_{30}, r_{31})$	12	$t_{70} = g_{21} \oplus g_{20}$
1	$t_{18} = x_2 \oplus x_6$	4	$g_1 = AND(r_2, r_3)$	9	$t_{51} = t_{39} \oplus g_{13}$	12	$t_{72} = g_{29} \oplus g_{28}$
1	$r_6 = t_0$	4	$g_2 = AND(r_4, r_5)$	9	$t_{54} = g_{13} \oplus t_{53}$	12	$t_{89} = g_{24} \oplus g_{28}$
1	$r_{12} = t_1$	4	$g_4 = AND(r_8, r_9)$	9	$t_{57} = g_{13} \oplus t_{56}$	12	$t_{90} = g_{18} \oplus g_{30}$
1	$r_{14} = t_2$	4	$g_5 = AND(r_{10}, r_{11})$	9	$t_{61} = g_{13} \oplus t_{60}$	12	$t_{96} = g_{27} \oplus g_{26}$
1	$r_{16} = t_4$	4	$g_8 = AND(r_{16}, r_{17})$	10	$t_{42} = g_{11} \oplus t_{50}$	13	$t_{64} = g_{31} \oplus g_{32}$
1	$r_{57} = t_0$	4	$t_{22} = t_{15} \oplus g_6$	10	$t_{43} = t_{35} \oplus g_{10}$	13	$t_{65} = g_{26} \oplus g_{25}$
1	$r_{63} = t_1$	4	$t_{27} = t_{14} \oplus g_7$	10	$t_{46} = g_{15} \oplus t_{45}$	13	$t_{67} = g_{17} \oplus g_{16}$
1	$r_{65} = t_2$	4	$t_{29} = t_{13} \oplus g_6$	10	$t_{52} = t_{31} \oplus t_{51}$	13	$t_{68} = g_{22} \oplus g_{23}$
1	$r_{67} = t_4$	4	$t_{36} = t_0 \oplus g_3$	10	$t_{55} = g_{15} \oplus t_{54}$	13	$t_{71} = g_{18} \oplus t_{70}$
2	$t_3 = t_0 \oplus t_2$	4	$t_{48} = x_7 \oplus g_3$	10	$t_{58} = g_{10} \oplus t_{57}$	13	$t_{82} = g_{24} \oplus g_{23}$
2	$t_6 = x_0 \oplus t_5$	5	$t_{20} = g_4 \oplus g_7$	10	$t_{59} = g_{15} \oplus g_{11}$	13	$t_{85} = g_{16} \oplus t_{69}$
2	$t_{11} = t_1 \oplus t_{10}$	5	$t_{21} = g_8 \oplus g_5$	10	$t_{62} = g_{10} \oplus t_{61}$	13	$t_{88} = g_{22} \oplus g_{31}$
2	$t_{15} = t_{10} \oplus t_{14}$	5	$t_{28} = g_1 \oplus t_{27}$	10	$r_{34} = t_{46}$	13	$t_{91} = t_{89} \oplus t_{90}$
2	$t_{17} = t_1 \oplus t_{14}$	5	$t_{30} = g_0 \oplus t_{29}$	10	$r_{36} = t_{42}$	13	$t_{97} = g_{23} \oplus t_{96}$
2	$t_{19} = t_{10} \oplus t_{18}$	5	$t_{32} = t_4 \oplus g_8$	10	$r_{38} = t_{58}$	14	$t_{66} = t_{64} \oplus t_{65}$
2	$t_{25} = x_1 \oplus t_4$	5	$t_{37} = t_{22} \oplus t_{36}$	10	$r_{40} = t_{52}$	14	$t_{73} = t_{64} \oplus t_{72}$
2	$r_0 = t_3$	5	$t_{49} = t_{22} \oplus t_{48}$	10	$r_{42} = t_{43}$	14	$t_{74} = t_{68} \oplus t_{69}$
2	$r_1 = t_{11}$	6	$t_{23} = x_1 \oplus t_{21}$	10	$r_{48} = t_{55}$	14	$t_{76} = g_{17} \oplus t_{71}$
2	$r_7 = t_{15}$	6	$t_{31} = t_{28} \oplus t_{30}$	10	$r_{52} = t_{46}$	14	$t_{78} = t_{67} \oplus t_{69}$
2	$r_9 = t_6$	6	$t_{33} = g_2 \oplus t_{32}$	10	$r_{54} = t_{42}$	14	$t_{80} = t_{67} \oplus t_{68}$
2	$r_{13} = t_{19}$	6	$t_{38} = t_{20} \oplus t_{37}$	10	$r_{56} = t_{58}$	14	$t_{83} = t_{70} \oplus t_{82}$
2	$r_{15} = t_{17}$	6	$t_{50} = t_{21} \oplus t_{49}$	10	$r_{58} = t_{52}$	14	$t_{86} = t_{71} \oplus t_{85}$
2	$r_{33} = t_{11}$	6	$r_{18} = t_{38}$	10	$r_{60} = t_{43}$	14	$t_{92} = g_{16} \oplus t_{91}$
2	$r_{39} = t_{15}$	6	$r_{19} = t_{31}$	10	$r_{66} = t_{55}$	14	$t_{93} = g_{33} \oplus t_{88}$
2	$r_{41} = t_6$	6	$r_{24} = t_{31}$	11	$g_{17} = AND(r_{34}, r_{35})$	14	$t_{95} = t_{85} \oplus t_{91}$
2	$r_{45} = t_{19}$	6	$r_{25} = t_{50}$	11	$g_{18} = AND(r_{36}, r_{37})$	14	$t_{98} = t_{64} \oplus t_{97}$
2	$r_{47} = t_{17}$	6	$r_{29} = t_{38}$	11	$g_{19} = AND(r_{38}, r_{39})$	15	$t_{75} = t_{66} \oplus t_{74}$
2	$r_{51} = t_3$	7	$g_9 = AND(r_{18}, r_{19})$	11	$g_{20} = AND(r_{40}, r_{41})$	15	$t_{77} = t_{66} \oplus t_{76}$
3	$g_0 = AND(r_0, r_1)$	7	$g_{12} = AND(r_{24}, r_{25})$	11	$g_{21} = AND(r_{42}, r_{43})$	15	$t_{79} = t_{66} \oplus t_{78}$
3	$g_3 = AND(r_6, r_7)$	7	$t_{24} = t_{20} \oplus t_{23}$	11	$g_{24} = AND(r_{48}, r_{49})$	15	$t_{81} = t_{66} \oplus t_{80} \oplus 1$
3	$g_6 = AND(r_{12}, r_{13})$	7	$t_{34} = t_{28} \oplus t_{33}$	11	$g_{26} = AND(r_{52}, r_{53})$	15	$t_{84} = t_{73} \oplus t_{83} \oplus 1$
3	$g_7 = AND(r_{14}, r_{15})$	7	$t_{35} = t_{30} \oplus t_{33}$	11	$g_{27} = AND(r_{54}, r_{55})$	15	$t_{87} = t_{73} \oplus t_{86} \oplus 1$
3	$t_7 = x_4 \oplus t_6$	7	$t_{50} = t_{23} \oplus t_{37}$	11	$g_{28} = AND(r_{56}, r_{57})$	15	$t_{94} = t_{92} \oplus t_{93} \oplus 1$
3	$t_8 = x_1 \oplus t_6$	7	$t_{60} = t_{31} \oplus t_{38}$	11	$g_{29} = AND(r_{58}, r_{59})$	15	$t_{99} = t_{95} \oplus t_{98}$
3	$t_9 = x_7 \oplus t_6$	7	$r_{21} = t_{34}$	11	$g_{30} = AND(r_{60}, r_{61})$	15	$\boldsymbol{y_0 = t_{87}}$
3	$t_{12} = x_0 \oplus t_{11}$	7	$r_{23} = t_{24}$	11	$g_{33} = AND(r_{66}, r_{67})$	15	$\boldsymbol{y_1 = t_{84}}$
3	$t_{13} = t_5 \oplus t_{11}$	7	$r_{26} = t_{34}$	11	$t_{44} = t_{42} \oplus t_{43}$	15	$\boldsymbol{y_2 = t_{99}}$
3	$t_{16} = t_6 \oplus t_{15}$	7	$r_{27} = g_{12}$	11	$t_{47} = t_{42} \oplus t_{46}$	15	$\boldsymbol{y_3 = t_{77}}$
3	$t_{26} = t_6 \oplus t_{25}$	7	$r_{28} = t_{35}$	11	$t_{63} = t_{59} \oplus t_{62}$	15	$\boldsymbol{y_4 = t_{79}}$
3	$r_2 = t_{26}$	7	$r_{30} = t_{24}$	11	$r_{32} = t_{47}$	15	$\boldsymbol{y_5 = t_{94}}$
3	$r_3 = t_{12}$	8	$g_{13} = AND(r_{26}, r_{27})$	11	$r_{44} = t_{44}$	15	$\boldsymbol{y_6 = t_{81}}$
3	$r_4 = t_7$	8	$g_{14} = AND(r_{28}, r_{29})$	11	$r_{46} = t_{63}$	15	$\boldsymbol{y_7 = t_{75}}$
3	$r_8 = t_8$	8	$t_{39} = t_{35} \oplus g_9$	11	$r_{50} = t_{47}$		
3	$r_{10} = t_9$	8	$t_{41} = g_9 \oplus t_{50}$	11	$r_{62} = t_{44}$		

Listing 18: New `AES` S-box circuit (D: 17, AD: 5, #NL: 32, #L: 93, #(gate): 125)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$t_{21} = t_4 \oplus t_{20}$	10	$t_{44} = g_9 \oplus g_{12}$	14	$g_{21} = AND(r_{42}, r_{43})$
0	$r_{33} = x_0$	3	$r_2 = t_{21}$	10	$t_{46} = t_{36} \oplus g_{12}$	14	$g_{22} = AND(r_{44}, r_{45})$
1	$t_0 = x_1 \oplus x_7$	3	$r_3 = t_7$	10	$t_{49} = t_{34} \oplus g_{10}$	14	$g_{24} = AND(r_{48}, r_{49})$
1	$t_1 = x_4 \oplus x_7$	3	$r_4 = t_{10}$	10	$t_{52} = t_{30} \oplus g_{10}$	14	$g_{30} = AND(r_{60}, r_{61})$
1	$t_2 = x_2 \oplus x_4$	3	$r_{10} = t_{11}$	10	$r_{23} = t_{42}$	14	$g_{31} = AND(r_{62}, r_{63})$
1	$t_4 = x_2 \oplus x_7$	3	$r_{11} = t_{15}$	10	$r_{27} = t_{44}$	14	$t_{61} = g_{17} \oplus g_{18}$
1	$t_5 = x_1 \oplus x_3$	3	$r_{17} = t_{12}$	10	$r_{32} = t_{46}$	14	$t_{63} = g_{19} \oplus g_{18}$
1	$t_8 = x_5 \oplus x_6$	3	$r_{31} = t_7$	10	$r_{38} = t_{49}$	14	$t_{66} = g_{14} \oplus g_{26}$
1	$t_{13} = x_2 \oplus x_5$	3	$r_{39} = t_{15}$	10	$r_{50} = t_{46}$	15	$t_{54} = g_{29} \oplus g_{30}$
1	$t_{17} = x_2 \oplus x_6$	3	$r_{45} = t_{12}$	10	$r_{56} = t_{49}$	15	$t_{55} = g_{23} \oplus g_{24}$
1	$t_{19} = x_0 \oplus x_1$	3	$r_{49} = t_{21}$	11	$g_{11} = AND(r_{22}, r_{23})$	15	$t_{60} = g_{14} \oplus g_{15}$
1	$r_6 = t_0$	3	$r_{51} = t_{10}$	11	$g_{13} = AND(r_{26}, r_{27})$	15	$t_{62} = g_{20} \oplus g_{21}$
1	$r_{12} = t_1$	3	$r_{57} = t_{11}$	11	$g_{16} = AND(r_{32}, r_{33})$	15	$t_{64} = g_{16} \oplus t_{63}$
1	$r_{14} = t_2$	4	$g_1 = AND(r_2, r_3)$	11	$g_{19} = AND(r_{38}, r_{39})$	15	$t_{75} = t_{61} \oplus t_{66}$
1	$r_{16} = t_4$	4	$g_2 = AND(r_4, r_5)$	11	$g_{25} = AND(r_{50}, r_{51})$	15	$t_{76} = g_{21} \oplus g_{22}$
1	$r_{53} = t_0$	4	$g_5 = AND(r_{10}, r_{11})$	11	$g_{28} = AND(r_{56}, r_{57})$	15	$t_{80} = g_{26} \oplus t_{63}$
1	$r_{59} = t_1$	4	$g_8 = AND(r_{16}, r_{17})$	11	$t_{50} = t_{46} \oplus t_{49}$	15	$t_{83} = g_{31} \oplus t_{66}$
1	$r_{61} = t_2$	4	$t_{22} = g_7 \oplus g_4$	11	$t_{57} = t_{46} \oplus t_{52}$	15	$t_{88} = g_{25} \oplus g_{24}$
1	$r_{63} = t_4$	4	$t_{24} = t_{14} \oplus g_6$	11	$r_{40} = t_{50}$	15	$t_{90} = g_{30} \oplus t_{85}$
2	$t_3 = t_0 \oplus t_2$	4	$t_{26} = t_{16} \oplus g_7$	11	$r_{58} = t_{50}$	16	$t_{56} = t_{54} \oplus t_{55}$
2	$t_6 = t_1 \oplus t_5$	4	$t_{31} = g_0 \oplus t_{17}$	12	$g_{20} = AND(r_{40}, r_{41})$	16	$t_{65} = g_{27} \oplus t_{54}$
2	$t_9 = x_0 \oplus t_8$	5	$t_{23} = g_8 \oplus g_5$	12	$g_{29} = AND(r_{58}, r_{59})$	16	$t_{67} = t_{60} \oplus t_{62}$
2	$t_{14} = t_5 \oplus t_{13}$	5	$t_{25} = g_3 \oplus t_{24}$	12	$t_{45} = t_{40} \oplus g_{13}$	16	$t_{69} = t_{61} \oplus t_{62}$
2	$t_{16} = t_1 \oplus t_{13}$	5	$t_{27} = g_1 \oplus t_{26}$	12	$t_{48} = t_{33} \oplus g_{11}$	16	$t_{71} = t_{60} \oplus t_{61}$
2	$t_{18} = t_5 \oplus t_{17}$	5	$t_{28} = t_2 \oplus g_8$	12	$t_{53} = g_{11} \oplus t_{52}$	16	$t_{73} = g_{15} \oplus t_{64}$
2	$t_{20} = t_8 \oplus t_{19}$	5	$t_{32} = t_{24} \oplus t_{31}$	12	$t_{58} = g_{11} \oplus t_{57}$	16	$t_{78} = t_{64} \oplus t_{75}$
2	$r_0 = t_3$	5	$t_{39} = t_0 \oplus t_{22}$	12	$t_{77} = g_{16} \oplus g_{28}$	16	$t_{81} = t_{76} \oplus t_{80}$
2	$r_1 = t_6$	6	$t_{29} = g_2 \oplus t_{28}$	12	$r_{28} = t_{45}$	16	$t_{84} = t_{62} \oplus t_{83}$
2	$r_7 = t_{14}$	6	$t_{33} = t_{27} \oplus t_{32}$	12	$r_{34} = t_{48}$	16	$t_{86} = t_{76} \oplus t_{85}$
2	$r_8 = t_{20}$	6	$t_{35} = t_{23} \oplus t_{25}$	12	$r_{36} = t_{53}$	16	$t_{89} = t_{75} \oplus t_{76}$
2	$r_9 = t_9$	6	$t_{37} = x_1 \oplus t_{23}$	12	$r_{46} = t_{45}$	16	$t_{91} = t_{88} \oplus t_{90}$
2	$r_{13} = t_{18}$	6	$t_{40} = t_{25} \oplus t_{39}$	12	$r_{52} = t_{48}$	17	$t_{68} = t_{56} \oplus t_{67} \oplus 1$
2	$r_{15} = t_{16}$	6	$r_{18} = t_{33}$	12	$r_{54} = t_{53}$	17	$t_{70} = t_{56} \oplus t_{69}$
2	$r_{29} = t_6$	6	$r_{19} = t_{40}$	13	$g_{14} = AND(r_{28}, r_{29})$	17	$t_{72} = t_{56} \oplus t_{71}$
2	$r_{35} = t_{14}$	7	$g_9 = AND(r_{18}, r_{19})$	13	$g_{17} = AND(r_{34}, r_{35})$	17	$t_{74} = t_{56} \oplus t_{73}$
2	$r_{37} = t_9$	7	$t_{30} = t_{27} \oplus t_{29}$	13	$g_{18} = AND(r_{36}, r_{37})$	17	$t_{79} = t_{65} \oplus t_{78} \oplus 1$
2	$r_{41} = t_{18}$	7	$t_{34} = t_{29} \oplus t_{32}$	13	$g_{23} = AND(r_{46}, r_{47})$	17	$t_{82} = t_{65} \oplus t_{81} \oplus 1$
2	$r_{43} = t_{16}$	7	$t_{36} = x_7 \oplus t_{35}$	13	$g_{26} = AND(r_{52}, r_{53})$	17	$t_{87} = t_{84} \oplus t_{86} \oplus 1$
2	$r_{47} = t_3$	7	$t_{38} = t_{22} \oplus t_{37}$	13	$g_{27} = AND(r_{54}, r_{55})$	17	$t_{92} = t_{89} \oplus t_{91}$
2	$r_{55} = t_{20}$	7	$r_{20} = t_{30}$	13	$t_{47} = t_{45} \oplus t_{46}$	17	$\boldsymbol{y_0 = t_{79}}$
3	$g_0 = AND(r_0, r_1)$	7	$r_{22} = t_{34}$	13	$t_{51} = t_{45} \oplus t_{48}$	17	$\boldsymbol{y_1 = t_{82}}$
3	$g_3 = AND(r_6, r_7)$	7	$r_{24} = t_{38}$	13	$t_{59} = t_{45} \oplus t_{58}$	17	$\boldsymbol{y_2 = t_{92}}$
3	$g_4 = AND(r_8, r_9)$	7	$r_{26} = t_{36}$	13	$t_{85} = g_{29} \oplus t_{77}$	17	$\boldsymbol{y_3 = t_{74}}$
3	$g_6 = AND(r_{12}, r_{13})$	8	$t_{41} = t_{36} \oplus g_9$	13	$r_{30} = t_{47}$	17	$\boldsymbol{y_4 = t_{72}}$
3	$g_7 = AND(r_{14}, r_{15})$	8	$t_{43} = t_{34} \oplus g_9$	13	$r_{42} = t_{51}$	17	$\boldsymbol{y_5 = t_{87}}$
3	$t_7 = x_0 \oplus t_6$	8	$r_{21} = t_{41}$	13	$r_{44} = t_{59}$	17	$\boldsymbol{y_6 = t_{68}}$
3	$t_{10} = x_4 \oplus t_9$	8	$r_{25} = t_{43}$	13	$r_{48} = t_{47}$	17	$\boldsymbol{y_7 = t_{70}}$
3	$t_{11} = x_7 \oplus t_9$	9	$g_{10} = AND(r_{20}, r_{21})$	13	$r_{60} = t_{51}$		
3	$t_{12} = t_6 \oplus t_8$	9	$g_{12} = AND(r_{24}, r_{25})$	13	$r_{62} = t_{59}$		
3	$t_{15} = t_9 \oplus t_{14}$	10	$t_{42} = g_9 \oplus g_{10}$	14	$g_{15} = AND(r_{30}, r_{31})$		

Listing 19: New AES S-box circuit (D: 16, AD: 4, #NL: 33, #L: 101, #(gate): 134)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_5 = x_0$	3	$r_{33} = t_{13}$	9	$t_{38} = g_9 \oplus t_{37}$	13	$g_{15} = AND(r_{30}, r_{31})$
0	$r_{35} = x_0$	3	$r_{41} = t_{17}$	9	$t_{41} = g_9 \oplus t_{47}$	13	$g_{21} = AND(r_{42}, r_{43})$
1	$t_0 = x_1 \oplus x_7$	3	$r_{47} = t_{14}$	9	$t_{56} = t_{26} \oplus g_9$	13	$g_{22} = AND(r_{44}, r_{45})$
1	$t_1 = x_4 \oplus x_7$	3	$r_{53} = t_7$	9	$t_{59} = t_{29} \oplus g_9$	13	$g_{24} = AND(r_{48}, r_{49})$
1	$t_2 = x_2 \oplus x_4$	3	$r_{57} = t_9$	9	$r_{21} = t_{38}$	13	$g_{30} = AND(r_{60}, r_{61})$
1	$t_4 = x_2 \oplus x_7$	3	$r_{59} = t_{10}$	9	$r_{23} = t_{41}$	13	$g_{31} = AND(r_{62}, r_{63})$
1	$t_5 = x_5 \oplus x_6$	4	$g_2 = AND(r_4, r_5)$	10	$g_{10} = AND(r_{20}, r_{21})$	13	$t_{66} = g_{25} \oplus g_{18}$
1	$t_{11} = x_1 \oplus x_3$	4	$g_4 = AND(r_8, r_9)$	10	$g_{11} = AND(r_{22}, r_{23})$	13	$t_{68} = g_{17} \oplus g_{20}$
1	$t_{15} = x_2 \oplus x_5$	4	$g_5 = AND(r_{10}, r_{11})$	10	$t_{50} = t_{39} \oplus g_{14}$	13	$t_{69} = g_{28} \oplus g_{27}$
1	$t_{19} = x_2 \oplus x_6$	4	$g_8 = AND(r_{16}, r_{17})$	10	$t_{53} = t_{34} \oplus g_{13}$	13	$t_{82} = g_{17} \oplus g_{27}$
1	$r_6 = t_0$	4	$t_8 = t_3 \oplus t_7$	10	$t_{57} = g_{13} \oplus t_{56}$	13	$t_{83} = g_{29} \oplus g_{23}$
1	$r_{12} = t_1$	4	$t_{21} = g_7 \oplus g_6$	10	$t_{60} = g_{14} \oplus t_{59}$	13	$t_{93} = g_{26} \oplus g_{19}$
1	$r_{14} = t_2$	4	$t_{23} = g_0 \oplus t_{14}$	11	$t_{42} = t_{37} \oplus g_{11}$	14	$t_{63} = g_{30} \oplus g_{31}$
1	$r_{16} = t_4$	4	$t_{24} = t_{16} \oplus g_3$	11	$t_{43} = g_{10} \oplus t_{47}$	14	$t_{65} = g_{16} \oplus g_{24}$
1	$r_{55} = t_0$	4	$t_{35} = x_7 \oplus g_6$	11	$t_{51} = g_9 \oplus t_{50}$	14	$t_{67} = g_{21} \oplus g_{22}$
1	$r_{61} = t_1$	4	$t_{45} = t_4 \oplus g_6$	11	$t_{54} = g_9 \oplus t_{53}$	14	$t_{70} = g_{24} \oplus t_{66}$
1	$r_{63} = t_2$	4	$r_2 = t_8$	11	$t_{55} = t_{50} \oplus t_{53}$	14	$t_{73} = g_{15} \oplus t_{66}$
1	$r_{65} = t_4$	4	$r_{51} = t_8$	11	$t_{58} = g_{10} \oplus t_{57}$	14	$t_{74} = g_{25} \oplus t_{68}$
2	$t_3 = t_0 \oplus t_2$	5	$g_1 = AND(r_2, r_3)$	11	$t_{61} = g_{11} \oplus t_{60}$	14	$t_{84} = t_{82} \oplus t_{83}$
2	$t_6 = x_0 \oplus t_5$	5	$t_{25} = t_{21} \oplus t_{23}$	11	$r_{32} = t_{51}$	14	$t_{85} = g_{20} \oplus t_{69}$
2	$t_{12} = t_1 \oplus t_{11}$	5	$t_{27} = g_4 \oplus t_{24}$	11	$r_{34} = t_{42}$	14	$t_{86} = g_{23} \oplus g_{22}$
2	$t_{16} = t_{11} \oplus t_{15}$	5	$t_{30} = g_2 \oplus g_8$	11	$r_{36} = t_{58}$	14	$t_{89} = g_{30} \oplus g_{32}$
2	$t_{18} = t_1 \oplus t_{15}$	5	$t_{31} = g_8 \oplus g_5$	11	$r_{38} = t_{54}$	14	$t_{94} = g_{22} \oplus t_{93}$
2	$t_{20} = t_{11} \oplus t_{19}$	5	$t_{36} = t_{24} \oplus t_{35}$	11	$r_{40} = t_{43}$	14	$t_{97} = g_{25} \oplus g_{15}$
2	$r_0 = t_3$	5	$t_{46} = t_{23} \oplus t_{45}$	11	$r_{46} = t_{55}$	15	$t_{64} = g_{19} \oplus t_{63}$
2	$r_1 = t_{12}$	6	$t_{22} = g_1 \oplus t_{15}$	11	$r_{50} = t_{51}$	15	$t_{71} = t_{67} \oplus t_{70}$
2	$r_7 = t_{16}$	6	$t_{28} = t_0 \oplus t_{27}$	11	$r_{52} = t_{42}$	15	$t_{75} = t_{65} \oplus t_{74}$
2	$r_9 = t_6$	6	$t_{32} = t_4 \oplus t_{30}$	11	$r_{54} = t_{58}$	15	$t_{77} = t_{65} \oplus t_{73}$
2	$r_{13} = t_{20}$	6	$t_{37} = t_{31} \oplus t_{36}$	11	$r_{56} = t_{54}$	15	$t_{79} = t_{69} \oplus t_{74}$
2	$r_{15} = t_{18}$	6	$t_{47} = t_{30} \oplus t_{46}$	11	$r_{58} = t_{43}$	15	$t_{80} = t_{63} \oplus t_{73}$
2	$r_{31} = t_{12}$	6	$r_{24} = t_{47}$	11	$r_{64} = t_{55}$	15	$t_{87} = t_{85} \oplus t_{86}$
2	$r_{37} = t_{16}$	6	$r_{25} = t_{37}$	12	$g_{16} = AND(r_{32}, r_{33})$	15	$t_{90} = g_{15} \oplus t_{84}$
2	$r_{39} = t_6$	7	$g_{12} = AND(r_{24}, r_{25})$	12	$g_{17} = AND(r_{34}, r_{35})$	15	$t_{91} = g_{21} \oplus t_{89}$
2	$r_{43} = t_{20}$	7	$t_{26} = t_{22} \oplus t_{25}$	12	$g_{18} = AND(r_{36}, r_{37})$	15	$t_{95} = t_{84} \oplus t_{94}$
2	$r_{45} = t_{18}$	7	$t_{29} = t_{21} \oplus t_{28}$	12	$g_{19} = AND(r_{38}, r_{39})$	15	$t_{98} = t_{63} \oplus t_{67}$
2	$r_{49} = t_3$	7	$t_{33} = g_7 \oplus t_{32}$	12	$g_{20} = AND(r_{40}, r_{41})$	15	$t_{99} = t_{65} \oplus t_{97}$
3	$g_0 = AND(r_0, r_1)$	7	$r_{18} = t_{26}$	12	$g_{23} = AND(r_{46}, r_{47})$	16	$t_{72} = t_{64} \oplus t_{71}$
3	$g_3 = AND(r_6, r_7)$	7	$r_{19} = t_{29}$	12	$g_{25} = AND(r_{50}, r_{51})$	16	$t_{76} = t_{64} \oplus t_{75}$
3	$g_6 = AND(r_{12}, r_{13})$	7	$r_{26} = t_{26}$	12	$g_{26} = AND(r_{52}, r_{53})$	16	$t_{78} = t_{64} \oplus t_{77}$
3	$g_7 = AND(r_{14}, r_{15})$	7	$r_{28} = t_{29}$	12	$g_{27} = AND(r_{54}, r_{55})$	16	$t_{81} = t_{79} \oplus t_{80} \oplus 1$
3	$t_7 = x_4 \oplus t_6$	8	$g_9 = AND(r_{18}, r_{19})$	12	$g_{28} = AND(r_{56}, r_{57})$	16	$t_{88} = t_{64} \oplus t_{87} \oplus 1$
3	$t_9 = x_1 \oplus t_6$	8	$t_{34} = t_{22} \oplus t_{33}$	12	$g_{29} = AND(r_{58}, r_{59})$	16	$t_{92} = t_{90} \oplus t_{91} \oplus 1$
3	$t_{10} = x_7 \oplus t_6$	8	$t_{39} = t_{29} \oplus t_{37}$	12	$g_{32} = AND(r_{64}, r_{65})$	16	$t_{96} = t_{80} \oplus t_{95}$
3	$t_{13} = x_0 \oplus t_{12}$	8	$t_{40} = t_{25} \oplus t_{33}$	12	$t_{44} = t_{42} \oplus t_{43}$	16	$t_{100} = t_{98} \oplus t_{99} \oplus 1$
3	$t_{14} = t_5 \oplus t_{12}$	8	$t_{48} = t_{37} \oplus g_{12}$	12	$t_{52} = t_{42} \oplus t_{51}$	16	$\boldsymbol{y_0 = t_{81}}$
3	$t_{17} = t_6 \oplus t_{16}$	8	$t_{49} = t_{47} \oplus g_{12}$	12	$t_{62} = t_{58} \oplus t_{61}$	16	$\boldsymbol{y_1 = t_{88}}$
3	$r_3 = t_{13}$	8	$r_{20} = t_{34}$	12	$r_{30} = t_{61}$	16	$\boldsymbol{y_2 = t_{96}}$
3	$r_4 = t_7$	8	$r_{22} = t_{39}$	12	$r_{42} = t_{44}$	16	$\boldsymbol{y_3 = t_{76}}$
3	$r_8 = t_9$	8	$r_{27} = t_{48}$	12	$r_{44} = t_{62}$	16	$\boldsymbol{y_4 = t_{78}}$
3	$r_{10} = t_{10}$	8	$r_{29} = t_{49}$	12	$r_{48} = t_{61}$	16	$\boldsymbol{y_5 = t_{92}}$
3	$r_{11} = t_{17}$	9	$g_{13} = AND(r_{26}, r_{27})$	12	$r_{60} = t_{44}$	16	$\boldsymbol{y_6 = t_{100}}$
3	$r_{17} = t_{14}$	9	$g_{14} = AND(r_{28}, r_{29})$	12	$r_{62} = t_{62}$	16	$\boldsymbol{y_7 = t_{72}}$

Listing 20: New SNOW3G S-box circuit (D: 36, AD: 4, #NL: 90, #L: 366, #(gate): 456)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
1	$t_0 = x_2 \oplus x_3$	6	$t_{149} = t_{88} \oplus t_{91}$	12	$g_{25} = AND(t_{26}, t_{110})$	17	$t_{147} = g_{28} \oplus g_{31}$
1	$t_1 = x_4 \oplus x_5$	6	$t_{151} = t_{88} \oplus t_{93}$	12	$g_{27} = AND(t_{95}, t_{99})$	17	$t_{173} = t_{171} \oplus t_{172}$
1	$t_2 = x_6 \oplus x_7$	6	$t_{153} = t_{93} \oplus t_{94}$	12	$g_{35} = AND(t_{98}, t_{102})$	17	$t_{174} = t_{121} \oplus t_{124}$
1	$t_5 = x_4 \oplus x_6$	6	$t_{158} = t_{91} \oplus t_{94}$	12	$g_{42} = AND(t_{93}, t_{78})$	17	$t_{175} = t_{124} \oplus t_{164}$
1	$t_6 = x_1 \oplus x_2$	7	$g_7 = AND(t_{36}, t_{38})$	12	$t_{77} = t_{72} \oplus t_{76}$	17	$t_{176} = t_{114} \oplus t_{167}$
1	$t_7 = x_3 \oplus x_4$	7	$g_8 = AND(t_{40}, x_6)$	12	$t_{101} = t_{71} \oplus t_{78}$	17	$t_{181} = t_{145} \oplus t_{170}$
1	$t_8 = x_5 \oplus x_6$	7	$g_{12} = AND(t_{49}, t_{50})$	12	$t_{108} = t_{83} \oplus t_{85}$	17	$t_{188} = t_{177} \oplus t_{187}$
1	$t_{12} = x_3 \oplus x_5$	7	$t_{22} = t_{18} \oplus g_2$	12	$t_{111} = g_{23} \oplus g_{18}$	18	$t_{148} = t_{146} \oplus t_{147}$
1	$t_{86} = x_0 \oplus x_7$	7	$t_{24} = t_5 \oplus g_1$	12	$t_{119} = g_{24} \oplus g_{18}$	18	$t_{178} = t_{174} \oplus t_{173}$
2	$g_{15} = AND(t_5, t_8)$	7	$t_{32} = t_{27} \oplus g_5$	12	$t_{122} = g_{18} \oplus t_{115}$	18	$t_{179} = t_{139} \oplus t_{164}$
2	$t_3 = t_0 \oplus t_1$	7	$t_{34} = t_8 \oplus g_4$	12	$t_{152} = t_{75} \oplus t_{78}$	18	$t_{180} = t_{142} \oplus t_{167}$
2	$t_9 = x_7 \oplus t_6$	7	$t_{55} = t_{53} \oplus t_{54}$	12	$t_{160} = t_{78} \oplus t_{80}$	18	$t_{184} = t_{175} \oplus t_{183}$
2	$t_{10} = t_7 \oplus t_8$	7	$t_{57} = g_9 \oplus g_{11}$	12	$t_{161} = g_{44} \oplus g_{36}$	18	$t_{186} = t_{176} \oplus t_{185}$
2	$t_{13} = x_7 \oplus t_{12}$	7	$t_{61} = g_{15} \oplus g_9$	12	$t_{187} = t_5 \oplus t_{78}$	18	$t_{196} = t_{181} \oplus t_{195}$
2	$t_{16} = t_8 \oplus t_5$	7	$t_{62} = g_{10} \oplus g_{11}$	12	$t_{193} = t_{13} \oplus t_{83}$	19	$g_{45} = AND(t_{184}, t_{186})$
2	$t_{48} = t_8 \oplus x_7$	7	$t_{106} = t_{104} \oplus t_{105}$	13	$g_{33} = AND(t_{97}, t_{101})$	19	$g_{60} = AND(t_{188}, t_{196})$
2	$t_{49} = x_0 \oplus t_5$	7	$t_{125} = t_{95} \oplus t_{96}$	13	$g_{38} = AND(t_{91}, t_{77})$	19	$t_{182} = t_{148} \oplus t_{173}$
2	$t_{51} = t_5 \oplus t_2$	7	$t_{127} = t_{95} \oplus t_{97}$	13	$g_{39} = AND(t_{151}, t_{152})$	19	$t_{190} = t_{178} \oplus t_{189}$
2	$t_{87} = t_8 \oplus t_{86}$	7	$t_{129} = t_{97} \oplus t_{98}$	13	$g_{43} = AND(t_{153}, t_{160})$	19	$t_{192} = t_{179} \oplus t_{191}$
2	$t_{89} = x_7 \oplus t_2$	7	$t_{133} = t_{96} \oplus t_{98}$	13	$t_{100} = t_{83} \oplus t_{77}$	19	$t_{194} = t_{180} \oplus t_{193}$
3	$g_{16} = AND(t_{51}, t_{13})$	7	$t_{154} = t_{149} \oplus t_{153}$	13	$t_{109} = t_{107} \oplus t_{108}$	19	$t_{201} = t_{196} \oplus t_{188}$
3	$t_4 = t_2 \oplus t_3$	8	$g_{13} = AND(t_{52}, t_{55})$	13	$t_{112} = g_{20} \oplus g_{26}$	19	$t_{203} = t_{186} \oplus t_{188}$
3	$t_{11} = t_9 \oplus t_{10}$	8	$t_{23} = t_{21} \oplus t_{22}$	13	$t_{113} = g_{25} \oplus t_{111}$	19	$t_{204} = t_{184} \oplus t_{186}$
3	$t_{26} = t_{13} \oplus t_8$	8	$t_{25} = g_2 \oplus t_{24}$	13	$t_{116} = g_{18} \oplus g_{20}$	19	$t_{206} = t_{188} \oplus t_{184}$
3	$t_{47} = t_{13} \oplus x_7$	8	$t_{33} = t_{31} \oplus t_{32}$	13	$t_{117} = t_{115} \oplus g_{25}$	19	$t_{236} = t_{184} \oplus t_{188}$
3	$t_{88} = t_{51} \oplus t_{87}$	8	$t_{35} = g_5 \oplus t_{34}$	13	$t_{120} = g_{21} \oplus t_{119}$	20	$g_{48} = AND(t_{192}, t_{194})$
4	$g_0 = AND(x_0, t_4)$	8	$t_{42} = t_{37} \oplus g_8$	13	$t_{128} = t_{99} \oplus t_{101}$	20	$t_{198} = t_{182} \oplus t_{197}$
4	$g_3 = AND(t_{11}, t_{13})$	8	$t_{44} = t_{16} \oplus g_7$	13	$t_{135} = t_{101} \oplus t_{102}$	20	$t_{199} = t_{192} \oplus t_{184}$
4	$g_{11} = AND(t_4, t_{48})$	8	$t_{59} = g_{16} \oplus t_{57}$	13	$t_{136} = g_{27} \oplus g_{35}$	20	$t_{200} = t_{194} \oplus t_{186}$
4	$g_{17} = AND(t_2, t_{26})$	8	$t_{63} = g_{16} \oplus t_{61}$	13	$t_{150} = t_{75} \oplus t_{77}$	20	$t_{205} = t_{190} \oplus t_{204}$
4	$t_{14} = t_{11} \oplus x_0$	8	$t_{66} = g_{12} \oplus t_{61}$	13	$t_{156} = t_{78} \oplus t_{77}$	20	$t_{207} = t_{186} \oplus t_{206}$
4	$t_{15} = t_{13} \oplus t_4$	8	$t_{68} = g_{10} \oplus g_{12}$	13	$t_{159} = t_{77} \oplus t_{80}$	20	$t_{208} = t_{190} \oplus g_{45}$
4	$t_{17} = t_4 \oplus t_5$	8	$t_{130} = t_{125} \oplus t_{129}$	13	$t_{165} = g_{36} \oplus g_{42}$	20	$t_{213} = t_{194} \oplus t_{196}$
4	$t_{18} = x_0 \oplus t_4$	9	$g_{23} = AND(t_8, t_{33})$	13	$t_{185} = t_4 \oplus t_{77}$	20	$t_{214} = t_{192} \oplus t_{194}$
4	$t_{27} = x_7 \oplus t_{11}$	9	$t_{43} = t_{41} \oplus t_{42}$	14	$g_{22} = AND(t_{106}, t_{109})$	20	$t_{216} = t_{196} \oplus t_{192}$
4	$t_{29} = t_{11} \oplus t_{13}$	9	$t_{45} = g_8 \oplus t_{44}$	14	$g_{29} = AND(t_{96}, t_{100})$	20	$t_{238} = t_{186} \oplus t_{190}$
4	$t_{54} = t_{48} \oplus t_{26}$	9	$t_{60} = t_{58} \oplus t_{59}$	14	$g_{30} = AND(t_{127}, t_{128})$	20	$t_{243} = t_{188} \oplus t_{190}$
4	$t_{56} = t_4 \oplus t_2$	9	$t_{64} = t_{62} \oplus t_{63}$	14	$g_{34} = AND(t_{129}, t_{135})$	20	$t_{273} = t_{190} \oplus t_{196}$
4	$t_{90} = t_{11} \oplus t_8$	9	$t_{67} = t_{65} \oplus t_{66}$	14	$g_{37} = AND(t_{149}, t_{150})$	20	$t_{279} = t_{196} \oplus t_{194}$
4	$t_{92} = x_7 \oplus t_4$	9	$t_{69} = g_{13} \oplus t_{61}$	14	$g_{41} = AND(t_{158}, t_{159})$	21	$g_{46} = AND(t_{203}, t_{205})$
4	$t_{94} = t_{51} \oplus t_{26}$	9	$t_{71} = t_{33} \oplus t_{35}$	14	$t_{114} = t_{112} \oplus t_{113}$	21	$g_{47} = AND(t_{207}, t_{190})$
4	$t_{105} = t_{47} \oplus t_{48}$	9	$t_{74} = t_{23} \oplus t_{35}$	14	$t_{118} = t_{116} \oplus t_{117}$	21	$g_{51} = AND(t_{199}, t_{200})$
5	$g_6 = AND(t_{14}, t_{15})$	9	$t_{76} = t_{25} \oplus t_{33}$	14	$t_{121} = t_{112} \oplus t_{120}$	21	$g_{61} = AND(t_{243}, t_{194})$
5	$g_{14} = AND(t_{56}, t_{47})$	9	$t_{79} = t_{25} \oplus t_{35}$	14	$t_{126} = t_{99} \oplus t_{100}$	21	$g_{62} = AND(t_{190}, t_{213})$
5	$t_{19} = t_2 \oplus t_{18}$	9	$t_{84} = t_{35} \oplus t_{25}$	14	$t_{131} = t_{102} \oplus t_{100}$	21	$t_{202} = t_{198} \oplus t_{190}$
5	$t_{20} = t_5 \oplus t_{18}$	10	$g_{19} = AND(t_{55}, t_{67})$	14	$t_{134} = t_{100} \oplus t_{102}$	21	$t_{215} = t_{198} \oplus t_{214}$
5	$t_{21} = t_2 \oplus g_0$	10	$g_{24} = AND(t_{47}, t_{71})$	14	$t_{140} = g_{27} \oplus g_{33}$	21	$t_{217} = t_{194} \oplus t_{216}$
5	$t_{28} = t_{13} \oplus t_{27}$	10	$t_{70} = t_{68} \oplus t_{69}$	14	$t_{157} = t_{155} \oplus t_{156}$	21	$t_{218} = t_{198} \oplus g_{48}$
5	$t_{30} = t_8 \oplus t_{29}$	10	$t_{73} = t_{60} \oplus t_{64}$	14	$t_{162} = g_{38} \oplus g_{43}$	21	$t_{223} = t_{200} \oplus t_{201}$
5	$t_{31} = t_{13} \oplus g_3$	10	$t_{75} = t_{67} \oplus t_{74}$	14	$t_{168} = g_{42} \oplus g_{38}$	21	$t_{224} = t_{199} \oplus t_{200}$
5	$t_{36} = t_{15} \oplus t_{16}$	10	$t_{80} = t_{64} \oplus t_{79}$	14	$t_{169} = g_{39} \oplus t_{161}$	21	$t_{226} = t_{201} \oplus t_{199}$
5	$t_{37} = x_6 \oplus t_{14}$	10	$t_{81} = t_{43} \oplus t_{23}$	14	$t_{171} = g_{39} \oplus t_{165}$	21	$t_{233} = t_{198} \oplus t_{216}$
5	$t_{39} = t_{14} \oplus t_{15}$	10	$t_{82} = t_{25} \oplus t_{45}$	15	$g_{28} = AND(t_{125}, t_{126})$	21	$t_{234} = t_{194} \oplus t_{198}$
5	$t_{46} = t_8 \oplus t_{27}$	10	$t_{85} = t_{45} \oplus t_{84}$	15	$g_{32} = AND(t_{133}, t_{134})$	21	$t_{235} = t_{196} \oplus t_{198}$
5	$t_{52} = t_{18} \oplus t_{51}$	10	$t_{195} = t_8 \oplus t_{71}$	15	$g_{40} = AND(t_{154}, t_{157})$	21	$t_{239} = t_{206} \oplus t_{238}$
5	$t_{65} = g_{11} \oplus g_{17}$	11	$g_{18} = AND(t_{46}, t_{81})$	15	$t_{123} = g_{21} \oplus g_{22}$	21	$t_{274} = t_{198} \oplus t_{206}$
5	$t_{91} = t_{89} \oplus t_{90}$	11	$g_{26} = AND(t_{48}, t_{85})$	15	$t_{132} = t_{128} \oplus t_{131}$	21	$t_{276} = t_{192} \oplus t_{198}$
5	$t_{93} = t_2 \oplus t_{92}$	11	$g_{36} = AND(t_{88}, t_{75})$	15	$t_{137} = g_{29} \oplus g_{34}$	21	$t_{278} = t_{198} \oplus t_{238}$
5	$t_{98} = t_{48} \oplus t_{94}$	11	$g_{44} = AND(t_{94}, t_{80})$	15	$t_{143} = g_{35} \oplus g_{29}$	21	$t_{280} = t_{243} \oplus t_{279}$
6	$g_1 = AND(t_{17}, t_{19})$	11	$t_{72} = t_{60} \oplus t_{70}$	15	$t_{144} = g_{30} \oplus t_{140}$	22	$g_{49} = AND(t_{213}, t_{215})$
6	$g_2 = AND(t_{20}, t_2)$	11	$t_{78} = t_{35} \oplus t_{73}$	15	$t_{146} = g_{30} \oplus t_{140}$	22	$g_{50} = AND(t_{217}, t_{198})$
6	$g_4 = AND(t_{26}, t_{28})$	11	$t_{83} = t_{71} \oplus t_{82}$	15	$t_{163} = t_{161} \oplus g_{41}$	22	$g_{54} = AND(t_{184}, t_{215})$
6	$g_5 = AND(t_{30}, x_7)$	11	$t_{99} = t_{81} \oplus t_{75}$	15	$t_{166} = t_{165} \oplus g_{37}$	22	$g_{55} = AND(t_{204}, t_{217})$
6	$g_9 = AND(x_0, t_{28})$	11	$t_{102} = t_{85} \oplus t_{80}$	15	$t_{170} = t_{168} \oplus t_{169}$	22	$g_{56} = AND(t_{186}, t_{235})$
6	$g_{10} = AND(t_{18}, t_{30})$	11	$t_{103} = t_{81} \oplus t_{71}$	16	$g_{31} = AND(t_{130}, t_{132})$	22	$g_{59} = AND(t_{238}, t_{234})$
6	$t_{38} = t_{15} \oplus t_{37}$	11	$t_{107} = t_{71} \oplus t_{81}$	16	$t_{124} = t_{122} \oplus t_{123}$	22	$t_{209} = t_{204} \oplus g_{47}$
6	$t_{40} = t_{16} \oplus t_{39}$	11	$t_{110} = t_{71} \oplus t_{85}$	16	$t_{138} = t_{136} \oplus g_{32}$	22	$t_{211} = t_{188} \oplus g_{46}$
6	$t_{41} = t_{15} \oplus g_6$	11	$t_{115} = g_{19} \oplus g_{24}$	16	$t_{141} = t_{140} \oplus g_{28}$	22	$t_{225} = t_{202} \oplus t_{224}$
6	$t_{50} = t_{28} \oplus t_8$	11	$t_{155} = t_{80} \oplus t_{75}$	16	$t_{145} = t_{143} \oplus t_{144}$	22	$t_{227} = t_{200} \oplus t_{226}$
6	$t_{53} = t_8 \oplus t_{28}$	11	$t_{183} = x_0 \oplus t_{75}$	16	$t_{164} = t_{162} \oplus t_{163}$	22	$t_{228} = t_{202} \oplus g_{51}$
6	$t_{58} = g_{14} \oplus g_{17}$	11	$t_{189} = t_2 \oplus t_{80}$	16	$t_{167} = t_{162} \oplus t_{166}$	22	$t_{237} = t_{215} \oplus t_{196}$
6	$t_{95} = t_{46} \oplus t_{88}$	11	$t_{191} = t_{11} \oplus t_{81}$	16	$t_{172} = g_{37} \oplus g_{40}$	22	$t_{240} = t_{196} \oplus t_{215}$
6	$t_{96} = x_7 \oplus t_{91}$	11	$t_{197} = x_7 \oplus t_{85}$	16	$t_{177} = t_{118} \oplus t_{170}$	22	$t_{241} = t_{235} \oplus t_{213}$
6	$t_{97} = t_{47} \oplus t_{93}$	12	$g_{20} = AND(x_7, t_{83})$	17	$t_{139} = t_{137} \oplus t_{138}$	22	$t_{248} = g_{60} \oplus g_{61}$
6	$t_{104} = x_7 \oplus t_{46}$	12	$g_{21} = AND(t_{30}, t_{103})$	17	$t_{142} = t_{137} \oplus t_{141}$	22	$t_{275} = t_{273} \oplus t_{274}$

Listing 20: New SNOW3G S-box circuit (continued) (D: 36, AD: 4, #NL: 90, #L: 366, #(gate): 456)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
22	$t_{277} = t_{273} \oplus t_{276}$	25	$t_{262} = t_{210} \oplus t_{222}$	28	$t_{373} = t_{188} \oplus t_{266}$	31	$t_{332} = g_{75} \oplus t_{326}$
22	$t_{283} = t_{234} \oplus t_{278}$	25	$t_{264} = t_{212} \oplus t_{220}$	28	$t_{379} = t_{194} \oplus t_{271}$	31	$t_{349} = t_{347} \oplus g_{86}$
22	$t_{284} = t_{235} \oplus t_{280}$	25	$t_{267} = t_{212} \oplus t_{222}$	29	$g_{78} = AND(t_{283}, t_{287})$	31	$t_{352} = t_{351} \oplus g_{82}$
22	$t_{290} = t_{198} \oplus t_{233}$	25	$t_{316} = t_{311} \oplus t_{315}$	29	$g_{83} = AND(t_{277}, t_{265})$	31	$t_{356} = t_{354} \oplus t_{355}$
22	$t_{291} = t_{234} \oplus t_{235}$	26	$g_{64} = AND(t_{242}, t_{255})$	29	$g_{84} = AND(t_{337}, t_{338})$	32	$g_{76} = AND(t_{316}, t_{318})$
22	$t_{339} = t_{278} \oplus t_{280}$	26	$g_{69} = AND(t_{234}, t_{259})$	29	$g_{88} = AND(t_{339}, t_{346})$	32	$t_{310} = t_{308} \oplus t_{309}$
23	$g_{52} = AND(t_{223}, t_{225})$	26	$t_{258} = t_{256} \oplus t_{257}$	29	$t_{286} = t_{271} \oplus t_{265}$	32	$t_{324} = t_{322} \oplus g_{77}$
23	$g_{53} = AND(t_{227}, t_{202})$	26	$t_{261} = t_{247} \oplus t_{251}$	29	$t_{295} = t_{293} \oplus t_{294}$	32	$t_{327} = t_{326} \oplus g_{73}$
23	$g_{57} = AND(t_{236}, t_{237})$	26	$t_{263} = t_{255} \oplus t_{262}$	29	$t_{298} = g_{65} \oplus g_{71}$	32	$t_{331} = t_{329} \oplus t_{330}$
23	$t_{210} = t_{208} \oplus t_{209}$	26	$t_{268} = t_{251} \oplus t_{267}$	29	$t_{299} = g_{70} \oplus t_{297}$	32	$t_{350} = t_{348} \oplus t_{349}$
23	$t_{212} = g_{47} \oplus t_{211}$	26	$t_{269} = t_{230} \oplus t_{210}$	29	$t_{302} = g_{63} \oplus g_{65}$	32	$t_{353} = t_{348} \oplus t_{352}$
23	$t_{219} = t_{214} \oplus g_{50}$	26	$t_{270} = t_{212} \oplus t_{232}$	29	$t_{303} = t_{301} \oplus g_{70}$	32	$t_{358} = g_{82} \oplus g_{85}$
23	$t_{221} = t_{196} \oplus g_{49}$	26	$t_{272} = t_{232} \oplus t_{267}$	29	$t_{306} = g_{66} \oplus t_{305}$	32	$t_{363} = t_{304} \oplus t_{356}$
23	$t_{242} = t_{240} \oplus t_{241}$	26	$t_{381} = t_{196} \oplus t_{259}$	29	$t_{314} = t_{285} \oplus t_{287}$	33	$t_{325} = t_{323} \oplus t_{324}$
23	$t_{244} = g_{61} \oplus g_{54}$	27	$g_{63} = AND(t_{233}, t_{269})$	29	$t_{321} = t_{287} \oplus t_{288}$	33	$t_{328} = t_{323} \oplus t_{327}$
23	$t_{245} = g_{56} \oplus g_{59}$	27	$g_{71} = AND(t_{235}, t_{272})$	29	$t_{322} = g_{72} \oplus g_{80}$	33	$t_{333} = g_{73} \oplus g_{76}$
23	$t_{249} = g_{54} \oplus g_{55}$	27	$g_{81} = AND(t_{275}, t_{263})$	29	$t_{336} = t_{263} \oplus t_{265}$	33	$t_{359} = t_{357} \oplus t_{358}$
23	$t_{250} = g_{56} \oplus t_{248}$	27	$g_{89} = AND(t_{280}, t_{268})$	29	$t_{342} = t_{266} \oplus t_{265}$	33	$t_{360} = t_{307} \oplus t_{310}$
23	$t_{252} = g_{60} \oplus g_{54}$	27	$t_{260} = t_{247} \oplus t_{258}$	29	$t_{345} = t_{265} \oplus t_{268}$	33	$t_{361} = t_{310} \oplus t_{350}$
23	$t_{253} = g_{56} \oplus g_{62}$	27	$t_{266} = t_{222} \oplus t_{261}$	29	$t_{351} = g_{81} \oplus g_{87}$	33	$t_{362} = t_{300} \oplus t_{353}$
23	$t_{281} = t_{233} \oplus t_{275}$	27	$t_{271} = t_{259} \oplus t_{270}$	29	$t_{371} = t_{186} \oplus t_{265}$	33	$t_{367} = t_{331} \oplus t_{356}$
23	$t_{282} = t_{198} \oplus t_{277}$	27	$t_{285} = t_{269} \oplus t_{263}$	30	$g_{67} = AND(t_{292}, t_{295})$	33	$t_{374} = t_{363} \oplus t_{373}$
23	$t_{292} = t_{290} \oplus t_{291}$	27	$t_{288} = t_{272} \oplus t_{268}$	30	$g_{74} = AND(t_{282}, t_{286})$	34	$t_{334} = t_{332} \oplus t_{333}$
23	$t_{315} = t_{283} \oplus t_{284}$	27	$t_{289} = t_{269} \oplus t_{259}$	30	$g_{75} = AND(t_{313}, t_{314})$	34	$t_{364} = t_{360} \oplus t_{359}$
23	$t_{335} = t_{275} \oplus t_{277}$	27	$t_{293} = t_{259} \oplus t_{269}$	30	$g_{79} = AND(t_{315}, t_{321})$	34	$t_{365} = t_{325} \oplus t_{350}$
23	$t_{337} = t_{275} \oplus t_{278}$	27	$t_{296} = t_{259} \oplus t_{272}$	30	$g_{82} = AND(t_{335}, t_{336})$	34	$t_{366} = t_{328} \oplus t_{353}$
23	$t_{344} = t_{277} \oplus t_{280}$	27	$t_{301} = g_{64} \oplus g_{69}$	30	$g_{86} = AND(t_{344}, t_{345})$	34	$t_{370} = t_{361} \oplus t_{369}$
24	$g_{58} = AND(t_{239}, t_{242})$	27	$t_{341} = t_{268} \oplus t_{263}$	30	$t_{300} = t_{298} \oplus t_{299}$	34	$t_{372} = t_{362} \oplus t_{371} \oplus 1$
24	$t_{220} = t_{218} \oplus t_{219}$	27	$t_{369} = t_{184} \oplus t_{263}$	30	$t_{304} = t_{302} \oplus t_{303}$	34	$t_{382} = t_{367} \oplus t_{381}$
24	$t_{222} = g_{50} \oplus t_{221}$	27	$t_{375} = t_{190} \oplus t_{268}$	30	$t_{307} = t_{298} \oplus t_{306}$	34	$\boldsymbol{y_0 = t_{370}}$
24	$t_{229} = t_{224} \oplus g_{53}$	27	$t_{377} = t_{192} \oplus t_{269}$	30	$t_{312} = t_{285} \oplus t_{286}$	34	$\boldsymbol{y_1 = t_{372}}$
24	$t_{231} = t_{201} \oplus g_{52}$	27	$t_{383} = t_{198} \oplus t_{272}$	30	$t_{317} = t_{288} \oplus t_{286}$	35	$t_{368} = t_{334} \oplus t_{359}$
24	$t_{246} = g_{62} \oplus t_{244}$	28	$g_{65} = AND(t_{198}, t_{271})$	30	$t_{320} = t_{286} \oplus t_{288}$	35	$t_{376} = t_{364} \oplus t_{375} \oplus 1$
24	$t_{251} = t_{249} \oplus t_{250}$	28	$g_{66} = AND(t_{217}, t_{289})$	30	$t_{326} = g_{72} \oplus g_{78}$	35	$t_{378} = t_{365} \oplus t_{377}$
24	$t_{254} = g_{57} \oplus t_{252}$	28	$g_{70} = AND(t_{213}, t_{296})$	30	$t_{343} = t_{341} \oplus t_{342}$	35	$t_{380} = t_{366} \oplus t_{379}$
24	$t_{256} = g_{55} \oplus g_{57}$	28	$g_{72} = AND(t_{281}, t_{285})$	30	$t_{348} = g_{83} \oplus g_{88}$	35	$t_{385} = t_{374} \oplus t_{372} \oplus 1$
24	$t_{311} = t_{281} \oplus t_{282}$	28	$g_{80} = AND(t_{284}, t_{288})$	30	$t_{354} = g_{87} \oplus g_{83}$	35	$\boldsymbol{y_2 = t_{380} \oplus 1}$
24	$t_{313} = t_{281} \oplus t_{283}$	28	$g_{87} = AND(t_{278}, t_{266})$	30	$t_{355} = g_{84} \oplus t_{347}$	35	$\boldsymbol{y_3 = t_{380} \oplus 1}$
24	$t_{319} = t_{282} \oplus t_{284}$	28	$t_{265} = t_{260} \oplus t_{264}$	30	$t_{357} = g_{84} \oplus t_{351}$	35	$\boldsymbol{y_6 = t_{376}}$
24	$t_{340} = t_{335} \oplus t_{339}$	28	$t_{287} = t_{259} \oplus t_{266}$	31	$g_{73} = AND(t_{311}, t_{312})$	36	$t_{384} = t_{368} \oplus t_{383}$
25	$g_{68} = AND(t_{196}, t_{220})$	28	$t_{294} = t_{271} \oplus t_{272}$	31	$g_{77} = AND(t_{319}, t_{320})$	36	$t_{386} = t_{376} \oplus t_{382} \oplus 1$
25	$t_{230} = t_{228} \oplus t_{229}$	28	$t_{297} = g_{68} \oplus g_{63}$	31	$g_{85} = AND(t_{340}, t_{343})$	36	$t_{387} = t_{374} \oplus t_{376} \oplus 1$
25	$t_{232} = g_{53} \oplus t_{231}$	28	$t_{305} = g_{69} \oplus g_{63}$	31	$t_{309} = g_{66} \oplus g_{67}$	36	$\boldsymbol{y_4 = t_{384} \oplus 1}$
25	$t_{247} = t_{245} \oplus t_{246}$	28	$t_{308} = g_{63} \oplus t_{301}$	31	$t_{318} = t_{314} \oplus t_{317}$	36	$\boldsymbol{y_5 = t_{384} \oplus 1}$
25	$t_{255} = t_{253} \oplus t_{254}$	28	$t_{338} = t_{263} \oplus t_{266}$	31	$t_{323} = g_{74} \oplus g_{79}$	36	$\boldsymbol{y_7 = t_{384}}$
25	$t_{257} = g_{58} \oplus t_{252}$	28	$t_{346} = t_{266} \oplus t_{268}$	31	$t_{329} = g_{80} \oplus g_{74}$		
25	$t_{259} = t_{220} \oplus t_{222}$	28	$t_{347} = g_{89} \oplus g_{81}$	31	$t_{330} = g_{75} \oplus t_{326}$		

Listing 21: New SNOW3G S-box circuit (D: 24, AD: 4, #NL: 90, #L: 533, #(gate): 623)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_0 = x_0$	3	$t_{39} = t_{12} \oplus t_{34}$	4	$r_{76} = t_{68}$	7	$t_{86} = t_{48} \oplus t_{83}$
0	$r_{11} = x_7$	3	$t_{40} = x_3 \oplus t_{16}$	4	$r_{78} = t_{69}$	7	$t_{94} = t_{52} \oplus t_{80}$
0	$r_{17} = x_6$	3	$t_{46} = t_{18} \oplus t_{43}$	5	$g_3 = AND(r_6, r_7)$	7	$t_{95} = g_9 \oplus t_{53}$
0	$r_{18} = x_0$	3	$t_{54} = t_1 \oplus t_{16}$	5	$t_{22} = g_4 \oplus t_{16}$	7	$t_{99} = t_{93} \oplus t_{98}$
0	$r_{40} = x_7$	3	$t_{55} = x_1 \oplus t_6$	5	$t_{33} = g_{11} \oplus g_8$	7	$t_{105} = t_{43} \oplus t_{97}$
1	$t_0 = x_2 \oplus x_4$	3	$t_{60} = t_5 \oplus t_{16}$	5	$t_{37} = t_{23} \oplus g_{12}$	7	$t_{107} = t_{36} \oplus t_{85}$
1	$t_1 = x_3 \oplus x_7$	3	$t_{62} = t_{16} \oplus t_{18}$	5	$t_{38} = g_4 \oplus g_9$	7	$t_{111} = t_{48} \oplus t_{110}$
1	$t_2 = x_6 \oplus x_7$	3	$t_{66} = x_5 \oplus t_{34}$	5	$t_{41} = t_{19} \oplus g_{13}$	7	$t_{120} = g_4 \oplus t_{109}$
1	$t_{10} = x_0 \oplus x_1$	3	$t_{70} = t_2 \oplus t_{18}$	5	$t_{42} = t_{32} \oplus g_{12}$	7	$t_{123} = t_{50} \oplus t_{122}$
1	$t_{11} = x_3 \oplus x_5$	3	$t_{71} = x_2 \oplus t_{65}$	5	$t_{44} = g_{11} \oplus g_{15}$	7	$t_{126} = t_{117} \oplus t_{125}$
1	$t_{13} = x_1 \oplus x_7$	3	$t_{72} = x_2 \oplus t_9$	5	$t_{47} = g_4 \oplus t_{19}$	7	$t_{129} = t_{80} \oplus t_{128}$
1	$t_{15} = x_4 \oplus x_5$	3	$t_{88} = t_{18} \oplus t_{87}$	5	$t_{51} = g_{17} \oplus g_9$	7	$t_{133} = t_{16} \oplus t_{110}$
1	$t_{26} = x_4 \oplus x_6$	3	$t_{91} = t_3 \oplus t_{90}$	5	$t_{52} = g_1 \oplus g_{16}$	7	$t_{134} = t_{89} \oplus t_{132}$
1	$t_{43} = x_5 \oplus x_6$	3	$t_{114} = t_5 \oplus t_{113}$	5	$t_{57} = g_0 \oplus t_{45}$	7	$t_{137} = t_{117} \oplus t_{136}$
1	$t_{49} = x_4 \oplus x_7$	3	$t_{148} = t_{43} \oplus g_{15}$	5	$t_{77} = g_7 \oplus g_{16}$	7	$t_{140} = t_{43} \oplus t_{56}$
1	$t_{74} = x_1 \oplus x_5$	3	$r_1 = t_7$	5	$t_{78} = g_{11} \oplus g_{12}$	7	$t_{144} = t_{109} \oplus t_{143}$
1	$t_{90} = x_0 \oplus x_2$	3	$r_2 = t_4$	5	$t_{92} = g_8 \oplus g_2$	7	$t_{160} = t_{69} \oplus t_{122}$
1	$r_5 = t_2$	3	$r_3 = t_{25}$	5	$t_{98} = t_{14} \oplus g_6$	7	$t_{164} = t_{162} \oplus t_{163}$
1	$r_{29} = t_{11}$	3	$r_4 = t_{91}$	5	$t_{102} = t_{85} \oplus g_2$	7	$t_{172} = t_{132} \oplus t_{171}$
1	$r_{30} = t_{26}$	3	$r_9 = t_{14}$	5	$t_{108} = g_{13} \oplus g_2$	7	$t_{176} = t_{110} \oplus t_{175}$
1	$r_{31} = t_{43}$	3	$r_{12} = t_{88}$	5	$t_{115} = g_9 \oplus g_{10}$	7	$t_{181} = g_0 \oplus t_{180}$
1	$r_{32} = t_{49}$	3	$r_{14} = t_{30}$	5	$t_{116} = t_{32} \oplus g_{10}$	7	$t_{190} = t_{187} \oplus t_{189}$
1	$r_{34} = t_2$	3	$r_{15} = t_{46}$	5	$t_{119} = t_4 \oplus g_{10}$	7	$t_{198} = t_{96} \oplus t_{104}$
1	$r_{46} = t_{43}$	3	$r_{16} = t_{31}$	5	$t_{124} = t_{15} \oplus g_8$	7	$t_{215} = t_{52} \oplus t_{97}$
1	$r_{48} = t_{11}$	3	$r_{19} = t_{14}$	5	$t_{136} = t_{15} \oplus g_2$	7	$t_{219} = t_{96} \oplus t_{218}$
2	$g_{15} = AND(r_{30}, r_{31})$	3	$r_{20} = t_{114}$	5	$t_{150} = g_0 \oplus g_2$	7	$t_{220} = t_3 \oplus t_{80}$
2	$t_3 = x_5 \oplus t_1$	3	$r_{22} = t_7$	5	$t_{151} = g_4 \oplus t_{149}$	7	$t_{222} = t_{80} \oplus t_{221}$
2	$t_5 = x_3 \oplus t_2$	3	$r_{25} = t_{19}$	5	$t_{170} = t_{25} \oplus g_{13}$	7	$t_{228} = t_{96} \oplus t_{227}$
2	$t_6 = x_6 \oplus t_0$	3	$r_{26} = t_{39}$	5	$t_{178} = t_{85} \oplus t_{177}$	7	$r_{37} = t_{99}$
2	$t_9 = x_5 \oplus t_2$	3	$r_{27} = t_{40}$	5	$t_{188} = g_6 \oplus t_{179}$	7	$r_{55} = t_{219}$
2	$t_{12} = t_0 \oplus t_{11}$	3	$r_{36} = t_{54}$	5	$t_{217} = g_8 \oplus g_6$	7	$r_{57} = t_{190}$
2	$t_{16} = t_0 \oplus t_{13}$	3	$r_{38} = t_{40}$	5	$t_{226} = t_{149} \oplus t_{225}$	7	$r_{65} = t_{86}$
2	$t_{18} = t_1 \oplus t_{10}$	3	$r_{44} = t_{55}$	6	$t_{24} = g_0 \oplus g_3$	7	$r_{67} = t_{129}$
2	$t_{27} = x_2 \oplus t_{13}$	3	$r_{58} = t_{60}$	6	$t_{35} = g_3 \oplus g_{14}$	7	$r_{71} = t_{126}$
2	$t_{34} = x_0 \oplus t_{26}$	3	$r_{62} = t_{62}$	6	$t_{36} = g_3 \oplus t_{27}$	7	$r_{73} = t_{228}$
2	$t_{59} = x_0 \oplus t_{15}$	3	$r_{72} = t_{66}$	6	$t_{48} = t_{41} \oplus t_{42}$	7	$r_{79} = t_{164}$
2	$t_{63} = x_2 \oplus t_{49}$	3	$r_{80} = t_{70}$	6	$t_{50} = t_{42} \oplus t_{44}$	7	$r_{83} = t_{111}$
2	$t_{64} = x_2 \oplus t_{11}$	3	$r_{84} = t_{71}$	6	$t_{53} = t_{26} \oplus t_{44}$	8	$g_{18} = AND(r_{36}, r_{37})$
2	$t_{65} = t_1 \oplus t_{15}$	3	$r_{86} = t_{72}$	6	$t_{56} = g_3 \oplus t_{47}$	8	$g_{27} = AND(r_{54}, r_{55})$
2	$t_{73} = x_3 \oplus t_{26}$	4	$g_0 = AND(r_0, r_1)$	6	$t_{80} = g_3 \oplus t_{79}$	8	$g_{28} = AND(r_{56}, r_{57})$
2	$t_{75} = t_0 \oplus t_{74}$	4	$g_1 = AND(r_2, r_3)$	6	$t_{83} = t_{38} \oplus t_{79}$	8	$g_{32} = AND(r_{64}, r_{65})$
2	$t_{87} = t_0 \oplus t_{43}$	4	$g_2 = AND(r_4, r_5)$	6	$t_{84} = t_{20} \oplus t_{51}$	8	$g_{33} = AND(r_{66}, r_{67})$
2	$t_{113} = t_{15} \oplus t_{90}$	4	$g_4 = AND(r_8, r_9)$	6	$t_{89} = t_{33} \oplus t_{37}$	8	$g_{35} = AND(r_{70}, r_{71})$
2	$r_7 = t_3$	4	$g_6 = AND(r_{12}, r_{13})$	6	$t_{93} = g_0 \oplus t_{92}$	8	$g_{36} = AND(r_{72}, r_{73})$
2	$r_8 = t_5$	4	$g_7 = AND(r_{14}, r_{15})$	6	$t_{96} = t_{38} \oplus t_{78}$	8	$g_{39} = AND(r_{78}, r_{79})$
2	$r_{10} = t_{75}$	4	$g_8 = AND(r_{16}, r_{17})$	6	$t_{97} = t_{77} \oplus t_{92}$	8	$g_{41} = AND(r_{82}, r_{83})$
2	$r_{13} = t_6$	4	$g_9 = AND(r_{18}, r_{19})$	6	$t_{104} = t_{57} \oplus t_{102}$	8	$t_{82} = t_{32} \oplus t_{81}$
2	$r_{21} = t_{75}$	4	$g_{10} = AND(r_{20}, r_{21})$	6	$t_{109} = t_{52} \oplus g_5$	8	$t_{101} = g_{23} \oplus t_{94}$
2	$r_{23} = t_9$	4	$g_{11} = AND(r_{22}, r_{23})$	6	$t_{110} = g_3 \oplus t_{38}$	8	$t_{103} = t_{56} \oplus t_{99}$
2	$r_{24} = t_{34}$	4	$g_{12} = AND(r_{24}, r_{25})$	6	$t_{117} = t_{44} \oplus t_{115}$	8	$t_{106} = t_{94} \oplus t_{105}$
2	$r_{28} = t_{12}$	4	$g_{13} = AND(r_{26}, r_{27})$	6	$t_{122} = t_{108} \oplus t_{119}$	8	$t_{118} = g_{24} \oplus t_{107}$
2	$r_{33} = t_3$	4	$t_8 = x_1 \oplus t_7$	6	$t_{125} = t_{77} \oplus t_{124}$	8	$t_{121} = t_{97} \oplus t_{120}$
2	$r_{35} = t_5$	4	$t_{20} = t_{14} \oplus t_{15}$	6	$t_{128} = g_{15} \oplus t_{116}$	8	$t_{127} = t_{86} \oplus t_{126}$
2	$r_{42} = t_{75}$	4	$t_{23} = g_{17} \oplus t_{17}$	6	$t_{132} = g_6 \oplus t_{116}$	8	$t_{130} = t_{126} \oplus t_{129}$
2	$r_{50} = t_5$	4	$t_{28} = t_{17} \oplus t_{27}$	6	$t_{143} = t_{32} \oplus t_{102}$	8	$t_{135} = t_{133} \oplus t_{134}$
2	$r_{52} = t_9$	4	$t_{29} = t_4 \oplus g_{14}$	6	$t_{152} = t_{116} \oplus t_{151}$	8	$t_{138} = t_{120} \oplus t_{137}$
2	$r_{56} = t_{59}$	4	$t_{32} = g_{17} \oplus g_{14}$	6	$t_{157} = g_{15} \oplus t_{151}$	8	$t_{145} = t_{95} \oplus t_{144}$
2	$r_{66} = t_{63}$	4	$t_{45} = g_{17} \oplus t_{21}$	6	$t_{162} = t_{150} \oplus t_{161}$	8	$t_{158} = t_{99} \oplus t_{157}$
2	$r_{68} = t_{64}$	4	$t_{58} = x_1 \oplus t_{39}$	6	$t_{163} = t_{78} \oplus t_{115}$	8	$t_{168} = t_{111} \oplus t_{164}$
2	$r_{70} = t_{65}$	4	$t_{61} = x_4 \oplus t_{46}$	6	$t_{171} = t_{33} \oplus t_{170}$	8	$t_{169} = t_2 \oplus g_{42}$
2	$r_{82} = t_{27}$	4	$t_{67} = t_4 \oplus t_{10}$	6	$t_{175} = t_{52} \oplus g_{10}$	8	$t_{173} = t_{76} \oplus t_{172}$
2	$r_{88} = t_{73}$	4	$t_{68} = x_3 \oplus t_{14}$	6	$t_{180} = t_{41} \oplus t_{179}$	8	$t_{182} = t_{176} \oplus t_{181}$
3	$g_5 = AND(r_{10}, r_{11})$	4	$t_{69} = t_7 \oplus t_{59}$	6	$t_{187} = t_{41} \oplus t_{77}$	8	$t_{183} = t_{123} \oplus g_{42}$
3	$g_{14} = AND(r_{28}, r_{29})$	4	$t_{79} = t_{14} \oplus g_5$	6	$t_{189} = t_{115} \oplus t_{188}$	8	$t_{201} = t_8 \oplus t_{99}$
3	$g_{16} = AND(r_{32}, r_{33})$	4	$t_{85} = g_{15} \oplus g_5$	6	$t_{218} = t_{178} \oplus t_{217}$	8	$t_{203} = g_{24} \oplus t_{198}$
3	$g_{17} = AND(r_{34}, r_{35})$	4	$t_{149} = g_5 \oplus t_{148}$	6	$t_{221} = t_7 \oplus t_{52}$	8	$t_{204} = t_{116} \oplus g_{42}$
3	$t_4 = x_2 \oplus t_3$	4	$t_{161} = g_{14} \oplus t_{25}$	6	$t_{227} = t_{150} \oplus t_{226}$	8	$t_{216} = t_{140} \oplus t_{215}$
3	$t_7 = t_3 \oplus t_6$	4	$t_{177} = g_{17} \oplus t_{18}$	6	$r_{47} = t_{80}$	8	$t_{223} = t_{123} \oplus t_{222}$
3	$t_{14} = t_6 \oplus t_{13}$	4	$t_{179} = g_{14} \oplus t_{39}$	6	$r_{49} = t_{56}$	8	$t_{224} = g_{42} \oplus t_{220}$
3	$t_{17} = t_5 \oplus t_{10}$	4	$t_{225} = g_{17} \oplus t_{25}$	6	$r_{85} = t_{152}$	8	$r_{39} = t_{82}$
3	$t_{19} = x_5 \oplus t_{16}$	4	$r_6 = t_8$	7	$g_{23} = AND(r_{46}, r_{47})$	8	$r_{41} = t_{216}$
3	$t_{21} = x_3 \oplus t_6$	4	$r_{54} = t_{58}$	7	$g_{24} = AND(r_{48}, r_{49})$	8	$r_{43} = t_{103}$
3	$t_{25} = x_0 \oplus t_{12}$	4	$r_{60} = t_{61}$	7	$g_{42} = AND(r_{84}, r_{85})$	8	$r_{45} = t_{158}$
3	$t_{30} = t_6 \oplus t_{15}$	4	$r_{64} = t_{20}$	7	$t_{76} = t_{35} \oplus g_5$	8	$r_{51} = t_{106}$
3	$t_{31} = x_4 \oplus t_{18}$	4	$r_{74} = t_{67}$	7	$t_{81} = t_{50} \oplus t_{51}$	8	$r_{53} = t_{121}$

Listing 21: New SNOW3G S-box circuit (continued) (D: 24, AD: 4, #NL: 90, #L: 533, #(gate): 623)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
8	$r_{59} = t_{127}$	11	$t_{210} = t_{155} \oplus t_{167}$	14	$t_{266} = t_{233} \oplus t_{263}$	15	$r_{106} = t_{289}$
8	$r_{61} = t_{135}$	11	$t_{212} = t_{197} \oplus t_{206}$	14	$t_{267} = t_{246} \oplus t_{262}$	15	$r_{150} = t_{340}$
8	$r_{63} = t_{173}$	11	$t_{214} = t_{156} \oplus t_{202}$	14	$t_{276} = t_{246} \oplus t_{263}$	15	$r_{154} = t_{305}$
8	$r_{69} = t_{130}$	11	$t_{232} = t_{209} \oplus t_{230}$	14	$t_{280} = t_{233} \oplus t_{259}$	15	$r_{162} = t_{345}$
8	$r_{75} = t_{182}$	11	$t_{234} = t_{196} \oplus t_{230}$	14	$t_{287} = t_{259} \oplus t_{263}$	15	$r_{168} = t_{348}$
8	$r_{77} = t_{223}$	11	$t_{237} = t_{211} \oplus t_{236}$	14	$t_{302} = t_{242} \oplus g_{60}$	15	$r_{170} = t_{349}$
8	$r_{81} = t_{168}$	11	$t_{241} = t_{231} \oplus t_{240}$	14	$t_{306} = t_{235} \oplus t_{290}$	15	$r_{172} = t_{268}$
8	$r_{87} = t_{145}$	11	$t_{245} = t_{208} \oplus t_{244}$	14	$t_{312} = t_{260} \oplus t_{262}$	15	$r_{176} = t_{351}$
8	$r_{89} = t_{138}$	11	$t_{249} = t_{211} \oplus t_{248}$	14	$t_{333} = t_{233} \oplus t_{303}$	16	$g_{52} = AND(r_{104}, r_{105})$
9	$g_{19} = AND(r_{38}, r_{39})$	11	$t_{253} = t_{231} \oplus t_{252}$	14	$t_{337} = t_{283} \oplus t_{325}$	16	$g_{53} = AND(r_{106}, r_{107})$
9	$g_{20} = AND(r_{40}, r_{41})$	11	$t_{257} = t_{230} \oplus t_{256}$	14	$t_{338} = t_{235} \oplus t_{260}$	16	$t_{272} = g_{60} \oplus g_{57}$
9	$g_{21} = AND(r_{42}, r_{43})$	12	$t_{233} = t_{195} \oplus t_{232}$	14	$t_{339} = t_{250} \oplus t_{313}$	16	$t_{274} = g_{48} \oplus g_{49}$
9	$g_{22} = AND(r_{44}, r_{45})$	12	$t_{235} = t_{212} \oplus t_{234}$	14	$t_{341} = t_{295} \oplus t_{303}$	16	$t_{275} = t_{262} \oplus g_{49}$
9	$g_{25} = AND(r_{50}, r_{51})$	12	$t_{238} = t_{199} \oplus t_{237}$	14	$t_{342} = t_{250} \oplus t_{284}$	16	$t_{277} = t_{260} \oplus t_{271}$
9	$g_{26} = AND(r_{52}, r_{53})$	12	$t_{242} = t_{210} \oplus t_{241}$	14	$t_{343} = t_{238} \oplus t_{263}$	16	$t_{278} = g_{45} \oplus g_{49}$
9	$g_{29} = AND(r_{58}, r_{59})$	12	$t_{246} = t_{159} \oplus t_{245}$	14	$t_{344} = t_{317} \oplus t_{325}$	16	$t_{282} = g_{54} \oplus g_{47}$
9	$g_{30} = AND(r_{60}, r_{61})$	12	$t_{250} = t_{200} \oplus t_{249}$	14	$t_{346} = t_{233} \oplus t_{260}$	16	$t_{285} = g_{62} \oplus g_{49}$
9	$g_{31} = AND(r_{62}, r_{63})$	12	$t_{254} = t_{214} \oplus t_{253}$	14	$t_{347} = t_{290} \oplus t_{313}$	16	$t_{293} = g_{46} \oplus g_{50}$
9	$g_{34} = AND(r_{68}, r_{69})$	12	$t_{258} = t_{192} \oplus t_{257}$	14	$t_{350} = t_{238} \oplus t_{262}$	16	$t_{294} = g_{50} \oplus g_{51}$
9	$g_{37} = AND(r_{74}, r_{75})$	12	$r_{90} = t_{246}$	14	$t_{352} = t_{259} \oplus t_{325}$	16	$t_{301} = g_{50} \oplus g_{55}$
9	$g_{38} = AND(r_{76}, r_{77})$	12	$r_{91} = t_{254}$	14	$t_{483} = g_{48} \oplus g_{60}$	16	$t_{314} = t_{269} \oplus g_{58}$
9	$g_{40} = AND(r_{80}, r_{81})$	12	$r_{95} = t_{250}$	14	$r_{93} = t_{267}$	16	$t_{316} = t_{270} \oplus g_{54}$
9	$g_{43} = AND(r_{86}, r_{87})$	12	$r_{96} = t_{233}$	14	$r_{94} = t_{276}$	16	$t_{318} = g_{57} \oplus g_{59}$
9	$g_{44} = AND(r_{88}, r_{89})$	12	$r_{97} = t_{258}$	14	$r_{99} = t_{265}$	16	$t_{328} = g_{55} \oplus t_{310}$
9	$t_{100} = t_{32} \oplus g_{18}$	12	$r_{101} = t_{238}$	14	$r_{100} = t_{280}$	16	$t_{329} = g_{58} \oplus g_{61}$
9	$t_{112} = g_{18} \oplus g_{41}$	12	$r_{108} = t_{246}$	14	$r_{104} = t_{287}$	16	$t_{331} = g_{55} \oplus t_{324}$
9	$t_{131} = g_{32} \oplus g_{35}$	12	$r_{112} = t_{254}$	14	$r_{109} = t_{265}$	16	$t_{372} = t_{289} \oplus t_{324}$
9	$t_{139} = t_{56} \oplus t_{118}$	12	$r_{120} = t_{242}$	14	$r_{111} = t_{280}$	16	$t_{378} = g_{48} \oplus g_{50}$
9	$t_{153} = g_{35} \oplus g_{33}$	12	$r_{121} = t_{235}$	14	$r_{115} = t_{264}$	16	$t_{388} = t_{235} \oplus t_{361}$
9	$t_{154} = t_{121} \oplus g_{33}$	12	$r_{123} = t_{258}$	14	$r_{116} = t_{312}$	16	$t_{405} = t_{265} \oplus t_{361}$
9	$t_{166} = t_{140} \oplus g_{39}$	12	$r_{124} = t_{250}$	14	$r_{126} = t_{333}$	16	$t_{423} = t_{267} \oplus t_{308}$
9	$t_{184} = g_{39} \oplus t_{169}$	12	$r_{130} = t_{238}$	14	$r_{132} = t_{280}$	16	$t_{431} = g_{58} \oplus t_{332}$
9	$t_{194} = t_{101} \oplus t_{183}$	12	$r_{136} = t_{235}$	14	$r_{144} = t_{337}$	16	$t_{454} = g_{62} \oplus g_{46}$
9	$t_{205} = g_{41} \oplus t_{201}$	13	$g_{45} = AND(r_{90}, r_{91})$	14	$r_{146} = t_{338}$	16	$t_{459} = t_{271} \oplus t_{308}$
9	$t_{207} = g_{18} \oplus g_{39}$	13	$g_{48} = AND(r_{96}, r_{97})$	14	$r_{148} = t_{339}$	16	$t_{467} = t_{267} \oplus g_{49}$
9	$t_{213} = x_6 \oplus g_{28}$	13	$g_{60} = AND(r_{120}, r_{121})$	14	$r_{152} = t_{341}$	16	$t_{476} = g_{50} \oplus g_{58}$
9	$t_{229} = g_{27} \oplus g_{36}$	13	$t_{259} = t_{235} \oplus t_{258}$	14	$r_{156} = t_{342}$	16	$t_{478} = t_{235} \oplus g_{54}$
9	$t_{239} = t_{204} \oplus g_{36}$	13	$t_{260} = t_{242} \oplus t_{246}$	14	$r_{158} = t_{343}$	16	$t_{485} = t_{482} \oplus t_{484}$
9	$t_{243} = t_{203} \oplus g_{36}$	13	$t_{261} = t_{233} \oplus t_{238}$	14	$r_{160} = t_{344}$	16	$t_{503} = g_{54} \oplus t_{502}$
9	$t_{247} = t_{138} \oplus g_{36}$	13	$t_{262} = t_{250} \oplus t_{254}$	14	$r_{164} = t_{346}$	17	$t_{279} = t_{275} \oplus g_{47}$
9	$t_{251} = g_{18} \oplus g_{36}$	13	$t_{263} = t_{242} \oplus t_{254}$	14	$r_{166} = t_{347}$	17	$t_{286} = g_{45} \oplus t_{272}$
9	$t_{255} = g_{28} \oplus t_{224}$	13	$t_{283} = t_{233} \oplus t_{246}$	14	$r_{174} = t_{350}$	17	$t_{291} = g_{47} \oplus g_{53}$
10	$t_{141} = g_{29} \oplus t_{131}$	13	$t_{284} = t_{254} \oplus t_{258}$	14	$r_{178} = t_{352}$	17	$t_{297} = g_{46} \oplus t_{274}$
10	$t_{142} = g_{19} \oplus g_{21}$	13	$t_{290} = t_{238} \oplus t_{250}$	15	$g_{46} = AND(r_{92}, r_{93})$	17	$t_{300} = g_{50} \oplus g_{53}$
10	$t_{146} = g_{44} \oplus g_{43}$	13	$t_{295} = t_{246} \oplus t_{254}$	15	$g_{47} = AND(r_{94}, r_{95})$	17	$t_{304} = t_{272} \oplus g_{56}$
10	$t_{147} = g_{29} \oplus g_{34}$	13	$t_{303} = t_{235} \oplus t_{238}$	15	$g_{49} = AND(r_{98}, r_{99})$	17	$t_{309} = t_{285} \oplus t_{308}$
10	$t_{155} = g_{19} \oplus g_{25}$	13	$t_{313} = t_{233} \oplus t_{235}$	15	$g_{50} = AND(r_{100}, r_{101})$	17	$t_{315} = g_{53} \oplus t_{301}$
10	$t_{156} = g_{25} \oplus g_{43}$	13	$t_{317} = t_{238} \oplus t_{258}$	15	$g_{54} = AND(r_{108}, r_{109})$	17	$t_{319} = t_{282} \oplus g_{56}$
10	$t_{165} = g_{19} \oplus g_{26}$	13	$t_{325} = t_{242} \oplus t_{250}$	15	$g_{55} = AND(r_{110}, r_{111})$	17	$t_{320} = g_{55} \oplus t_{318}$
10	$t_{167} = g_{44} \oplus t_{139}$	13	$t_{334} = t_{233} \oplus t_{258}$	15	$g_{57} = AND(r_{114}, r_{115})$	17	$t_{321} = t_{314} \oplus t_{316}$
10	$t_{174} = g_{39} \oplus g_{40}$	13	$r_{92} = t_{263}$	15	$g_{58} = AND(r_{116}, r_{117})$	17	$t_{327} = t_{285} \oplus t_{324}$
10	$t_{185} = g_{30} \oplus t_{184}$	13	$r_{98} = t_{259}$	15	$t_{268} = t_{242} \oplus t_{265}$	17	$t_{330} = g_{52} \oplus t_{329}$
10	$t_{186} = g_{43} \oplus t_{154}$	13	$r_{102} = t_{283}$	15	$t_{269} = g_{48} \oplus g_{62}$	17	$t_{335} = t_{264} \oplus t_{274}$
10	$t_{191} = t_{154} \oplus g_{31}$	13	$r_{103} = t_{284}$	15	$t_{270} = t_{264} \oplus t_{267}$	17	$t_{336} = g_{52} \oplus t_{316}$
10	$t_{193} = g_{22} \oplus t_{184}$	13	$r_{107} = t_{290}$	15	$t_{271} = t_{235} \oplus t_{267}$	17	$t_{353} = g_{49} \oplus t_{293}$
10	$t_{196} = g_{42} \oplus t_{166}$	13	$r_{110} = t_{295}$	15	$t_{273} = t_{262} \oplus t_{266}$	17	$t_{364} = t_{271} \oplus t_{282}$
10	$t_{197} = g_{29} \oplus t_{153}$	13	$r_{113} = t_{303}$	15	$t_{288} = t_{265} \oplus t_{267}$	17	$t_{366} = t_{242} \oplus g_{53}$
10	$t_{202} = g_{37} \oplus t_{194}$	13	$r_{114} = t_{260}$	15	$t_{289} = t_{276} \oplus t_{280}$	17	$t_{374} = g_{50} \oplus t_{328}$
10	$t_{206} = g_{30} \oplus g_{44}$	13	$r_{117} = t_{313}$	15	$t_{296} = t_{233} \oplus t_{287}$	17	$t_{381} = t_{265} \oplus t_{378}$
10	$t_{208} = t_{112} \oplus g_{22}$	13	$r_{118} = t_{262}$	15	$t_{305} = t_{242} \oplus t_{264}$	17	$t_{386} = t_{347} \oplus t_{378}$
10	$t_{209} = g_{34} \oplus t_{205}$	13	$r_{119} = t_{317}$	15	$t_{308} = g_{51} \oplus g_{56}$	17	$t_{399} = t_{272} \oplus t_{316}$
10	$t_{211} = g_{40} \oplus g_{37}$	13	$r_{122} = t_{325}$	15	$t_{310} = t_{235} \oplus t_{302}$	17	$t_{424} = t_{314} \oplus t_{423}$
10	$t_{230} = g_{38} \oplus t_{229}$	13	$r_{125} = t_{259}$	15	$t_{311} = g_{60} \oplus t_{287}$	17	$t_{432} = t_{331} \oplus t_{431}$
10	$t_{231} = g_{20} \oplus g_{38}$	13	$r_{128} = t_{313}$	15	$t_{324} = t_{242} \oplus g_{59}$	17	$t_{444} = g_{45} \oplus t_{331}$
10	$t_{236} = t_{213} \oplus t_{229}$	13	$r_{134} = t_{334}$	15	$t_{332} = g_{51} \oplus g_{61}$	17	$t_{455} = t_{324} \oplus t_{454}$
10	$t_{240} = t_{207} \oplus t_{239}$	13	$r_{138} = t_{317}$	15	$t_{340} = t_{276} \oplus t_{334}$	17	$t_{460} = t_{282} \oplus t_{459}$
10	$t_{244} = g_{38} \oplus t_{243}$	13	$r_{140} = t_{259}$	15	$t_{345} = t_{260} \oplus t_{306}$	17	$t_{468} = t_{318} \oplus t_{467}$
10	$t_{248} = g_{20} \oplus t_{247}$	13	$r_{142} = t_{303}$	15	$t_{348} = t_{235} \oplus t_{276}$	17	$t_{477} = t_{318} \oplus t_{476}$
10	$t_{252} = g_{26} \oplus t_{251}$	14	$g_{51} = AND(r_{102}, r_{103})$	15	$t_{349} = t_{264} \oplus t_{295}$	17	$t_{479} = t_{285} \oplus t_{478}$
10	$t_{256} = g_{37} \oplus t_{255}$	14	$g_{56} = AND(r_{112}, r_{113})$	15	$t_{351} = t_{238} \oplus t_{287}$	17	$t_{486} = t_{301} \oplus t_{485}$
11	$t_{159} = t_{142} \oplus t_{146}$	14	$g_{59} = AND(r_{118}, r_{119})$	15	$t_{361} = g_{45} \oplus g_{51}$	17	$t_{501} = g_{52} \oplus t_{328}$
11	$t_{192} = t_{147} \oplus t_{186}$	14	$g_{61} = AND(r_{122}, r_{123})$	15	$t_{482} = g_{62} \oplus g_{59}$	17	$t_{504} = g_{53} \oplus t_{503}$
11	$t_{195} = t_{141} \oplus t_{146}$	14	$g_{62} = AND(r_{124}, r_{125})$	15	$t_{484} = t_{265} \oplus t_{483}$	17	$r_{137} = t_{381}$
11	$t_{199} = t_{185} \oplus t_{191}$	14	$t_{264} = t_{259} \oplus t_{261}$	15	$t_{502} = g_{56} \oplus g_{61}$	17	$r_{139} = t_{335}$
11	$t_{200} = t_{165} \oplus t_{193}$	14	$t_{265} = t_{258} \oplus t_{261}$	15	$r_{105} = t_{288}$	17	$r_{157} = t_{486}$

Listing 21: New SNOW3G S-box circuit (continued) (D: 24, AD: 4, #NL: 90, #L: 533, #(gate): 623)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
18	$g_{68} = AND(r_{136}, r_{137})$	19	$t_{391} = g_{62} \oplus t_{390}$	20	$t_{506} = g_{73} \oplus g_{80}$	22	$t_{438} = t_{394} \oplus t_{416}$
18	$g_{69} = AND(r_{138}, r_{139})$	19	$t_{393} = t_{246} \oplus g_{69}$	20	$t_{508} = g_{73} \oplus t_{490}$	22	$t_{439} = g_{85} \oplus t_{430}$
18	$g_{78} = AND(r_{156}, r_{157})$	19	$t_{397} = t_{355} \oplus t_{396}$	20	$t_{518} = g_{73} \oplus t_{488}$	22	$t_{441} = t_{416} \oplus g_{79}$
18	$t_{281} = g_{54} \oplus t_{279}$	19	$t_{400} = t_{322} \oplus t_{399}$	20	$t_{528} = g_{77} \oplus g_{80}$	22	$t_{442} = t_{367} \oplus t_{408}$
18	$t_{292} = g_{52} \oplus t_{291}$	19	$t_{411} = t_{298} \oplus t_{410}$	20	$r_{131} = t_{384}$	22	$t_{447} = t_{354} \oplus t_{404}$
18	$t_{298} = t_{274} \oplus t_{291}$	19	$t_{418} = t_{299} \oplus t_{417}$	20	$r_{141} = t_{358}$	22	$t_{448} = g_{70} \oplus t_{402}$
18	$t_{299} = t_{286} \oplus t_{294}$	19	$t_{440} = t_{425} \oplus t_{433}$	20	$r_{167} = t_{449}$	22	$t_{450} = t_{419} \oplus g_{83}$
18	$t_{322} = t_{300} \oplus t_{309}$	19	$t_{446} = t_{356} \oplus t_{445}$	20	$r_{171} = t_{429}$	22	$t_{452} = t_{435} \oplus g_{83}$
18	$t_{323} = g_{45} \oplus t_{320}$	19	$t_{456} = t_{326} \oplus t_{455}$	20	$r_{179} = t_{363}$	22	$t_{453} = t_{422} \oplus g_{83}$
18	$t_{326} = t_{319} \oplus g_{61}$	19	$t_{462} = t_{298} \oplus t_{461}$	21	$g_{65} = AND(r_{130}, r_{131})$	22	$t_{473} = t_{470} \oplus t_{472}$
18	$t_{355} = t_{304} \oplus t_{330}$	19	$t_{488} = t_{380} \oplus g_{78}$	21	$g_{70} = AND(r_{140}, r_{141})$	22	$t_{491} = t_{238} \oplus t_{487}$
18	$t_{356} = t_{297} \oplus t_{329}$	19	$t_{489} = t_{311} \oplus g_{78}$	21	$g_{83} = AND(r_{166}, r_{167})$	22	$t_{493} = t_{464} \oplus g_{78}$
18	$t_{369} = t_{267} \oplus t_{319}$	19	$t_{490} = t_{466} \oplus g_{78}$	21	$g_{85} = AND(r_{170}, r_{171})$	22	$t_{498} = t_{403} \oplus t_{497}$
18	$t_{375} = t_{327} \oplus t_{374}$	19	$r_{129} = t_{391}$	21	$g_{89} = AND(r_{178}, r_{179})$	22	$t_{510} = t_{413} \oplus t_{509}$
18	$t_{380} = t_{336} \oplus t_{372}$	19	$r_{133} = t_{389}$	21	$t_{357} = t_{332} \oplus g_{71}$	22	$t_{513} = t_{443} \oplus t_{458}$
18	$t_{390} = g_{54} \oplus t_{304}$	19	$r_{135} = t_{411}$	21	$t_{367} = g_{71} \oplus t_{360}$	22	$t_{515} = t_{412} \oplus t_{514}$
18	$t_{396} = t_{315} \oplus t_{327}$	19	$r_{143} = t_{354}$	21	$t_{385} = t_{306} \oplus t_{377}$	22	$t_{520} = t_{464} \oplus t_{519}$
18	$t_{406} = t_{291} \oplus t_{405}$	19	$r_{145} = t_{400}$	21	$t_{394} = g_{84} \oplus g_{64}$	22	$t_{525} = g_{83} \oplus t_{523}$
18	$t_{410} = t_{381} \oplus t_{388}$	19	$r_{149} = t_{397}$	21	$t_{402} = t_{387} \oplus g_{74}$	22	$t_{530} = t_{481} \oplus t_{529}$
18	$t_{417} = t_{309} \oplus t_{364}$	19	$r_{151} = t_{462}$	21	$t_{403} = t_{373} \oplus t_{392}$	23	$t_{434} = g_{71} \oplus t_{401}$
18	$t_{425} = t_{315} \oplus t_{424}$	19	$r_{159} = t_{440}$	21	$t_{404} = g_{84} \oplus g_{72}$	23	$t_{437} = t_{368} \oplus t_{409}$
18	$t_{433} = t_{336} \oplus t_{432}$	19	$r_{163} = t_{418}$	21	$t_{408} = t_{398} \oplus g_{72}$	23	$t_{457} = g_{67} \oplus t_{414}$
18	$t_{445} = t_{316} \oplus t_{444}$	19	$r_{165} = t_{446}$	21	$t_{412} = t_{377} \oplus g_{67}$	23	$t_{463} = g_{81} \oplus t_{447}$
18	$t_{461} = t_{320} \oplus t_{460}$	19	$r_{169} = t_{370}$	21	$t_{413} = g_{64} \oplus g_{72}$	23	$t_{465} = t_{395} \oplus t_{439}$
18	$t_{466} = t_{290} \oplus t_{335}$	19	$r_{177} = t_{456}$	21	$t_{416} = g_{71} \oplus g_{74}$	23	$t_{474} = t_{450} \oplus t_{473}$
18	$t_{469} = t_{321} \oplus t_{468}$	20	$g_{64} = AND(r_{128}, r_{129})$	21	$t_{419} = t_{418} \oplus g_{81}$	23	$t_{492} = t_{436} \oplus t_{447}$
18	$t_{480} = t_{477} \oplus t_{479}$	20	$g_{66} = AND(r_{132}, r_{133})$	21	$t_{420} = t_{362} \oplus g_{81}$	23	$t_{494} = t_{491} \oplus t_{493}$
18	$t_{505} = t_{501} \oplus t_{504}$	20	$g_{67} = AND(r_{134}, r_{135})$	21	$t_{422} = g_{67} \oplus t_{415}$	23	$t_{496} = t_{409} \oplus t_{452}$
18	$r_{127} = t_{406}$	20	$g_{71} = AND(r_{142}, r_{143})$	21	$t_{430} = g_{81} \oplus t_{421}$	23	$t_{499} = t_{441} \oplus t_{498}$
18	$r_{147} = t_{433}$	20	$g_{72} = AND(r_{144}, r_{145})$	21	$t_{435} = g_{64} \oplus g_{73}$	23	$t_{507} = t_{442} \oplus t_{448}$
18	$r_{153} = t_{425}$	20	$g_{74} = AND(r_{148}, r_{149})$	21	$t_{443} = g_{71} \oplus g_{64}$	23	$t_{511} = t_{428} \oplus t_{510}$
18	$r_{155} = t_{480}$	20	$g_{75} = AND(r_{150}, r_{151})$	21	$t_{458} = g_{79} \oplus g_{88}$	23	$t_{516} = t_{513} \oplus t_{515}$
18	$r_{161} = t_{505}$	20	$g_{79} = AND(r_{158}, r_{159})$	21	$t_{464} = g_{81} \oplus g_{75}$	23	$t_{521} = t_{453} \oplus t_{520}$
18	$r_{173} = t_{469}$	20	$g_{81} = AND(r_{162}, r_{163})$	21	$t_{470} = g_{64} \oplus g_{88}$	23	$t_{524} = t_{395} \oplus t_{426}$
18	$r_{175} = t_{375}$	20	$g_{82} = AND(r_{164}, r_{165})$	21	$t_{472} = t_{393} \oplus t_{471}$	23	$t_{526} = t_{438} \oplus t_{525}$
19	$g_{63} = AND(r_{126}, r_{127})$	20	$g_{84} = AND(r_{168}, r_{169})$	21	$t_{481} = g_{82} \oplus t_{471}$	23	$t_{531} = t_{395} \oplus t_{530}$
19	$g_{73} = AND(r_{146}, r_{147})$	20	$g_{88} = AND(r_{176}, r_{177})$	21	$t_{487} = t_{427} \oplus g_{82}$	24	$t_{475} = t_{457} \oplus t_{474} \oplus 1$
19	$g_{76} = AND(r_{152}, r_{153})$	20	$t_{358} = t_{335} \oplus t_{354}$	21	$t_{497} = g_{81} \oplus t_{489}$	24	$t_{495} = t_{492} \oplus t_{494}$
19	$g_{77} = AND(r_{154}, r_{155})$	20	$t_{363} = t_{353} \oplus t_{362}$	21	$t_{509} = g_{75} \oplus t_{508}$	24	$t_{500} = t_{496} \oplus t_{499} \oplus 1$
19	$g_{80} = AND(r_{160}, r_{161})$	20	$t_{365} = t_{284} \oplus t_{362}$	21	$t_{514} = g_{75} \oplus t_{506}$	24	$t_{512} = t_{434} \oplus t_{511}$
19	$g_{86} = AND(r_{172}, r_{173})$	20	$t_{377} = t_{371} \oplus g_{87}$	21	$t_{519} = t_{427} \oplus t_{518}$	24	$t_{517} = t_{465} \oplus t_{516}$
19	$g_{87} = AND(r_{174}, r_{175})$	20	$t_{384} = t_{354} \oplus t_{381}$	21	$t_{523} = t_{451} \oplus t_{506}$	24	$t_{522} = t_{437} \oplus t_{521}$
19	$t_{307} = g_{48} \oplus t_{292}$	20	$t_{387} = t_{323} \oplus g_{87}$	21	$t_{529} = g_{79} \oplus t_{528}$	24	$t_{527} = t_{524} \oplus t_{526} \oplus 1$
19	$t_{354} = t_{292} \oplus t_{353}$	20	$t_{392} = g_{87} \oplus t_{382}$	22	$t_{368} = t_{357} \oplus g_{70}$	24	$t_{532} = t_{507} \oplus t_{531}$
19	$t_{359} = t_{322} \oplus g_{69}$	20	$t_{398} = t_{322} \oplus t_{383}$	22	$t_{376} = t_{311} \oplus g_{89}$	24	$\boldsymbol{y_0 = t_{475}}$
19	$t_{360} = t_{280} \oplus t_{356}$	20	$t_{407} = t_{393} \oplus t_{406}$	22	$t_{379} = g_{70} \oplus g_{89}$	24	$\boldsymbol{y_1 = t_{532}}$
19	$t_{362} = t_{326} \oplus t_{328}$	20	$t_{415} = t_{359} \oplus g_{63}$	22	$t_{395} = g_{89} \oplus g_{65}$	24	$\boldsymbol{y_2 = t_{500}}$
19	$t_{370} = t_{323} \oplus t_{369}$	20	$t_{421} = t_{362} \oplus t_{386}$	22	$t_{401} = t_{362} \oplus g_{65}$	24	$\boldsymbol{y_3 = t_{517}}$
19	$t_{371} = t_{292} \oplus t_{335}$	20	$t_{427} = g_{87} \oplus g_{76}$	22	$t_{409} = g_{89} \oplus t_{404}$	24	$\boldsymbol{y_4 = t_{522}}$
19	$t_{373} = t_{355} \oplus t_{366}$	20	$t_{429} = t_{411} \oplus t_{425}$	22	$t_{414} = g_{89} \oplus g_{66}$	24	$\boldsymbol{y_5 = t_{527}}$
19	$t_{382} = g_{69} \oplus g_{68}$	20	$t_{449} = t_{418} \oplus t_{446}$	22	$t_{426} = t_{412} \oplus t_{420}$	24	$\boldsymbol{y_6 = t_{512}}$
19	$t_{383} = t_{311} \oplus g_{68}$	20	$t_{451} = t_{306} \oplus g_{76}$	22	$t_{428} = t_{412} \oplus t_{427}$	24	$\boldsymbol{y_7 = t_{495}}$
19	$t_{389} = t_{298} \oplus t_{388}$	20	$t_{471} = g_{63} \oplus g_{86}$	22	$t_{436} = g_{85} \oplus g_{73}$		

Listing 22: New `Saturnin` super S-box circuit (D: 25, AD: 12, #NL: 48, #L: 143, #(gate): 191)

Depth	Operation	Depth	Operation	Depth	Operation	Depth	Operation
0	$r_0 = x_2$	5	$g_{14} = OR(r_{28}, r_{29})$	11	$t_{100} = t_{96} \oplus t_{99}$	17	$t_{71} = t_{65} \oplus g_{37}$
0	$r_1 = x_3$	5	$g_{20} = OR(r_{40}, r_{41})$	11	$t_{132} = t_{128} \oplus t_{131}$	17	$t_{106} = t_{102} \oplus g_{31}$
0	$r_3 = x_0$	5	$t_{91} = t_{88} \oplus t_{89}$	12	$t_{20} = t_5 \oplus g_{11}$	17	$t_{138} = t_{134} \oplus g_{43}$
0	$r_5 = x_3$	5	$t_{124} = t_{121} \oplus t_{122}$	12	$t_{21} = t_{15} \oplus g_{23}$	17	$r_{52} = t_{54}$
0	$r_{12} = x_5$	6	$t_2 = x_0 \oplus g_2$	12	$t_{26} = g_5 \oplus t_{25}$	17	$r_{54} = t_{54}$
0	$r_{13} = x_4$	6	$t_7 = x_6 \oplus g_8$	12	$t_{30} = g_{17} \oplus t_{29}$	17	$r_{64} = t_{106}$
0	$r_{15} = x_6$	6	$t_{12} = x_8 \oplus g_{14}$	12	$t_{37} = g_{11} \oplus t_{36}$	17	$r_{66} = t_{106}$
0	$r_{17} = x_4$	6	$t_{17} = x_{14} \oplus g_{20}$	12	$t_{43} = g_{23} \oplus t_{42}$	17	$r_{76} = t_{71}$
0	$r_{24} = x_{10}$	6	$t_{92} = g_{20} \oplus t_{90}$	12	$t_{48} = t_{19} \oplus t_{40}$	17	$r_{78} = t_{71}$
0	$r_{25} = x_{11}$	6	$t_{125} = g_8 \oplus t_{123}$	12	$t_{50} = t_{17} \oplus t_{40}$	17	$r_{88} = t_{138}$
0	$r_{27} = x_8$	6	$r_7 = t_2$	12	$t_{59} = g_{23} \oplus t_{40}$	17	$r_{90} = t_{138}$
0	$r_{29} = x_{11}$	6	$r_{11} = t_2$	12	$t_{61} = g_{11} \oplus t_{60}$	18	$g_{26} = OR(r_{52}, r_{53})$
0	$r_{36} = x_{13}$	6	$r_{19} = t_7$	12	$t_{64} = t_{41} \oplus t_{63}$	18	$g_{32} = OR(r_{64}, r_{65})$
0	$r_{37} = x_{12}$	6	$r_{23} = t_7$	12	$t_{68} = t_7 \oplus t_{66}$	18	$g_{38} = OR(r_{76}, r_{77})$
0	$r_{39} = x_{14}$	6	$r_{31} = t_{12}$	12	$t_{97} = g_5 \oplus g_{17}$	18	$g_{44} = OR(r_{88}, r_{89})$
0	$r_{41} = x_{12}$	6	$r_{35} = t_{12}$	12	$t_{101} = g_{11} \oplus t_{100}$	19	$t_{55} = t_{46} \oplus g_{26}$
1	$g_0 = AND(r_0, r_1)$	6	$r_{43} = t_{17}$	12	$t_{133} = g_{23} \oplus t_{132}$	19	$t_{72} = t_{47} \oplus g_{38}$
1	$g_6 = AND(r_{12}, r_{13})$	6	$r_{47} = t_{17}$	13	$t_{27} = t_{21} \oplus t_{26}$	19	$t_{107} = t_{77} \oplus g_{32}$
1	$g_{12} = AND(r_{24}, r_{25})$	7	$g_3 = AND(r_6, r_7)$	13	$t_{31} = t_{20} \oplus t_{30}$	19	$t_{139} = t_{49} \oplus g_{44}$
1	$g_{18} = AND(r_{36}, r_{37})$	7	$g_9 = AND(r_{18}, r_{19})$	13	$t_{39} = t_{37} \oplus t_{38}$	19	$r_{55} = t_{55}$
1	$t_{78} = x_1 \oplus x_4$	7	$g_{15} = AND(r_{30}, r_{31})$	13	$t_{44} = t_{37} \oplus t_{43}$	19	$r_{59} = t_{55}$
1	$t_{79} = x_5 \oplus x_7$	7	$g_{21} = AND(r_{42}, r_{43})$	13	$t_{45} = t_{20} \oplus t_{32}$	19	$r_{67} = t_{107}$
1	$t_{80} = x_9 \oplus x_{10}$	7	$t_{33} = t_2 \oplus t_5$	13	$t_{51} = t_8 \oplus t_{50}$	19	$r_{71} = t_{107}$
1	$t_{81} = x_{11} \oplus x_{12}$	7	$t_{93} = t_{91} \oplus t_{92}$	13	$t_{62} = t_{59} \oplus t_{61}$	19	$r_{79} = t_{72}$
1	$t_{82} = x_{13} \oplus x_{14}$	7	$t_{126} = t_{124} \oplus t_{125}$	13	$t_{65} = t_{59} \oplus t_{64}$	19	$r_{83} = t_{72}$
1	$t_{111} = x_1 \oplus x_2$	8	$t_3 = x_3 \oplus g_3$	13	$t_{67} = t_{18} \oplus t_{26}$	19	$r_{91} = t_{139}$
1	$t_{112} = x_3 \oplus x_4$	8	$t_8 = x_4 \oplus g_9$	13	$t_{102} = t_{97} \oplus t_{101}$	19	$r_{95} = t_{139}$
1	$t_{113} = x_5 \oplus x_6$	8	$t_{13} = x_{11} \oplus g_{15}$	13	$t_{103} = t_{21} \oplus t_{22}$	19	$\boldsymbol{y_0 = t_{55}}$
1	$t_{114} = x_9 \oplus x_{12}$	8	$t_{18} = x_{12} \oplus g_{21}$	13	$t_{134} = t_{97} \oplus t_{133}$	19	$\boldsymbol{y_6 = t_{107}}$
1	$t_{115} = x_{13} \oplus x_{15}$	8	$t_{94} = g_9 \oplus g_{15}$	13	$t_{135} = t_{20} \oplus t_{23}$	19	$\boldsymbol{y_8 = t_{72}}$
2	$t_0 = x_1 \oplus g_0$	8	$t_{95} = g_{21} \oplus t_{93}$	13	$r_{48} = t_{39}$	19	$\boldsymbol{y_{14} = t_{139}}$
2	$t_5 = x_7 \oplus g_6$	8	$t_{127} = g_3 \oplus g_9$	13	$r_{49} = t_{27}$	20	$g_{27} = AND(r_{54}, r_{55})$
2	$t_{10} = x_9 \oplus g_{12}$	8	$t_{129} = g_{21} \oplus t_{126}$	13	$r_{53} = t_{27}$	20	$g_{33} = AND(r_{66}, r_{67})$
2	$t_{15} = x_{15} \oplus g_{18}$	8	$r_9 = t_3$	13	$r_{60} = t_{102}$	20	$g_{39} = AND(r_{78}, r_{79})$
2	$t_{83} = g_0 \oplus g_6$	8	$r_{21} = t_8$	13	$r_{61} = t_{44}$	20	$g_{45} = AND(r_{90}, r_{91})$
2	$t_{84} = g_{12} \oplus t_{78}$	8	$r_{33} = t_{13}$	13	$r_{65} = t_{44}$	21	$t_{56} = t_{27} \oplus g_{27}$
2	$t_{85} = t_{79} \oplus t_{80}$	8	$r_{45} = t_{18}$	13	$r_{72} = t_{65}$	21	$t_{73} = t_{31} \oplus g_{39}$
2	$t_{86} = t_{81} \oplus t_{82}$	9	$g_4 = OR(r_8, r_9)$	13	$r_{73} = t_{31}$	21	$t_{108} = t_{44} \oplus g_{33}$
2	$t_{116} = g_0 \oplus g_{12}$	9	$g_{10} = OR(r_{20}, r_{21})$	13	$r_{77} = t_{31}$	21	$t_{140} = t_{62} \oplus g_{45}$
2	$t_{117} = g_{18} \oplus t_{111}$	9	$g_{16} = OR(r_{32}, r_{33})$	13	$r_{84} = t_{134}$	21	$r_{57} = t_{56}$
2	$t_{118} = t_{112} \oplus t_{113}$	9	$g_{22} = OR(r_{44}, r_{45})$	13	$r_{85} = t_{62}$	21	$r_{69} = t_{108}$
2	$t_{119} = t_{114} \oplus t_{115}$	9	$t_{22} = t_7 \oplus t_{13}$	13	$r_{89} = t_{62}$	21	$r_{81} = t_{73}$
2	$r_2 = t_0$	9	$t_{23} = t_3 \oplus t_{17}$	14	$g_{24} = AND(r_{48}, r_{49})$	21	$r_{93} = t_{140}$
2	$r_8 = t_0$	9	$t_{32} = t_{12} \oplus t_{18}$	14	$g_{30} = AND(r_{60}, r_{61})$	21	$\boldsymbol{y_3 = t_{56}}$
2	$r_{14} = t_5$	9	$t_{35} = t_8 \oplus t_{33}$	14	$g_{36} = AND(r_{72}, r_{73})$	21	$\boldsymbol{y_4 = t_{108}}$
2	$r_{20} = t_5$	9	$t_{98} = t_{94} \oplus t_{95}$	14	$g_{42} = AND(r_{84}, r_{85})$	21	$\boldsymbol{y_{11} = t_{73}}$
2	$r_{26} = t_{10}$	9	$t_{130} = t_{127} \oplus t_{129}$	14	$t_{46} = t_{40} \oplus t_{45}$	21	$\boldsymbol{y_{12} = t_{140}}$
2	$r_{32} = t_{10}$	10	$t_4 = t_1 \oplus g_4$	14	$t_{47} = t_{44} \oplus t_{45}$	22	$g_{28} = OR(r_{56}, r_{57})$
2	$r_{38} = t_{15}$	10	$t_9 = t_6 \oplus g_{10}$	14	$t_{49} = t_{39} \oplus t_{48}$	22	$g_{34} = OR(r_{68}, r_{69})$
2	$r_{44} = t_{15}$	10	$t_{14} = t_{11} \oplus g_{16}$	14	$t_{52} = t_{30} \oplus t_{51}$	22	$g_{40} = OR(r_{80}, r_{81})$
3	$g_1 = OR(r_2, r_3)$	10	$t_{19} = t_{16} \oplus g_{22}$	14	$t_{69} = t_{67} \oplus t_{68}$	22	$g_{46} = OR(r_{92}, r_{93})$
3	$g_7 = OR(r_{14}, r_{15})$	10	$t_{24} = t_0 \oplus t_{22}$	14	$t_{76} = t_9 \oplus t_{65}$	23	$t_{57} = t_{54} \oplus g_{28}$
3	$g_{13} = OR(r_{26}, r_{27})$	10	$t_{28} = t_{10} \oplus t_{23}$	14	$t_{104} = t_{31} \oplus t_{103}$	23	$t_{74} = t_{71} \oplus g_{40}$
3	$g_{19} = OR(r_{38}, r_{39})$	10	$t_{41} = t_{15} \oplus t_{32}$	14	$t_{136} = t_{27} \oplus t_{135}$	23	$t_{109} = t_{106} \oplus g_{34}$
3	$t_{87} = t_{83} \oplus t_{84}$	10	$t_{96} = g_{16} \oplus g_{22}$	14	$r_{51} = t_{46}$	23	$t_{141} = t_{138} \oplus g_{46}$
3	$t_{88} = t_{85} \oplus t_{86}$	10	$t_{99} = g_{10} \oplus t_{98}$	14	$r_{75} = t_{47}$	23	$r_{58} = t_{57}$
3	$t_{120} = t_{116} \oplus t_{117}$	10	$t_{128} = g_4 \oplus g_{22}$	14	$r_{87} = t_{49}$	23	$r_{70} = t_{109}$
3	$t_{121} = t_{118} \oplus t_{119}$	10	$t_{131} = g_{10} \oplus t_{130}$	15	$t_{53} = g_{24} \oplus t_{52}$	23	$r_{82} = t_{74}$
4	$t_1 = x_2 \oplus g_1$	10	$r_{10} = t_4$	15	$t_{70} = g_{36} \oplus t_{69}$	23	$r_{94} = t_{141}$
4	$t_6 = x_5 \oplus g_7$	10	$r_{22} = t_9$	15	$t_{77} = t_{66} \oplus t_{76}$	23	$\boldsymbol{y_2 = t_{57}}$
4	$t_{11} = x_{10} \oplus g_{13}$	10	$r_{34} = t_{14}$	15	$t_{105} = g_{30} \oplus t_{104}$	23	$\boldsymbol{y_5 = t_{109}}$
4	$t_{16} = x_{13} \oplus g_{19}$	10	$r_{46} = t_{19}$	15	$t_{137} = g_{42} \oplus t_{136}$	23	$\boldsymbol{y_{10} = t_{74}}$
4	$t_{89} = g_7 \oplus g_{13}$	11	$g_5 = OR(r_{10}, r_{11})$	15	$r_{50} = t_{53}$	23	$\boldsymbol{y_{13} = t_{141}}$
4	$t_{90} = g_{19} \oplus t_{87}$	11	$g_{11} = OR(r_{22}, r_{23})$	15	$r_{56} = t_{53}$	24	$g_{29} = OR(r_{58}, r_{59})$
4	$t_{122} = g_1 \oplus g_7$	11	$g_{17} = OR(r_{34}, r_{35})$	15	$r_{62} = t_{105}$	24	$g_{35} = OR(r_{70}, r_{71})$
4	$t_{123} = g_{19} \oplus t_{120}$	11	$g_{23} = OR(r_{46}, r_{47})$	15	$r_{63} = t_{77}$	24	$g_{41} = OR(r_{82}, r_{83})$
4	$r_4 = t_1$	11	$t_{25} = t_9 \oplus t_{24}$	15	$r_{68} = t_{105}$	24	$g_{47} = OR(r_{94}, r_{95})$
4	$r_6 = t_1$	11	$t_{29} = t_{19} \oplus t_{28}$	15	$r_{74} = t_{70}$	25	$t_{58} = t_{53} \oplus g_{29}$
4	$r_{16} = t_6$	11	$t_{34} = t_4 \oplus t_{32}$	15	$r_{80} = t_{70}$	25	$t_{75} = t_{70} \oplus g_{41}$
4	$r_{18} = t_6$	11	$t_{36} = t_{14} \oplus t_{35}$	15	$r_{86} = t_{137}$	25	$t_{110} = t_{105} \oplus g_{35}$
4	$r_{28} = t_{11}$	11	$t_{38} = t_9 \oplus t_{23}$	15	$r_{92} = t_{137}$	25	$t_{142} = t_{137} \oplus g_{47}$
4	$r_{30} = t_{11}$	11	$t_{40} = t_4 \oplus t_7$	16	$g_{25} = OR(r_{50}, r_{51})$	25	$\boldsymbol{y_1 = t_{58}}$
4	$r_{40} = t_{16}$	11	$t_{42} = t_{17} \oplus t_{41}$	16	$g_{31} = OR(r_{62}, r_{63})$	25	$\boldsymbol{y_7 = t_{110}}$
4	$r_{42} = t_{16}$	11	$t_{60} = t_{35} \oplus t_{41}$	16	$g_{37} = OR(r_{74}, r_{75})$	25	$\boldsymbol{y_9 = t_{75}}$
5	$g_2 = OR(r_4, r_5)$	11	$t_{63} = t_{13} \oplus t_{19}$	16	$g_{43} = OR(r_{86}, r_{87})$	25	$\boldsymbol{y_{15} = t_{142}}$
5	$g_8 = OR(r_{16}, r_{17})$	11	$t_{66} = t_{14} \oplus t_{17}$	17	$t_{54} = t_{39} \oplus g_{25}$		