IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2020, No. 1, pp. 144–184. DOI:10.13154/tosc.v2020.i1.144-184

Low AND Depth and Efficient Inverses: a Guide on S-boxes for Low-latency Masking

Begül Bilgin[1], Lauren De Meyer[2], Sébastien Duval[3], Itamar Levi[3,4] and François-Xavier Standaert[3]

[1] Rambus, Cryptography Research, Rotterdam, Netherlands, bbilgin@rambus.com
[2] Computer Security and Industrial Cryptography (COSIC), KU Leuven, Leuven, Belgium, lauren.demeyer@kuleuven.be,
[3] UCLouvain, Louvain-la-Neuve, Belgium, fstandae@uclouvain.be, s.duval@uclouvain.be
[4] Bar-Ilan University (BIU), Ramat Gan, Israel, itamarlevi@gmail.com

Abstract. In this work, we perform an extensive investigation and construct a portfolio of S-boxes suitable for secure lightweight implementations, which aligns well with the ongoing NIST Lightweight Cryptography competition. In particular, we target good functional properties on the one hand and efficient implementations in terms of AND depth and AND gate complexity on the other. Moreover, we also consider the implementation of the inverse S-box and the possibility for it to share resources with the forward S-box. We take our exploration beyond the conventional small (and even) S-box sizes. Our investigation is twofold: (1) we note that implementations of existing S-boxes are not optimized for the criteria which define masking complexity (AND depth and AND gate complexity) and improve a tool published at FSE 2016 by Stoffelen in order to fill this gap. (2) We search for new S-box designs which take these implementation properties into account from the start. We perform a systematic search based on the properties of not only the S-box but also its inverse as well as an exploration of larger S-box sizes using length-doubling structures. The result of our investigation is not only a wide selection of very good S-boxes, but we also provide complete descriptions of their circuits, enabling their integration into future work.

Keywords: S-box · lightweight cryptography · masking · multiplicative complexity · AND depth

1 Introduction

The implementation complexity has always played a role in the choice of S-boxes for ciphers. For example, in the design process of the Data Encryption Standard (DES) [oS77], the eight DES S-boxes were chosen so that (given the cryptographic criteria), they have a low number of minterms [MM82]. Several tools and methods are available today to minimize the gate count of S-box implementations [BMP13a, Sto16]. However, gate count is not necessarily the best optimization metric for cryptographic implementations.

Resistance against side-channel analysis attacks has become a quite mainstream requirement for cipher implementations. This is for example witnessed by the ongoing NIST Lightweight Cryptography competition, which states it as an important goal[1]. In this context, enabling secure and efficient Boolean masked implementations typically implies reducing the number of multiplications of the algorithms to implement,

[1] https://csrc.nist.gov/Projects/Lightweight-Cryptography

Received: 2019-09-01, Revised: 2019-11-23, Accepted: 2020-01-23, Published: 2020-05-07

since they are the costly operations to mask [ISW03]. Minimizing the number of multiplications required to implement S-boxes which are designed without such considerations is a challenging task [ÇTP19, GR16]. As a result, several modern cipher proposals considered this during design phase, building on quite different design principles [BBK+13, GGNS13, GLSV14, JSV17, PRC12], and many submissions to the NIST Lightweight Cryptography competition also follow this approach. For example, submissions such as ASCON [DEMS16], ForkAE [ALP+19], ISAP [DEM+17], Pyjamask [GJK+], Spook [BBB+] and TRIFLE [DGM+] mention explicitly efficient masking as a design goal, while other submissions are re-using small S-boxes from existing designs (such as Photon [GPP11], Skinny [BJK+16], Gift [BPP+17]) which are known to be easy to mask.

Low-latency is also gaining attention as the need for high-performance cryptography increases together with the connectivity of devices. Minimizing the logical depth of an existing S-box, such as that of the AES, is again non-trivial [BP11]. Being a relatively young area of research, there are only a handful of low-latency (authenticated) encryption schemes [Ava17, BJK+16, BCG+12] in literature. Even though these designs provide low-latency when side-channel attacks are not of concern, their protected implementations suffer from loss of performance, the main culprit being the multiplicative depth of the underlying S-box [BKN18]. Therefore, it is important to consider not only the number of multiplications but also the AND depth while designing a cryptographic algorithm. One has a significant impact on the latency of hardware implementations which are prone to glitches [NRS11], while the other affects the implementations' (circuit and randomness) complexity [GR17].

Motivation and Contribution. The literature shows that there is still a lack of understanding of the relationship between S-box design and their implementation efficiency (with SCA protection). This is exemplified on the one hand in how existing S-boxes are implemented (1) and on the other in how S-boxes for new designs are chosen (2). In this work, we will address both aspects.

(1) In Section 3, we consider the issue of efficiently implementing specific S-boxes. The cost optimization of a given S-box' circuit is a hard problem, even for only one optimization criterion [BMP13a, GR16, KPPY14, UDCI+11]. For small S-box sizes, some optimization tools exist [UDCI+11, Gla07, BMP13b, Sto16, JPST17, BGLS19]. In the context of masked implementations, it is common to consider the number of AND gates (G) as primary quantity to minimize. Minimal circuit depth is targeted when low latency is important. However, none of these tools consider the AND depth (D), which is a very important cost indicator for the latency of masked hardware implementations. Moreover S-boxes are never optimized for the AND depth and AND gate count *jointly*. To this end, we extend the functionality of a tool by Stoffelen [Sto16], so that it becomes possible to optimize for multiple criteria *jointly*. In this way, we are able to obtain small AND depth *and* small AND gate count for various existing S-boxes, which improves their masked implementation complexity. In particular, we show that most 4-bit S-boxes can be implemented with the minimal AND gate count and AND depth (4 ANDs with AND depth 2). This demonstrates that previous works did not always consider the implementation cost of masking.

(2) Low latency in hardware does not carry over from unprotected to SCA-protected implementations: one needs to consider the AND depth. We will show that currently, S-box circuits are not optimized for this criterion and that by extension, the way new S-boxes are chosen for SCA-efficient primitives in the literature is sub-optimal. For instance in the current NIST LWC call, it is specified that "The implementations of the AEAD algorithms and the optional hash function algorithms should lend themselves to countermeasures against various side-channel attacks", yet most candidates were not designed with AND depth in mind. We also observe that a lot of the NIST submissions are based on existing

designs, which can be explained by NIST's encouragement that submissions already be scrutinized by third parties. As a result, a majority of the proposals use 4-bit S-boxes, which according to our analysis, offer very little advantages compared to larger sized S-boxes (see Table 9). The popularity of S-boxes of size 2^k can historically be explained by the size of CPU data paths. However, for hardware implementations and with the possibility of bitslicing in software, this restriction is not reasonable. Still, there is a clear lack of research on unconvential (*e.g.* odd) S-box sizes. The introduction of the Keccak function [BDPA09] with its 5-bit S-box and its subsequent choice as the SHA-3 standard were a positive development in this direction, yet further research using odd-sized S-boxes remains absent. The lack of use and the lack of research of the broader search space of S-boxes seem to reinforce each other in a cycle. Nevertheless, our research shows that S-boxes of odd size n tend to have better properties and lower cost than S-boxes of even size $n+1$ (see Table 9). In Sections 4 and 5, we consider the question of which S-boxes have both good cryptanalytic properties and can be efficiently implemented. We introduce principled criteria to guide S-box selection, and propose a dictionary of ready-to-use candidates, which extends the search space well beyond the conventional options. Specifically, we focus on the following aspects, which did not receive much attention in previous works:

1. Since low latency is a very important criterion and in the case of masked hardware implementations depends strongly on the algebraic degree, we guide our search in the first place by this property.

2. The implementation cost of the *inverse* S-box is often overlooked. Indeed while many modes of operations are inverse-free (many lightweight ones [CDNY18]), other modes require an inverse. Popular examples include the Tweakable Authenticated Encryption (TAE) [LRW11], Authenticated Permutation-based Encryption for Lightweight Cryptography (APE) [ABB+14] and OCB3 (CAESAR laureate for high-performance[2]). For side-channel security, it has also been observed that an efficiently invertible block cipher is instrumental in providing a secure tag verification in the presence of leakage [BPPS17]. For this purpose, we do not only consider the implementation properties of the forward S-box. We additionally consider various levels of resource sharing between the inverse and forward S-box, such that the inverse S-box can be implemented using the same building blocks (*e.g.* involutions, zero-overhead constructions, self-inversely-equivalent S-boxes, ...).

3. The size of S-boxes used in easy-to-mask ciphers is variable, yet biased towards small S-boxes. We investigate whether large(r) S-boxes may be useful. We observe that while many systematic investigations exist for 4-bit S-boxes, both for cryptanalytic and masking properties (e.g., [BNN+12, LP07]), much less is known for larger bit sizes [BBS17, DB18]. We push the limits of the best-known large(r) S-boxes for masking in different directions and provide a dictionary of suitable S-boxes.

4. S-boxes are often described using a Lookup Table (LUT) or algebraic normal form, neither of which is trivially converted to an efficient circuit description. As a final contribution, we provide concrete ready-to-use optimized circuit descriptions of various S-boxes discussed in this paper (see Appendix) that might lead to tweaks for existing designs and/or improve the cost of their side-channel secure implementations.

Remark. We acknowledge that the cryptographic strength of a cipher depends on the intricate relationship between both the S-boxes and the linear layers. We consider here only the S-boxes because our focus lies especially in their masked implementation efficiency. It remains important for us to consider also the cryptanalytic properties of the S-box,

[2] https://competitions.cr.yp.to/caesar-submissions.html

even though the exact nature of the relationship with the strength of the cipher cannot be determined without the knowledge of linear layers. We leave a more global study that combines our S-boxes with linear layers for future work.

2 Background: S-box properties

2.1 Cryptanalytic Properties

In many symmetric primitives, S-boxes are the only non-linear components. Hence, the S-box properties have a significant impact on the strength of a cipher against attacks. In order to determine the quality of an S-box S, it is common to measure the distance between itself and any linear function. In this work, we will use three (standard) metrics for this purpose: the *algebraic degree*, the *differential uniformity* and the *linearity*. We introduce them using the following set of definitions:

Definition 1 (Algebraic Normal Form (ANF))**.** Any Boolean function f of s variables can be represented as a unique multivariate polynomial with coefficients in $\mathbb{F}_2$ called the *algebraic normal form* (ANF) of f, defined by:

$$\mathsf{f}(x_0, \ldots, x_{s-1}) = \sum_{u \in \mathbb{F}_2^s} a_u \left(\prod_{i=0}^{s-1} x_i^{u_i} \right) ,$$

where u_i is the ith bit of u.

Definition 2 (Algebraic Degree)**.** Let f be a Boolean function of s variables. We call the *algebraic degree* of f, denoted as $\deg(\mathsf{f})$, the maximum Hamming weight of the degrees of its ANF:

$$\deg(\mathsf{f}) = \max_{u \in \mathbb{F}_2^s} \{\mathsf{w}(u) | a_u \neq 0\} ,$$

where a_u are the coefficients of the ANF of f. Let F be a vectorial Boolean function from $\mathbb{F}_2^s$ into $\mathbb{F}_2^s$, we call the *algebraic degree* of F, denoted $\deg(\mathsf{F})$, the maximum of the algebraic degrees of its coordinate functions $\mathsf{f}_i : (x_1, \ldots, x_s) \mapsto (\mathsf{F}(x_1, \ldots, x_s))_i$, $1 \leq i \leq s$, with $(\mathsf{F}(x_1, \ldots, x_s))_i$ the i-th bit of $\mathsf{F}(x_1, \ldots, x_s)$.

Definition 3 (Derivative of a Function)**.** Let F be a function from $\mathbb{F}_2^s$ into $\mathbb{F}_2^s$. The *derivative of* F *with respect to* $a \in \mathbb{F}_2^s$ is the function $D_a\mathsf{F} : x \in \mathbb{F}_2^s \mapsto \mathsf{F}(x + a) + \mathsf{F}(x)$.

Definition 4 (Differential Uniformity [Nyb94])**.** Let F be a function from $\mathbb{F}_2^s$ into $\mathbb{F}_2^s$. For any $a \in \mathbb{F}_2^s$ and $b \in \mathbb{F}_2^s$, we define $\delta(a, b) = |\{x \in \mathbb{F}_2^s, D_a\mathsf{F}(x) = b\}|$. The multi-set $\{\delta(a, b),\ a \in \mathbb{F}_2^s \setminus \{0\}, b \in \mathbb{F}_2^s\}$ is the *difference distribution table* of F, and its maximum:

$$\delta(\mathsf{F}) = \max_{a \neq 0, b} \delta(a, b) ,$$

is the *differential uniformity* of F. We will also use a normalization of the differential uniformity, called *differential probability*: $\mathrm{DP}(F) = \frac{\delta(F)}{2^s}$.

F is called *almost perfect nonlinear* (APN) if it is differentially 2-uniform, *i.e.* $\delta(\mathsf{F}) = 2$.

Definition 5 (Linearity [CV94])**.** Given a function F from $\mathbb{F}_2^s$ to $\mathbb{F}_2^s$ with Walsh coefficients:

$$\widehat{\mathsf{F}}(u, v) = \sum_{x \in \mathbb{F}_2^s} (-1)^{v \cdot \mathsf{F}(x) + u \cdot x} , u \in \mathbb{F}_2^s, v \in \mathbb{F}_2^s ,$$

the multi-set $\widehat{\mathsf{F}}(u, v)$, $v \neq 0$ is called the *linear approximations table* of F. The *linearity* of F, is the highest magnitude of its Walsh coefficients:

$$\mathcal{L}(\mathsf{F}) = \max_{v \in \mathbb{F}_2^s \setminus \{0\}} \max_{u \in \mathbb{F}_2^s} |\widehat{\mathsf{F}}, (u, v)| .$$

and the squared normalized linearity is called *linear potential* (or *linear probability*):

$$\mathrm{LP}(F) = \left(\frac{\mathcal{L}(\mathsf{F})}{2^s}\right)^2 .$$

Finally, F is called *almost bent* (AB) if $|\mathcal{L}(\mathsf{F})| \leq 2^{(s+1)/2}$.

Definition 6 (Worst Probability (WP))**.** The *worst probability* (WP) of a function F from $\mathbb{F}_2^s$ to $\mathbb{F}_2^s$ is the maximum between $\mathrm{DP}(F)$ and $\mathrm{LP}(F)$, which corresponds to the resistance provided by F against differential and linear attacks.

Although other cryptanalytic security criteria exist, we will restrict ourselves to these three most fundamental ones, which are usually used to extrapolate the security of a full cryptographic primitive, for instance using the wide-trail strategy [DR01].

Remark 1. Two definitions of linearity coexist in the literature, which differ by a factor 2. One is based on the Hamming distance and the other is based on the Walsh transform. We chose to use the latter which is usually easier to manipulate.

Remark 2. An S-box and its inverse have equal differential uniformity and linearity, but not generally equal algebraic degree (it is equal for 3-bit and 4-bit S-boxes though [DB18]).

2.2 Implementation Properties

Traditionally in hardware implementations, XOR gates were considered more expensive than AND gates. Indeed, in CMOS technology, a 2-input NAND gate requires only 4 transistors, whereas a 2-input XOR gate requires 8. However, with the advent of side-channel attacks and masked implementations as countermeasure, the weights have shifted and AND gates have become the most important cost factor[3]. In the case of hardware masked implementations, not only the number of such nonlinear gates should be minimized, but also the AND *depth* becomes very important. Larger AND depths are detrimental for the latency, as nonlinear layers in masked implementations need to be separated by a register stage [Bil15]. In contrast, XOR gates do not cause any increase in the number of clock cycles. In recent literature, we indeed see a trend of new cipher designs with nonlinear layers of minimal AND depth, such as Keccak [BDPA09] or PRIMATES [ABB+14]. Also in this work, when it comes to implementation properties, we will in the first place look at the *AND depth* of an S-box. Note that we only consider 2-input AND gates.

Definition 7 (AND depth)**.** The AND depth D of a function's circuit is defined as the maximum number of 2-input AND gates on any path from a function input to a function output over the basis (AND, XOR, NOT).

This implementation property is directly related to the cryptanalytic property of algebraic degree.

Lemma 1. *The implementation of a function* F *of algebraic degree* $\deg(\mathsf{F}) = d$ *has AND depth at least* $\lceil log_2(d) \rceil$.

While it is possible to implement any function with its theoretical minimal depth by considering every monomial in the ANF separately, we will only consider AND depths that result in reasonable circuit complexity. For example, the AES S-box has algebraic degree 7, but many practical circuits in literature use AND depth 4 or more [CB09, BP10].

Next, we consider the number of AND gates required to implement a function. Consider first the following definition.

[3] A Boolean masked implementation of an AND gate requires at least $(d+1)^2$ AND and $2(d^2+d)$ XOR gates; whereas of an XOR gate requires $d+1$ XOR gates where d corresponds to the security level [ISW03].

Definition 8 (Multiplicative Complexity [Sch88])**.** The multiplicative complexity MC of a function F is defined as the minimal number of AND gates required to evaluate F over the basis (AND, XOR, NOT).

However, a circuit with the absolute minimal number of AND gates may require more than the minimal AND depth. Mirwald and Schnorr [MS92] introduced the concept of level-1 multiplicative complexity, which we generalize as follows:

Definition 9 (Level-D Multiplicative Complexity)**.** The level-D multiplicative complexity MC_D of a function F is defined as the multiplicative complexity of F when constrained to D layers of AND gates.

They show that for quadratic Boolean functions and pairs of quadratic Boolean functions, $MC = MC_1$. Whether this is true for more general vectorial Boolean functions remains an open question [BF18].

In this work, in the context of low-latency masked hardware implementations, reducing AND depth is considered more important than reducing the AND gate complexity. For brevity, we refer to level-D multiplicative complexity as the AND gate complexity $G = MC_D$ where D is clear from the context.

Finally, for some applications, we also consider the cost (D and G) of the inverse S-box. For this purpose, we will introduce some new properties in § 4.1.

2.3 S-box Classification

Definition 10 (Affine Equivalence (AE))**.** Two S-boxes $\mathsf{S}_1, \mathsf{S}_2$ from $\mathbb{F}_2^s$ into $\mathbb{F}_2^s$ are *affine equivalent* ($\mathsf{S}_1 \sim \mathsf{S}_2$) if and only if there exists a pair of affine permutations A, B from $\mathbb{F}_2^s$ into $\mathbb{F}_2^s$ such that

$$\mathsf{S}_1 = \mathsf{B} \circ \mathsf{S}_2 \circ \mathsf{A}$$

where $\circ$ denotes function composition.

The following properties are all invariant under affine equivalence (AE):

- Differential uniformity δ
- Linearity $\mathcal{L}$
- Algebraic degree
- Possibility to implement with AND depth D
- Multiplicative complexities MC, MC_D

More precisely, affine equivalent S-boxes can be implemented with the same non-linear block. For these reasons, AE is a popular tool for classifying S-boxes. For instance for 4-bit S-boxes, rather than exploring 16! S-boxes, one can restrict the search to the 302 AE classes [Can07, Saa11]. Since linear operations are considered costless for masking, one can restrict to analyzing only one representative per AE class for an exhaustive exploration of masked implementation complexities. Full AE classification is available for 4-bit permutations, for APN S-boxes up to dimension five [BL08] and for *quadratic* S-boxes up to dimensions five [BBS17] and six [DB18] (note that quadratic S-boxes are useful for masking since they have minimal AND depth).

3 Optimizing Implementations for Masking

Circuit minimization for a given function is a complex problem. Still, for small-input functions, finding efficient implementations may be doable. For S-boxes, one usually aims at minimizing the number of gates, or the multiplicative complexity MC (*e.g.* in [SP14, Sto16, ÇTP19]). However, we focus here on jointly minimizing the AND gate count G and the AND depth D to enable low-latency masked hardware implementations.

In this section, we survey the S-box optimization tools from the literature and conclude that none of them consider the best criteria for masked hardware implementations. In this context, we adapt one of these tools for our purpose and apply it to various existing 4-bit S-boxes. We do not consider 3-bit S-boxes here, since they are quadratic and thus trivial to optimize. We do consider them in our overview Table 9 for comparison with other sizes. Our results show that the *joint* optimization for both G and D was previously not considered, as for some S-boxes, we reduce the AND depth D while maintaining the same AND gate count G. While this section introduces a tool that is instrumental in obtaining these results, the more important take-away is that the cost of masked hardware implementations has so far not been correctly perceived in the literature. Additionally, we provide specific circuit descriptions for all the results we obtain.

3.1 State of the Art of S-box optimization

Several tools exist to obtain implementations of S-boxes. We summarize some relevant tools for minimizing G and D in Table 1. Many tools look for bit-sliced implementations, *i.e.* with 2-input gates (AND and XOR, optionally OR, NAND, NOR, MOV and NOT).

One ground work is that of Ullrich *et al.* [UDCI+11] which uses an iterative-deepening depth-first-search (DFS) algorithm. We note that the purpose of this tool is not to optimize the implementation of a given S-box, but to find 4-bit S-boxes which satisfy given properties. It gives implementations with optimal number of bit-sliced gates. Another DFS algorithm was developped by Gladman [Gla07] to optimize the Serpent S-boxes, the code is available online[4]. The tool in [BMP13b] is based on short straight line programs (SLP) and is practical for up to 5-bit inputs for nonlinear functions. They optimize for multiplicative complexity and/or circuit depth.

The LIGHTER tool [JPST17] and the new platform PEIGEN[BGLS19] use the same core of optimizations: heuristic breadth-first search (BFS) and graph meet-in-the-middle strategy. They can optimize either for MC, number of gates or gate-equivalent-complexity (GEC), with a restriction on the set of operations: each operation must be invertible. These tools cannot handle S-boxes on more than 4 bits. Stoffelen's tool [Sto16] uses a SAT solver (CryptoMiniSat-5[5] [SNC09]) to find optimal circuit representations for a given metric. It can be applied to find circuits for S-boxes on up to 5 bits and becomes impractical for 6 bits. It is designed to minimize one of the following metrics: circuit depth, multiplicative complexity, bitslice gate complexity or logic gate complexity.

Minimizing for AND depth and AND gate complexity. None of the above described tools can optimize for AND depth, which is our primary target. Thus we build our own tool based on Stoffelen's [Sto16], since it can easily be adapted to minimize AND depth D. We also care about AND gate count G for masking, but Stoffelen's tool cannot optimize *jointly* for G and D, nor for G then D (or the reverse), since Stoffelen's tool takes as input a look-up table and therefore cannot make use of a previously optimized circuit.

Our tool builds upon Stoffelen's tool and extends its functionality (1) by allowing the optimization of D (a simple tweak) and (2) by enabling the *joint* optimization of G and D. We achieve this by generating the input for the SAT solver in an integrated way so that both G and D are optimized together (with priority on D). A more detailed description of our tool is given in Appendix A and in Algorithm 1.

3.2 Application to 4-bit S-boxes

We use the 4-bit S-boxes (and their inverses) as a case-study to demonstrate previous trends in the literature and to test the power of our tool in Table 2. Quadratic permutations on 4

[4] http://brg.a2hosted.com//oldsite/cryptography_technology/serpent/anal1.cpp
[5] https://www.msoos.org/cryptominisat5

Table 1: Capabilities of several state-of-the-art tools regarding G and D.

Tool	Ref.	method	G	D	(G, D)	size ($\leq n$)
Gladman	[Gla07]	DFS	×	×	×	4
Ullrich *et al.*	[UDCI+11]	ID-DFS	×	×	×	4
Boyar *et al.*	[BMP13b]	ad hoc + SLP	✓	×	×	5
Stoffelen	[Sto16]	SAT	✓	×	×	5
LIGHTER	[JPST17]	BFS-MitM	✓	×	×	4
PEIGEN	[BGLS19]	-//-	✓	×	×	4
This work	-	SAT	✓	✓	✓	*7

* very long run-times for $n \geq 6$

Table 2: Overview of optimization for various 4-bit S-boxes. The rows marked "inv" are involutions.

S	Cryptanalytic Prop.					Implementation Prop.						Prop.
	δ	$\mathcal{L}$	WP	Degr.		D		# AND		# XOR		
				S	S^{-1}	S	S^{-1}	S	S^{-1}	S	S^{-1}	
iClass13 [GLSV14]	4	8	2^{-2}	3	3	2	2	**4**	**4**	8	8	**inv**
Prøst [KLL+14]	4	8	2^{-2}	3	3	2	2	**4**	**4**	17	17	**inv**
Noekeon [DPVAR00]	4	8	2^{-2}	3	3	2	2	**4**	**4**	17	17	**inv**
Littlun-4 [KG16]	4	8	2^{-2}	3	3	2	2	**4**	**4**	4	5	-
Piccolo [SIH+11]	4	8	2^{-2}	3	3	2	2	**4**	**4**	4	11	-
Skinny [BJK+16]	4	8	2^{-2}	3	3	2	2	**4**	**4**	4	11	-
Class13 [UDCI+11]	4	8	2^{-2}	3	3	2	2	**4**	**4**	4	17	-
Rectangle [ZBL+15]	4	8	2^{-2}	3	3	2	2	**4**	**4**	14	19	-
Present [BKL+07]	4	8	2^{-2}	3	3	2	2	**4**	**4**	19	19	-
Gift [BPP+17]	6	8	2^{-2}	3	3	2	2	5	5	19	20	-
Prince [BCG+12]	4	8	2^{-2}	3	3	2	2	6	6	24	22	-
x^{-1}	4	8	2^{-2}	3	3	2	2	6	6	25	25	**inv**
x^3	**2**	8	2^{-2}	2	-	**1**	-	5	-	15	-	non-bij
x^6	**2**	8	2^{-2}	2	-	**1**	-	5	-	14	-	non-bij

bits have bad cryptanalytic properties, hence we focus on permutations with AND depth 2. Table 2 lists the evaluated 4-bit S-boxes along with their cryptanalytic and implementation properties, obtained with our tool. Observe that most of these S-boxes can have AND depth 2 and 4 AND gates. In fact, according to [CDL15, Lemma 4], 4 AND gates is the minimal G for 4-bit S-boxes with $(\delta, \mathcal{L}) = (4, 8)$.

Note that the PRESENT S-box [BKL+07] has a slightly better diffusion and that x^{-1} defined modulo $X^4 + X + 1$ and the Gift [BPP+17] and Prince [BCG+12] S-boxes have stronger algebraic properties[6]. We remark that these stronger properties seem to come with a slightly increased cost.

We add two non-bijective quadratic AB functions x^3 and x^6 over $\mathbb{F}_{2^4}$, as good building blocks for Feistel-like constructions (see §5).

Full circuit representations of all the S-boxes are given in supplementary material.

Improvements over the state-of-the-art: Table 3 demonstrates the improvements (in terms of masked cost) we were able to obtain over the implementations that exist in the literature. Since previous works often targeted minimal AND gate complexity, our most significant impact is naturally on the AND depth.

In some cases, such as for x^{-1} of [ZJ14] or the Gift S-box of [BPP+17], the difference in results clearly follows from a different optimization target, since we obtain lower AND depth at the cost of higher AND gate count. On the other hand, Table 3 also shows various

[6] Any linear combination of the output bits has degree 3, which helps against more sophisticated attacks than differential and linear.

Table 3: Improvements over the state-of-the-art

S	Ref.	D	G^*		D	G
iClass13	[GLSV14]**	3	4	⇒	2	4
Prøst	[Sto16]	3	4	⇒	2	4
Present	[PMK+11]	2	9	⇒	2	4
	[ZJ14]	4	4			
Rectangle	[Sto16]	4	4	⇒	2	4
Rectangle^{-1}	[Sto16]	4	4	⇒	2	4
Piccolo^{-1}	[SIH+11]	4	4	⇒	2	4
Skinny^{-1}	[BJK+16]	4	4	⇒	2	4
Prince	[BKN18]	3	6	⇒	2	6
x^{-1}	[ZJ14]	5	5	⇒	2	6
	[BP11]	2	7			
Gift	[BPP+17]	4	4	⇒	2	5
Noekeon	[DPVAR00]	4	4	⇒	2	6

* # AND gates or equivalents (OR,NAND,NOR)

** Note that the circuit in [GLSV14] is wrong, the last AND should have input bits 0 and 2, not 1 and 2 as depicted.

cases where our tool was able to lower D while achieving the same G.

Note that the implementations of the Present [PMK+11] and Prince [BKN18] S-boxes were meant for hardware masking (with TI) and that their optimization goal was thus similar to that of our tool.

3.3 Conclusion

Our results in this section can be seen as an improvement over the state-of-the-art for low latency masked implementations, but this is easily explained by the fact that these criteria were not previously considered in the literature. If they were not considered for the optimization of S-box circuits, they could not have been considered for the choice of S-boxes in new primitive designs. Hence, in the remainder of this work, we will explore suitable S-box choices for low latency masking, since it is essential that side-channel attacks are taken into account at design time. We will also use the tool of this section to obtain specific circuits for the proposed S-boxes.

4 AE Class-based Search of Low-depth S-boxes

While 4-bit S-boxes are very popular in the literature, a quick look at Table 2 reveals none of those with good cryptographic properties can be implemented with minimal AND depth ($D = 1$). As such, we extend the search space beyond this size and perform a search for larger S-boxes using affine equivalence classes, as many of the properties we are interested in are invariant within a class. We aim for high resistance against differential and linear cryptanalysis, but low algebraic degree, since we use it as a predictor for the AND depth D.

In the search for good S-boxes, the properties of the inverse S-box are often overlooked. Cryptographically, there is no need to worry about the differential uniformity and linearity, since they are identical to that of the forward S-box. For implementations however, the inverse S-box can be considerably more complex, especially when the algebraic degree is higher for the inverse than for the forward S-box.

The knowledge of S-boxes that have efficient implementations both forwards and backwards, would be a useful addition to the designer's toolbox. Especially interesting

are those S-boxes, which can be implemented together with their inverse, while sharing hardware resources. We will refer to them as *auto-invertible S-boxes*. The straightforward example in this respect is the AES S-box, which is based on the algebraic inversion in $\mathbb{F}_{2^8}$. However, in the context of masking, we target low AND depth S-boxes. For 3- and 4-bit S-boxes, the algebraic inverse mappings (resp. x^6 and x^{14}) are obvious candidates, since they can be implemented with AND depth resp. one and two. The algebraic degree of the inverse mapping in $\mathbb{F}_{2^n}$ is $n-1$. Hence, for $n > 4$, we are interested in finding more efficient alternatives with good cryptanalytic properties.

4.1 Inversion Properties

We start by introducing a series of properties related to the efficiency of an implementation of an inverse S-box together with the forward S-box. In these properties, we focus completely on the non-linear aspects of an implementation (D,G) since they constitute the largest cost factor in masked implementations. This also means that, in addition to the properties listed in §2.3, these inversion properties are invariant under affine equivalence. Hence, we can limit our search to the representatives of affine equivalence classes.

Involutive S-boxes (*e.g.* the algebraic inverse) are clearly superior when it comes to the implementation of the inverse S-box, but their use is not that common. Moreover, affine transformations do not preserve the involutive property. For example, the AES S-box is not involutive. However, it is auto-invertible because it is affine equivalent with the algebraic inverse and therefore also affine equivalent with its own inverse. We therefore first consider the following property:

Property 1. Consider an n-bit S-box S, which is affine equivalent to its inverse S^{-1}, *i.e.* $\mathsf{S} \sim \mathsf{S}^{-1} = \mathsf{B} \circ \mathsf{S} \circ \mathsf{A}$. Hence, the S-box S completely shares its non-linear components with the inverse S-box S^{-1}. We consider such an S-box auto-invertible.

An S-box that satisfies this property is an involution apart from the affine transformations. The same is true for all S-boxes affine equivalent to it.

S-box composition is a popular mechanism for obtaining higher-quality and higher-degree S-boxes which can be efficiently implemented with masking [BNN+12, KNP13, CPRR15, BGG+17]. This is useful if the depth-one S-boxes that satisfy Property 1 do not have sufficient quality for cryptographic purposes. In that case, we need to look for depth-two S-boxes that either satisfy Property 1 or can be decomposed into S-boxes that satisfy Property 1. We note that S-box decompositions have been studied many times [CPRR15, NNR19], but in this case, our particular focus lies in the joint consideration of the S-box itself with its inverse.

Moreover, even better than an auto-invertible S-box with depth two in the forward and backward direction, is an auto-invertible S-box of depth one with a depth-two inverse. This can be achieved as follows:

Property 2. Consider an n-bit S-box S with an inverse S^{-1} which can be decomposed as follows: $\mathsf{S}^{-1} = \mathsf{S} \circ \mathsf{F}$ or $\mathsf{S}^{-1} = \mathsf{F} \circ \mathsf{S}$ with $\lceil \log_2(\deg(\mathsf{F})) \rceil \leq \lceil \log_2(\deg(\mathsf{S}^{-1})) \rceil - \lceil \log_2(\deg(\mathsf{S})) \rceil$. Then, the inverse S-box S^{-1} only requires an additional implementation of F next to the original S-box S. We consider such an S-box auto-invertible.

S-boxes that satisfy this property can be implemented together with their inverse by implementing the inverse S-box only. The component F can simply be bypassed in the forward direction. The requirement $\lceil \log_2(\deg(\mathsf{F})) \rceil \leq \lceil \log_2(\deg(\mathsf{S}^{-1})) \rceil - \lceil \log_2(\deg(\mathsf{S})) \rceil$ makes sure that the total AND depth of the composition $\mathsf{F} \circ \mathsf{S}$ is not larger than the AND depth with which S^{-1} can be implemented.

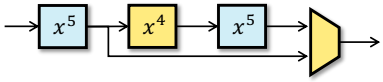

Figure 1: Efficient implementation of the AB power map S-box x^5 (Class 75) together with its inverse x^7.

4.2 5-bit S-boxes

Minimal depth. The work of Bozilov *et al.* [BBS17] gives us an exhaustive overview of 5-bit S-boxes with the minimal AND depth of one. Among these, classes 74 and 75, affine equivalent respectively to power maps x^3 and x^5 in $\mathbb{F}_{2^5}$, are AB functions. Their inverses are also AB, but of cubic degree and thus not with minimal AND depth.

Table 1 in [BBS17] notes all quadratic 5-bit S-box classes which have a quadratic inverse. Interestingly, we found that all 18 classes in this table satisfy Property 1.

Proposition 1. *Any quadratic 5-bit S-box* S *such that* $\deg(\mathsf{S}) = \deg(\mathsf{S}^{-1}) = 2$ *satisfies Property 1.*

This property is particularly useful when one wants to share resources between the encryption and decryption implementations. However, as the best cryptanalytic properties among these classes are $(\delta, \mathcal{L}) = (16, 32)$, none of them constitutes a suitable candidate. The number of rounds required to obtain a sufficiently low differential and linear property would nullify the advantage of low AND depth.

Remark 3. There exist no 5-bit S-boxes with good cryptanalytic properties and minimal AND depth for both the forward and backward direction.

Higher AND depth. Non-quadratic 5-bit S-boxes have not been classified so far. However, by composing quadratic functions, we can obtain higher-degree S-boxes with AND depth exactly two. This was done for example in [DB18, Table 7]. It is shown that the quartic APN function (x^{15}) can be decomposed using classes 74 and 75 from [BBS17], *i.e.* has AND depth two. This can also be shown using power maps [NNR19]: $x^{15} = (x^3) \circ (x^5)$. This S-box is thus useful when one is willing to trade minimal AND depth for higher algebraic degree. Moreover, since x^{15} is affine equivalent to the inversion ($x^{30} = (x^{15}) \circ (x^2)$) in $\mathbb{F}_{2^5}$, this S-box satisfies Property 1. Hence, this is an excellent auto-invertible candidate of depth two.

However, a 5-bit S-box that satisfies Property 2 also exists and is well known. It was shown in [DB18, NNR19] that the inverse of quadratic AB class 75 (power map x^5), is in fact a composition of class 75 *with itself*. Indeed: $(x^5) \circ (x^5) \circ (x^5) = x^{125} = x^{1 \bmod 31}$. This forward and inverse S-box can therefore be implemented together as shown in Figure 1. For implementation purposes, this makes class 75 far superior above class 74, which has the same cryptanalytic properties and has been used in the Fides authenticated encryption algorithm [BBK+13]. The most important 5-bit S-boxes are summarized in Table 4. Any of the AB's or APN suffice when the inverse S-box is not required, but only the AB x^5 and the APN x^{15} are good candidates when they should be implemented together with their inverse.

4.3 6-bit S-boxes

Minimal depth. As for 5-bit S-boxes, all 6-bit quadratic S-boxes have been classified according to affine equivalence [DB18]. There are no 6-bit AB functions and the only

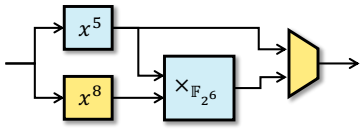

Figure 2: Efficient implementation of the 6-bit quadratic power map x^5 (class 2263) together with its inverse.

known APN has depth three. The search did however deliver eight quadratic classes (classes 2256 to 2263) that are far better than the others in terms of cryptanalytic properties with $\delta = 4$ and $\mathcal{L} = 16$. We note that these are the same cryptanalytic properties as for the Galois field inversion $x^{-1} = x^{62}$, which has algebraic degree 5 and AND depth 3. However, none of these eight S-boxes have a quadratic inverse.

We again search first for the equivalence classes that satisfy Property 1. Of the 70 classes that have a quadratic inverse, again all of those inverses belong to the same class.

Proposition 2. *Any quadratic 6-bit S-box* S *such that* $\deg(\mathsf{S}) = \deg(\mathsf{S}^{-1}) = 2$ *satisfies Property 1.*

All but one of these classes have differential uniformity at least 32 or linearity at least 64 and are thus not interesting. Only class 2230 achieves $(\delta, \mathcal{L}) = (16, 32)$, which is remarkably good considering the quality of the remaining quadratic S-boxes (see [DB18, Table 14]). In fact, there are only two quadratic 6-bit S-boxes with better properties (classes 2256 to 2263), but those do not satisfy Property 1. Nevertheless, we continue the search for better quality S-boxes.

Higher AND depth. We first attempt to find quadratic S-boxes that satisfy Property 2. For this, we only consider the eight best classes (2256 to 2263) since they have the best cryptanalytic properties and since the next best quality for quadratics ($(\delta, \mathcal{L}) = (16, 32)$) is obtained by the self-inverse class 2230, which already satisfies Property 1. We use the decomposition algorithm of [DB18] for each S^{-1}, in which we constrain one of the components to be S. This algorithm allows us to find F such that $\deg(\mathsf{F}) = 2$ and $\mathsf{S}^{-1} \sim \mathsf{F} \circ \mathsf{S}$. We find that for none of these eight classes, such a function F exists. This does not necessarily mean that none of the classes satisfy Property 2, but it is a lot more difficult to verify whether an F exists such that $\mathsf{S}^{-1} \sim \mathsf{S} \circ \mathsf{F}$. The algorithm from [DB18] would have to search for F^{-1} such that $\mathsf{S} \sim \mathsf{F}^{-1} \circ \mathsf{S}^{-1}$, in which case F^{-1} is not necessarily quadratic. Hence, the complexity of the search becomes too large.

Alternatively, we look at power maps in $\mathbb{F}_{2^6}$ and realize that odd class 2263 is AE to the power map x^5. The inverse of this map is x^{38} which is affine equivalent to x^{13}. Neither this exponent 13 nor any other $2^i \cdot 13$ is divisible by 5. However, apart from concatenation ($f \circ g$), another popular mechanism for function composition is that of multiplication chains. For example, the AES S-box has been decomposed using many variants of multiplication

Table 4: Minimal-depth 5-bit S-boxes Overview

S	**Cryptanalytic Prop.**					**Implementation Prop.**						Prop.
	δ	$\mathcal{L}$	WP	Degr.		D		# AND		# XOR		
				S	S^{-1}	S	S^{-1}	S	S^{-1}	S	S^{-1}	
Ascon (∼Keccak)	8	16	2^{-2}	2	3	**1**	2	**5**	**9**	5	38	-
Fides ($\sim x^3$)	2	8	$\mathbf{2^{-4}}$	2	3	**1**	2	7	10	29	50	-
(x^5)	2	8	$\mathbf{2^{-4}}$	2	3	**1**	2	7	10	26	54	**2**
(x^{15})	2	12	$2^{-2.8}$	4	4	2	2	≤ 14	≤ 14	≤ 55	≤ 55	**1**

chains [GPS14]. This can be considered as composition at the algebraic level (in the field $\mathbb{F}_{2^6}$) instead of at bit-level. In this case, x^{13} can be written as a multiplication of x^5 itself with the linear map x^8, which allows a very large degree of resource sharing between the forward S-box x^5 and its inverse. In the forward direction, the composition with x^8 can simply be bypassed (see Figure 2).

We summarize the results for 6 bits in Table 5. We do not include all classes since at this point, the tool is not able to find implementations for their inverses. However, in the forward direction, they all have an AND gate complexity of 8 at AND depth 1. We mention in particular class 2263 for its power map equivalence, and class 2258, to give a (far from optimal) estimate of a cost. For its inverse, we were able to reduce the cost of the implementation from the ANF to 22 AND gates. We also compare with the non-bijective cube function x^3 over $\mathbb{F}_{2^6}$.

Table 5: Minimal-depth 6-bit S-boxes Overview

S	Cryptanalytic Prop.					Implementation Prop.				
	δ	$\mathcal{L}$	WP	Degr.		D		# AND		Prop.
				S	S^{-1}	S	S^{-1}	S	S^{-1}	
Cl. 2230	16	32	2^{-2}	2	2	1	**1**	$\leq$ **6**	$\leq$ **6**	**1**
Cl. 2258	4	16	$\mathbf{2^{-4}}$	2	3	1	2	8	22	-
Cl. 2263 ($\sim x^5$)	4	16	$\mathbf{2^{-4}}$	2	3	1	2	8	≤ 26	**2**
(x^3)	2	16	$\mathbf{2^{-4}}$	2	-	1	-	9	-	non-bij

4.4 7-bit S-boxes

The space of 7-bit S-boxes (even only quadratic) is too large to classify with today's resources. Hence, very little is known about it. We do know that with odd size 7, we again get quadratic AB functions from power maps: x^3, x^5 and x^9 [Gol68]. The inverses of these permutations all have algebraic degree four.

It is clear that none of these functions satisfy Property 1. Our next best option is to find one that satisfies Property 2, but for simplicity, we now limit our search to power maps only.

First, for each power map x^q, we attempt to find a length-two decomposition of the inverse map using x^q as one of the components. We find the following results:

- $x^{1/3} \sim x^{45} = x^3 \circ x^{15}$ with $\deg(x^{15}) = 4$
- $x^{1/5} \sim x^{27} = x^5 \circ x^{107}$ with $\deg(x^{107}) = 5$
- $x^{1/9} \sim x^{15} = x^9 \circ x^{44}$ with $\deg(x^{44}) = 3$

While such decompositions exist, they are not useful in any of the three cases, since the total AND depth D of the composed inverse would be at least 3, which is larger than the lower bound (2) for quartic functions. Hence, when restricted to power maps, these permutations do not satisfy Property 2.

However, for each of the inverses, we do find length-two decompositions consisting only of quadratic components, as shown in Table 6. Interestingly, each quadratic power map's inverse is a composition of the other two. So while they do not satisfy any of the properties in § 4.1, we *can* implement them all with a considerable amount of resource sharing. To

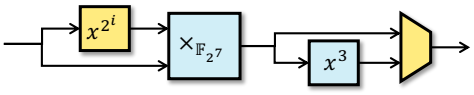

Figure 3: Efficient implementation of the 7-bit quadratic power maps x^5 or x^9 together with their inverse. The linear block can evaluate either x^4 or x^8.

Table 6: Minimal-depth 7-bit S-boxes Overview

S	Cryptanalytic Prop. δ	$\mathcal{L}$	WP	Degree S	Degree S^{-1}	Implementation Prop. D S	D S^{-1}	Prop.
x^3	2	16	2^{-6}	2	4	1	2	$S^{-1} \sim x^5 \circ x^9$
x^5	2	16	2^{-6}	2	4	1	2	$S^{-1} \sim x^3 \circ x^9$
x^9	2	16	2^{-6}	2	4	1	2	$S^{-1} \sim x^3 \circ x^5$

see this, consider their implementations at the algebraic level in $\mathbb{F}_{2^7}$. Each of these power maps can be implemented using a linear power-two exponentiation, followed by a Galois field multiplication in $\mathbb{F}_{2^7}$. The dominating component for the cost is the multiplication, which is common to all three functions. Hence, an implementation of such a quadratic map (for example x^5 or x^9) together with its inverse could be realised as in Figure 3. We do note that implementing a power map by means of a finite field multiplication $\times_{\mathbb{F}_{2^7}}$ is not as efficient as by optimization of the Boolean circuit.

We do not extend our search beyond these power maps, since they already obtain the best cryptanalytic properties and can also be implemented together with their inverse with a very high level of sharing. We summarize the properties in Table 6. From this point, it becomes infeasible for the tool to calculate the AND gate complexity. The remaining search aims primarily at AND depth and resource sharing with inverse S-boxes.

4.5 Larger S-boxes

With increasing S-box size, a comprehensive search becomes more and more challenging. We finish our search with an exploration of low-depth power functions of various sizes that satisfy one of the properties of § 4.1. The results are summarized in Table 7. At a size of 8 bits, the AES S-box is currently the best known. There are no quadratic power maps over $\mathbb{F}_{2^8}$ which form a bijection. For 9 bits, there are four quadratic power maps: x^3, x^5, x^9 and x^{17}, of which all but x^9 are AB. For two of the others, we found that they satisfy Property 2:

- $x^{1/5} = x^{409} \sim x^5 \circ x^{23}$ with $\deg(x^{23}) = 3$
- $x^{1/17} = x^{481} \sim x^{17} \circ x^{23}$ with $\deg(x^{23}) = 3$

Moreover, Nikova *et al.* found in [NNR19] that the $\mathbb{F}_{2^9}$ inversion x^{510} can be decomposed into the three quadratic ABs: $x^{-1} = x^{510} \sim x^{17} \circ x^5 \circ x^3$.

Increasing the size brings us to 10 bits, which is even. Hence, there are no quadratic AB power maps. Furthermore, the $\mathbb{F}_{2^{10}}$ inversion's decomposition into quadratic power maps has a depth of 15 [NNR19] and is thus not a good option at the moment. Nevertheless, x^5 and x^{17} are bijective with very good cryptanalytic properties $(\delta, \mathcal{L}) = (4, 64)$. In addition, they both satisfy Property 2 since $x^{17} \circ x^{17} \circ x^5 \circ x^5 \sim x$, *i.e.*

- $x^{1/5} = x^{614} \sim x^5 \circ x^{17} \circ x^{17}$
- $x^{1/17} = x^{662} \sim x^{17} \circ x^5 \circ x^5$

We also learn from this that there exists an involution of AND depth 2: $x^{340} = x^4 \circ x^5 \circ x^{17}$ and $x^{1/340} = x^{340}$. Its cryptanalytic properties are $(\delta, \mathcal{L}) = (10, 112)$ with algebraic degree 4.

Finally, with 11 bits, the AB power map x^{17} has a nicely decomposable inverse $x^{1445} = x^{17} \circ x^{17} \circ x^5$ and thus also satisfies Property 2. The finite field inversion x^{2046} has AND depth 8 when composed into quadratics [NNR19].

Table 7: Low-depth 8- to 11-bit S-boxes Overview

s	S	Cryptanalytic Prop. δ	$\mathcal{L}$	WP	Degree S	Degree S^{-1}	Implementation Prop. D S	D S^{-1}	Prop.
8	x^{254}	4	32	2^{-6}	7	7	4	4	**1**
9	x^5	2	32	2^{-8}	2	5	**1**	≥ 3	**2**
	x^{17}	2	32	2^{-8}	2	5	**1**	≥ 3	**2**
	x^{510} [NNR19]	2	44	2^{-7}	8	8	3	3	**1**
10	x^5	4	64	2^{-8}	2	5	**1**	3	**2**
	x^{17}	4	64	2^{-8}	2	5	**1**	3	**2**
	x^{340}	10	112	$2^{-6.4}$	4	4	2	**2**	**1**
11	x^{17}	2	64	$\mathbf{2^{-10}}$	2	6	**1**	3	**2**

5 Growing up: S-boxes from Domain-Extension Structures

Goal. The previous section showed that a class-based approach does not work when the S-box size becomes large. As of 7 bits, the search is limited to power maps. Also at this point, it becomes unfeasible for the tool from §3 to find efficient implementations. Hence in this section, we continue with a (no longer exhaustive) exploration based on domain-extending constructions. We use known constructions from literature and also introduce a new one. These constructions allow us (1) to control the AND depth and the level of resource sharing with the inverse from the start and (2) to determine the implementation costs of our S-boxes, using the results from previous sections. For simplicity, we will restrict to length-doubling structures.

Domain-extension structures. We consider three structures: 3-round Feistel, 3-round Misty and Bridge (new). Feistel and Misty are classical length-doubling structures, respectively introduced in [Fei73, DES77] and [Mat97] to design ciphers. In [LW14], Li and Wang gave initial bounds of security for 3-round Feistel S-boxes. These results were extended by Canteaut *et al.* in [CDL15] and used to find 8-bit S-boxes with few AND gates. Boss *et al.* [BGG+17] then reduced the area of 8-bit S-boxes at the cost of depth (including AND depth). The advantage of Feistel and Misty is that theoretical results are known on how to build them and what security to expect, from [LW14, CDL15] in general, and from [PUB16] for a particular case of Feistel which is an instance of the Butterfly structure. An interesting S-box for low AND depth is Littlun [KG16] by Karpman, with a Lai-Massey-like structure [LM90], whose inverse has a low AND depth. Bridge is a new structure, which can be seen as AE to the Littlun structure with a slightly lower cost.

Overview of the results. By plugging in quadratic components obtained from the tool, we get a variety of results with trade-offs between AND depth, AND gate count, cost of inverse and cryptanalytic properties $(\delta, \mathcal{L})$. These results are summarized in Table 8.

5.1 Definition of the Schemes

The schemes that we use and their inverses are defined in Figures 4(a), 4(b) and 4(c). For comparison with Bridge, we also show the Littlun-like Lai Massey network in Figure 4(d).

Lemma 2 (Feistel, Misty, Bridge AND depth)**.** *Let F, M and B be respectively a 3-round Feistel, a 3-round Misty and a Bridge schemes, with internal functions S_1, S_2 and S_3. Then for the AND depth of the forward and inverse S-boxes we have:*

- $D(F) = D(F^{-1}) = D(S_1) + D(S_2) + D(S_3)$,
- $D(M) = D(S_1) + \max_{i=2,3} D(S_i)$, $D(M^{-1}) = D(S_1^{-1}) + D(S_2^{-1}) + D(S_3^{-1})$,

Table 8: S-boxes obtained using length-doubling structures and low-depth components. The $\star$ symbol means that no good implementation was found by the tool for one of the components. The last column indicates whether the S-box is involutive (inv) or has a zero-overhead inverse (zo).

s	S	Cryptanalytic Prop. δ	$\mathcal{L}$	WP	Degr. S	Degr. S^{-1}	Implementation Prop. D S	D S^{-1}	# AND S	# AND S^{-1}	# XOR S	# XOR S^{-1}	Prop.
6	$\mathsf{Feistel}_{3,3,3}(x^3, x^3, x^3)$	4	16	2^{-4}	4	4	3	3	9	9	27	27	**inv**
	$\mathsf{Misty}_{3,3,3}(x^6, x^6, x^6)$	4	16	2^{-4}	3	4	**2**	3	9	9	21	21	**zo**
	$\mathsf{Bridge}_{3,3,3}(x^6, x^6, x^6)$	4	16	2^{-4}	3	4	**2**	**2**	9	9	21	21	**zo**
8	$\mathsf{Feistel}_{4,4,4}(x^3, iC13, x^3)$	8	64	2^{-4}	5	5	4	4	12	12	50	50	**inv**
	$\mathsf{Bridge}_{4,4,4}(x^3, iC13, iC13)$	16	64	2^{-4}	5	6	3	**3**	12	12	39	39	**zo**
	$\mathsf{Misty}_{4,4,4}(iC13, iC13, iC13)$	24	64	$2^{-3.4}$	5	6	4	6	12	12	30	32	**zo**
	$\mathsf{M} = \mathsf{Misty}_{5,3,5}(x^3, x^6, x^3)$	10	64	2^{-4}	3	5	**2**	5	17	27	71	71	-
10	$\mathsf{Feistel}_{5,5,5}(x^3, x^{\frac{1}{3}}, x^3)$	4	64	$\mathbf{2^{-8}}$	5	5	4	4	25	25	128	128	**inv**
	$\mathsf{Feistel}_{5,5,5}(x^3, x^3, x^3)$	6	96	$2^{-6.6}$	4	4	3	**3**	21	21	102	102	**inv**
	$\mathsf{Bridge}_{5,5,5}(x^3, x^3, x^3)$	10	64	$2^{-6.7}$	3	6	**2**	**3**	21	29	97	159	-
	$\mathsf{Misty}_{5,5,5}(x^3, x^3, x^3)$	10	96	$2^{-6.7}$	3	6	**2**	6	21	29	97	175	-
12	$\mathsf{Feistel}_{6,6,6}(x^3, Q2258, x^3)$	12	256	$\mathbf{2^{-8}}$	7	7	3	**3**	26	26	140	140	**inv**
	$\mathsf{Bridge}_{6,6,6}(x^3, Q2258, Q2258)$	18	512	2^{-6}	4	6	**2**	**3**	25	$53^\star$	131	161	-
	$\mathsf{Misty}_{6,6,6}(Q2258, Q2258, Q2258)$	24	512	2^{-6}	4	7	**2**	6	24	$66^\star$	126	171	-
14	$\mathsf{Feistel}_{7,7,7}(x^3, x^{1/3}, x^3)$	4	256	$\mathbf{2^{-12}}$	8	8	4	4	$121^\star$	$121^\star$	-	-	**inv**
	$\mathsf{Feistel}_{7,7,7}(x^3, x^3, x^3)$	12	512	2^{-10}	4	4	3	**3**	45	45	261	261	**inv**
	$\mathsf{Bridge}_{7,7,7}(x^3, x^3, x^3)$	12	256	$2^{-10.4}$	3	8	**2**	**3**	45	$197^\star$	254	-	-
	$\mathsf{Misty}_{7,7,7}(x^3, x^3, x^3)$	16	512	2^{-10}	3	8	**2**	6	45	$241^\star$	254	-	-
16	$\mathsf{Feistel}_{8,8,8}(x^3, x^{-1}, x^3)$	10	1280	$\mathbf{2^{-11.3}}$	11	11	6	6	$90^\star$	$90^\star$	-	-	**inv**
	$\mathsf{Feistel}_{8,8,8}(x^3, \mathsf{M}, x^3)$	20	2048	2^{-10}	10	10	4	**4**	$63^\star$	$63^\star$	-	-	**inv**
	$\mathsf{Bridge}_{8,8,8}(x^3, \mathsf{M}, \mathsf{M})$	64	3072	2^{-8}	6	10	**3**	6	$62^\star$	$72^\star$	-	-	-
	$\mathsf{Misty}_{8,8,8}(\mathsf{M}, \mathsf{M}, \mathsf{M})$	100	4096	2^{-8}	6	12	4	15	51	81	229	229	-

- $D(B) = D(S_1) + \max_{i=2,3} D(S_i)$, $D(B^{-1}) = D(S_1) + \max_{i=2,3} D(S_i^{-1})$

Remark 4 (Non-bijective components). The Feistel scheme is bijective independently of the bijectivity of its components (although according to [LW14, CDL15], S_2 must be bijective to have good cryptanalytic properties) and Bridge is bijective independently of the bijectivity of S_1. We will exploit this, since using non-bijective components is less restrictive and sometimes useful. For instance, there are no quadratic APN permutations on even sizes, but there are quadratic APN functions, such as x^3.

Field polynomials. In the following, many components are quadratic power maps over finite fields of size m. These fields are defined using the following irreducible polynomials:

- $\mathbb{F}_{2^3}$: $X^3 + X + 1$;
- $\mathbb{F}_{2^4}$: $X^4 + X + 1$;
- $\mathbb{F}_{2^5}$: $X^5 + X^2 + 1$;
- $\mathbb{F}_{2^6}$: $X^6 + X^4 + X^3 + 1$;
- $\mathbb{F}_{2^7}$: $X^7 + X + 1$;
- $\mathbb{F}_{2^8}$: $X^8 + X^4 + X^3 + X^2 + 1$.

5.1.1 Butterfly-like Feistel

This structure is so well understood from results in [PUB16] and further results from [CDP17, FFW17, LTYW18, CPT19] that we can get all the results we need from theory. It is only defined for $n = 2m$, m odd, and corresponds to the 3-round $\mathsf{Feistel}_{m,m,m}(x^e, x^{1/e}, x^e)$, with e of Hamming weight 2. We know that it always has $\delta = 4$, $\mathcal{L} = 2^{m+1}$, $\deg = m + 1$ and, since x^e is quadratic, it can be implemented with $D = 1$. We obtain the cost for the inverse at low D from §4.5, and the cost in gates is the sum of the cost of the components,

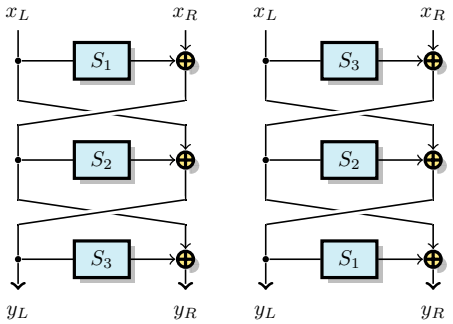

Figure 4(a): 3-round Feistel (left) and inverse (right).

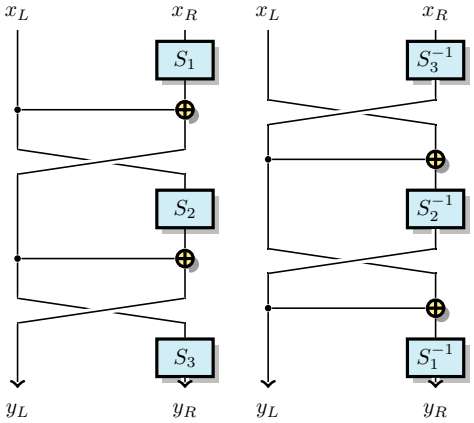

Figure 4(b): 3-round Misty (left) and inverse (right).

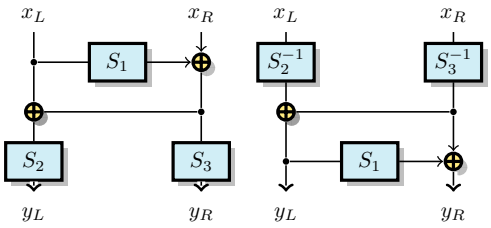

Figure 4(c): Bridge (left) and inverse (right).

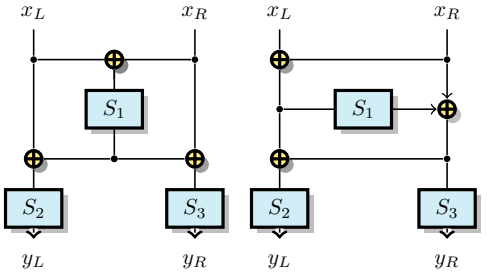

Figure 4(d): Littlun-like scheme equivalent representations.

plus the cost of three m-bit XORs. Moreover, a Feistel structure with $S_1 = S_3 = x^e$ is automatically an involution, which makes this structure excellent for the inversion criterion. For simplicity, we restrict ourselves to $e = 3$. The results are summarized in Table 8.

5.1.2 Feistel

Although the Butterfly-like Feistel gives the best cryptanalytic properties that a 3-round Feistel network can reach, the use of the inverse of a quadratic permutation is costly. We hereby study Feistel networks on $n = 2m$ bits for which all the components are quadratic. Following [LW14, CDL15], we restrict S_2 to be bijective to get good cryptanalytic properties. As long as it is possible, we use x^3 on $\mathbb{F}_{2^m}$ as component. When this component is not bijective (*i.e.* when m is even), we use a quadratic bijection when available. In particular, we use the best 4-bit bijective S-box from the tool iClass13, and on 8 bits, we use x^{-1}, or alternatively an unbalanced Misty structure with $D = 2$, defined in §5.1.3. We also keep the restriction of $S_1 = S_3$ so that our resulting S-boxes are always involutive. Some components cannot be run by the tool, such as x^3 on $\mathbb{F}_{2^8}$, $x^{1/3}$ on $\mathbb{F}_{2^7}$ and $Q2258^{-1}$. Therefore, we use ad hoc sub-optimal implementations obtained from the ANF.

The resulting S-boxes have weaker $(\delta, \mathcal{L})$ than the Butterfly-like Feistel, but at a lower cost. On 8 bits, we can compare with the Scream v3 S-box [GLS+14], a 3-round Feistel based on [CDL15] with 12 ANDs at AND depth 5 (we get AND depth 4).

5.1.3 Misty

As was observed in [CDL15], Misty requires bijective components to get a bijective construction and may lead to worse cryptanalytic properties than Feistel. Yet apart from the special case with 4-bit components, it seems that both Feistel and Misty give similar cryptanalytic properties. Misty has the advantage of allowing to spare one m-bit XOR and of having a lower D for the forward direction.

We use the same components as the bijective components of the Feistel network. The Misty structure has as drawback that it does not yield involutive S-boxes. Yet if we use involutive components, the inverse can be implemented with zero overhead over the forward S-box (barring multiplexers and control logic). We therefore use x^6 rather than x^3 on $\mathbb{F}_{2^3}$.

On 8 bits, we can compare with the Robin S-box [GLSV14], a 3-round Misty defined as $\mathsf{Misty}_{4,4,4}(Class13, Class13, Class13)$. Its properties are the same as the one using $iClass13$ instead (see Table 8), which are not very good compared to other 8-bit schemes.

Unbalanced Misty. Following the reasoning in [CDL15], we add an 8-bit unbalanced Misty network. We use $\mathsf{Misty}_{5,3,5}(x^3, x^6, x^3)$, where the compression function used on the left input of the round 1 XOR is $(x_0, x_1, x_2, x_3, x_4) \mapsto (x_2, x_3, x_0)$ and the expansion function used on the left input of the round 2 XOR is $(x_0, x_1, x_2) \mapsto (x_0, 0, x_2, x_1, 0)$. This gives a similar result as the one from [CDL15].

5.1.4 Bridge

The Bridge scheme derives from the Littlun structure, which in itself derives from the Lai-Massey structure [LM90]. Bridge can also be seen as a mix between Feistel and Misty, or Feistel and SPN. It has a low AND depth, both for the forward and backward directions. Like Misty, it cannot result in an involutive S-box, but if S_2 and S_3 are involutions, the inverse has zero overhead. We thus use the same bijective components as the Misty case (to have involutions) and the same non-bijective components as the Feistel case.

On 8 bits, we can compare with Littlun [KG16], which uses $S_1 = S_2 = S_3 = Class13$, has $(D, G) = (4, 12)$. Our 8-bit example reaches $(D, G) = (3, 12)$, with the same $(\delta, \mathcal{L})$. Note however that Littlun has branch number 3, which we do not consider.

5.2 Discussion

Bridge > Misty. In practice, it appears that balanced Bridge and Misty give similar δ and $\mathcal{L}$. They also have similar D in the forward direction, but Bridge has a lower D in the backward direction, which makes it a better candidate than balanced Misty in general. Additionally, in the case of Bridge, the scheme can be bijective even if S_1 is not bijective, which allows for more choices of S_1 than in the case of Misty.

Bridge vs Feistel. Bridge and Feistel usually give similar results in terms of δ and $\mathcal{L}$, but Feistel has a worse D in the forward direction. However, the inverse of Bridge requires the use of S_2^{-1} and S_3^{-1} which, in general, are more costly and have a higher D than S_2 and S_3. Therefore, Feistel can still give a better overall D than Bridge, but Bridge can be better when lightweight inverses for S_2 and S_3 are available (in particular, inverses with low D).

Unbalanced Feistel and Bridge. Note that an unbalanced Feistel network built in the same way as the Misty one (dropping bits on odd rounds and inserting bits at round 2, without changing anything else), cannot give good cryptanalytic properties since it breaks the rule of having S_2 bijective, required from [LW14, CDL15]. Other unbalanced schemes can be considered (as in [BGG+17] for instance, were the linear layer is modified)

to avoid this issue, but this is a more complicated approach which is out of our scope. The Bridge structure does not share this rule of needing one bijective component to get good cryptanalytic properties, but in practice, the same way of building an unbalanced Bridge seems to give bad cryptanalytic properties.

Significance of the Search Space. We chose a limited search space for our length-doubling search: we only used few choices of components S_i. Yet, this is enough to get some idea of what to expect. Indeed, focusing on the Feistel structure, we expect the best possible WP, given by LP, to be roughly $\max_{i,j\neq i} LP(S_i)LP(S_j)$. We reach this optimum apart from the 16-bit case (the optimum is 2^{-12} and we reach $2^{-11.3}$). With Misty and Bridge, we expect to be able to reach something close to this bound with another choice of S_i. This is enough to give us an idea of what to expect from S-boxes built from length-doubling structures and to have a first idea of how they compare with smaller S-boxes.

Widening the Search Space. Our approach can be extended in various ways. First, we only considered length-doubling structures and some very simple unbalanced structures. Considering more complex domain-extension structures, in particular on more than two branches, may give some very different results. We also limited our search to the use of only three components, in order to limit the number of AND gates, but maybe a trade-off is possible between number of ANDs and AND depth by using more components (for instance with 2-round SPN, like investigated in [BGG+17]).

The main limitation on the implementation properties of the results comes from the use of inverses, which are generally costly. The use of non-bijective components helps in this case, because we have them at a lower cost, even though they are less studied, which implies that more work on non-bijective components should be able to mitigate the cost.

Finally, we should note that all three structures considered here, Feistel, Misty and Bridge, have a common issue when it comes to linearity, see Lemma 3. Identifying some new structures able to reach a low LP as well as a low DP would be a worthwhile work, not only in this context, since it deals with the security of widely-used structures.

Lemma 3 (Sub-optimality for LP)**.** *Feistel and Misty are notably worse for LP than for DP. In particular, on $n = 2m$ bits, with $WP(S_i) = DP(S_i) = LP(S_i)$ equal for all i:*

$$DP \geq \tfrac{2}{2^m} WP(S_i)\,, \quad LP \geq \tfrac{16}{2^m} WP(S_i)\,.$$

Proof. From [CDL15], for Feistel and Misty, $\delta \geq 2\delta(S_i)$ and $\mathcal{L} \geq 4\mathcal{L}(S_i)$. Then:

$$DP \geq \tfrac{2}{2^{2m}}\delta = \tfrac{2}{2^m} WP(S_i)\,,$$

$$LP \geq \left(\tfrac{4}{2^{2m}}\mathcal{L}\right)^2 = \tfrac{16}{2^m} WP(S_i)\,.$$

□

We conjecture the same for Bridge.

6 Conclusions

Our work produces a toolbox of ready-to-use S-boxes with low AND depth, low AND complexity and efficient inverses. We demonstrated optimal S-box circuits on 4 bits for low latency masking, by introducing a tool that is able to jointly minimize two criteria. For larger sizes, we provide new insights into the properties of existing S-boxes or construct new S-boxes according to our criteria. Our research demonstrates that it is possible to

combine strong functional properties with efficient implementations, even when sharing resources with the inverse S-box is desired.

We observed that odd S-box sizes, despite being very unpopular in cipher designs, typically result in better functional properties at lower cost. In particular, Table 9 shows that we did not encounter any $2n$-bit S-box with a lower WP than the $2n-1$-bit S-boxes.

Additionally, there is a bias towards small bit sizes in the state-of-the-art, which seems to be due to the simpler exhaustive exploration of the search space more than due to qualitative considerations. Our observations naturally suggest the further exploration of unconventional design choices (odd and larger S-box sizes) as an interesting research direction.

Finally, considering S-boxes with differential, linear and algebraic criteria is not enough. Several research directions include (1) considering more cryptanalytic properties, (2) exploring and comparing diffusion layers and (3) exploring and comparing full primitives based on S-boxes and diffusion layers. In this view, odd and large S-boxes appear as interesting candidates which need testing at the primitive level.

Acknowledgements

This work was partly supported by CyberSecurity Research Flanders with reference number VR20192203. Lauren De Meyer is funded by a PhD fellowship of the Fund for Scientific Research - Flanders (FWO). François-Xavier Standaert is a senior research associate of the Belgian Fund for Scientific Research (F.R.S.-FNRS). This work has been funded in parts by the European Union through the ERC project SWORD (724725), the H2020 project REASSURE and the European Union and Walloon Region FEDER USERMedia project 501907-3791.

References

[ABB+14] Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda. APE: authenticated permutation-based encryption for lightweight cryptography. In Cid and Rechberger [CR15], pages 168–186.

[ALP+19] Elena Andreeva, Virginie Lallemand, Antoon Purnal, Reza Reyhanitabar, Arnab Roy, and Damian Vizár. Forkcipher: a new primitive for authenticated encryption of very short messages. *IACR Cryptology ePrint Archive*, 2019:1004, 2019.

[Ava17] Roberto Avanzi. The QARMA block cipher family. almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency S-boxes. *IACR Trans. Symmetric Cryptol.*, 2017(1):4–44, 2017.

[BBB+] Davide Bellizia, Francesco Berti, Olivier Bronchain, Gaëtan Cassiers, Sébastien Duval, Chun Guo, Gregor Leander, et al. Spook. submission to the NIST LWC competition. https://www.spook.dev.

[BBK+13] Begül Bilgin, Andrey Bogdanov, Miroslav Knezevic, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Bertoni and Coron [BC13], pages 142–158.

[BBS17] Dusan Bozilov, Begül Bilgin, and Haci Ali Sahin. A note on 5-bit quadratic permutations' classification. *IACR Trans. Symmetric Cryptol.*, 2017(1):398–404, 2017.

[BC13] Guido Bertoni and Jean-Sébastien Coron, editors. *Cryptographic Hardware and Embedded Systems - CHES 2013, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *LNCS*. Springer, 2013.

[BCG+12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *LNCS*, pages 208–225. Springer, 2012.

[BDPA09] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The road from panama to keccak via radiogatún. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography*, number 09031 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2009. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.

[BF18] Joan Boyar and Magnus Gausdal Find. Multiplicative complexity of vector valued boolean functions. *Theor. Comput. Sci.*, 720:36–46, 2018.

[BGG+17] Erik Boss, Vincent Grosso, Tim Güneysu, Gregor Leander, Amir Moradi, and Tobias Schneider. Strong 8-bit S-boxes with efficient masking in hardware extended version. *J. Cryptographic Engineering*, 7(2):149–165, 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*, pages 330–394, 2019.

[Bil15] Begül Bilgin. *Threshold Implementations: As Countermeasure Against Higher-Order Differential Power Analysis*. PhD thesis, KU Leuven, Belgium & UTwente, The Netherlands, 2015.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Robshaw and Katz [RK16], pages 123–153.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.

[BKN18] Dusan Bozilov, Miroslav Knezevic, and Ventzislav Nikov. Optimized threshold implementations: Securing cryptographic accelerators for low-energy and low-latency applications. *IACR Cryptology ePrint Archive*, 2018:922, 2018.

[BL08] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptography*, 49(1-3):273–288, 2008.

[BMP13a] Joan Boyar, Philip Matthews, and René Peralta. Logic minimization techniques with applications to cryptology. *J. Cryptology*, 26(2):280–312, 2013.

[BMP13b] Joan Boyar, Philip Matthews, and René Peralta. Logic minimization techniques with applications to cryptology. *Journal of Cryptology*, 26(2):280–312, 2013.

[BNN+12] Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, and Georg Stütz. Threshold implementations of all 3x3 and 4x4 S-boxes. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *LNCS*, pages 76–91. Springer, 2012.

[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 *LNCS*, pages 178–189. Springer, 2010.

[BP11] Joan Boyar and René Peralta. A depth-16 circuit for the AES S-box. *IACR Cryptology ePrint Archive*, 2011:332, 2011.

[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, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *LNCS*, pages 321–345. Springer, 2017.

[BPPS17] Francesco Berti, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. On leakage-resilient authenticated encryption with decryption leakages. *IACR Trans. Symmetric Cryptol.*, 2017(3):271–293, 2017.

[BR14] Lejla Batina and Matthew Robshaw, editors. *Cryptographic Hardware and Embedded Systems - CHES 2014, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *LNCS*. Springer, 2014.

[Bri07] Marcus Brinkmann. Classification of Almost Perfect Nonlinear Functions up to Dimension Five. Master's thesis, Ruhr-Universität Bochum, 2007.

[Can07] Christophe De Cannière. *Analysis and Design of Symmetric Encryption Algorithms*. PhD thesis, Katholieke Universiteit Leuven, 2007.

[CB09] D. Canright and Lejla Batina. A very compact "perfectly masked" S-box for AES (corrected). *IACR Cryptology ePrint Archive*, 2009:11, 2009.

[CDL15] Anne Canteaut, Sébastien Duval, and Gaëtan Leurent. Construction of lightweight S-boxes using Feistel and MISTY structures. In Orr Dunkelman and Liam Keliher, editors, *Selected Areas in Cryptography - SAC 2015, Sackville, NB, Canada, August 12-14, 2015*, volume 9566 of *LNCS*, pages 373–393. Springer, 2015.

[CDNY18] Avik Chakraborti, Nilanjan Datta, Mridul Nandi, and Kan Yasuda. Beetle family of lightweight and secure authenticated encryption ciphers. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):218–241, 2018.

[CDP17] Anne Canteaut, Sébastien Duval, and Léo Perrin. A generalisation of dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. *IEEE Trans. Information Theory*, 63(11):7575–7591, 2017.

[CPRR15] Claude Carlet, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Algebraic decomposition for probing security. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *LNCS*, pages 742–763. Springer, 2015.

[CPT19] Anne Canteaut, Léo Perrin, and Shizhu Tian. If a generalised butterfly is APN then it operates on 6 bits. *Cryptography and Communications*, Apr 2019.

[CR15] Carlos Cid and Christian Rechberger, editors. *Fast Software Encryption - FSE 2014, London, UK, March 3-5, 2014*, volume 8540 of *LNCS*. Springer, 2015.

[ÇTP19] Çagdas Çalik, Meltem Sönmez Turan, and René Peralta. The multiplicative complexity of 6-variable boolean functions. *Cryptography and Communications*, 11(1):93–107, 2019.

[CV94] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *EUROCRYPT '94, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *LNCS*, pages 356–365. Springer, 1994.

[DB18] Lauren De Meyer and Begül Bilgin. Classification of balanced quadratic functions. *IACR Cryptology ePrint Archive*, 2018:113, 2018.

[DEM+17] Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, and Thomas Unterluggauer. ISAP - towards side-channel secure authenticated encryption. *IACR Trans. Symmetric Cryptol.*, 2017(1):80–105, 2017.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. *CAESAR Competition, Finalist*, 2016.

[DES77] Data encryption standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce, January 1977.

[DGM+] Nilanjan Datta, Ashrujit Ghoshal, Debdeep Mukhopadhyay, Sikhar Patranabis, Stjepan Picek, and Rajat Sadhukhan. TRIFLE. submission to the NIST LWC competition. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/trifle-spec.pdf.

[DPVAR00] Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. Nessie proposal: Noekeon. In *First Open NESSIE Workshop*, pages 213–230, 2000.

[DR01] Joan Daemen and Vincent Rijmen. The wide trail design strategy. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, volume 2260 of *LNCS*, pages 222–238. Springer, 2001.

[Fei73] Horst Feistel. Cryptography and computer privacy. *Scientific american*, 228(5):15–23, 1973.

[FFW17] Shihui Fu, Xiutao Feng, and Baofeng Wu. Differentially 4-uniform permutations with the best known nonlinearity from butterflies. *IACR Trans. Symmetric Cryptol.*, 2017(2):228–249, 2017.

[GGNS13] Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In Bertoni and Coron [BC13], pages 383–399.

[GJK+] Dahmun Goudarzi, Jérémy Jean, Stefan Kölbl, Thomas Peyrin, Matthieu Rivain, Yu Sasaki, and Siang Meng Sim. Pyjamask. submission to the NIST LWC competition. https://pyjamask-cipher.github.io.

[Gla07] Brian Gladman. Finding efficient boolean function decompositions for the serpent s-boxes and their inverses. Accessed: 2019-07.

[GLS+14] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, François Durvaux, Lubos Gaspar, and Stéphanie Kerckhof. SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption with Masking. *CAESAR competition*, 2014.

[GLSV14] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. LS-designs: Bitslice encryption for efficient masked software implementations. In Cid and Rechberger [CR15], pages 18–37.

[Gol68] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, January 1968.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *CRYPTO 2011, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *LNCS*, pages 222–239. Springer, 2011.

[GPS14] Vincent Grosso, Emmanuel Prouff, and François-Xavier Standaert. Efficient masked S-boxes processing - A step forward -. In David Pointcheval and Damien Vergnaud, editors, *AFRICACRYPT 2014, Marrakesh, Morocco, May 28-30, 2014. Proceedings*, volume 8469 of *LNCS*, pages 251–266. Springer, 2014.

[GR16] Dahmun Goudarzi and Matthieu Rivain. On the multiplicative complexity of boolean functions and bitsliced higher-order masking. In Benedikt Gierlichs and Axel Y. Poschmann, editors, *Cryptographic Hardware and Embedded Systems - CHES 2016, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, volume 9813 of *LNCS*, pages 457–478. Springer, 2016.

[GR17] Dahmun Goudarzi and Matthieu Rivain. How fast can higher-order masking be in software? In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *LNCS*, pages 567–597, 2017.

[ISW03] Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *LNCS*, pages 463–481. Springer, 2003.

[JPST17] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing implementations of lightweight building blocks. *IACR Transactions on Symmetric Cryptology*, pages 130–168, 2017.

[JSV17] Anthony Journault, François-Xavier Standaert, and Kerem Varici. Improving the security and efficiency of block ciphers based on LS-designs. *Des. Codes Cryptography*, 82(1-2):495–509, 2017.

[KG16] Pierre Karpman and Benjamin Grégoire. The littlun s-box and the fly block cipher. In *Lightweight Cryptography Workshop*, pages 17–18, 2016.

[KLL+14] Elif Bilge Kavun, Martin M Lauridsen, Gregor Leander, Christian Rechberger, Peter Schwabe, Tolga Yalçın, and DTU Compute. Prøst v1.1. *CAESAR Competition, Round 1 Candidate*, 2014.

[KNP13] Sebastian Kutzner, Phuong Ha Nguyen, and Axel Poschmann. Enabling 3-share threshold implementations for all 4-bit S-boxes. In Hyang-Sook Lee and Dong-Guk Han, editors, *Information Security and Cryptology - ICISC 2013, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, volume 8565 of *LNCS*, pages 91–108. Springer, 2013.

[KPPY14] Khoongming Khoo, Thomas Peyrin, Axel York Poschmann, and Huihui Yap. FOAM: searching for hardware-optimal SPN structures and components with a fair comparison. In Batina and Robshaw [BR14], pages 433–450.

[LM90] Xuejia Lai and James L. Massey. A proposal for a new block encryption standard. In Ivan Damgård, editor, *EUROCRYPT '90, Aarhus, Denmark, May 21-24, 1990, Proceedings*, volume 473 of *LNCS*, pages 389–404. Springer, 1990.

[LP07] Gregor Leander and Axel Poschmann. On the classification of 4 bit S-boxes. In Claude Carlet and Berk Sunar, editors, *Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings*, volume 4547 of *LNCS*, pages 159–176. Springer, 2007.

[LRW11] Moses Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. *J. Cryptology*, 24(3):588–613, 2011.

[LTYW18] Yongqiang Li, Shizhu Tian, Yuyin Yu, and Mingsheng Wang. On the generalization of butterfly structure. *IACR Trans. Symmetric Cryptol.*, 2018(1):160–179, 2018.

[LW14] Yongqiang Li and Mingsheng Wang. Constructing S-boxes for lightweight cryptography with feistel structure. In Batina and Robshaw [BR14], pages 127–146.

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *Fast Software Encryption - FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *LNCS*, pages 54–68. Springer, 1997.

[MM82] Carl H. Meyer and Stephen M. Matyas. *Cryptography: A New Dimension in Computer Data Security*, chapter Implementation Considerations for the S-box Design, pages 163–165. John Wiley & Sons, 1982.

[MS92] Roland Mirwald and Claus-Peter Schnorr. The multiplicative complexity of quadratic boolean forms. *Theor. Comput. Sci.*, 102(2):307–328, 1992.

[NNR19] Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Decomposition of permutations in a finite field. *Cryptography and Communications*, 11(3):379–384, 2019.

[NRS11] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *J. Cryptology*, 24(2):292–321, 2011.

[Nyb94] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, pages 111–130, 1994.

[oS77] National Bureau of Standards. Data encryption standard. FIPS-Pub.46, January 1977.

[PMK+11] Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-channel resistant crypto for less than 2,300 ge. *Journal of Cryptology*, 24(2):322–345, 2011.

[PRC12] Gilles Piret, Thomas Roche, and Claude Carlet. PICARO - A block cipher allowing efficient higher-order side-channel resistance. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Applied Cryptography and Network Security - ACNS 2012, Singapore, June 26-29, 2012. Proceedings*, volume 7341 of *LNCS*, pages 311–328. Springer, 2012.

[PUB16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In Robshaw and Katz [RK16], pages 93–122.

[RK16] Matthew Robshaw and Jonathan Katz, editors. *CRYPTO 2016, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *LNCS*. Springer, 2016.

[Saa11] Markku-Juhani O. Saarinen. Cryptographic analysis of all 4 x 4-bit S-boxes. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - SAC 2011, Toronto, ON, Canada, August 11-12, 2011*, volume 7118 of *LNCS*, pages 118–133. Springer, 2011.

[Sch88] Claus-Peter Schnorr. The multiplicative complexity of boolean functions. In Teo Mora, editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 6th International Conference, AAECC-6, Rome, Italy, July 4-8, 1988, Proceedings*, volume 357 of *LNCS*, pages 45–58. Springer, 1988.

[SIH+11] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: an ultra-lightweight blockcipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 342–357. Springer, 2011.

[SNC09] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending SAT solvers to cryptographic problems. In Oliver Kullmann, editor, *Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings*, volume 5584 of *LNCS*, pages 244–257. Springer, 2009.

[SP14] Meltem Turan Sönmez and René Peralta. The multiplicative complexity of boolean functions on four and five variables. In *International Workshop on Lightweight Cryptography for Security and Privacy*, pages 21–33. Springer, 2014.

[Sto16] Ko Stoffelen. Optimizing S-box implementations for several criteria using SAT solvers. In Thomas Peyrin, editor, *Fast Software Encryption - FSE 2016, Bochum, Germany, March 20-23, 2016*, volume 9783 of *LNCS*, pages 140–160. Springer, 2016.

[UDCI+11] Markus Ullrich, Christophe De Canniere, Sebastiaan Indesteege, Özgül Küçük, Nicky Mouha, and Bart Preneel. Finding optimal bitsliced implementations of 4× 4-bit S-boxes. In *SKEW 2011 Symmetric Key Encryption Workshop, Copenhagen, Denmark*, pages 16–17, 2011.

[ZBL+15] Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, and Ingrid Verbauwhede. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *SCIENCE CHINA Information Sciences*, 58(12):1–15, 2015.

[ZJ14] Pavol Zajac and Matúš Jókay. Multiplicative complexity of bijective 4× 4 S-boxes. *Cryptography and Communications*, 6(3):255–277, 2014.

A Description of the tool

Our tool works in two steps. First, it extends Stoffelen's tool by minimizing jointly G and D. Second, we isolate the input and output affine layers and optimize them using the CADENCE Genus synthesizer[7]. We use the naming and notation from [Sto16]: The variables x_i and y_i represent S-box inputs and outputs respectively.

SAT (satisfiability) solver step. As done in [Sto16], we create a generic model of gates and a set of constraints on wiring and feed it to a SAT solver. The SAT solver assigns the wires such that the circuit implements the correct S-box. Our model is shown in Figure 5 and is built in order to optimize our criteria of AND depth D and AND gate count G. There are D layers of AND gates, separated by affine layers. This means that the inputs of any AND gate can be assigned to some affine combination of the inputs and outputs of the previous layers. The same is true for the circuit outputs y_i. We restrict to AND, XOR and NOT gates, since OR, NAND and NOR gates can be obtained with few additional NOTs, which hardly matter for our purposes. We introduce an additional meta-parameter WFD which is the number of AND chains of full AND-depth. This parameter gives more control over the implementation, as it allows to reduce G for target D and ultimately reduce the runtime. We start with WFD full chains of AND depth D, then potentially treat a last un-full chain (of length $mod(G, D)$)[8]. To allow for the algebraic degree of the un-full chain to be maximal, we place the ANDs of the un-full chain at maximal depth (*i.e.* their inputs can come of any x_i or AND gates at depth less than $D-1$). Algorithm 1 describes more specifically how we generate the equations for the SAT solver.

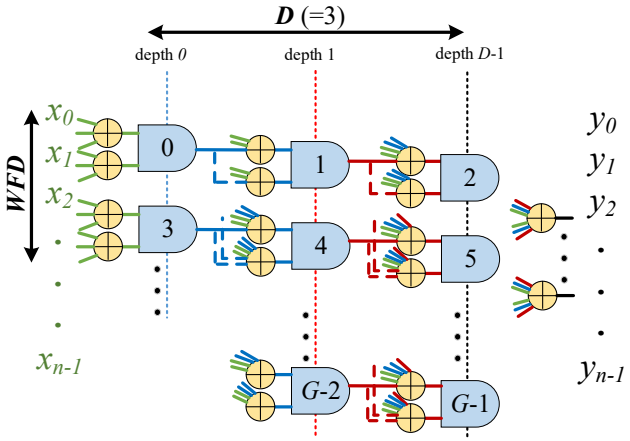

Figure 5: Generated circuit structure by Algorithm 1 for the SAT solver

Synthesis-tool step. We use the CADENCE Genus synthesizer to optimize the affine layers (*i.e.* minimize the number of XOR and NOT gates). We restrict the cell library (*.lib* file) by using the *librar_domain* and *avoid* attributes and give a reprehensive cost for AND cells (using the *multiply* attribute). This way, we ensure that only XOR and NOT gates are used in the implementation of the affine layers.

[7] https://www.cadence.com/content/dam/cadence-www/global/en_US/documents/tools/digital-design-signoff/genus-synthesis-solution-ds.pdf

[8] The algorithm branches to D-1 cases which correspond to the possible values of $mod(G, D)$.

Overview of the results

Table 9: Overview of all S-boxes.

s	S	Functional Prop. δ	$\mathcal{L}$	WP	Degr. S	Degr. S^{-1}	Implementation Prop. D S	D S^{-1}	# AND S	# AND S^{-1}	Prop.
3	x^3 and AE-equivalents*	2	4	2^{-2}	2	2	1	1	3	3	
4	Class13, Prøst, Noekeon, Piccolo, Skinny, Present, ...	4	8	2^{-2}	3	3	2	2	4	4	
5	(x^{30})	2	12	$2^{-2.8}$	4	4	2	2	≤ 14	≤ 14	**inv**
	(x^5)	2	8	$\mathbf{2^{-4}}$	2	3	**1**	2	7	10	**2**
	Fides ($\sim x^3$)	2	8	$\mathbf{2^{-4}}$	2	3	**1**	2	7	10	-
	Ascon (∼Keccak)	8	16	2^{-2}	2	3	**1**	2	**5**	**9**	-
6	$\mathsf{Feistel}_{3,3,3}(x^3, x^3, x^3)$	4	16	$\mathbf{2^{-4}}$	4	4	3	3	9	9	**inv**
	$\mathsf{Misty}_{3,3,3}(x^6, x^6, x^6)$	4	16	$\mathbf{2^{-4}}$	3	4	2	3	9	9	**zo**
	$\mathsf{Bridge}_{3,3,3}(x^6, x^6, x^6)$	4	16	$\mathbf{2^{-4}}$	3	4	2	2	9	9	**zo**
	Q2230	16	32	2^{-2}	2	2	**1**	**1**	$\leq$ **6**	$\leq$ **6**	**1**
	Q2258	4	16	$\mathbf{2^{-4}}$	2	3	**1**	2	8	22	-
	Q2263 ($\sim x^5$)	4	16	$\mathbf{2^{-4}}$	2	3	**1**	2	8	≤ 26	**2**
7	x^3	2	16	$\mathbf{2^{-6}}$	2	4	**1**	2	$\leq$ **15**		§4.4
	x^5	2	16	$\mathbf{2^{-6}}$	2	4	**1**	2	≤ 21		§4.4
	x^9	2	16	$\mathbf{2^{-6}}$	2	4	**1**	2	≤ 21		§4.4
8	x^{254} [CB09]	4	32	$\mathbf{2^{-6}}$	7	7	4	4	32	32	**inv**
	$\mathsf{Feistel}_{4,4,4}(x^3, iC13, x^3)$	8	64	2^{-4}	5	5	4	4	**12**	**12**	**inv**
	$\mathsf{Bridge}_{4,4,4}(x^6, iC13, iC13)$	16	64	2^{-4}	5	6	3	**3**	**12**	**12**	**zo**
	$M = \mathsf{Misty}_{5,3,5}(x^3, x^6, x^3)$	8	64	2^{-4}	3	5	**2**	5	17	27	-
9	x^{510} [NNR19]	2	44	2^{-7}	8	8	3	3			**inv**
	x^5	2	32	$\mathbf{2^{-8}}$	2	5	**1**	≥ 3			**2**
	x^{17}	2	32	$\mathbf{2^{-8}}$	2	5	**1**	≥ 3			**2**
10	$\mathsf{Feistel}_{5,5,5}(x^3, x^{\frac{1}{3}}, x^3)$	4	64	$\mathbf{2^{-8}}$	5	5	4	4	25	25	**inv**
	$\mathsf{Feistel}_{5,5,5}(x^3, x^3, x^3)$	6	96	$2^{-6.6}$	4	4	3	3	**21**	**21**	**inv**
	x^{340}	10	112	$2^{-6.4}$	4	4	2	**2**			**inv**
	x^5	4	64	$\mathbf{2^{-8}}$	2	5	**1**	3			**2**
	x^{17}	4	64	$\mathbf{2^{-8}}$	2	5	**1**	3			**2**
	$\mathsf{Bridge}_{5,5,5}(x^3, x^3, x^3)$	10	64	$2^{-6.7}$	3	6	2	3	**21**	29	-
11	x^{17}	2	64	$\mathbf{2^{-10}}$	2	6	**1**	3			**2**
12	$\mathsf{Feistel}_{6,6,6}(x^3, Q2258, x^3)$	12	256	$\mathbf{2^{-8}}$	7	7	3	3	26	**26**	**inv**
	$\mathsf{Bridge}_{6,6,6}(x^3, Q2258, Q2258)$	18	512	2^{-6}	4	6	**2**	3	**25**	53⋆	-
14	$\mathsf{Feistel}_{7,7,7}(x^3, x^{1/3}, x^3)$	4	256	$\mathbf{2^{-12}}$	8	8	4	4	121⋆	121⋆	**inv**
	$\mathsf{Feistel}_{7,7,7}(x^3, x^3, x^3)$	12	512	2^{-10}	4	4	3	**3**	**45**	**45**	**inv**
	$\mathsf{Bridge}_{7,7,7}(x^3, x^3, x^3)$	12	256	$2^{-10.4}$	3	8	**2**	**3**	**45**	197⋆	-
16	$\mathsf{Feistel}_{8,8,8}(x^3, x^{-1}, x^3)$	10	1280	$\mathbf{2^{-11.3}}$	11	11	6	6	90⋆	90⋆	**inv**
	$\mathsf{Feistel}_{8,8,8}(x^3, \mathsf{M}, x^3)$	20	2048	2^{-10}	10	10	4	**4**	63⋆	**63**⋆	**inv**
	$\mathsf{Bridge}_{8,8,8}(x^3, \mathsf{M}, \mathsf{M})$	64	3072	2^{-8}	6	10	**3**	6	**62**⋆	72⋆	-

* All APN 3-bit permutations are AE-equivalent (see [Bri07], Theorem 4.17 for instance).

Algorithm 1 Generate ANF equations for joint multiplicative-depth (D) and multiplicative-complexity(G) target

Input: G, D, WFD.
Output: Eq.-set for q_*, t_*, y_*.
$q_b = t_b = a_b = 0$;
$\mathcal{Z} = \{x_l\}$, $l \in \{0, ..., n-1\}$;
$G_{full} = WFD \cdot D$;
for $g' = 0$ **to** $G - 1$ **do** ▷ Gen. ANDs loop
  for $q' = 0$ **to** 1 **do** ▷ Gen. AND inputs
    $q_{q'+q_b} = a_{a_b}$; a_b++1
    $\forall z \in Z$: $q_{q'+q_b} += a_{a_b} \cdot z$; a_b++1;
  $t_{t_b} = q_{q_b} \cdot q_{q_b+1}$; ▷ Gen. ANDs
  if $G_{full} > D - 1$ **then** ▷ Full-depth layers
    if $g' < D - 1$ **then**
      $\mathcal{Z} = \mathcal{Z} \cup t_{t_b}$
    else
      if $\mod(g' + 1, D) = 0$ **then**
        $\mathcal{Z} = \{x_l\}$, $l \in \{0, ..., n-1\}$;
      else
        for $ii = 0$ **to** $mod(g', D) + 1$ **do**
          for $jj = 0$ **to** $\lfloor g'/D \rfloor + 1$ **do**
            $\mathcal{Z} = \mathcal{Z} \cup t_{ii+D \cdot jj}$
  else ▷ Partial-depth layers
    if $g' < D - 1$ **then**
      $\mathcal{Z} = \mathcal{Z} \cup t_{t_b}$
    else
      if $\mod(g' + 1, D) = 0$ **then** ▷ Example depth=1
        $\mathcal{Z} = \{x_l\}$, $l \in \{0, ..., n-1\}$;
        for $ii = 0$ **to** $mod(g', D)$ **do**
          for $jj = 0$ **to** $\lfloor WFD - 1 \rfloor + 1$ **do**
            $\mathcal{Z} = \mathcal{Z} \cup t_{ii+D \cdot jj}$
      else ▷ Example depth=2
        $\mathcal{Z} = \{x_l\}$, $l \in \{0, ..., n-1\}$;
        for $ii = 0$ **to** $mod(g', D) + 1$ **do**
          for $jj = 0$ **to** $\lfloor WFD - 1 \rfloor + 1$ **do**
            $\mathcal{Z} = \mathcal{Z} \cup t_{ii+D \cdot jj}$
      ▷ Continue if deeded ($D > 3$)
  t_b++1; q_b++2; G_{full}- -1;
$\mathcal{Z} = \{x_l\}$, $l \in \{0, ..., n-1\}$; ▷ Assign outputs
for $l = 0$ **to** $g' - 1$ **do**
  $\mathcal{Z} = \mathcal{Z} \cup t_{t_{ii}}$
for $l = 0$ **to** $n - 1$ **do**
  $\forall z \in \mathcal{Z} : y_l = a_{a_b} \cdot z$; a_b++1;
return $\boldsymbol{q_*}$, $\boldsymbol{t_*}$, $\boldsymbol{y_*}$

S-box circuits

3-bit S-box circuits[9]

[9]For the circuits description appended we use the following notations for the XOR, AND, OR and

LowMC S: **SEA S:** x^3 **S:** x^5 **S:** x^6 **S:**

D=1 G=3. **D=1 G=3.** **D=1 G=3.** **D=1 G=3.** **D=1 G=3.**

- $p_0 = x_0 \cdot x_2$;
- $p_1 = x_0 \cdot x_1$;
- $p_2 = x_1 \cdot x_2$;
- $y_0 = x_0 \oplus p_2$;
- $l_1 = x_0 \oplus x_1$;
- $y_1 = l_1 \oplus p_0$;
- $l_2 = x_0 \oplus x_1$;
- $l_3 = l_2 \oplus x_2$;
- $y_2 = l_3 \oplus p_1$;

- $p_0 = x_0 \cdot x_2$;
- $p_1 = x_0 \cdot x_1$;
- $p_2 = x_1 \cdot x_2$;
- $y_0 = x_0 \oplus p_2$;
- $l_1 = x_1 \oplus p_0$;
- $y_1 = l_1 \oplus p_2$;
- $l_2 = x_0 \oplus x_1$;
- $l_3 = l_2 \oplus x_2$;
- $y_2 = l_3 \oplus p_1$;

- $p_0 = x_0 \cdot x_2$;
- $p_1 = x_0 \cdot x_1$;
- $p_2 = x_1 \cdot x_2$;
- $l_0 = x_0 \oplus x_1$;
- $l_1 = l_0 \oplus x_2$;
- $y_0 = l_1 \oplus p_2$;
- $l_2 = x_1 \oplus p_0$;
- $y_1 = l_2 \oplus p_1$;
- $y_2 = x_2 \oplus p_1$;

- $p_0 = x_0 \cdot x_2$;
- $p_1 = x_0 \cdot x_1$;
- $p_2 = x_1 \cdot x_2$;
- $l_0 = x_0 \oplus x_1$;
- $l_1 = l_0 \oplus x_2$;
- $y_0 = l_1 \oplus p_2$;
- $l_2 = x_1 \oplus x_2$;
- $y_1 = l_2 \oplus p_0$;
- $l_3 = x_1 \oplus p_1$;
- $y_2 = l_3 \oplus p_0$;

- $p_0 = x_0 \cdot x_2$;
- $p_1 = x_0 \cdot x_1$;
- $p_2 = x_1 \cdot x_2$;
- $l_1 = x_1 \oplus x_2$;
- $l_0 = x_0 \oplus l_1$;
- $y_0 = l_0 \oplus p_2$;
- $y_1 = x_2 \oplus p_1$;
- $y_2 = l_1 \oplus p_0$;

4-bit S-box circuits

Present S: **Present S^{-1}:** **Rectangle S:** **Rectangle S^{-1}:**

D=2 G=4. **D=2 G=4.** **D=2 G=4.**

- $l_0 = x_1 \oplus x_2$;
- $q_0 = \sim l_0$;
- $l_1 = x_0 \oplus x_1$;
- $q_1 = \sim l_1$;
- $t_0 = q_0 \cdot q_1$;
- $l_2 = q_1 \oplus x_2$;
- $q_2 = l_2 \oplus t_0$;
- $q_3 = \sim x_3$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim x_2$;
- $t_2 = q_4 \cdot x_1$;
- $l_3 = q_0 \oplus x_3$;
- $l_4 = t_0 \oplus t_2$;
- $q_6 = l_3 \oplus l_4$;
- $l_5 = x_0 \oplus x_3$;
- $q_7 = l_5 \oplus t_0$;
- $t_3 = q_6 \cdot q_7$;
- $l_6 = x_3 \oplus t_2$;
- $l_7 = t_0 \oplus t_1$;
- $y_0 = l_6 \oplus l_7$;
- $l_8 = x_0 \oplus x_2$;
- $l_9 = l_7 \oplus t_3$;
- $y_1 = l_8 \oplus l_9$;
- $l_{10} = \sim l_2$;
- $l_{11} = l_{10} \oplus t_1$;
- $y_2 = l_{11} \oplus t_2$;
- $l_{12} = x_0 \oplus x_3$;
- $y_3 = l_{12} \oplus t_2$;

- $l_0 = x_0 \oplus x_2$;
- $l_1 = x_1 \oplus x_3$;
- $l_2 = l_1 \oplus x_2$;
- $l_3 = l_1 \oplus x_0$;
- $l_4 = l_0 \oplus l_1$;
- $l_5 = l_0 \oplus x_3$;
- $q_0 = \sim l_2$;
- $q_1 = l_3$;
- $t_0 = q_0 \cdot q_1$;
- $q_2 = x_0 \oplus x_3 \oplus t_0$;
- $q_3 = \sim l_4 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_0$;
- $q_5 = \sim l_1$;
- $t_2 = q_4 \cdot q_5$;
- $l_6 = t_0 \oplus t_2$;
- $q_6 = \sim x_0 \oplus l_6$;
- $q_7 = l_5 \oplus l_6$;
- $t_3 = q_6 \cdot q_7$;
- $y_0 = x_1 \oplus t_0 \oplus t_1 \oplus t_3$;
- $y_1 = l_2 \oplus t_1 \oplus t_2$;
- $y_2 = l_5 \oplus t_1$;
- $y_3 = x_2 \oplus l_6$;

- $q_6 = x_0 \oplus x_1$;
- $l_0 = x_0 \oplus x_3$;
- $q_3 = x_1 \oplus x_2$;
- $l_1 = x_2 \oplus x_3$;
- $l_2 = q_6 \oplus l_1$;
- $q_1 = \sim x_3$;
- $t_0 = x_2 \cdot q_1$;
- $q_2 = \sim l_0 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_0$;
- $q_5 = \sim x_2$;
- $t_2 = q_4 \cdot q_5$;
- $l_3 = t_0 \oplus t_2$;
- $q_7 = \sim q_3 \oplus l_3$;
- $t_3 = q_6 \cdot q_7$;
- $y_0 = q_3 \oplus t_3$;
- $y_1 = l_1 \oplus t_1 \oplus t_2$;
- $y_2 = q_6 \oplus x_2 \oplus l_3$;
- $y_3 = l_2 \oplus t_0$;

- $q_0 = \sim x_3$;
- $q_1 = x_0 \oplus x_1$;
- $q_5 = x_1 \oplus x_3$;
- $l_0 = x_0 \oplus x_3$;
- $l_1 = x_0 \oplus x_2$;
- $t_0 = q_0 \cdot q_1$;
- $q_2 = \sim l_0 \oplus t_0$;
- $q_3 = l_1 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim x_1$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = \sim l_1 \oplus x_3 \oplus t_0$;
- $q_7 = \sim l_0 \oplus t_2$;
- $t_3 = q_6 \cdot q_7$;
- $y_0 = q_1 \oplus x_3 \oplus t_1 \oplus t_2 \oplus t_3$;
- $y_1 = x_2 \oplus t_0 \oplus t_2$;
- $y_2 = l_1 \oplus t_0$;
- $y_3 = q_1 \oplus x_2 \oplus t_0 \oplus t_3$;

Class-13 S: **Class-13 S^{-1}:**

D=2 G=4. **D=2 G=4.**

- $y_0 = (x_0 \cdot x_1) \oplus x_2$;
- $y_2 = (x_1 | x_2) \oplus x_3$;
- $y_3 = (y_0 \cdot x_3) \oplus x_0$;
- $y_1 = (y_2 \cdot x_0) \oplus x_1$;

- $l_0 = x_1 \oplus x_3$;
- $l_1 = x_2 \oplus x_3$;
- $q_1 = \sim x_0$;
- $t_0 = x_1 \cdot q_1$;
- $q_2 = x_2 \oplus t_0$;
- $q_3 = \sim l_1 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = x_0 \oplus l_0$;
- $t_2 = q_4 \cdot x_1$;
- $l_3 = t_0 \oplus t_2$;
- $q_6 = x_0 \oplus l_1 \oplus l_3$;
- $t_3 = q_6 \cdot x_2$;
- $y_0 = l_1 \oplus t_1 \oplus t_2$;
- $y_1 = x_1 \oplus l_1 \oplus t_0 \oplus t_3$;
- $y_2 = x_1 \oplus x_2 \oplus t_0$;
- $y_3 = x_0 \oplus x_3 \oplus l_3$;

NOT gates, respectively: $\oplus$, $\cdot$, $|$ and $\sim$.

Skinny S: D=**2** G=**4.**

- $y_0 = \sim(x_0 | x_1) \oplus x_3$;
- $y_1 = \sim(x_1 | x_2) \oplus x_0$;
- $y_2 = \sim(x_2 | y_0) \oplus x_1$;
- $y_3 = \sim(y_0 | y_1) \oplus x_2$;

Skinny S^{-1}: D=**2** G=**4.**

- $q_0 = \sim x_1$;
- $q_1 = \sim x_0$;
- $t_0 = q_0 \cdot q_1$;
- $q_7 = \sim x_2$;
- $q_2 = q_7 \oplus t_0$;
- $q_4 = x_1 \oplus x_3$;
- $q_3 = q_4 \oplus x_2$;
- $t_1 = q_2 \cdot q_3$;
- $q_5 = \sim x_0$;
- $t_2 = q_4 \cdot q_5$;
- $y_2 = x_3 \oplus t_0$;
- $q_6 = q_7 \oplus y_2$;
- $t_3 = q_6 \cdot q_7$;
- $y_0 = x_1 \oplus t_2 \oplus t_3$;
- $y_1 = x_2 \oplus t_2$;
- $y_3 = x_0 \oplus t_0 \oplus t_1 \oplus t_2$;

Piccolo: Equal to Skinny with a NOT on y_2 (resp. on x_2 for the inverse).

Gift S: D=**2** G=**5.**

- $l_0 = x_2 \oplus x_3$;
- $q_8 = x_0 \oplus x_1$;
- $q_6 = x_0 \oplus x_3$;
- $l_1 = l_0 \oplus q_8$;
- $l_2 = x_1 \oplus x_2$;
- $q_0 = \sim l_0$;
- $q_1 = \sim x_0$;
- $t_0 = q_0 \cdot q_1$;
- $q_3 = \sim x_1 \oplus x_3 \oplus t_0$;
- $t_1 = l_1 \cdot q_3$;
- $q_5 = \sim l_2$;
- $t_2 = x_3 \cdot q_5$;
- $q_7 = \sim t_0 \oplus t_2$;
- $t_3 = q_6 \cdot q_7$;
- $l_4 = x_0 \oplus x_2$;
- $q_9 = l_4 \oplus t_0$;
- $t_4 = q_8 \cdot q_9$;
- $l_3 = t_3 \oplus t_4$;
- $y_0 = l_4 \oplus t_1 \oplus t_2 \oplus l_3$;
- $y_1 = x_2 \oplus l_3$;
- $y_2 = q_8 \oplus t_2$;
- $y_3 = l_2 \oplus t_0 \oplus t_1 \oplus t_4$;

Gift S^{-1}: D=**2** G=**5.**

- $l_0 = x_1 \oplus x_3$;
- $l_1 = l_0 \oplus x_2$;
- $l_2 = x_0 \oplus x_2$;
- $l_3 = l_0 \oplus l_2$;
- $q_0 = \sim l_0$;
- $t_0 = q_0 \cdot x_1$;
- $q_2 = \sim l_1$;
- $q_3 = \sim l_2 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim x_3$;
- $q_5 = \sim x_0 \oplus l_0$;
- $t_2 = q_4 \cdot q_5$;
- $l_4 = t_0 \oplus t_2$;
- $q_6 = \sim l_4$;
- $q_7 = x_2 \oplus x_3 \oplus l_4$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = l_3 \oplus t_2$;
- $q_9 = l_1 \oplus t_0$;
- $t_4 = q_8 \cdot q_9$;
- $l_5 = t_2 \oplus t_4$;
- $y_0 = x_0 \oplus x_1 \oplus l_5 \oplus t_3$;
- $y_1 = l_2 \oplus l_4$;
- $y_2 = l_2 \oplus x_1 \oplus l_4 \oplus t_1$;
- $y_3 = l_1 \oplus l_5$;

Prince S: D=**2** G=**6.**

- $q_0 = x_1 \oplus x_3$;
- $l_0 = q_0 \oplus x_2$;
- $q_2 = x_2 \oplus x_3$;
- $q_8 = x_0 \oplus x_1$;
- $l_1 = q_8 \oplus q_2$;
- $l_2 = x_0 \oplus x_3$;
- $q_1 = \sim l_0$;
- $t_0 = q_0 \cdot q_1$;
- $q_3 = q_8 \oplus x_2 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_2$;
- $q_5 = \sim l_1$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = \sim x_3$;
- $q_7 = x_2 \oplus t_2$;
- $t_3 = q_6 \cdot q_7$;
- $q_9 = x_0 \oplus t_2$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = q_4 \oplus t_0 \oplus t_2$;
- $q_{11} = q_4 \oplus x_2$;
- $t_5 = q_{10} \cdot q_{11}$;
- $l_3 = t_1 \oplus t_2$;
- $l_4 = t_3 \oplus t_4$;
- $l_5 = l_3 \oplus l_4$;
- $y_0 = q_0 \oplus t_0 \oplus t_1 \oplus t_3$;
- $y_1 = q_0 \oplus l_5 \oplus t_5$;
- $y_2 = q_0 \oplus l_4$;
- $y_3 = x_3 \oplus t_0 \oplus l_3$;

Prince S^{-1}: D=**2** G=**6.**

- $l_0 = x_1 \oplus x_3$;
- $l_1 = x_2 \oplus x_3$;
- $l_2 = x_0 \oplus x_3$;
- $l_3 = x_0 \oplus x_1$;
- $l_4 = l_1 \oplus l_3$;
- $l_5 = \sim l_2$;
- $l_6 = l_1 \oplus x_1$;
- $q_0 = \sim x_2$;
- $t_0 = q_0 \cdot l_4$;
- $q_2 = l_5 \oplus t_0$;
- $q_3 = \sim l_1 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_0$;
- $q_5 = \sim l_1$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = x_3 \oplus t_0$;
- $q_7 = q_4 \oplus t_0$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = l_5 \oplus t_2$;
- $q_9 = \sim x_3 \oplus t_2$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = l_6 \oplus t_2$;
- $q_{11} = \sim l_3$;
- $t_5 = q_{10} \cdot q_{11}$;
- $l_7 = t_1 \oplus t_3$;
- $y_0 = l_4 \oplus l_7 \oplus t_4$;
- $y_1 = x_0 \oplus l_7 \oplus t_2$;
- $y_2 = x_0 \oplus x_2 \oplus t_4 \oplus t_5$;
- $y_3 = t_3 \oplus t_5$;

Prøst S:
D=2 G=4.

$l_0 = x_0 \oplus x_1;$
$l_1 = l_0 \oplus x_2;$
$l_2 = l_0 \oplus x_3;$
$l_3 = x_2 \oplus x_3;$
$l_4 = l_0 \oplus l_3;$
$q_1 = \sim x_1;$
$t_0 = l_1 \cdot q_1;$
$q_2 = q_1 \oplus l_3 \oplus t_0;$
$t_1 = q_2 \cdot x_0;$
$t_2 = x_1 \cdot x_0;$
$l_6 = t_0 \oplus t_2;$
$q_6 = \sim l_2 \oplus t_0;$
$q_7 = l_4 \oplus l_6;$
$t_3 = q_6 \cdot q_7;$
$l_5 = t_0 \oplus t_3;$
$y_0 = x_2 \oplus t_2;$
$y_1 = x_0 \oplus l_3 \oplus l_6;$
$y_2 = x_2 \oplus l_5;$
$y_3 = l_1 \oplus l_5 \oplus t_1;$

iClass13 S:
D=2 G=4.

$t_0 = x_1 \cdot x_2;$
$t_1 = x_0 \cdot x_2;$
$l_2 = t_0 \oplus t_1;$
$l_3 = x_3 \oplus t_1;$
$n_1 = x_0 \oplus t_0;$
$t_3 = x_3 \cdot n_1;$
$n_3 = x_2 \oplus t_0;$
$l_4 = x_1 \oplus l_2;$
$t_4 = l_3 \cdot x_1;$
$y_2 = x_3 \oplus l_2;$
$y_0 = l_4 \oplus t_3;$
$y_3 = n_3 \oplus t_4;$
$y_1 = n_1;$

x^3 S:
D=2 G=4.

$q_3 = x_0 \oplus x_3;$
$q_1 = x_1 \oplus x_3;$
$l_0 = x_0 \oplus x_2;$
$l_1 = l_0 \oplus q_1;$
$l_2 = l_0 \oplus x_1;$
$q_0 = \sim x_2;$
$t_0 = q_0 \cdot q_1;$
$q_2 = \sim l_0;$
$t_1 = q_2 \cdot q_3;$
$q_5 = \sim x_0;$
$t_2 = l_2 \cdot q_5;$
$q_7 = q_3 \oplus x_2;$
$t_3 = l_1 \cdot q_7;$
$y_0 = x_0 \oplus t_2;$
$y_1 = l_2 \oplus t_1 \oplus t_3;$
$y_2 = x_1 \oplus x_2 \oplus t_0 \oplus t_3;$
$y_3 = x_0 \oplus x_1 \oplus t_2 \oplus t_3;$

x^6 S:
D=2 G=4.

$q_3 = x_0 \oplus x_1;$
$q_5 = x_2 \oplus x_3;$
$l_0 = q_3 \oplus q_5;$
$q_7 = x_1 \oplus x_2;$
$l_2 = q_3 \oplus x_3;$
$l_3 = \sim x_0;$
$q_1 = x_0 \oplus q_5;$
$t_0 = l_0 \cdot q_1;$
$q_2 = \sim l_2;$
$t_1 = q_2 \cdot q_3;$
$q_4 = l_3 \oplus x_3;$
$t_2 = q_4 \cdot q_5;$
$t_3 = l_3 \cdot q_7;$
$y_0 = x_0 \oplus t_3;$
$y_1 = x_1 \oplus t_1 \oplus t_2;$
$y_2 = l_2 \oplus t_0 \oplus t_2;$
$y_3 = x_3 \oplus t_2 \oplus t_3;$

NOEKEON S:
D=2 G=4.

$q_0 = \sim x_0;$
$q_1 = \sim x_1;$
$t_0 = q_0 \cdot q_1;$
$q_2 = \sim x_2 \oplus x_3;$
$q_3 = q_0 \oplus x_1 \oplus x_2 \oplus t_0;$
$t_1 = q_2 \cdot q_3;$
$q_4 = q_1 \oplus x_2;$
$t_2 = q_4 \cdot x_1;$
$l_0 = x_0 \oplus x_1 \oplus x_3;$
$q_6 = l_0 \oplus t_2;$
$q_7 = x_2 \oplus t_0;$
$t_3 = q_6 \cdot q_7;$
$l_1 = t_0 \oplus t_2;$
$y_0 = x_3 \oplus t_2;$
$y_1 = l_0 \oplus x_2 \oplus l_1;$
$y_2 = t_1 \oplus l_1;$
$y_3 = x_0 \oplus x_2 \oplus t_0 \oplus t_3;$

x^{-1} S:
D=2 G=6.

- $l_0 = x_0 \oplus x_3;$
- $l_1 = x_1 \oplus x_2;$
- $l_2 = l_0 \oplus l_1;$
- $l_3 = x_0 \oplus x_2;$
- $l_4 = x_1 \oplus x_3;$
- $l_5 = l_0 \oplus x_1;$
- $l_6 = l_0 \oplus x_2;$
- $q_{10} = \sim l_2;$
- $q_0 = \sim l_0;$
- $q_1 = \sim x_0 \oplus l_1;$
- $t_0 = q_0 \cdot q_1;$
- $q_2 = \sim x_2;$
- $q_3 = l_5 \oplus t_0;$
- $t_1 = q_2 \cdot q_3;$
- $t_2 = q_2 \cdot x_1;$
- $l_9 = t_0 \oplus t_2;$
- $q_6 = q_{10} \oplus l_9;$
- $q_7 = l_3 \oplus l_9;$
- $t_3 = q_6 \cdot q_7;$
- $q_8 = l_6 \oplus t_2;$
- $q_9 = x_2 \oplus x_3 \oplus t_2;$
- $t_4 = q_8 \cdot q_9;$
- $q_{11} = x_0 \oplus l_9;$
- $t_5 = q_{10} \cdot q_{11};$
- $l_7 = t_2 \oplus t_4;$
- $l_8 = l_7 \oplus t_3;$
- $y_0 = l_5 \oplus l_6;$
- $y_1 = x_3 \oplus t_1 \oplus t_5;$
- $y_2 = l_2 \oplus l_7;$
- $y_3 = l_4 \oplus t_0 \oplus t_1 \oplus l_7;$

Look-up tables (LUTs):

iClass13, $S =$	$[0, 2, 1, 3, 8, 15, 6, 9, 4, 7, 13, 14, 12, 10, 11, 5]$
Present, $S =$	$[12, 5, 6, 11, 9, 0, 10, 13, 3, 14, 15, 8, 4, 7, 1, 2]$
Present, $S^{-1} =$	$[5, 14, 15, 8, 12, 1, 2, 13, 11, 4, 6, 3, 0, 7, 9, 10]$
Rectangle, $S =$	$[6, 5, 12, 10, 1, 14, 7, 9, 11, 0, 3, 13, 8, 15, 4, 2]$
Rectangle, $S =$	$[9, 4, 15, 10, 14, 1, 0, 6, 12, 7, 3, 8, 2, 11, 5, 13]$
Class13, $S =$	$[0, 8, 6, 13, 5, 15, 7, 12, 4, 14, 2, 3, 9, 1, 11, 10]$
Class13, $S^{-1} =$	$[0, 13, 10, 11, 8, 4, 2, 6, 1, 12, 15, 14, 7, 3, 9, 5]$
NOEKEON, $S =$	$[7, 10, 2, 12, 4, 8, 15, 0, 5, 9, 1, 14, 3, 13, 11, 6]$
Prost, $S =$	$[0, 4, 8, 15, 1, 5, 14, 9, 2, 7, 10, 12, 11, 13, 6, 3]$
Skinny, $S =$	$[12, 6, 9, 0, 1, 10, 2, 11, 3, 8, 5, 13, 4, 14, 7, 15]$
Skinny, $S =$	$[3, 4, 6, 8, 12, 10, 1, 14, 9, 2, 5, 7, 0, 11, 13, 15]$
Prince, $S =$	$[11, 15, 3, 2, 10, 12, 9, 1, 6, 7, 8, 0, 14, 5, 13, 4]$
Prince, $S^{-1} =$	$[11, 7, 3, 2, 15, 13, 8, 9, 10, 6, 4, 0, 5, 14, 12, 1]$
Gift, $S =$	$[1, 10, 4, 12, 6, 15, 3, 9, 2, 13, 11, 7, 5, 0, 8, 14]$
Gift, $S^{-1} =$	$[13, 0, 8, 6, 2, 12, 4, 11, 14, 7, 1, 10, 3, 9, 15, 5]$
$x^{-1}, S =$	$[0, 1, 9, 14, 13, 11, 7, 6, 15, 2, 12, 5, 10, 4, 3, 8]$
$x^3(non - bij) =$	$[0, 1, 8, 15, 12, 10, 1, 1, 10, 15, 15, 12, 8, 10, 8, 12]$
$x^6(non - bij) =$	$[0, 1, 12, 10, 15, 8, 1, 1, 8, 10, 10, 15, 12, 8, 12, 15]$

5-bit S-box circuits

Keccak S^{-1}:
D=2 G=9.

- $l_0 = x_0 \oplus x_2$;
- $l_1 = x_0 \oplus x_4$;
- $l_2 = x_1 \oplus x_2$;
- $l_3 = x_2 \oplus x_4$;
- $l_4 = l_2 \oplus x_3$;
- $l_5 = x_1 \oplus x_3$;
- $l_6 = l_5 \oplus l_0$;
- $q_0 = \sim l_0$;
- $t_0 = q_0 \cdot x_2$;
- $q_2 = \sim x_2 \oplus t_0$;
- $q_3 = \sim x_3 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_1$;
- $q_5 = \sim x_1$;
- $t_2 = q_4 \cdot q_5$;
- $l_9 = t_0 \oplus t_2$;
- $q_6 = \sim x_4 \oplus l_9$;
- $q_7 = \sim l_4$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = \sim l_2$;
- $t_4 = q_8 \cdot x_0$;
- $l_{10} = l_9 \oplus t_4$;
- $l_{11} = t_0 \oplus t_4$;
- $q_{10} = l_3 \oplus l_{11}$;
- $q_{11} = \sim l_1 \oplus x_3 \oplus l_{10}$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = \sim l_6 \oplus t_2 \oplus t_4$;
- $q_{13} = \sim l_5 \oplus l_9$;
- $t_6 = q_{12} \cdot q_{13}$;
- $q_{14} = \sim t_4$;
- $q_{15} = \sim x_0 \oplus l_5 \oplus t_0$;
- $t_7 = q_{14} \cdot q_{15}$;
- $q_{16} = l_5 \oplus x_4$;
- $q_{17} = \sim l_{10}$;
- $t_8 = q_{16} \cdot q_{17}$;
- $l_{12} = t_3 \oplus t_8$;
- $y_0 = t_2 \oplus l_{12} \oplus t_7$;
- $y_1 = x_2 \oplus t_0 \oplus l_{12} \oplus t_5$;
- $y_2 = l_6 \oplus l_{11} \oplus t_8$;
- $y_3 = x_1 \oplus x_4 \oplus t_4 \oplus t_5 \oplus t_6$;
- $y_4 = l_1 \oplus x_1 \oplus t_1 \oplus t_4 \oplus t_7$;

Fides S:
D=1 G=7.

- $n_0 = \sim x_2$;
- $n_1 = \sim x_4$;
- $q_1 = x_1 \oplus n_1$;
- $q_2 = x_3 \oplus q_1$;
- $q_0 = n_0 \oplus q_2$;
- $t_0 = q_0 \cdot q_1$;
- $n_3 = x_0 \oplus x_2$;
- $n_2 = \sim n_3$;
- $l_2 = \sim q_1$;
- $q_3 = l_2 \oplus n_2$;
- $t_1 = q_2 \cdot q_3$;
- $l_0 = x_1 \oplus x_2$;
- $q_4 = l_0$;
- $l_1 = x_1 \oplus x_3$;
- $q_5 = l_1 \oplus n_3$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = x_3 \oplus n_1$;
- $q_7 = x_1 \oplus n_3$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = x_4 \oplus n_3$;
- $q_9 = x_4$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = x_2$;
- $q_{11} = n_2 \oplus q_2$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = n_0 \oplus q_6$;
- $n_7 = \sim l_1$;
- $q_{13} = x_0 \oplus n_7$;
- $t_6 = q_{12} \cdot q_{13}$;
- $m_1 = t_4 \oplus t_6$;
- $m_2 = t_1 \oplus t_2$;
- $m_3 = t_0 \oplus t_2$;
- $m_4 = t_3 \oplus t_5$;
- $m_5 = t_0 \oplus t_6$;
- $m_6 = m_1 \oplus t_3$;
- $y_0 = l_0 \oplus t_0 \oplus m_1$;
- $y_1 = l_2 \oplus m_4 \oplus m_5$;
- $y_2 = l_1 \oplus m_3 \oplus m_6$;
- $y_3 = x_1 \oplus m_6$;
- $y_4 = x_3 \oplus m_2 \oplus m_6$;

Fides S^{-1}:
D=2 G=10.

- $l_0 = x_0 \oplus x_2$;
- $q_1 = x_1 \oplus x_2$;
- $q_2 = x_2 \oplus x_4$;
- $q_{13} = x_1 \oplus x_3$;
- $l_1 = l_0 \oplus x_4$;
- $l_2 = q_{13} \oplus x_0$;
- $l_3 = l_2 \oplus x_4$;
- $l_4 = x_0 \oplus x_1$;
- $l_5 = l_4 \oplus x_4$;
- $l_6 = x_2 \oplus x_3$;
- $q_0 = \sim l_0$;
- $t_0 = q_0 \cdot q_1$;
- $q_3 = \sim l_4 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_6 \oplus x_4$;
- $q_5 = \sim l_2$;
- $t_2 = q_4 \cdot q_5$;
- $l_8 = t_0 \oplus t_2$;
- $q_6 = l_3 \oplus x_2 \oplus l_8$;
- $t_3 = q_6 \cdot x_1$;
- $q_8 = \sim x_0 \oplus l_6$;
- $q_9 = \sim x_0$;
- $t_4 = q_8 \cdot q_9$;
- $l_9 = t_2 \oplus t_4$;
- $l_{10} = t_4 \oplus t_6$;
- $q_{10} = \sim x_0 \oplus x_4 \oplus t_4$;
- $q_{11} = \sim l_2 \oplus x_2$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = \sim l_3$;
- $t_6 = q_{12} \cdot q_{13}$;
- $q_{14} = l_1 \oplus l_9$;
- $q_{15} = x_4 \oplus t_6$;
- $t_7 = q_{14} \cdot q_{15}$;
- $q_{16} = \sim l_3 \oplus l_9$;
- $q_{17} = l_5 \oplus t_2 \oplus l_{10}$;
- $t_8 = q_{16} \cdot q_{17}$;
- $l_{11} = t_1 \oplus t_8$;
- $l_{12} = t_3 \oplus t_5$;
- $q_{18} = \sim l_5$;
- $q_{19} = \sim x_4 \oplus l_9$;
- $t_9 = q_{18} \cdot q_{19}$;
- $y_0 = l_1 \oplus t_0 \oplus l_{11} \oplus t_3 \oplus t_6$;
- $y_1 = x_1 \oplus x_3 \oplus l_{11} \oplus l_9$;
- $y_2 = l_4 \oplus x_2 \oplus l_9 \oplus l_{12} \oplus t_8 \oplus t_9$;
- $y_3 = l_3 \oplus t_1 \oplus l_9 \oplus t_5$;
- $y_4 = l_1 \oplus x_1 \oplus t_0 \oplus l_{11} \oplus l_{12} \oplus l_{10} \oplus t_7$;

x^3 S**:**
D=1 G=7.

- $q_1 = x_0 \oplus x_3$;
- $q_0 = q_1 \oplus x_2$;
- $q_3 = x_2 \oplus x_4$;
- $q_5 = x_0 \oplus q_3$;
- $q_9 = q_3 \oplus x_3$;
- $q_7 = x_0 \oplus x_1$;
- $q_8 = x_0 \oplus x_2$;
- $l_0 = q_7 \oplus q_3$;
- $l_2 = x_1 \oplus x_4$;
- $l_3 = x_2 \oplus x_3$;
- $l_4 = x_1 \oplus x_2$;
- $t_0 = q_0 \cdot q_1$;
- $q_2 = \sim x_3 \oplus x_4$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_2$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = \sim q_9$;
- $t_3 = q_6 \cdot q_7$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = \sim x_0 \oplus x_4$;
- $t_5 = q_{10} \cdot l_0$;
- $q_{13} = \sim x_1$;
- $t_6 = x_3 \cdot q_{13}$;
- $l_6 = t_0 \oplus t_5$;
- $l_7 = t_2 \oplus t_6$;
- $y_0 = l_4 \oplus x_3 \oplus l_6 \oplus t_3$;
- $y_1 = l_3 \oplus t_2 \oplus t_5$;
- $y_2 = l_4 \oplus t_0 \oplus t_1 \oplus l_7 \oplus t_3 \oplus t_4$;
- $y_3 = l_3 \oplus l_6 \oplus t_1$;
- $y_4 = l_2 \oplus l_6 \oplus l_7$;

x^3 S^{-1}**:**
D=2 G=12.

- $q_{22} = x_0 \oplus x_1$;
- $l_0 = x_3 \oplus x_4$;
- $q_2 = q_{22} \oplus l_0$;
- $l_2 = q_{22} \oplus x_3$;
- $l_3 = q_{22} \oplus x_2$;
- $l_4 = l_0 \oplus x_2$;
- $l_5 = l_0 \oplus x_0$;
- $l_6 = x_1 \oplus x_3$;
- $l_7 = l_6 \oplus x_4$;
- $l_8 = x_0 \oplus x_4$;
- $q_0 = q_2 \oplus x_2$;
- $q_1 = \sim q_{22}$;
- $t_0 = q_0 \cdot q_1$;
- $q_3 = l_6 \oplus x_2 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_6$;
- $t_2 = q_4 \cdot q_1$;
- $l_9 = t_0 \oplus t_2$;
- $q_6 = \sim x_1 \oplus l_9$;
- $q_7 = \sim l_3$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = l_3 \oplus x_4$;
- $q_9 = \sim x_1 \oplus x_4$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = \sim l_5 \oplus x_2$;
- $q_{11} = l_8 \oplus t_4$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = \sim x_2 \oplus x_3$;
- $q_{13} = \sim x_2$;
- $t_6 = q_{12} \cdot q_{13}$;
- $l_{10} = l_9 \oplus t_6$;
- $l_{11} = t_4 \oplus t_6$;
- $l_{12} = l_{11} \oplus t_0$;
- $q_{14} = \sim q_2 \oplus l_{10}$;
- $q_{15} = l_8 \oplus l_{10}$;
- $t_7 = q_{14} \cdot q_{15}$;
- $q_{16} = \sim l_7 \oplus l_{12}$;
- $t_8 = q_{16} \cdot l_5$;
- $q_{19} = l_6 \oplus l_{11}$;
- $t_9 = x_4 \cdot q_19$;
- $q_{20} = l_5 \oplus x_2 \oplus t_0$;
- $q_{21} = \sim l_3 \oplus t_2$;
- $t_{10} = q_{20} \cdot q_{21}$;
- $q_{23} = l_8 \oplus x_2 \oplus l_{12}$;
- $t_{11} = q_{22} \cdot q_{23}$;
- $l_{13} = t_5 \oplus t_8$;
- $l_{14} = l_{13} \oplus t_{10}$;
- $l_{15} = t_{10} \oplus t_{11}$;
- $l_{16} = t_7 \oplus t_9$;
- $y_0 = l_2 \oplus t_4 \oplus t_5 \oplus t_9 \oplus l_{15}$;
- $y_1 = x_1 \oplus t_2 \oplus t_3 \oplus l_{14} \oplus t_6$;
- $y_2 = q_2 \oplus l_{13} \oplus t_{11}$;
- $y_3 = l_4 \oplus t_0 \oplus t_1 \oplus t_3 \oplus l_{14} \oplus l_{16} \oplus t_{11}$;
- $y_4 = l_2 \oplus t_3 \oplus t_5 \oplus l_{16}$;

x^5 S**:**
D=1 G=7.

- $l_0 = x_0 \oplus x_3$;
- $l_1 = x_2 \oplus x_3$;
- $l_2 = x_0 \oplus x_4$;
- $l_3 = x_1 \oplus x_2$;
- $l_4 = l_2 \oplus l_3$;
- $l_5 = l_2 \oplus x_2$;
- $l_6 = x_1 \oplus x_4$;
- $l_7 = l_1 \oplus l_6$;
- $q_0 = x_0 \oplus l_3$;
- $t_0 = q_0 \cdot l_4$;
- $q_2 = \sim l_2 \oplus x_3$;
- $q_3 = \sim x_3$;
- $t_1 = q_2 \cdot q_3$;
- $q_5 = \sim l_1$;
- $t_2 = x_1 \cdot q_5$;
- $q_6 = \sim x_4$;
- $t_3 = q_6 \cdot q_3$;
- $q_8 = \sim l_5$;
- $q_9 = \sim l_0$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = \sim l_2 \oplus x_1$;
- $q_{11} = \sim l_7$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = l_6 \oplus x_3$;
- $t_6 = q_{12} \cdot l_5$;
- $l_9 = t_2 \oplus t_5$;
- $y_0 = l_2 \oplus t_0 \oplus t_6$;
- $y_1 = x_2 \oplus t_3 \oplus t_5$;
- $y_2 = l_0 \oplus t_0 \oplus l_9 \oplus t_3$;
- $y_3 = l_6 \oplus l_9 \oplus t_4 \oplus t_6$;
- $y_4 = l_6 \oplus x_3 \oplus t_1 \oplus l_9$;

x^5 S^{-1}**:**
D**=2** G**=10.**

- $q_1 = x_1 \oplus x_3$;
- $l_0 = x_1 \oplus x_2$;
- $l_1 = x_1 \oplus x_4$;
- $q_{12} = \sim l_0$;
- $q_0 = \sim l_1$;
- $l_2 = l_0 \oplus x_3$;
- $l_3 = x_0 \oplus x_1$;
- $l_4 = x_3 \oplus x_4$;
- $l_5 = l_4 \oplus x_2$;
- $l_6 = l_3 \oplus x_2$;
- $t_0 = q_0 \cdot q_1$;
- $q_2 = x_2 \oplus x_3 \oplus t_0$;
- $q_3 = x_1 \oplus t_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = x_1 \oplus l_5$;
- $t_2 = q_4 \cdot q_1$;
- $l_8 = t_0 \oplus t_2$;
- $q_6 = \sim l_2 \oplus t_0$;
- $q_7 = \sim x_0 \oplus x_2 \oplus x_3 \oplus l_8$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = l_2$;
- $q_9 = \sim l_3 \oplus l_4$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = \sim l_6 \oplus x_4$;
- $q_{11} = l_3 \oplus x_3 \oplus t_0 \oplus t_4$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{13} = \sim x_1 \oplus l_4$;
- $t_6 = q_{12} \cdot q_{13}$;
- $l_9 = t_4 \oplus t_6$;
- $l_{10} = t_2 \oplus t_4$;
- $q_{14} = \sim l_6 \oplus l_9$;
- $q_{15} = \sim l_6 \oplus x_4$;
- $t_7 = q_{14} \cdot q_{15}$;
- $q_{16} = \sim x_0 \oplus l_4 \oplus l_{10}$;
- $q_{17} = l_4 \oplus l_{10}$;
- $t_8 = q_{16} \cdot q_{17}$;
- $q_{18} = l_6 \oplus x_3$;
- $q_{19} = \sim x_0 \oplus l_5 \oplus l_8 \oplus t_6$;
- $t_9 = q_{18} \cdot q_{19}$;
- $l_{11} = t_7 \oplus t_8$;
- $l_{12} = t_7 \oplus t_9$;
- $l_{13} = l_{11} \oplus t_9$;
- $l_{14} = l_8 \oplus t_1$;
- $y_0 = x_2 \oplus l_{14} \oplus t_4 \oplus l_{13}$;
- $y_1 = l_4 \oplus t_1 \oplus t_2 \oplus t_3 \oplus t_6 \oplus l_{12}$;
- $y_2 = l_0 \oplus t_0 \oplus t_5 \oplus l_{13}$;
- $y_3 = l_2 \oplus l_{14} \oplus t_7$;
- $y_4 = l_5 \oplus t_0 \oplus t_4 \oplus l_{11}$;

Look-up tables (LUTs):

- x^3:
  $[0, 1, 8, 15, 10, 31, 23, 4, 26, 25, 3, 6, 9, 30, 5, 20, 14, 18, 22, 12, 24, 16, 21, 27, 2, 28, 11, 19, 13, 7, 17, 29]$
- x^3 inv:
  $[0, 1, 24, 10, 7, 14, 11, 29, 2, 12, 4, 26, 19, 28, 16, 3, 21, 30, 17, 27, 15, 22, 18, 6, 20, 9, 8, 23, 25, 31, 13, 5]$
- FIDES:
  $[1, 0, 25, 26, 17, 29, 21, 27, 20, 5, 4, 23, 14, 18, 2, 28, 15, 8, 6, 3, 13, 7, 24, 16, 30, 9, 31, 10, 22, 12, 11, 19]$
- FIDES inv:
  $[1, 0, 14, 19, 10, 9, 18, 21, 17, 25, 27, 30, 29, 20, 12, 16, 23, 4, 13, 31, 8, 6, 28, 11, 22, 2, 3, 7, 15, 5, 24, 26]$
- Keccak:
  $[0, 9, 18, 11, 5, 12, 22, 15, 10, 3, 24, 1, 13, 4, 30, 7, 20, 21, 6, 23, 17, 16, 2, 19, 26, 27, 8, 25, 29, 28, 14, 31]$
- Keccak inv:
  $[0, 11, 22, 9, 13, 4, 18, 15, 26, 1, 8, 3, 5, 12, 30, 7, 21, 20, 2, 23, 16, 17, 6, 19, 10, 27, 24, 25, 29, 28, 14, 31]$
- x^5:
  $[0, 1, 5, 22, 17, 25, 4, 30, 31, 24, 18, 7, 20, 26, 9, 21, 12, 6, 23, 15, 16, 19, 27, 10, 14, 2, 29, 3, 8, 13, 11, 28]$
- x^5 inv:
  $[0, 1, 25, 27, 6, 2, 17, 11, 28, 14, 23, 30, 16, 29, 24, 19, 20, 4, 10, 21, 12, 15, 3, 18, 9, 5, 13, 22, 31, 26, 7, 8]$

6-bit S-box circuits

$Q2256$ S:
D=**1** G=**8.**

- $l_0 = x_0 \oplus x_1;$
- $q_7 = \sim l_0;$
- $q_9 = x_1 \oplus x_2;$
- $q_{12} = x_2 \oplus x_4;$
- $q_{13} = x_0 \oplus x_3;$
- $l_1 = x_0 \oplus x_5;$
- $q_{15} = \sim l_1;$
- $l_2 = q_9 \oplus x_3;$
- $l_3 = q_9 \oplus x_4;$
- $l_4 = q_{12} \oplus x_0;$
- $l_5 = x_3 \oplus x_5;$
- $q_0 = l_2 \oplus x_4 \oplus x_5;$
- $q_1 = \sim x_0 \oplus q_9;$
- $t_0 = q_0 \cdot q_1;$
- $q_2 = \sim x_0 \oplus l_2;$
- $t_1 = q_2 \cdot x_5;$
- $q_4 = \sim l_4;$
- $t_2 = q_4 \cdot x_1;$
- $q_6 = l_3;$
- $t_3 = q_6 \cdot q_7;$
- $q_8 = l_4 \oplus x_5;$
- $t_4 = q_8 \cdot q_9;$
- $q_{10} = \sim x_2;$
- $q_{11} = l_2 \oplus x_5;$
- $t_5 = q_{10} \cdot q_{11};$
- $t_6 = q_{12} \cdot q_{13};$
- $t_7 = x_2 \cdot q_15;$
- $l_7 = t_3 \oplus t_4;$
- $l_8 = l_7 \oplus t_2;$
- $l_9 = l_7 \oplus t_7;$
- $l_{10} = l_8 \oplus t_1;$
- $y_0 = x_1 \oplus l_5 \oplus t_0 \oplus l_8;$
- $y_1 = l_3 \oplus t_2 \oplus l_9;$
- $y_2 = x_0 \oplus l_5 \oplus t_4 \oplus t_5;$
- $y_3 = x_2 \oplus x_5 \oplus t_0 \oplus l_9;$
- $y_4 = l_1 \oplus x_1 \oplus l_{10};$
- $y_5 = l_5 \oplus t_0 \oplus l_{10} \oplus t_6;$

$Q2257$ S:
D=**1** G=**8.**

- $l_0 = x_0 \oplus x_3;$
- $l_1 = x_3 \oplus x_4;$
- $l_2 = x_0 \oplus x_4;$
- $q_1 = \sim l_0;$
- $q_6 = \sim l_1;$
- $q_{11} = \sim l_2;$
- $l_3 = x_4 \oplus x_5;$
- $l_4 = l_3 \oplus x_2;$
- $l_5 = x_1 \oplus x_2;$
- $l_6 = x_0 \oplus x_5;$
- $l_7 = l_5 \oplus x_4;$
- $l_8 = l_1 \oplus x_1;$
- $l_9 = l_6 \oplus x_2;$
- $l_{10} = l_3 \oplus x_1;$
- $q_0 = \sim x_0 \oplus l_8;$
- $t_0 = q_0 \cdot q_1;$
- $q_2 = \sim l_{10};$
- $q_3 = \sim l_4;$
- $t_1 = q_2 \cdot q_3;$
- $q_4 = \sim l_0 \oplus x_2;$
- $q_5 = \sim x_0 \oplus l_{10};$
- $t_2 = q_4 \cdot q_5;$
- $q_7 = \sim l_8;$
- $t_3 = q_6 \cdot q_7;$
- $q_8 = \sim l_6 \oplus l_8;$
- $q_9 = \sim l_6 \oplus x_1;$
- $t_4 = q_8 \cdot q_9;$
- $q_{10} = l_9 \oplus x_1;$
- $t_5 = q_{10} \cdot q_{11};$
- $q_{12} = x_0 \oplus l_8;$
- $q_{13} = l_9 \oplus l_1;$
- $t_6 = q_{12} \cdot q_{13};$
- $q_{14} = l_9 \oplus x_4;$
- $t_7 = q_{14} \cdot l_7;$
- $l_{12} = t_0 \oplus t_2;$
- $l_{13} = t_3 \oplus t_4;$
- $l_{14} = l_{12} \oplus l_{13};$
- $l_{15} = t_4 \oplus t_5;$
- $l_{16} = t_6 \oplus t_7;$
- $l_{17} = l_{15} \oplus l_{16};$
- $y_0 = l_6 \oplus x_3 \oplus l_{12} \oplus l_{16};$
- $y_1 = l_2 \oplus l_{14} \oplus t_7;$
- $y_2 = x_0 \oplus x_5 \oplus t_1 \oplus l_{17};$
- $y_3 = x_1 \oplus t_3 \oplus l_{17};$
- $y_4 = l_7 \oplus l_{13} \oplus t_5;$
- $y_5 = l_7 \oplus t_0 \oplus t_4 \oplus t_7;$

$Q2258$ S:
D=**1** G=**8.**

- $l_0 = x_0 \oplus x_4;$
- $l_1 = x_2 \oplus x_5;$
- $l_2 = x_3 \oplus x_5;$
- $q_4 = \sim l_0;$
- $q_7 = \sim l_1;$
- $q_8 = \sim l_2;$
- $l_3 = x_1 \oplus x_5;$
- $l_4 = l_3 \oplus x_2;$
- $l_5 = l_1 \oplus x_4;$
- $l_6 = x_2 \oplus x_3;$
- $l_7 = x_1 \oplus x_2;$
- $l_8 = l_6 \oplus x_5;$
- $q_0 = \sim l_4;$
- $q_1 = \sim l_5;$
- $t_0 = q_0 \cdot q_1;$
- $q_3 = q_4 \oplus l_6;$
- $t_1 = q_1 \cdot q_3;$
- $t_2 = q_4 \cdot q_0;$
- $q_6 = q_4 \oplus x_2;$
- $t_3 = q_6 \cdot q_7;$
- $q_9 = \sim l_7 \oplus x_4;$
- $t_4 = q_8 \cdot q_9;$
- $q_{10} = x_0 \oplus l_7;$
- $q_{11} = l_6 \oplus x_4;$
- $t_5 = q_{10} \cdot q_{11};$
- $q_{12} = l_7 \oplus x_3;$
- $q_{13} = \sim l_0 \oplus x_5;$
- $t_6 = q_{12} \cdot q_{13};$
- $q_{14} = \sim x_1;$
- $q_{15} = l_8;$
- $t_7 = q_{14} \cdot q_{15};$
- $l_{10} = t_1 \oplus t_2;$
- $l_{11} = t_6 \oplus t_7;$
- $l_{12} = t_5 \oplus t_7;$
- $y_0 = l_2 \oplus l_{10} \oplus l_{11};$
- $y_1 = x_0 \oplus l_8 \oplus t_0 \oplus t_1 \oplus l_{12} \oplus t_6;$
- $y_2 = x_0 \oplus x_1 \oplus l_8 \oplus l_{12};$
- $y_3 = l_3 \oplus t_1 \oplus t_3 \oplus l_{11};$
- $y_4 = x_1 \oplus x_4 \oplus t_2 \oplus t_4 \oplus t_5 \oplus t_6;$
- $y_5 = l_{10} \oplus l_{12};$

$Q2260$ S**:**
D**=1** G**=8.**

- $q_4 = x_2 \oplus x_4$;
- $q_5 = x_1 \oplus x_4$;
- $q_{15} = x_0 \oplus x_1$;
- $l_0 = x_2 \oplus x_5$;
- $l_1 = x_0 \oplus x_5$;
- $q_6 = \sim q_{15}$;
- $q_8 = \sim l_0$;
- $q_{12} = \sim l_1$;
- $l_2 = x_2 \oplus x_3$;
- $l_3 = q_{15} \oplus x_2$;
- $l_4 = q_{15} \oplus l_2$;
- $l_5 = l_2 \oplus x_1$;
- $q_0 = l_1 \oplus x_3 \oplus q_5$;
- $t_0 = q_0 \cdot l_3$;
- $q_2 = \sim l_2 \oplus x_4$;
- $t_1 = q_2 \cdot l_3$;
- $t_2 = q_4 \cdot q_5$;
- $q_7 = l_2 \oplus x_4 \oplus x_5$;
- $t_3 = q_6 \cdot q_7$;
- $t_4 = q_8 \cdot l_5$;
- $q_{11} = \sim l_4$;
- $t_5 = x_4 \cdot q_{11}$;
- $t_6 = q_{12} \cdot l_3$;
- $q_{14} = l_5 \oplus x_5$;
- $t_7 = q_{14} \cdot q_{15}$;
- $l_7 = t_2 \oplus t_3$;
- $l_8 = t_1 \oplus t_7$;
- $l_9 = l_7 \oplus l_8$;
- $y_0 = l_1 \oplus l_2 \oplus l_9$;
- $y_1 = l_2 \oplus x_5 \oplus l_7$;
- $y_2 = x_3 \oplus x_5 \oplus t_0 \oplus l_7 \oplus t_4 \oplus t_6 \oplus t_7$;
- $y_3 = x_0 \oplus x_3 \oplus x_4 \oplus t_5 \oplus t_6$;
- $y_4 = l_0 \oplus l_9 \oplus t_4 \oplus t_5$;
- $y_5 = l_4 \oplus x_5 \oplus t_0 \oplus t_2 \oplus t_5 \oplus t_7$;

$Q2263$ S**:**
D**=1** G**=8.**

- $l_0 = x_1 \oplus x_5$;
- $l_1 = x_0 \oplus x_1$;
- $l_2 = x_2 \oplus x_4$;
- $q_3 = \sim l_0$;
- $q_7 = \sim l_1$;
- $q_{12} = \sim l_2$;
- $l_3 = l_1 \oplus x_4$;
- $l_4 = x_3 \oplus x_5$;
- $l_5 = l_2 \oplus x_3$;
- $l_6 = x_2 \oplus x_5$;
- $l_7 = l_6 \oplus l_1$;
- $l_8 = x_0 \oplus x_4$;
- $q_0 = x_0 \oplus l_2 \oplus l_4$;
- $t_0 = q_0 \cdot l_7$;
- $q_2 = q_7 \oplus x_3$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim l_3$;
- $q_5 = \sim x_3$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = \sim l_8 \oplus l_4$;
- $t_3 = q_6 \cdot q_7$;
- $q_8 = \sim x_1 \oplus l_2$;
- $q_9 = l_3 \oplus l_4$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = \sim l_4 \oplus x_4$;
- $q_{11} = \sim x_1 \oplus l_5$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{13} = \sim x_5$;
- $t_6 = q_{12} \cdot q_{13}$;
- $q_{14} = l_5$;
- $q_{15} = q_7 \oplus l_4$;
- $t_7 = q_{14} \cdot q_{15}$;
- $l_{10} = t_2 \oplus t_3$;
- $l_{11} = t_4 \oplus t_7$;
- $l_{12} = t_5 \oplus t_6$;
- $y_0 = l_8 \oplus x_5 \oplus t_2 \oplus t_5 \oplus t_7$;
- $y_1 = x_5 \oplus l_{10}$;
- $y_2 = x_1 \oplus x_2 \oplus t_0 \oplus t_1 \oplus t_6 \oplus l_{11}$;
- $y_3 = l_3 \oplus l_{10} \oplus l_{11}$;
- $y_4 = l_4 \oplus t_1 \oplus t_2 \oplus l_{12}$;
- $y_5 = l_7 \oplus x_3 \oplus l_{12}$;

$Q2256\ S^{-1}$**:**
D**=2** G**=31.**

- $l_0 = x_1 \cdot x_2$;
- $l_1 = x_0 \cdot x_3$;
- $l_2 = x_2 \cdot x_3$;
- $l_3 = x_2 \cdot x_4$;
- $l_4 = x_3 \cdot x_4$;
- $l_5 = x_2 \cdot x_5$;
- $l_6 = x_4 \cdot x_5$;
- $l_7 = x_0 \cdot x_2$;
- $l_8 = x_1 \cdot x_3$;
- $l_9 = x_0 \cdot x_4$;
- $l_{10} = x_1 \cdot x_4$;
- $l_{11} = x_0 \cdot x_5$;
- $l_{12} = x_1 \cdot x_5$;
- $l_{13} = x_3 \cdot x_5$;
- $l_{14} = l_0 \cdot x_3$;
- $l_{15} = l_0 \cdot x_4$;
- $l_{16} = l_1 \cdot x_4$;
- $l_{17} = l_5 \cdot x_0$;
- $l_{18} = l_0 \cdot x_5$;
- $l_{19} = l_1 \cdot x_5$;
- $l_{20} = l_8 \cdot x_5$;
- $l_{21} = l_2 \cdot x_5$;
- $l_{22} = l_6 \cdot x_1$;
- $l_{23} = l_3 \cdot x_5$;
- $l_{24} = l_2 \cdot x_4$;
- $l_{25} = l_9 \cdot x_1$;
- $l_{26} = l_{11} \cdot x_1$;
- $l_{27} = l_{11} \cdot x_4$;
- $l_{28} = l_{13} \cdot x_4$;
- $l_{29} = l_8 \cdot x_4$;
- $l_{30} = l_8 \cdot x_0$;
- $m_1 = l_{14} \oplus l_{15} \oplus l_{16} \oplus l_{17}$;
- $m_2 = m_1 \oplus l_{18}$;
- $m_3 = l_{20} \oplus l_{22}$;
- $m_4 = l_{21} \oplus l_{23}$;
- $m_5 = m_3 \oplus m_4$;
- $m_6 = m_4 \oplus l_{20}$;
- $m_7 = l_{19} \oplus l_{23} \oplus l_{29}$;
- $m_8 = l_{19} \oplus l_{21}$;
- $m_9 = m_3 \oplus m_8 \oplus l_{30} \oplus l_{25} \oplus l_{24}$;
- $m_{10} = m_5 \oplus l_{19}$;
- $d_1 = l_{26} \oplus l_{27}$;
- $d_2 = l_{26} \oplus l_{28}$;
- $d_3 = d_1 \oplus l_{28}$;
- $s_1 = l_5 \oplus l_6$;
- $s_2 = s_1 \oplus l_2 \oplus l_3$;
- $s_3 = x_2 \oplus x_5$;
- $s_4 = l_4 \oplus l_1 \oplus l_0 \oplus x_0$;
- $s_5 = l_8 \oplus l_{10}$;
- $s_6 = s_5 \oplus s_1$;
- $s_7 = l_4 \oplus l_{12}$;
- $s_8 = x_3 \oplus l_1 \oplus x_4 \oplus l_9 \oplus l_4 \oplus x_5$;
- $s_9 = x_1 \oplus l_7 \oplus l_0 \oplus x_4 \oplus l_9$;
- $s_{10} = l_1 \oplus l_9 \oplus l_{10} \oplus l_{11} \oplus l_{12} \oplus l_{13}$;
- $y_0 = m_2 \oplus m_{10} \oplus s_2 \oplus s_4$;
- $y_1 = m_2 \oplus m_9 \oplus d_3 \oplus s_5 \oplus s_9$;
- $y_2 = m_1 \oplus m_7 \oplus d_2 \oplus s_2 \oplus s_3$;
- $y_3 = m_2 \oplus m_5 \oplus d_1 \oplus s_6 \oplus s_8$;
- $y_4 = m_2 \oplus m_6 \oplus d_3 \oplus s_1 \oplus s_{10}$;
- $y_5 = m_3 \oplus s_6 \oplus s_7$;

x^3 *non-bij*,
D**=1** G**=9.**

- $l_0 = x_4 \oplus x_5$;
- $l_1 = x_1 \oplus x_2$;
- $l_2 = x_2 \oplus x_3$;
- $q_8 = \sim l_0$;
- $q_{10} = \sim l_1$;
- $q_{16} = \sim l_2$;
- $l_3 = x_0 \oplus x_1$;
- $l_4 = l_2 \oplus l_3$;
- $l_5 = x_3 \oplus x_5$;
- $l_6 = x_0 \oplus x_2$;
- $q_0 = \sim x_1 \oplus l_0$;
- $q_1 = \sim x_3 \oplus l_0$;
- $t_0 = q_0 \cdot q_1$;
- $q_2 = l_6 \oplus x_4$;
- $q_3 = x_1 \oplus x_2 \oplus l_0$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = \sim x_0 \oplus l_0$;
- $q_5 = \sim x_1 \oplus l_2$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = \sim x_4$;
- $q_7 = \sim x_2$;
- $t_3 = q_6 \cdot q_7$;
- $q_9 = \sim l_3 \oplus x_2$;
- $t_4 = q_8 \cdot q_9$;
- $q_{11} = x_0 \oplus l_2$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = \sim l_4 \oplus x_4$;
- $q_{13} = \sim x_1 \oplus l_5$;
- $t_6 = q_{12} \cdot q_{13}$;
- $q_{14} = l_6 \oplus x_5$;
- $q_{15} = l_0 \oplus l_3$;
- $t_7 = q_{14} \cdot q_{15}$;
- $q_{17} = l_3 \oplus l_5$;
- $t_8 = q_{16} \cdot q_{17}$;
- $l_8 = t_2 \oplus t_3$;
- $l_9 = t_4 \oplus t_6$;
- $l_{10} = l_8 \oplus l_9$;
- $y_0 = l_1 \oplus l_8 \oplus t_5 \oplus t_8$;
- $y_1 = x_1 \oplus x_4 \oplus t_1 \oplus l_8 \oplus t_7$;
- $y_2 = x_1 \oplus t_0 \oplus t_1 \oplus t_5 \oplus t_6$;
- $y_3 = l_6 \oplus l_{10} \oplus t_8$;
- $y_4 = x_1 \oplus x_5 \oplus t_5 \oplus l_{10}$;
- $y_5 = l_4 \oplus t_2 \oplus t_6 \oplus t_7$;

$Q2258$ S^{-1}**:**
D**=2** G**=22.**

- $l_0 = x_0 \oplus x_5$;
- $p_{12} = x_1 \cdot x_2$;
- $p_{03} = x_0 \cdot x_3$;
- $p_{15} = x_1 \cdot x_5$;
- $p_{13} = x_1 \cdot x_3$;
- $p_{34} = x_3 \cdot x_4$;
- $p_{25} = x_2 \cdot x_5$;
- $p_{02} = x_0 \cdot x_2$;
- $p_{23} = x_2 \cdot x_3$;
- $p_{05} = x_0 \cdot x_5$;
- $p_{35} = x_3 \cdot x_5$;
- $p_{14} = x_1 \cdot x_4$;
- $p_{45} = x_4 \cdot x_5$;
- $l_6 = x_0 \oplus x_3$;
- $l_1 = p_{13} \oplus p_{34}$;
- $l_2 = l_6 \oplus x_4$;
- $l_3 = l_6 \oplus x_2$;
- $l_4 = x_3 \oplus x_4 \oplus x_5$;
- $l_5 = l_1 \oplus p_{14}$;
- $l_7 = p_{12} \oplus p_{03} \oplus p_{15} \oplus p_{23}$;
- $l_8 = x_0 \oplus p_{13} \oplus p_{25} \oplus p_{03}$;
- $l_9 = p_{13} \oplus p_{05} \oplus p_{34} \oplus p_{02}$;
- $l_{10} = p_{23} \oplus p_{14} \oplus p_{45}$;
- $l_{11} = p_{34} \oplus p_{15}$;
- $l_{12} = x_4 \cdot \sim l_3 \cdot \sim x_1$;
- $l_{13} = p_{12} \cdot \sim x_4$;
- $l_{14} = l_8 \cdot \sim l_2$;
- $l_{15} = x4 \oplus l_5$;
- $l_{16} = x_2 \cdot l_{15}$;
- $l_{17} = \sim x_0 \oplus x_2$;
- $l_{18} = p_{34} \cdot l_{17}$;
- $l_{19} = x_0 \cdot l_5$;
- $m_1 = x_4 \cdot l_0$;
- $m_2 = x_5 \cdot l_1$;
- $m_3 = p_{25} \cdot l_2$;
- $m_4 = p_{14} \oplus p_{03} \oplus p_{25} \oplus p_{05}$;
- $m_5 = m_2 \oplus p_{35}$;
- $y_0 = x_0 \oplus x_4 \oplus m_1 \oplus l_7 \oplus l_{12}$;
- $y_1 = x_1 \oplus x_4 \oplus m_5 \oplus l_9 \oplus l_{13} \oplus l_{14}$;
- $y_2 = x_2 \oplus x_5 \oplus m_2 \oplus m_3 \oplus l_{10} \oplus l_{16}$;
- $y_3 = l_4 \oplus p_{13} \oplus m_1 \oplus m_4 \oplus l_{18}$;
- $y_4 = m_1 \oplus m_3 \oplus m_4 \oplus m_5 \oplus l_{11} \oplus l_{19}$;
- $y_5 = l_5 \oplus p_{05} \oplus p_{25} \oplus p_{35} \oplus p_{45}$;

Look-up tables (LUTs):

$Q2256 = [0, 1, 2, 3, 4, 6, 7, 5, 8, 12, 16, 20, 32, 39, 57, 62, 9, 17$
$21, 13, 40, 51, 53, 46, 50, 47, 52, 41, 63, 33, 56, 38, 10$
$45, 27, 60, 43, 15, 59, 31, 58, 24, 49, 19, 55, 22, 61, 28$
$29, 35, 18, 44, 25, 36, 23, 42, 30, 37, 11, 48, 54, 14, 34, 26]$

$Q2257 = [0, 1, 2, 3, 4, 6, 7, 5, 8, 12, 16, 20, 32, 39, 57, 62, 9, 17$
$21, 13, 41, 50, 52, 47, 40, 53, 46, 51, 36, 58, 35, 61, 10$
$25, 37, 54, 33, 49, 15, 31, 45, 59, 24, 14, 42, 63, 30, 11$
$29, 23, 44, 38, 18, 27, 34, 43, 19, 28, 56, 55, 48, 60, 26, 22]$

$Q2258 = [0, 1, 2, 3, 4, 6, 7, 5, 8, 12, 16, 20, 32, 39, 57, 62, 9, 17$
$21, 13, 41, 50, 52, 47, 55, 42, 49, 44, 59, 37, 60, 34, 10$
$25, 38, 53, 35, 51, 14, 30, 61, 43, 11, 29, 56, 45, 15, 26$
$22, 28, 36, 46, 27, 18, 40, 33, 23, 24, 63, 48, 54, 58, 31, 19]$

$Q2260 = [0, 1, 2, 3, 4, 6, 8, 10, 5, 11, 16, 30, 32, 45, 59, 54, 7, 24$
$40, 55, 48, 44, 17, 13, 9, 25, 49, 33, 31, 12, 41, 58, 14$
$27, 26, 15, 57, 47, 35, 53, 61, 39, 62, 36, 43, 50, 38, 63$
$46, 37, 23, 28, 42, 34, 29, 21, 22, 18, 56, 60, 51, 52, 19, 20]$

$Q2263 = [0, 1, 2, 3, 4, 8, 16, 28, 5, 12, 32, 41, 10, 14, 57, 61, 6$
$62, 23, 47, 33, 20, 38, 19, 43, 27, 29, 45, 7, 58, 39, 26, 9$
$22, 55, 40, 11, 25, 35, 49, 44, 59, 53, 34, 37, 63, 42, 48$
$21, 51, 56, 30, 52, 31, 15, 36, 24, 54, 18, 60, 50, 17, 46, 13]$

x^3 (non-bij)$= [0, 1, 8, 15, 27, 14, 35, 48, 53, 39, 43, 63, 47, 41, 1, 1$
$41, 15, 15, 47, 52, 6, 34, 22, 20, 33, 36, 23, 8, 41, 8, 47, 36$
$52, 35, 53, 35, 39, 20, 22, 33, 34, 48, 53, 39, 48, 6, 23, 22$
$33, 63, 14, 23, 52, 14, 43, 27, 63, 36, 6, 27, 43, 20, 34]$

7-bit S-box circuits

x^3 S**:**
D**=1** G**=15.**

- $q_{18} = x_0 \oplus x_6$;
- $l_0 = x_1 \oplus x_4$;
- $l_1 = x_1 \oplus x_3$;
- $l_2 = x_0 \oplus x_1$;
- $l_3 = x_1 \oplus x_5$;
- $l_4 = x_0 \oplus x_3$;
- $q_0 = \sim l_0$;
- $q_1 = \sim l_1$;
- $q_7 = \sim l_2$;
- $q_8 = \sim l_3$;
- $q_{19} = \sim l_4$;
- $l_5 = x_2 \oplus x_3$;
- $l_6 = x_4 \oplus x_6$;
- $l_7 = l_5 \oplus l_6$;
- $l_8 = l_6 \oplus x_5$;
- $l_9 = x_5 \oplus x_6$;
- $l_{10} = x_4 \oplus x_5$;
- $l_{11} = l_8 \oplus x_2$;
- $l_{12} = x_0 \oplus x_4$;
- $l_{13} = l_{12} \oplus l_5$;
- $l_{14} = l_2 \oplus l_5$;
- $l_{15} = l_5 \oplus l_9$;
- $t_0 = q_0 \cdot q_1$;
- $q_2 = x_1 \oplus l_{11}$;
- $q_3 = \sim q_{18} \oplus l_1$;
- $t_1 = q_2 \cdot q_3$;
- $q_4 = l_0 \oplus l_5$;
- $q_5 = x_0 \oplus l_{15}$;
- $t_2 = q_4 \cdot q_5$;
- $q_6 = q_7 \oplus x_4$;
- $t_3 = q_6 \cdot q_7$;
- $q_9 = l_{13}$;
- $t_4 = q_8 \cdot q_9$;
- $q_{10} = \sim x_0$;
- $q_{11} = l_0 \oplus x_2$;
- $t_5 = q_{10} \cdot q_{11}$;
- $q_{12} = x_0 \oplus l_{10}$;
- $q_{13} = l_2 \oplus x_5$;
- $t_6 = q_{12} \cdot q_{13}$;
- $q_{14} = l_{14} \oplus l_6$;
- $q_{15} = x_0 \oplus l_8$;
- $t_7 = q_{14} \cdot q_{15}$;
- $q_{16} = \sim l_7$;
- $q_{17} = \sim x_0 \oplus x_2 \oplus l_{10}$;
- $t_8 = q_{16} \cdot q_{17}$;
- $t_9 = q_{18} \cdot q_{19}$;
- $q_{20} = x_0 \oplus l_{15}$;
- $q_{21} = \sim x_3$;
- $t_{10} = q_{20} \cdot q_{21}$;
- $q_{22} = q_7 \oplus x_2 \oplus l_6$;
- $q_{23} = \sim l_4 \oplus l_9$;
- $t_{11} = q_{22} \cdot q_{23}$;
- $q_{24} = x_1 \oplus l_{10}$;
- $q_{25} = l_4 \oplus x_5$;
- $t_{12} = q_{24} \cdot q_{25}$;
- $q_{26} = l_2 \oplus x_3 \oplus x_5$;
- $q_{27} = \sim x_1 \oplus l_5 \oplus x_6$;
- $t_{13} = q_{26} \cdot q_{27}$;
- $q_{28} = \sim l_{12} \oplus x_2$;
- $q_{29} = q_7 \oplus x_6$;
- $t_{14} = q_{28} \cdot q_{29}$;
- $l_{16} = t_1 \oplus t_3$;
- $l_{17} = l_{16} \oplus t_6$;
- $l_{18} = t_9 \oplus t_{10}$;
- $l_{19} = t_{13} \oplus t_{14}$;
- $y_0 = x_1 \oplus l_{15} \oplus l_{17} \oplus t_8$;
- $y_1 = x_0 \oplus l_{11} \oplus t_0 \oplus t_3 \oplus t_5 \oplus t_8 \oplus t_{10} \oplus l_{19}$;
- $y_2 = l_2 \oplus l_{11} \oplus t_2 \oplus l_{16} \oplus t_8 \oplus t_{12}$;
- $y_3 = l_{14} \oplus l_9 \oplus t_0 \oplus t_2 \oplus t_6 \oplus l_{18} \oplus t_{14}$;
- $y_4 = l_{13} \oplus t_2 \oplus t_4 \oplus l_{18} \oplus t_{13}$;
- $y_5 = l_7 \oplus t_5 \oplus l_{17} \oplus t_7 \oplus t_9 \oplus t_{11} \oplus t_{12}$;
- $y_6 = x_3 \oplus l_9 \oplus t_6 \oplus t_{11} \oplus l_{19}$;

Look-up table (LUT):

$x^3, S =$ [0, 1, 8, 15, 64, 85, 120, 107, 12, 69, 39, 104, 73, 20, 82, 9, 96, 119, 36, 53, 62, 61, 74, 79, 68, 27, 35, 122, 31, 84, 72, 5, 10, 51, 49, 14, 38, 11, 45, 6, 117, 4, 109, 26, 92, 57, 116, 23, 44, 3, 91, 114, 30, 37, 89, 100, 123, 28, 47, 78, 76, 63, 40, 93, 80, 113, 29, 58, 13, 56, 112, 67, 54, 95, 88, 55, 110, 19, 48, 75, 33, 22, 32, 17, 98, 65, 83, 118, 111, 16, 77, 52, 41, 66, 59, 86, 102, 127, 24, 7, 87, 90, 25, 18, 115 34, 46, 121, 71, 2, 42, 105, 81, 94, 99, 106, 126, 101, 124, 97, 108, 43, 125, 60, 70, 21, 103, 50]