An Algorithm to Analyze Non-injective S-Boxes

Leandro Marin, Ludo Tolhuizen

An algorithm to analyze non-injective S-Boxes

Leandro Marin[1] and Ludo Tolhuizen[2]

[1] Department of Applied Mathematics,
Computer Sciences Faculty, University of Murcia,
Reg. Campus of Int. Excellence Campus MareNostrum,
Murcia, Spain.
leandro@um.es
[2] Philips Group Innovation, Research
High Tech Campus 34, 5656AE Eindhoven, The Netherlands
ludo.tolhuizen@philips.com

Abstract. We present an algorithm for constructing pairs of an invertible mapping A and an affine mapping B such that $AS = SB$ for a given S-box. For doing we so, we introduce and analyse the link graph of an S-box. We apply the algorithm to the eight DES S-boxes. All obtained pairs (A, B) are those reported in previous work, in which it was required that both A and B are invertible affine mappings. In particular, the relaxation that A need not be affine does not yield new pairs.

Keywords: Security, DES, S-Box, Non-injective maps, Link Graph, Link Path, Self Equivalences

1 Introduction

The study of invariant properties of cryptographic maps under actions of linear or affine groups is a well-known cryptanalysis tool [1]. In many cases, we can deal with bijective maps $S : \mathbb{F}_2^k \to \mathbb{F}_2^k$. This can be helpful to make an extensive search with computers, because we can take an affine transformation $A : \mathbb{F}_2^k \to \mathbb{F}_2^k$, compute $B = S^{-1} \circ A \circ S$ and check if B is also affine. It is also possible to have an early abort strategy to check the affine properties of B, see [1].

When S is not injective we have an extra difficulty, that is the exponential amplification that appears when we have not a unique B, but multiple choices for the values $B(p)$ such that $AS(p) = SB(p)$. The problem is even more complicated if we look for non-bijective affine maps B.

In this paper, we present an algorithm for constructing pairs of an invertible mapping A and an affine mapping B such that $AS = SB$ for a given S-box. Note that we do not require that A be affine, and therefore we may find more such pairs than in [1, Section 4.2], where for the seven of the eight DES S-boxes, we only can have A and B equal to the identity mapping, while for S_4, there is only one more choice. This work adds to the further analysis of the DES S-boxes, although the technique can be applied to any surjective map $S : \mathbb{F}_2^t \to \mathbb{F}_2^k$.

We are going to use the affine properties of B to reduce the number of options to a quantity that allows exhaustive look up.

Let $S : \mathbb{F}_2^t \to \mathbb{F}_2^k$ be a map, we are going to consider pairs $A : \mathbb{F}_2^k \to \mathbb{F}_2^k$ and $B : \mathbb{F}_2^t \to \mathbb{F}_2^t$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{F}_2^t & \xrightarrow{S} & \mathbb{F}_2^k \\ {\scriptstyle B}\downarrow & & \downarrow{\scriptstyle A} \\ \mathbb{F}_2^t & \xrightarrow{S} & \mathbb{F}_2^k \end{array}$$

We will consider the case when B is affine; there are no requirements on A, except that it should be chosen such that $AS = SB$.

2 Link Paths

For any $p \in \mathbb{F}_2^k$ we are going to consider the set $S^{-1}(p)$ and the affine subspace of $\mathbb{F}_2^t$ generated by these points, this affine subspace will be called $L(p)$.

We will use barycentric coordinates for the affine space $\mathbb{F}_2^t$, therefore for all $v \in L(p)$ we can find values $\lambda_w \in \mathbb{F}_2$, called the barycentric coordinates of v, such that $\sum_{w \in S^{-1}(p)} \lambda_w = 1$ and $v = \sum_{w \in S^{-1}(p)} \lambda_w \cdot w$. These values are unique if and only if the points are independent. A general reference about barycentric coordinates can be found in [2, pp. 216–221].

Definition 1. *Let $p, q \in \mathbb{F}_2^k$, we will say that p links q, and we will write $p \to q$, if $S^{-1}(q) \cap L(p) \neq \emptyset$.*

Proposition 1. *Let $A : \mathbb{F}_2^k \to \mathbb{F}_2^k$, and let $B : \mathbb{F}_2^t \to \mathbb{F}_2^t$ be affine, such that $AS = SB$. Let $p, q \in \mathbb{F}_2^k$ such that $p \to q$, then the values $\{B(w) : w \in S^{-1}(p)\}$ determine the value of $S(B(v'))$ for all $v' \in S^{-1}(q)$.*

Proof. We know that $p \to q$, therefore $S^{-1}(q) \cap L(p) \neq \emptyset$ and we can take a point v in this set.

This value v satisfies that $S(v) = q$ and $v = \sum_{w \in S^{-1}(p)} \lambda_w \cdot w$ for some values λ_w that satisfy $\sum_{w \in S^{-1}(p)} \lambda_w = 1$.

The map B is affine, therefore it preserves the barycentric combinations and we have $B(v) = \sum_{w \in S^{-1}(p)} \lambda_w \cdot B(w)$, which is a known value if the values $\{B(w) : w \in S^{-1}(p)\}$ are known.

For any $v' \in S^{-1}(q)$ we have that $S(v') = q = S(v)$, therefore $SB(v') = AS(v') = AS(v) = SB(v)$.

Definition 2. *Let $p_0 \to p_1 \to \cdots \to p_n$ be a path of links for the map $S : \mathbb{F}_2^t \to \mathbb{F}_2^k$. We will say that this path is exhaustive if the points $\cup_{i=0}^n S^{-1}(p_i)$ generate the whole affine space $\mathbb{F}_2^t$.*

The algorithm for constructing mappings A and B such that $AS = SB$ is the following:

1. Find an exhaustive link path $p_0 \to p_1 \to \cdots \to p_n$

2. Choose a value for $A(p_0)$
3. For every $v \in S^{-1}(p_0)$ choose an image $B(v)$ in $S^{-1}(A(p_0))$
4. Fix the value of $A(p_1)$ and at least the image by B of one point of $S^{-1}(p_1)$
5. Choose the other images in $S^{-1}(A(p_1))$
6. This process should continue until p_n is reached, then enough images will be chosen and the value of B fixed under these conditions
7. Check if $AS = SB$
8. If not, make new choices until all the possible values of B are checked

This algorithm, given in very general terms, will be applied to the DES S-Boxes.

3 Application to DES S-Boxes

Let $S_i : \mathbb{F}_2^6 \to \mathbb{F}_2^4$ be a DES S-box. We are going to apply the method described previously to study the existence of maps $A : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ (general) and $B : \mathbb{F}_2^6 \to \mathbb{F}_2^6$ (affine) such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{F}_2^6 & \xrightarrow{S_i} & \mathbb{F}_2^4 \\ {\scriptstyle B}\downarrow & & \downarrow{\scriptstyle A} \\ \mathbb{F}_2^6 & \xrightarrow{S_i} & \mathbb{F}_2^4 \end{array}$$

Notice that the existence of these kind of maps is trivial if we accept general maps for B, and the algorithm proposed is not applicable because it is based on the affiness of B.

Suppose that for S_i we can find an exhaustive path $p \to q$ with length 1. Then we choose a value for $A(p)$ (we have 2^4 choices) and then for each of the values in $S_i^{-1}(p)$ we choose the image of B in $S_i^{-1}(A(p))$. We have $4^4 = 2^8$ possible choices if we do not require injectivity of B.

The link relation $p \to q$ forces the value of $A(q)$ and the value for the point in $S_i^{-1}(q) \cap L_i(p)$. The other three values of $S_i^{-1}(q)$ can be chosen in $4^3 = 2^6$ different ways.

As $p \to q$ is exhaustive, these choices fix the value of B, and then we can check if the diagram commutes. The number of choices that we have is $2^4 \cdot 2^8 \cdot 2^6 = 2^{18}$, which is not a small number, but can be reached with a simple PC.

This can be done if the S-box has an exhaustive link $p \to q$. We are going to see that this is possible for all S-boxes but S_4, that will require an exhaustive path of length two.

Although in the analysis, any map A can be considered, we have imposed the extra condition of bijectivity of A. If this is not the case, a lot of options arise, for example constant maps $B : \mathbb{F}_2^6 \to \mathbb{F}_2^6$, that are not interesting for cryptographical purposes. Nonbijective maps B that could have generated bijective maps A are accepted, but none of them appear, as we can see in the following proposition:

Proposition 2. *Suppose A is invertible, B is affine such that $AS = SB$. If x_1, x_2 are such that $Bx_1 = Bx_2$, then for all y, we have $S(y + x_1 + x_2) = S(y)$.*

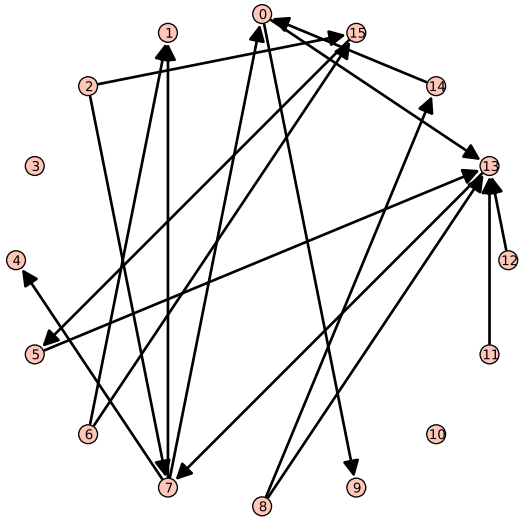
Proof. We are in characteristic 2, and $Bx_1 = Bx_2 = -Bx_2$, thus $Bx_1 + Bx_2 = 0$. We also know that B is affine, therefore for each y we have that $B(y+x_1+x_2) = B(y)+B(x_1)+B(x_2) = B(y)$. As $AS = SB$, this implies that $AS(y+x_1+x_2) = AS(y)$, and so, as A is invertible, $S(y + x_1 + x_2) = S(y)$.

We know from [1, Section 4.2] that the for all DES S-boxes S_j ($j = 1, \cdots, 8$), if $S_j(x+a) = S_j(x)$ holds then $a = 0$. Thus it follows from the above proposition that if $AS_j = S_jB$ with A invertible and B affine, then B is invertible as well.

In the following sections, we will show the graphs with the exhaustive links of the different DES S-Boxes. The vertices of the graphs will be the vectors written in decimal representation. An arrow between p and q is drawn if and only if we have an exhaustive link path $p \to q$.

4 The S-Box S_1

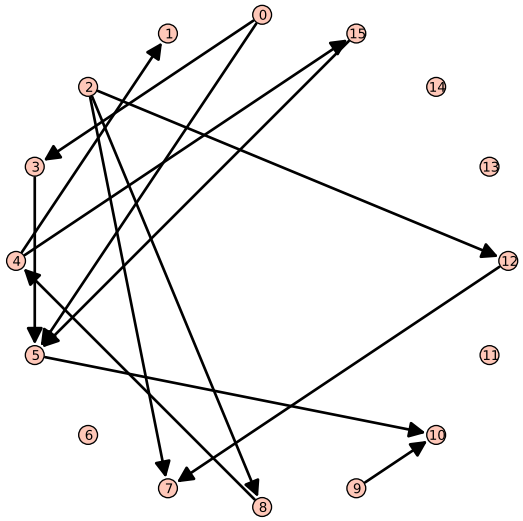
The graph with the exhaustive links of S_1 is



We have used for our analysis the values $p = 0$, $q = 9$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

5 The S-Box S_2

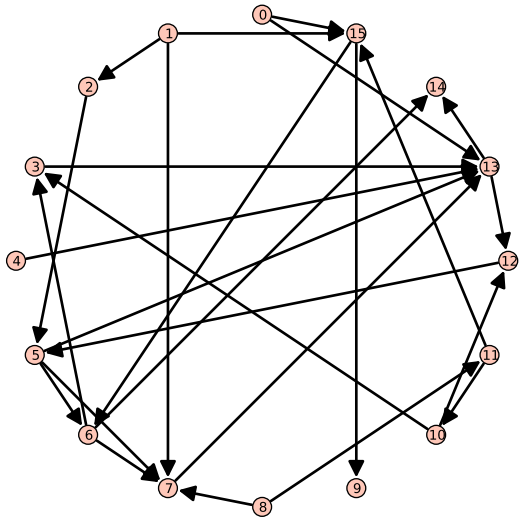
The graph with the exhaustive links of S_2 is



We have used for our analysis the values $p = 0$, $q = 3$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

6 The S-Box S_3

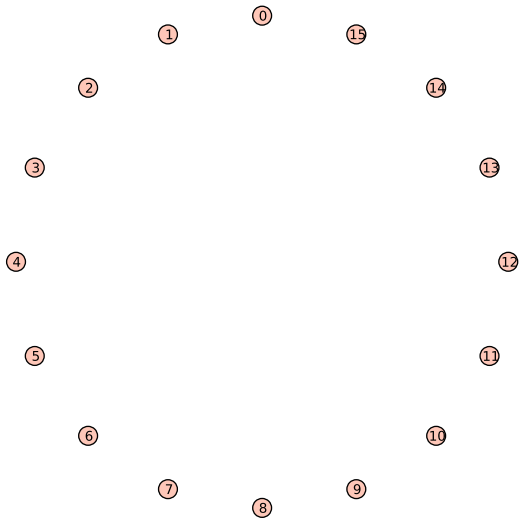
The graph with the exhaustive links of S_3 is



We have used for our analysis the values $p = 0$, $q = 13$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

7 The S-Box S_4

The graph with the exhaustive links of S_4 is



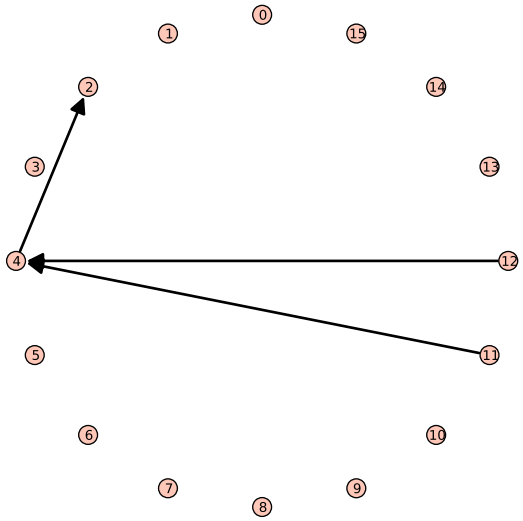
This means that we have not any exhaustive link path of length 1, but this is not a big problem, because we can find link paths of length two, for example $0 \to 10 \to 2$.

This search gave no example out of the identities and the already known affine transformation, that is obtained when the set $S_4^{-1}(0)$ is sent to $S_4^{-1}(6)$. The affine map B in this case is $B(v) = v + (1, 0, 1, 1, 1, 1)$ and $A(w) = w + (0, 1, 1, 0)$. This is already metioned in the literature several times (see [1, 3]).

The existence of S-Boxes without exhaustive link paths is not common, although a definition of the probability is not simple because S-Boxes are not taken randomly, this makes very difficult to define the sample space.

8 The S-Box S_5

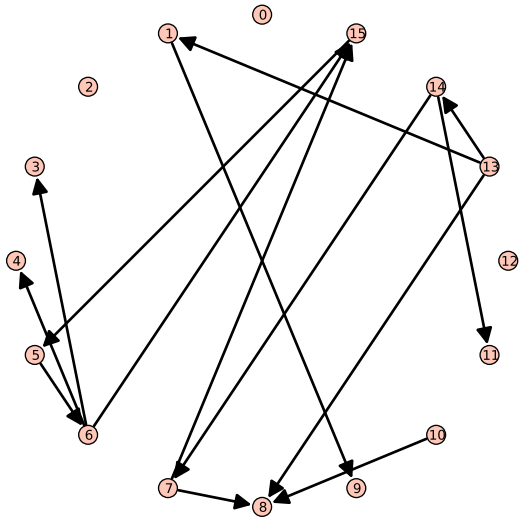
The graph with the exhaustive links of S_5 is



We have used for our analysis the values $p = 4$, $q = 2$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

9 The S-Box S_6

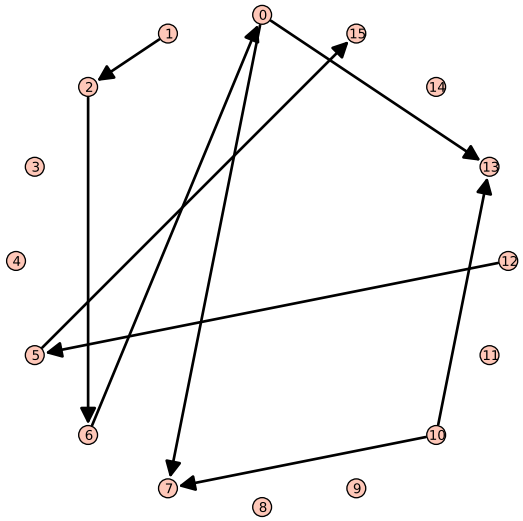
The graph with the exhaustive links of S_6 is



We have used for our analysis the values $p = 1$, $q = 9$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

10 The S-Box S_7

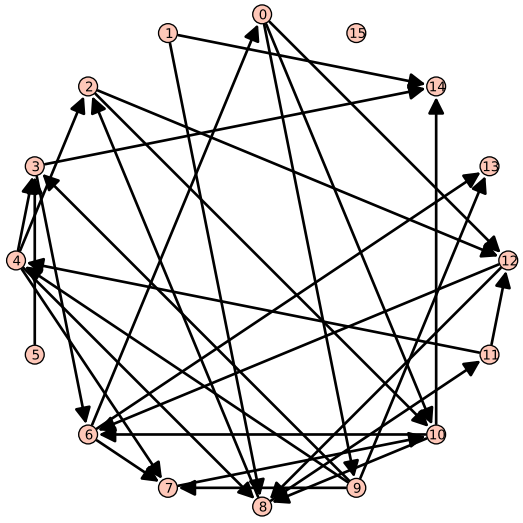
The graph with the exhaustive links of S_7 is



We have used for our analysis the values $p = 0$, $q = 7$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

11 The S-Box S_8

The graph with the exhaustive links of S_8 is



We have used for our analysis the values $p = 0$, $q = 9$. It turned out that the only choice for A and B are the identity maps on $\mathbb{F}_2^4$ and $\mathbb{F}_2^6$, respectively.

12 The Bijectivity of A

Although it is not interesting for cryptographic pourposes, this algorithm can give us also the possibilities for non bijective maps $A : \mathbb{F}_2^4 \to \mathbb{F}_2^4$. Think for example all constant maps.

As an application of the method, we have computed the pairs (A, B) for S_4, and we have obtained 74658 affine maps B, most of them constant or with only one independent vector. When B is chosen, the value of A can be determined for some values and for the others we have a complete freedom.

13 Conclusion and Evaluation

The existence of linear and affine equivalences between invertible S-boxes (permutations) have been considered and analyzed with general algorithms, for example in [1]. The exponential amplification that appears when S is non-bijective makes an exhaustive search much more difficult. In this paper we introduced the notion of link graph of an S-box. This technique focus the search of candidates for equivalences to a small set of choices, that compensate the exponential amplification and therefore let us develop an algorithm to find pairs of a bijective mapping A and an affine mapping B such that $AS = SB$.

We applied this algorithm to the eight DES S-boxes, and found that all such pairs were already obtained before under the condition that both A and B are bijective affine mappings. In particular, the relaxation of the requirement that A should be affine, as in [1], to the very general requirement of being bijective, does not yield new pairs of mappings.

The problem of nonbijective S-boxes has been considered in [1] with a different approach, because they require that A and B both should be affine. Their algorithm is not applicable to our case that is more general, and we both compensate the exponential amplification of the problem, but we can make some comments about the complexity of both methods.

The complexity given in [1, Section 4.2] for affine equivalences of noninvertible S-boxes is $n^3 \cdot 2^n \cdot (2^{n-m}!)^{\frac{n}{2^{n-m}}}$ that applied to $n = 6$ and $m = 4$ gives around 2^{20}. The number of choices in our case (for exhaustive link paths) is 2^{18}, but each choice generate an affine map B and a map A. For those we have to check the commutativity of the diagram and previously compute the link path, therefore the complexity of both algorithms for $n = 6$ and $m = 4$ could be similar, but our search is much more general.

Acknowledgement

The first author wishes to thank the financial support given by the Ministry of Science and Innovation of Spain, through the Walkie-Talkie project (TIN2011-27543-C03) and also the *Fundación Séneca*.

The authors wish to thank Paul Gorissen for the interesting discussions about this topic.

References

1. Biryukov, A., Cannière, C.D., Braeken, A., Preneel, B.: A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In Biham, E., ed.: EUROCRYPT. Volume 2656 of Lecture Notes in Computer Science., Springer (2003) 33–50
2. Coxeter, H.: Introduction to geometry. 2nd edn. John Wiley and Sons (1969)
3. Hellman, M., Merkle, R., Schroppel, R., Washington, L., Diffie, W., Pohlig, S., Schweitzer, P.: Results on an initial attempt to cryptanalyze the nbs data encryption standard. Technical report, Stanford University (September 1976)