Good S-Boxes Are Easy To Find

Carlisle Adams and Stafford Tavares
Department of Electrical Engineering
Queen's University, Kingston, Ontario, Canada, K7L 3N6

Abstract. *We describe an efficient design methodology for the s-boxes of DES-like cryptosystems. Our design guarantees that the resulting s-boxes will be bijective and nonlinear and will exhibit the strict avalanche criterion and the output bit independence criterion.*

1. Introduction

In this work we describe the structured design of substitution boxes (s-boxes) for cryptosystems built as substitution-permutation networks (DES-like systems). There are several motivations for research in this area:

- s-boxes are a critical element of any S-P network since the remainder of the network is linear;
- some design and evaluation criteria in DES s-boxes remain classified; study in this area may help to shed some light on how the DES s-boxes were chosen;
- a *structured* approach to s-box design may help to speed up the process of finding new s-boxes for any desired application;
- the design of pseudorandom mappings is itself an active research area, independent of any possible applications.

Because we design s-boxes to satisfy several criteria simultaneously, our approach overcomes the deficiencies in the s-boxes designed by Pieprzyk and Finkelstein [8]. This results in s-boxes which appear to be cryptographically "good" and which can be designed extremely efficiently.

2. Background

Pieprzyk and Finkelstein [8] have described a method for $n \times n$ bit s-box design which relies on finding n appropriate Boolean functions of n bits and setting these as the output bits. These Boolean functions can be found very easily: they give an algorithm for constructing one function and the rest are simple variations of this one. They focus on the nonlinearity property of an s-box (a necessary property since the remainder of the algorithm in an S-P network is linear) and state that an s-box will be as highly nonlinear as possible if its component Boolean functions are each as highly nonlinear as possible (this definition of s-box nonlinearity is similar to that proposed by Rueppel [10], who did some work on finding the closest linear approximation to any given s-box). The

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 612-615, 1990.

algorithm in [8], therefore, constructs a Boolean function of highest possible nonlinearity (subject to the restriction that it is 0-1 balanced) and gives n-1 simple variations which preserve nonlinearity. These n functions are then set as the output bits of the s-box.

S-boxes created by the method in [8] have several limitations, however. Firstly, the inverse s-box is almost completely linear (it has only one nonlinear function), which may be of some help to a cryptanalyst. Secondly, there is no guarantee that the s-boxes will have good avalanche (or "diffusion") [11, 5]. Thirdly, it is easy to show that ***every*** pair of output bits will have a correlation of ± 1 with respect to the inversion of a single input bit. Finally, their algorithm is useful for constructing $n \times n$ bit s-boxes only when n is odd.

3. Criteria for a "good" $n \times n$ bit s-box

We have chosen four properties which we feel are necessary for general, cryptographically "good" s-boxes. They are:

1. bijection;
2. nonlinearity;
3. strict avalanche;
4. independence of output bits.

For some applications it is important that the inverse s-box also possess these properties, so we may add "bidirectionality" as an optional fifth property. Note that all but one of the evaluation criteria released about the DES s-boxes [3, 4] are covered by the above properties; the one criterion not covered deals with combining four 4×4 bit s-boxes into one 6×4 bit s-box. This criterion deals not with an *internal* property of $n \times n$ bit s-boxes but rather with the relationship *between* $n \times n$ bit s-boxes, and so is not addressed in this paper.

We now describe a procedure for efficiently producing s-boxes which are guaranteed to possess the above four properties.

4. Methodology for s-box construction

In our $n \times n$ bit s-box design we choose n Boolean functions (each of n input variables) that satisfy the following properties and set these as the output bits. Let these functions be $f_1, f_2, \ldots, f_n$.

Bijection: Choose the f_i such that $wt\left(\sum_{i=1}^{n} a_i f_i\right) = 2^{n-1} \pmod 2$, where $a_i \in \{0, 1\}$ and *wt()* is the Hamming weight. This will guarantee that s-box S is bijective.

Nonlinearity: Choose the f_i to be as highly nonlinear as possible (see [8, 7, 10], and others). This will guarantee that S is nonlinear and that Rueppel's "closest linear approximation" to S is of no help to a cryptanalyst.

Strict Avalanche: Choose f_i which satisfy the Strict Avalanche Criterion [11]; this can be done using Forré's method [6] or some other. This will guarantee that S satisfies the SAC.

Output Bit Independence: Choose the f_i such that $(f_j \oplus f_k)$ is highly nonlinear and comes as close as possible to satisfying the SAC for all $j, k \in \{1, 2, \ldots, n\}$, $j \neq k$. This will guarantee that every pair of output bits will have a correlation as close as possible to zero when any single input bit is inverted (this is known as the output bit independence criterion [11]).

The proofs for the above statements are fairly straightforward and will appear in the full version of this paper [2].

5. Results

It turns out that there are no conflicting requirements in our design methodology so that all criteria can be met simultaneously. For 4×4 bit s-boxes there are only 2^{16} possible Boolean functions, so even an exhaustive search for functions which meet all our criteria is quite feasible. However, the search space is quickly reduced by relatively simple checks (weight, nonlinearity) so that more computationally intensive checks (SAC, for example) are only performed on a subset of the space. Furthermore, other methods (in particular, "bent" functions [9, 7, 1]) can be used to reduce the initial search space so that it may be possible to relatively quickly design 6×6 or 8×8 bit s-boxes.

We find that "good" s-boxes can be generated by our procedure in a few seconds of CPU time on a SUN workstation. Therefore, one can easily generate and store lists of "good" s-boxes so that new cryptosystem design may reduce to simply plugging new s-boxes into a general S-P framework (DES or an extended DES, for example). Furthermore, many "good" s-boxes exist, but not so many that they are easily found by random permutations of the numbers 1, 2, . . . , 2^n-1. We have generated and stored an exhaustive list of all 16-bit vectors which are 0-1 balanced, are highly nonlinear, and satisfy the SAC. From this list we can then choose vectors at random until we find four which combine in such a way as to guarantee bijection and output bit independence (as described above). A brief preliminary search for these 4×4 bit s-boxes has found:

- approximately 60 s-boxes which satisfy all our requirements in both forward and inverse direction;
- approximately 170 s-boxes which satisfy all our requirements if we consider the forward direction only;
- that if we relax the requirements slightly, the numbers quickly grow to 100's or 1000's of "fairly good" s-boxes — note that all of the DES s-boxes fall into this class.

Some example s-boxes generated by our procedure are:

$$S_1 = [9 \quad 13 \quad 10 \quad 15 \quad 11 \quad 14 \quad 7 \quad 3 \quad 12 \quad 8 \quad 6 \quad 2 \quad 4 \quad 1 \quad 0 \quad 5]^t$$
$$S_2 = [6 \quad 10 \quad 14 \quad 2 \quad 11 \quad 3 \quad 13 \quad 5 \quad 12 \quad 4 \quad 9 \quad 1 \quad 7 \quad 8 \quad 15 \quad 0]^t$$
$$S_3 = [11 \quad 10 \quad 9 \quad 8 \quad 13 \quad 15 \quad 6 \quad 7 \quad 5 \quad 3 \quad 2 \quad 14 \quad 4 \quad 1 \quad 12 \quad 0]^t$$

6. Suggestion

A simple way to extend DES in the short term might be to standardize a list of good s-boxes and have as part of the key the choice of s-boxes to use. In this way the algorithm itself would remain identical but the keysize would be made larger since the s-boxes would be replaced with other equally or more secure s-boxes in a key-dependent way. Whit Diffie has suggested (in the rump session of these proceedings) that it may be worthwhile to examine this "improved" DES using Shamir's algorithm for round-by-round cryptanalysis of the original DES.

Bibliography

[1] C. M. Adams and S. E. Tavares, *A Note on the Generation and Counting of Bent Sequences*, tech. rep., Department of Electrical Engineering, Queens's University, July 1989 (submitted to IEEE Transactions on Information Theory).

[2] ——, *The Structured Design of Cryptographically Good S-Boxes*, tech. rep., Department of Electrical Engineering, Queens's University, Mar. 1989 (submitted to the Journal of Cryptology).

[3] D. K. Branstad, J. Gait, and S. Katzke, *Report of the workshop on cryptography in support of computer security*, Tech. Rep. NBSIR 77-1291, National Bureau of Standards, Sept. 1976.

[4] E. F. Brickell, J. H. Moore, and M. R. Purtill, *Structure in the S-boxes of the DES (extended abstract)*, in Advances in Cryptology: Proc. of CRYPTO '86, Springer-Verlag, Berlin, 1987, pp. 3–8.

[5] H. Feistel, W. Notz, and J. L. Smith, *Some Cryptographic Techniques for Machine-to-Machine Data Communications*, Proceedings of the IEEE, 63 (1975), pp. 1545–1554.

[6] R. Forre, *The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition*, in Advances in Cryptology: Proc. of CRYPTO '88, Springer-Verlag, Berlin, 1989.

[7] W. Meier and O. Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, in Advances in Cryptology: Proc. of EUROCRYPT '89, to appear.

[8] J. Pieprzyk and G. Finkelstein, *Towards effective nonlinear cryptosystem design*, IEE Proceedings, Part E: Computers and Digital Techniques, 135 (1988), pp. 325–335.

[9] O. S. Rothaus, *On 'Bent' Functions*, Journal of Combinatorial Theory, 20(A) (1976), pp. 300–305.

[10] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Heidelberg and New York, 1986.

[11] A. F. Webster and S. E. Tavares, *On the Design of S-Boxes*, in Advances in Cryptology: Proc. of CRYPTO '85, Springer-Verlag, Berlin, 1986, pp. 523–534.