Proceedings of the International Multiconference on
Computer Science and Information Technology, pp. 453 – 457

ISSN 1896-7094

Parity-based Detection of Multiple Errors in S-boxes

Ewa Idzikowska, Krzysztof Bucholc

Poznań University of Technology, pl. M. Skłodowskiej-Curie 5
60-965 Poznań
Ewa.Idzikowska@put.poznan.pl, Krzysztof.Bucholc@put.poznan.pl

Abstract. In this paper we present low-cost, concurrent checking methods for multiple error detection in S-boxes of symmetric block ciphers. These are redundancy-based fault detection schemes. We describe some studies of parity based concurrent error detection in S-boxes. Probability of multiple error detection is analyzed for random data. In this work 48-input, 32-output substitution blocks are taken into consideration.

1 Introduction

Deliberate injection of faults into cryptographic devices is an effective cryptanalysis technique against symmetric and asymmetric encryption algorithms. In September 1996 Boneh, DeMillo and Lipton from Bellcore announced a new type of cryptanalytic attack which exploits computational errors to find cryptographic keys. This attack was based on the observation that errors induced in the hardware devices leak information about the implemented cryptoalgorithm [2, 4].

In October 1996 Biham and Shamir presented the first fault-based side channel cryptanalysis of Data Encryption Standard (DES) called Differential Fault Analysis (DFA) [1]. This attack used DES as the unknown cipher and required only about 500 faulty cipher texts to identify the bits of the right half, up to 5000 faulty cipher texts to identify the S-boxes and their input and output bits, and about 10000 faulty cipher texts to reconstruct the DES S-boxes [2].

These injected faults affect the memory as well as the combinational parts of a circuit. Concurrent checking, especially for cryptographic chips, is growing in importance. Since cryptographic chips are consumer products produced in large quantities, cheap solutions for concurrent checking are needed. Such faults can be detected using low-cost Concurrent Error Detection (CED) methods [3]. In this paper parity-based methods of concurrent checking for S-boxes are analyzed.

2 Errors in substitution blocks

A substitution box (S-box) is a basic component of block ciphers and is used to obscure the relationship between the plaintext and the ciphertext as in a mapping function f, which maps m -bit input strings X to n -bit output strings Y, where $Y=f(X)$ and $f:\{0,1\}^m \rightarrow \{0,1\}^n$.

An S-box is an important element of cryptographic algorithm and it should posses some properties, which make linear and differential cryptanalysis as difficult as possible. Concurrent error detection in S-boxes of cryptographic hardware is very important.

In this paper $m \times n$ S-boxes are considered, where $m > n$.

Let $D^1_{m-1} \ldots D^1_1 D^1_0$, be an input, error-free vector of bits, and $D^3_{n-1} \ldots D^3_1 D^3_0$ be an output vector. Let

E_{m-1} ... E_1 E_0 be an error vector, where $E_i \in \{0,1\}$; $E_i = 1$ indicates that bit i is faulty. The number of ones in this vector is equal the number of inserted faults. As a result, vector D^2_{m-1} ... D^2_1 D^2_0 is the erroneous vector, where $D^2_i = D^1_i \oplus E_i$ (Fig. 1) and the error is observable only on the S-box output.

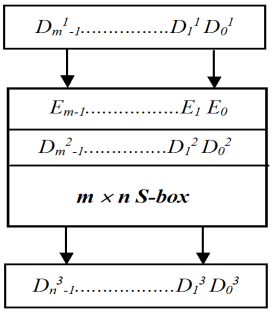

Fig. 1. The model of erroneous $m \times n$ S-box.

In this paper we will focus on the parity preserving properties of S-boxes. 48×32 S-box of DES algorithm will be examined in detail.

3 Concurrent checking of S-boxes

S-box designed for DES algorithm consists of 8 sub-S-boxes, *S1* to *S8*. Each of these boxes has 6 inputs and 4 outputs (Fig. 2).

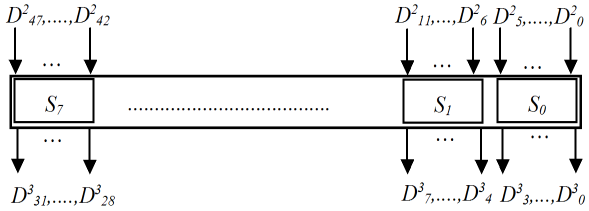

Fig. 2. The model of 48×32 S-box

In this chapter we want to show, how the number of parity bits influences the error detection. We adapt a general approach to develop a low-cost method for concurrent checking and we add one or more additional binary outputs to the S-box for error detection. These additional S-box outputs compute the parity of the corresponding output bits.

To calculate the probability of error detection, the sequence of random input vectors will be considered.

3.1 Parity checking

For error detection in S-box first we add an additional binary output bit P(Out), which implements exclusive-or of all 32 output bits.

$$P(Out) = D^3_0 \oplus D^3_1 \oplus, \ldots, \oplus D^3_{30} \oplus D^3_{31}$$

The modified S-box has a 48-bit input and a 33-bit output. In Fig. 3 this additional parity output is shown as a thick, grey box appended to the right hand side of an S-box.

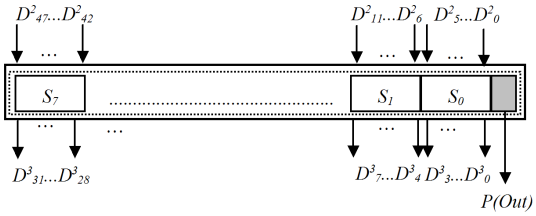

Fig. 3. The model of *48 × 32* S-box with 1parity bit

Then we add parity bits for groups of sub-boxes: one bit for each 4 sub-boxes group, one bit for each 2 sub-boxes group and one bit for each sub-box. For all of these proposed S-box modifications the probability of an error detection is proved.
If we add two parity bits then:

$$P(S_i\text{-}S_{i+3}) = P(S_i) \oplus , \ldots , \oplus P(S_{i+3}) = D^3_{i*4} \oplus D^3_{(i*4)+1} \oplus , \ldots , \oplus D^3_{(i+3)*4+3}$$
$$for\ i = 0, 4.$$

If there are 4 parity bits considered – one for two sub-boxes (Fig. 4) then:

$$P(S_i\text{-}S_{i+1}) = P(S_i) \oplus P(S_{i+1}) = D^3_{i*4} \oplus D^3_{(i*4)+1} \oplus , \ldots , \oplus D^3_{(i+1)*4+3} \qquad for\ i = 0, 2, 4\ 6.$$

One parity bit for each sub-box is also considered.

$$P(S_i) = D^3_{i*4} \oplus,\ldots,\oplus D^3_{i*4+3},\ for\ i = 0, 1, \ldots 7$$

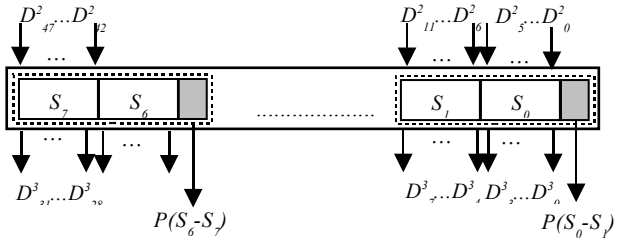

Fig. 4. The model of *48 × 32* S-box with 4 parity bits

Capability of multiple fault detection using 1, 2, 4 and 8 additional, parity bits is shown in the next chapter.

3.2 Fault detection capability

In our work VHDL was used for modeling the S-boxes, and simulation was realized using Active-HDL verification environment. Simulation of S-boxes was executed for random generated input vectors. We take into consideration random number of faulty input bits. These bits are indicated by error vector *E*.

Probabilities of error detection using one input vector, and one, two, four and eight parity bits are compared in Table 1.

Table 1. Probability of error detection using 1 input vector, for 48×32 S-box

	P(Out)	$P(S_i\text{-}S_{i+3})$	$P(S_i\text{-}S_{i+1})$	$P(S_i)$
Number of parity bits	1	2	4	8
Detection probability	46%	57%	64%	78%

The probability of error detection for more then one input vector is calculated using data from Table 1 and is shown in Table 2. The process of encryption and decryption of DES algorithm consists of 16 rounds. It means that all possible faults are detectable by 8 bit parity checking with high probability.
In our work it is also interesting, how the probability of error detection depends on the number of injected faults. This dependence is shown at Fig. 5.

Table 2. Probability of error detection in *k* -sequences

k	*P(Out)*	$P(S_i - S_{i+3})$	$P(S_i - S_{i+1})$	$P(S_i)$
1	0,463	0,571	0,636	0,78200000000
2	0,711631	0,815959	0,867504	0,95247600000
3	0,845145847	0,921046411	0,951771456	0,98963976800
4	0,91684332	0,96612891	0,98244481	0,99774146942
5	0,955344863	0,985469303	0,993609911	0,99950764033
6	0,976020191	0,993766331	0,997674008	0,99989266559
7	0,987122843	0,997325756	0,999153339	0,99997660110
8	0,993084967	0,998852749	0,999691815	0,99999489904
9	0,996286627	0,999507829	0,999887821	0,99999888799
10	0,998005919	0,999788859	0,999959167	0,99999975758
11	0,998929178	0,99990942	0,999985137	0,99999994715
12	0,999424969	0,999961141	0,99999459	0,99999998848
13	0,999691208	0,99998333	0,999998031	0,99999999749
14	0,999834179	0,999992848	0,999999283	0,99999999945
15	0,999910954	0,999996932	0,999999739	0,99999999988
16	0,999952182	0,999998684	0,999999905	0,99999999997

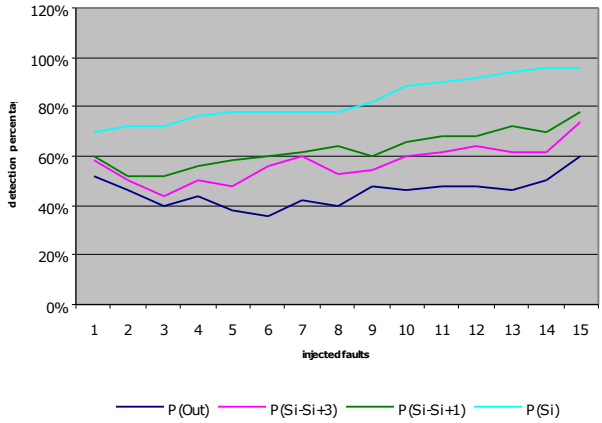

Fig. 5. Percentage of detected faults

One of the conclusions of our work is that error detection using parity code based approach can be successfully used in concurrent checking of substitution blocks. In this way it is possible to detect not only single errors and any odd number of errors but also even number of errors.

A percentage of undetected, multiple faults during concurrent error detection based on parity codes is very low and is shown in the Fig. 6.

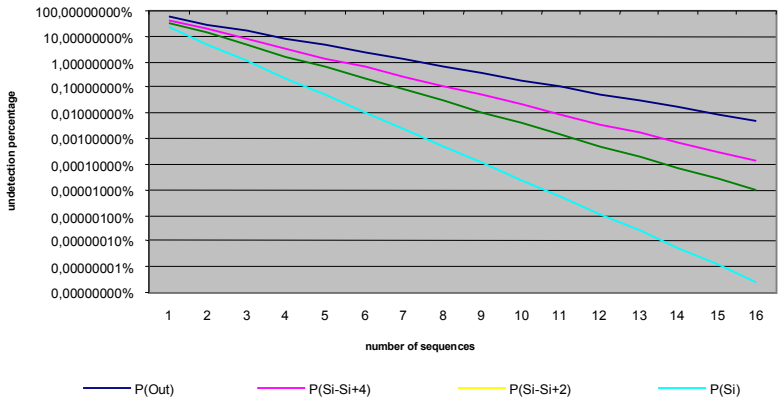

Fig. 6. Percentage of undetected faults in 48×32 S-box

4 Concluding remarks

The techniques used for error detection in digital circuits are based on adding redundancy to the circuit [4]. It can be relatively small redundancy, a few percent of the circuit area, but it may also lead to doubling of the hardware. Parity code based solutions require relatively small increase of the hardware complexity but are using first of all for detection single errors and odd number of errors.

In this paper we shown that the parity code based approach can be used also for even number error detection in S-boxes. The probability of error detection depends on the number of used parity bits and on the length of the input vectors sequence. Multiple errors in $m \times n$ S-boxes can be detected with high probability. For example, using 16 input vectors in DES S-box, the probability is equal 99.995% in the case of using only 1 parity bit, and 99.999999997% for 8 parity bits.

Acknowledgment

This research was supported by the Polish Ministry of Education and Science as a 2005−2008 research project.

References

1. Biham E., Shamir A.: *Differential Fault Analysis of Secret Key Cryptosystems,* Proceedings of Crypto'97 (1997).
2. Boneh D., DeMillo R.: Lipton R., *On the importance of checking cryptographic protocols for faults,* Proceedings of Eurocrypt, Lecture Notes in Computer Science, Vol. **1233**, Springer-Verlag, (1997) 37-51.
3. Karri R., Kuznetsov G., Goessel M.: *Parity Based Concurrent Error Detection in Symmetric Block Cyphers,* Proc. of International Test Conference (2003) 919-926.
4. Karri R., Wu K., Mishra P., Kim Y.: *Concurrent Error Detection Schemes for Fault-Based Side-Channel Cryptanalysis of Symmetric Block Ciphers.* IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems, Vol. **21**, No. 12, December (2002) 1509-1517.