International Journal of Computer Science & Applications
Vol. 4, No. 1, pp. 27 – 32

Concurrent Error Detection in S-boxes[1]

Ewa Idzikowska, Krzysztof Bucholc

Poznan University of Technology,
pl. M. Sklodowskiej-Curie 5
60-965 Poznan
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 Sboxes 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 cause information leakages 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.

[1] This research was supported by the Polish Ministry of Education and Science as a2005-2008 research project

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× 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 $E_{m-1},\ldots,E_1,E_0$ 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 $D^2_{m-1},\ldots,D^2_1,D^2_0$ 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.

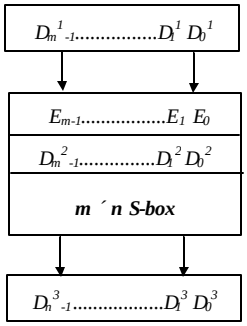

Fig. 1. The model of erroneous *m* × *n* S-box.

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

3 Concurrent checking of S-boxes

DES algorithm consists of 8 S-boxes, S_0 to S_7. Each of these boxes has 6 inputs and 4 outputs (Fig. 2). The six input bits give an address in S-box table (2 bits a number of row, 4 bits a number of column). This address indicates a 4 bit number – the S-box output. In this way eight groups of 6 bits (48 bits) are transformed into eight groups of 4 bits (32 bits). The table to determine a function of box *S1* is shown in the Table 1.

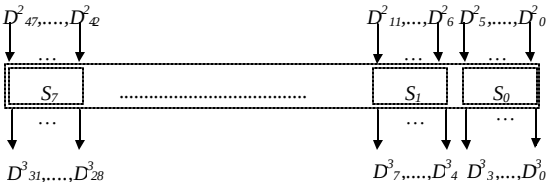

Fig. 2. The model of S-boxes in DES.

In this chapter we want to show, how the number of parity bits influences the error detection.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Table 1. The table defining the function S_0 of DES algorithm

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-boxes first we add an additional binary output bit P(Out), which implements exclusive-or of all S-boxes output bits.

$P(Out) = D^3_0 \oplus D^3_1 \oplus, ¼, \oplus D^3_{30} \oplus D^3_{31}$

The eight S-boxes have now 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.

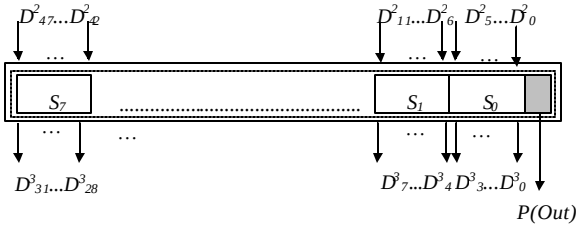

Fig. 3. The model of S-boxes with 1parity bit.

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

If we add two parity bits then:
$P(S_i\text{-}S_{i+3}) = P(S_i) \oplus ,¼, \oplus P(S_{i+3}) = D^3_{i*4} \oplus D^3_{i*4+1} \oplus ,...,\oplus D^3_{i*4+3} \oplus D^3_{(i+1)*4} \oplus ,¼, \oplus \oplus D^3_{(i+3)*4+3}$, *for i = 0, 4.*
If there are 4 parity bits considered (one for two S-boxes – see Fig. 4) then:

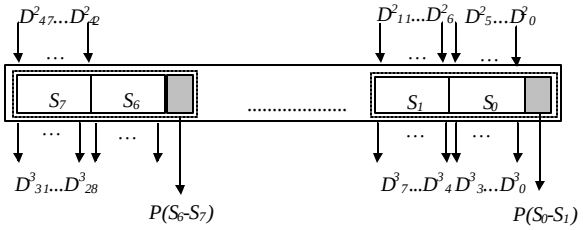

Fig. 4. The model of S-boxes with 4 parity bits.

$P(S_i\text{-}S_{i+1}) = P(S_i) \oplus P(S_{i+1}) = D^3_{i*4} \oplus D^3_{i*4+1} \oplus ,¼, \oplus D^3_{i*4+3} \oplus D^3_{(i+1)*4} \oplus ,¼, \oplus D^3_{(i+1)*4+3}$
for i = 0, 2, 4, 6.
One parity bit for each S-box is also considered.
$P(S_i) = D^3_{i*4} \oplus ,¼, \oplus D^3_{i*4+3}$, *for i = 0, 1, ¼ 7*

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 Sboxes was executed for random generated input vectors. We take into consideration single and multiple faults. The faulty bits are generated randomly and are indicated by error vector *E.*

	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%

Table 2. Probability of error detection using 1 input vector, for S-boxes of DES

Probabilities of error detection using one input vector, and one, two, four and eight parity bits are compared in Table 2.

The probability of error detection for more then one input vector is calculated using data from Table 2 and is shown in Table 3. The process of encryption and decryption of DES algorithm consists of 16 rounds. It means that single and multiple faults are detectable by 8 bit parity checking with high probability.

k	P(Out)	$P(S_i\text{-}S_{i+3})$	$P(S_i\text{-}S_{i+1})$	$P(S_i)$
1	0,463	0,571	0,636	0,78200000
2	0,711631	0,815959	0,867504	0,95247600
3	0,84514584	0,92104641	0,95177145	0,98963976
4	0,91684332	0,96612891	0,98244481	0,99774146
5	0,95534486	0,98546930	0,99360991	0,99950764
6	0,97602019	0,99376633	0,99767400	0,99989266
7	0,98712284	0,99732575	0,99915333	0,99997660
8	0,99308496	0,99885274	0,99969181	0,99999489
9	0,99628662	0,99950782	0,99988782	0,99999888
10	0,99800591	0,99978885	0,99995916	0,99999975
11	0,99892917	0,99990942	0,99998513	0,99999994
12	0,99942496	0,99996114	0,99999459	0,99999998
13	0,99969120	0,99998333	0,99999803	0,99999999
14	0,99983417	0,99999284	0,99999928	0,99999999
15	0,99991095	0,99999693	0,99999973	0,99999999
16	0,99995218	0,99999868	0,99999990	0,99999999

Table 3. Probability of error detection in *k*-sequences

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.

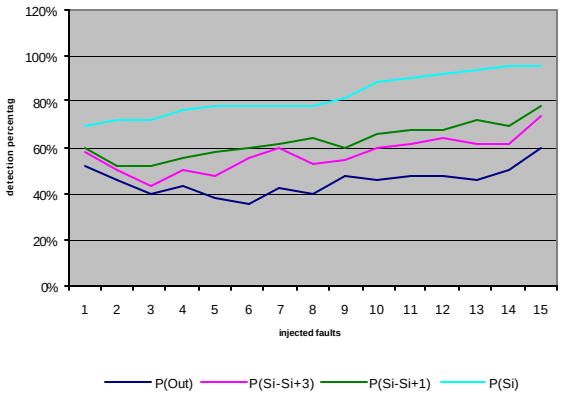

Fig. 5. Percentage of detected faults

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.

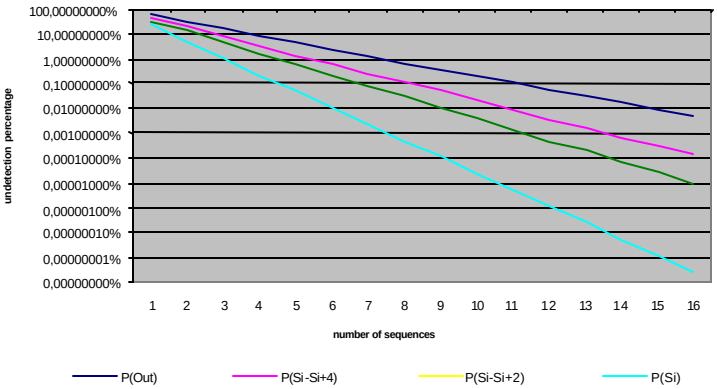

Fig. 6. Percentage of undetected faults in 48×32 S-box

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 in the hardware complexity but usually serve only for single error and any odd number of errors detection. 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×n S-boxes can be detected with high probability. solutions for concurrent checking cryptographic chips can be very useful. For example, the sequence of 16 input vectors detects error with probability 99.999999997% when 8 parity bits are used and with probability 99.995% in the case of using only 1 parity bit. Such cheap solutions for concurrent checking cryptographic chips can support security of embedded systems.

5 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