Ewa IDZIKOWSKA
POZNAŃ UNIVERSITY OF TECHNOLOGY,
pl. M. Skłodowskiej-Curie 5, 60-965 Poznań

CED for S-boxes of symmetric block ciphers

Ph.D. eng. Ewa IDZIKOWSKA

She received the M.Sc. degree in computer science from Wroclaw University of Technology and the Ph.D. degree in computer science from AGH University of Science and Technology, Cracow. She is currently a researcher at Poznan University of Technology. Her research interests include reliability and diagnosis of logical circuits, test generation, fault diagnosis, and concurrent error detection, especially in hardware implementations of cryptosystems.

e-mail: ewa.idzikowska@put.poznan.pl

Abstract

Concurrent Error Detection (CED) techniques based on hardware or time redundancy are widely used to enhance system dependability and to detect fault injection attacks, where faults are injected into chip to break the cryptographic key. In this paper we proposed hardware redundancy CED technique to detection errors in S-boxes of the PP-1 block cipher. Simulation results for single and multiple as well transient and permanent faults are presented and compared against another parity based method and to one of time redundancy method.

Keywords: Concurrent Error Detection, S-box, fault detection, parity based CED, involutional function.

Współbieżne wykrywanie błędów w S-blokach symetrycznych szyfratorów blokowych

Streszczenie

Techniki współbieżnego wykrywania błędów (CED) są szczególnie szeroko stosowane w celu wykrywania błędów w układach kryptograficznych. Związane jest to nie z większym prawdopodobieństwem wystąpienia uszkodzeń lecz z atakami na układy kryptograficzne, polegającymi na celowym wprowadzaniu błędów (*side channel attacks*). Już w 1997 roku [1, 3, 4] pokazano, ze wprowadzone błędy ułatwiają złamanie kryptosystemów zarówno symetrycznych jak i asymetrycznych. Współbieżne wykrywanie błędów związane jest z wprowadzeniem do układu redundancji sprzętowej lub czasowej ewentualnie jednej i drugiej. W prezentowanym artykule przedstawiono metodę współbieżnego wykrywania błędów w S-blokach symetrycznych szyfratorów blokowych. W metodzie tej wykorzystana została redundancja sprzętowa. S-bloki to istotne elementy szyfratorów, których zadaniem jest ukrycie zależności między tekstem jawnym a kryptogramem i utrudnienie kryptoanalizy liniowej i różnicowej. Do badań wykorzystany został S-blok zaprojektowany dla szyfratora PP-1. Badania symulacyjne pokazały skuteczność wprowadzonych zabezpieczeń. Badano prawdopodobieństwo wykrycia błędów pojedynczych i wielokrotnych a także błędów trwałych i przemijających. Uzyskane wyniki zostały porównane z wynikami uzyskanymi innymi metodami współbieżnego wykrywania błędów, przedstawionymi w [8] i [9].

Słowa kluczowe: współbieżne wykrywanie błędów, S-blok, wykrywanie błędów, współbieżne wykrywanie błędów, bity parzystości, inwolucja.

1. Introduction

Fault detection schemes for various implementations of cryptographic algorithm have recently been especially important. Several motivations led to increase the reliability of these circuits. From one side the circuit implementation of cryptographic algorithms can be quite complex and the probability of device failures is growing, but cryptographic chips are a consumer product produced in large quantities, therefore cheap solutions for concurrent fault detection are needed. From the other side, intentional intrusions and attacks based on the malicious injection of faults into the device are very efficient in order to extract the secret key [1, 3, 4]. Such attacks are based on the observation that faults deliberately introduced into a cryptodevice leak information about the implemented algorithms. First fault injection attack is presented in [5].

There are different types of faults and methods of fault injection in encryption algorithms. The faults can be transient or permanent. Several transient and permanent faults and methods of fault injection such as varying supply voltage, external clocks, temperature or inducing faults using white light, laser and X-rays methods of fault injection are discussed in detail in [2]. Even a single fault like change a flip-flop state or corruption of data values transferred from one digest operation to another can result in multiple errors in the end of a digest round.

Concurrent Error Detection (CED) techniques are widely used to enhance system dependability. All CED techniques introduce some form of redundancy. It may be noted that the general architecture of a CED relies on the use of hardware redundancy for error detection, but time redundancy techniques can also be used for concurrent error detection. The hardware cost of time redundancy techniques is generally smaller than that of hardware redundancy.

In this paper we focus on CED techniques targeting involutional functions. We will analyze the detection of errors in S-boxes of PP-1 block cipher implementation [6]. PP-1 is considered for use in essential security services and concurrent error detection (CED) is very important. The design goal is to achieve 100% error detection with minimal penalty.

In the paper a new parity based CED approach to protect the S-box core is presented. Conversely to the other computational blocks of the PP-1 algorithm, the S-box performs an operation that is not linear and is not invariant with respect to the parity of the processed data, i.e., the parity bit is not preserved after the transformation. We provide simulation results related to the fault coverage of the proposed approach and we compare these results with the results for architectures proposed in [8] and [9].

This paper is organized as follows. Sec. 2 and 3 present the PP-1 symmetric block cipher and S-box, respectively. Possible faults and faults models in S-boxes of PP-1 are described in Sec. 4. In Sec. 5 and 6 we present CED schemes for function S. Simulation results are presented in Sec. 7. Sec. 8 concludes the paper.

2. The PP-1 cipher

The scalable PP-1 cipher is a symmetric block cipher that in r rounds processes data blocks of n bits, using cipher keys with lengths of n or $2n$ bits. It is described in detail in [6]. The PP-1 was designed for platforms with very limited resources. Therefore it can be implemented for example in simple smart cards. The PP-1 algorithm is an SP-network. One round of the algorithm is presented in Fig. 1. It consists of $t = n/64$ parallel processing paths. A 64-bit nonlinear operation NL (Fig. 2) is performed in each path.

The 64-bit block is processed as eight 8-bit subblocks by four types of transformations: 8×8 S-boxes S, XOR (⊕), addition (∃), subtraction (&). These are modulo 256 transformations of integers represented by respective bytes. Additionally an n-bit permutation P is used. In the output transformation the permutation P is not performed.

Two round keys are in use in each round. The same algorithm is used for encryption and decryption because two components, substitution S and permutation P are involutions, i.e. $S^{-1}=S$, and $P^{-1}=P$. However, if round keys k_1, k_2,...,k_{2r} are used in the encryption process then they must be used in the reverse order, i.e. k_{2r}, k_{21},...,k_1 in the decryption process.

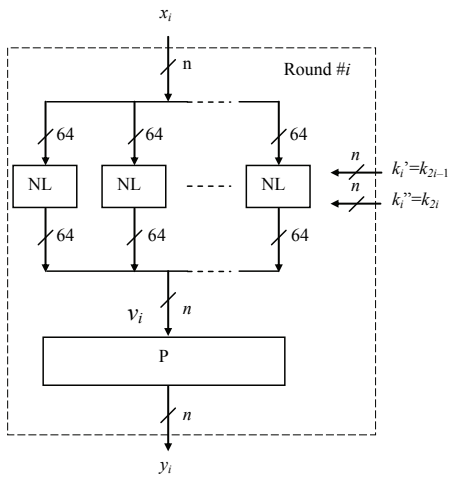

Fig. 1. One round of PP-1 (i = 1, 2, ..., r-1) [6]
Rys. 1. Jedna runda pracy szyfratora PP-1 (i = 1, 2, ..., r-1) [6]

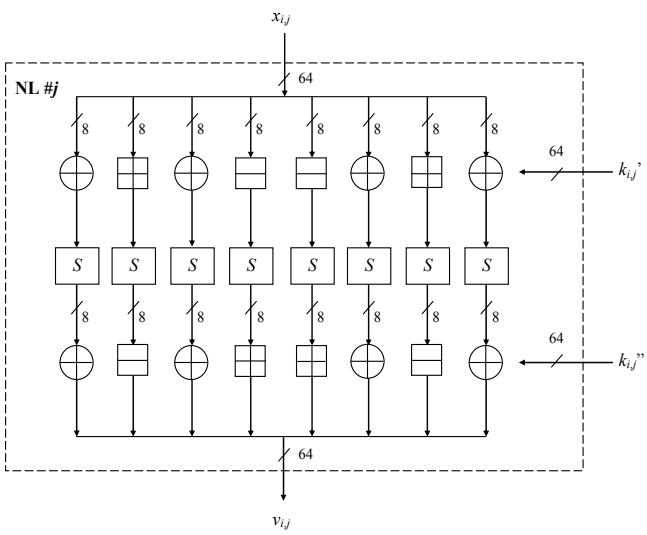

Fig. 2. Nonlinear element NL (j = 1, 2, ..., t) [6]
Rys. 2. Nieliniowy element NL (j = 1, 2, ..., t) [6]

3. Substitution function S

S-box is a substitution function taking 8 inputs and producing 8 outputs. It is a basic component of block ciphers and is used to obscure the relationship between the plaintext and the ciphertext. It 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.

The S-box in PP-1 is selected in such a way that it is its own inverse, i.e. $S^{-1} = S$. This S-box has been generated using multiplicative inverse procedure with randomly chosen primitive polynomial defining Galois Field. Nonlinearity of this S-box is 110 and its nonlinear degree is 7. Eight Boolean functions that constitute this S-box have the nonlinearities equal to 110 or 112 and all are of degree 7 [6].

4. Faults models

Fault attack tries to modify the functioning of the computing device in order to retrieve the secret key. The attacker induces a fault during cryptographic computations. The feasibility of a fault attack or at least its efficiency depends on the exact capabilities of the attacker and the type of faults he can induce.

In our considerations we use a realistic fault model wherein either transient or permanent faults are induced randomly into the device. We consider single and multiple faults. In this paper we will analyse the possibilities of errors detection in S-boxes of the PP-1 block cipher implementation.

Faults are modelled as an 8-bit error vector $E=\{e_7,...,e_i,...,e_1,e_0\}$, where $e_i \in \{0,1\}$ and $e_i = 1$ indicates that bit i is faulty. The number of ones in this vector is equal the number of inserted faults. Fault simulations were performed for two kind of fault models. In one model the fault flips the bit, and the other model introduces bit stuck-at faults (both stuck-at-1 and stuck-at-0).

Let $X=\{x_7,...,x_1,x_0\}$ be an S-box input, error-free vector of bits, and $Y=\{y_7,...,y_1,y_0\}$ be an S-box output vector [7]. Vector $Xe=\{xe_7,...,xe_1,xe_0\}$ is an erroneous input vector:

- if the fault flips the bit — $xe_i = x_i \oplus e_i$,
- for stuck-at-1 fault — $xe_i = x_i + e_i$,
- for stuck-at-0 fault — $xe_i = x_i \times (\text{not } e_i)$,

where: $\oplus$ - xor, + - or, $\times$ - and.

The error is observable on the S-box output [7].

5. Parity–Based CED

Most of CED techniques function according to the principle, that system under consideration realizes a function F, and produces output $F(i)$ in response to an input sequence i. They assume that there is a unit, which independently predicts some special characteristic of the systems output $F(i)$ for every input sequence i. There is also a checker unit, which checks if the special characteristic of the output actually produced by the system in response to input sequence i is the same as the predicted one. The checker produces an error signal when difference is detected. One of the characteristics of $F(i)$ is its parity.

Concurrent checking for S-boxes of PP-1 by parity prediction was presented in [8]. In this paper [8] different schemes of parity-based CED techniques are proposed and compared on their area overhead and their possibility of the detection of single and multiple failures. One of these schemes is shown in Fig. 3. In this approach one parity bit for each outgoing data is generated and this bit is compared against S-box output parity.

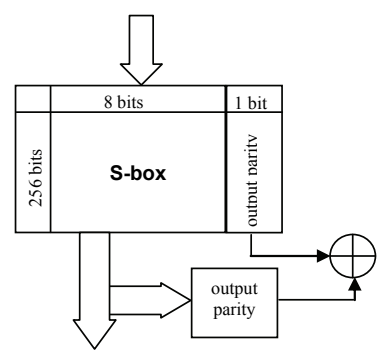

Fig. 3. Parity based CED with 1 parity bit [8]
Rys. 3. Współbieżne wykrywanie błędów w oparciu o 1 bit parzystości [8]

Now we present a new, hardware redundancy, parity based concurrent error detection approach. The S-box is usually implemented as a 256x8 bits memory, consisting of a data storage section and an address decoding circuit. To increase the dependability and detect input, output and internal memory errors of the S-box we propose replacing the 256x8 bits memory that stores the S-box values with 256 x10 bits memory. One of these two additional bits is parity bit generated for incoming data bytes, the other one is parity bit generated for outgoing data (Fig. 4).

Thus solution demands only 512 additional bits memory (redundancy is equal to 25%) and simple combinational circuit, and guarantees quite good fault coverage. Capability of single and multiple, transient and permanent fault detection using this scheme of parity prediction is presented in the Sec. 7.

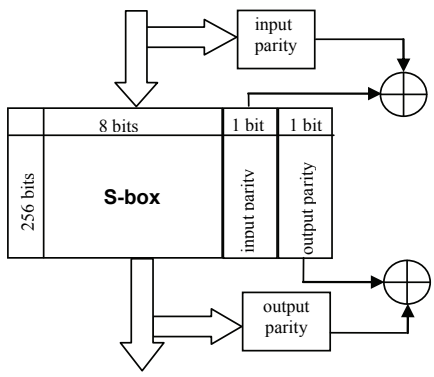

Fig. 4. Parity based CED with 2 parity bits
Rys. 4. Współbieżne wykrywanie błędów w oparciu o 2 bity parzystości

6. Time redundancy CED

In the majority of time redundancy CED methods the same hardware is used to perform both the normal computation and recomputation of the same input data. The advantage of this technique is that it uses minimum hardware, the drawbacks are that it entails ≥100% time overhead and it can only detect transient faults. The CED technique proposed in [9] exploits involution property of S-box to detect not only permanent but also transient faults. Function S is an involution, it means that $S(S(x))=x$. A scheme for time redundancy fault detection in involutional S-box is shown in Fig. 5. Simulation results on the vulnerability of this CED technique to single and multiple, permanent and temporary failures are presented in the next section and compared against results of parity bits CED methods.

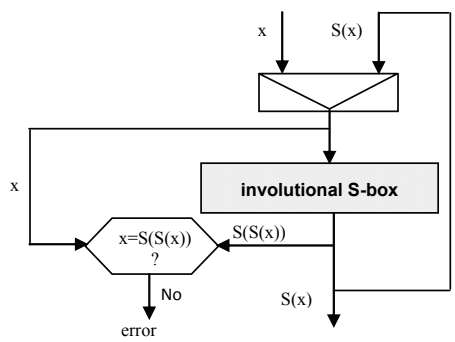

Fig. 5. CED for involution S [9]
Rys. 5. Współbieżne wykrywanie błędów w involucji S [9]

7. Simulation results

In this section, we provide simulation results related to the fault coverage of the proposed approach and we compare these results against the results for architecture proposed in [8] and [9]. We present simulation results on the vulnerability of these techniques for fault models from Section 3. The faults were injected into inputs, outputs and internal memory of the S-box.
We consider random faults, in the sense that the faulty value is assumed to be random and uniformly distributed.

In order to measure the detection capability of the proposed architecture (Fig. 4) we used VHDL hardware description language and the VHDL simulator provided by Aldec, Active-HDL. The VHDL model of the S-box has been modified with the faults. In our considerations we use a realistic fault model wherein faults are induced randomly into the device. The output signals have been compared to correct signals. In this way, the obtained fault coverage gives a measure of the detection capability when errors affect the circuit. In this experiment we focused on transient and permanent, single and multiple stuck-at faults and bit flips faults. The obtained faults coverage is shown in Fig. 6. Fig. 7, 8, 9 and 10 summarize some comparison between proposed 2 parity bit solution and the architectures proposed in [8] and [9]. Dependence of error detection probability on the number of injected faults for analyzed CED is shown in Fig. 8 and 9. Probabilities of stuck-at-0/1 and bit flip errors detection for S-box are shown in Fig. 10. Single, transient stuck-at-0/1 errors are detected by proposed 2 bit parity CED in 50% and in 76% by involutional CED, but permanent errors are detected in 100%. Detection percentage for single bit flip errors is close to 100% for both methods. The same is observable for permanent and transient faults.

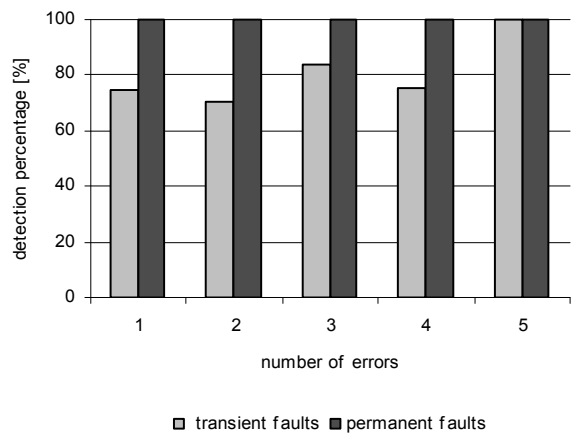

Fig. 6. Probability of error detection using proposed 2 parity bits CED
Rys. 6. Prawdopodobieństwo wykrycia błędów przy użyciu 2 bitów parzystości

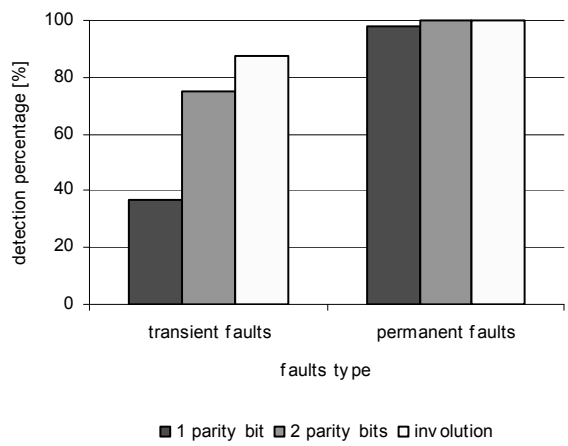

Fig. 7. Probability of single error detection using different CED methods
Rys. 7. Prawdopodobieństwo wykrycia pojedynczych błędów różnymi metodami

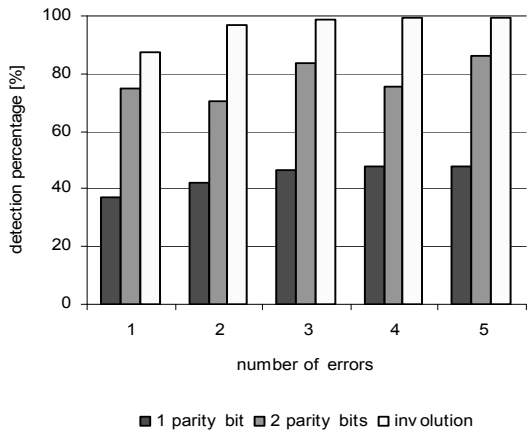

Fig. 8. Probability of transient error detection using different CED methods
Rys. 8. Prawdopodobieństwo wykrycia błędów przejściowych różnymi metodami

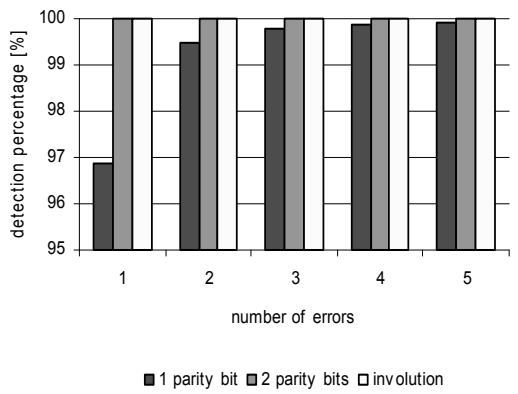

Fig. 9. Probability of permanent error detection using different CED methods
Rys. 9. Prawdopodobieństwo wykrycia błędów trwałych różnymi metodami

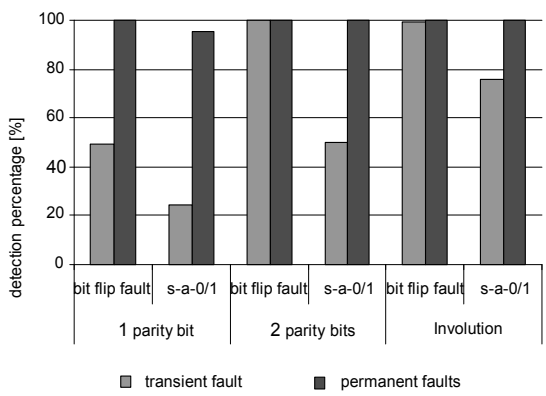

Fig. 10. Probability detection of single bit flip fault and s-a-0/1 using different CED methods
Rys. 10. Prawdopodobieństwo wykrycia błędów pojedynczych typu s-a-0/1 i zmiana wartości na przeciwną, różnymi metodami

In most cases involutional CED solution guarantees the highest fault coverage, but this solution is designed only for block ciphers with involutional functions.

The solution proposed in this paper is better as the 1 parity bit solution proposed in [8] and can be used for all S-boxes. For example single transient faults are detected in 75% using 2 parity bits solution and only 37% faults are detected by 1 parity bit solution (Fig. 7). Single permanent faults are detected respectively in 99.5% and 97.6% (Fig. 9).

8. Concluding remarks

Fault injection attacks on cryptographic chips are based on the observation that faults deliberately introduced into a crypto-device leak information about the implemented algorithms. These injected faults affect the memory as well as the combinational parts of a circuit. To detect them different concurrent error detection techniques are proposed. In this paper new parity based CED method for S-boxes of symmetric block ciphers was proposed. This method can provide high coverage for permanent bit errors, which are the most common in fault attacks. Solution proposed in this paper can be useful for concurrent checking cryptographic chips, especially designed for platforms with very limited resources.

The work was supported by finances of West Pomeranian Provincial Administration.

This research was partially supported by the Polish Ministry of Education and Science as a 2010-2013 research project.

9. References

[1] Akkar M., Giraud C.: An Implementation of DES and AES, Secure against some Attacks. Proc. of CHES'01, pp. 315-325, 2001.
[2] Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C.: The Sorcerer's Apprentice Guide to Fault Attacks. Proc. IEEE, vol. 94, pp. 370-382, Feb. 2006.
[3] Biham E., Shamir A.: Differential fault analysis of secret key cryptosystems. Proc of Crypto, 1997.
[4] Boneh D., DeMillo R., Lipton R.: On the Importance of Eliminating Errors in Cryptographic Computations, Journal of Cryptology, vol. 14, pp. 101-119, 2001.
[5] Boneh D., DeMillo R., Lipton R.: On the importance of checking cryptographic protocols for faults, Proceedings of Eurocrypt, Springer-Verlag LNCS 1233, pp. 37-51, 1997.
[6] Bucholc K., Chmiel K., Grocholewska-Czuryło A., Stokłosa J.: PP-1 block cipher. Polish Journal of Environmental Studies, vol. 16, No. 5B, 2007, 315−320.
[7] Idzikowska E., Bucholc K.: Concurrent Error Detection in S-boxes, International Journal of Computer Science & Applications, Vol. 4, No. 1, 2007, pp. 27 – 32.
[8] Idzikowska E., Bucholc K.: Error detection schemes for CED in block ciphers. Proc. of the 5th IEEE/IFIP Int. Conference on Embedded and Ubiquitous Computing EUC 2008, Shanghai 2008, pp. 22-27.
[9] Idzikowska E.: CED for involutional functions of PP-1 cipher, Proceedings of the 5th International Conference on Future Information Technology, Busan 2010.

otrzymano / received: 10.07.2010
przyjęto do druku / accepted: 01.09.2010 *artykuł recenzowany*