Bayesian System for Differential Cryptanalysis of DES

A. De Paola, L. Gagliano, G. Lo Re

In Proceedings of 2013 International Conference on Applied Computing, Computer Science, and Computer Engineering

Bayesian System for Differential Cryptanalysis of DES

A. De Paola[a]*, L. Gagliano, G. Lo Re[a]

[a]*Università degli Studi di Palermo, Viale delle Scienze, ed. 6, Palermo 90128, Italy*

Abstract

This paper proposes a new formalization for the differential cryptanalysis of DES (Data Encryption Standard) based on Bayesian Networks (BN), an artificial intelligence framework used for reasoning on data affected by uncertainty. Through the proposed approach it is possible to analyze DES from a novel point of view, thus paving the way for the development of a new class of cryptanalysis methods.

Selection and peer review under responsibility of Information Engineering Research Institute

Keywords: Cryptography; DES; differential cryptanalysis; Bayesian Networks;

1. Introduction

The DES (Data Encryption Standard) is a symmetric cryptosystem standardized in the 70's for encrypting sensitive data. The research about DES led to the modern design of block ciphers and the design of several techniques for their cryptanalysis. Because of short size DES's key, the algorithm is today considered not adequate for critical applications. However more recent block ciphers, like the AES [1], have been designed to make infeasible a brute force attack. Nevertheless, since DES is still used for less sensitive data, and also as building block of Triple DES [2], it still very interesting to analyze its vulnerabilities. Several works in the scientific literature have identified and analyzed some of the mains vulnerabilities of the DES. These works

* Corresponding author. Tel.: +39 091 23862064; fax: +39 091 23860840.
E-mail address: alessandra.depaola@unipa.it.

led to the development of new cryptanalysis techniques; among these, the most promising ones are linear cryptanalysis [3] and differential cryptanalysis [4]. Although these methods are extremely interesting from a theoretical point of view, because they contributed to identify serious vulnerabilities of DES, they are not usable in a real attack because of the huge amount of required encryption operations, even if it is less than a brute-force attack.

This work proposes a feasibility study for the implementation of the differential cryptanalysis [4]. With respect to the classical approach used for the formalization of such technique, we propose the adoption of Bayesian Networks (BN), an artificial intelligence tool used for dealing with data affected by uncertainty. To the best of our knowledge this approach is a novelty in the scientific literature.

The rest of the paper is structured as follows: Section 2 recalls DES properties and discusses some related works; Section 3 describes the proposed Bayesian Network for modeling the attack to the S-Box, and then extends the proposed approach for attacking the whole DES; finally Section 4 states our conclusions and discusses some future works.

2. DES description and related work

DES is a symmetric cryptosystem that transforms a 64-bit plaintext *P* in a 64-bit ciphertext *T*. A 64-bit key K, actually reduced to a 56-bit key, since 8 bits are used as parity bits, parameterizes the transformation. DES acts on the plaintext *P* through a series of transformations named rounds. The input to each round is transformed through the application of the DES's Feistel function, which consists of a sequence of permutations and substitutions. A 48-bit subkey obtained from K using a scheduling algorithm for subkey generation parameterizes each round. Fig. 1(a) shows the general DES scheme, and Fig. 1(b) shows details of a single round processing.

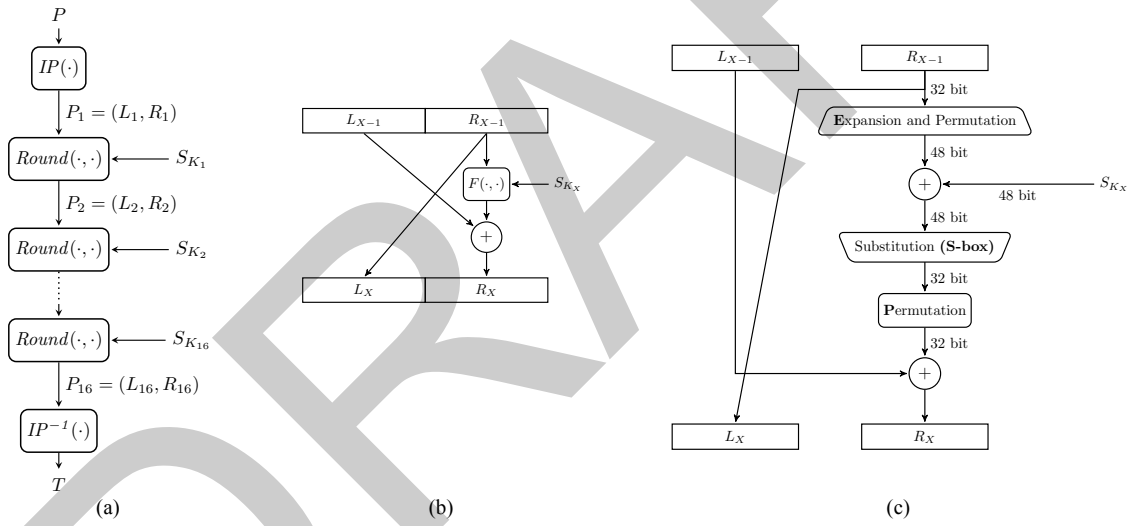


Fig. 1. (a) DES general block scheme. (b) Block scheme of the DES's round processing. (c) Detailed block diagram of the DES's Feistel Function.

For each round *X=2,..., 16*, the following equations are valid:

$$\begin{cases} L_X = & R_{X-1} \\ R_X = & L_{X-1} \oplus F(R_{X-1}, S_{K_X}) \end{cases} \quad (1)$$

namely, P_X is obtained from P_{X-1} by replacing the left 32-bits half L_{X-1} of P_{X-1} with its right 32-bits half R_{X-1} and by replacing its right half with a nonlinear combination of L_{X-1} and R_{X-1}, parameterized by the subkey S_{KX}. The core of a round is the Feistel function that contains the only non-linear component of DES, the S-Box.

In particular, the mapping F, expanded in Fig. 1(c), is defined as follows:

$$F(R_{X-1}, S_{K_X}) = P(S(E(R_{X-1}) \oplus S_{K_X})) \quad (2)$$

where E is called expansion function, S is called S-Box, and P is called permutation. Appropriate tables detailed in [5] define such mappings. Domains and codomains of these functions are defined as follows:

$$\begin{aligned} &E : \mathbf{Z}_2^{32} \rightarrow \mathbf{Z}_2^{48} \\ &S : \mathbf{Z}_2^{48} \rightarrow \mathbf{Z}_2^{32} \\ &P : \mathbf{Z}_2^{32} \rightarrow \mathbf{Z}_2^{32} \end{aligned} \quad (3)$$

It is worth noting that E and P are linear mappings, while S is the only nonlinear component of the algorithm; its goal is erasing the existing relations between the key S_K and the plaintext. S-Box is the major security component of DES and their violation makes the whole encryption system easily violable. Generally, S-Box is not analyzed as a unique block, since it is composed by eight submaps $S_i : \mathbf{Z}_2^6 \rightarrow \mathbf{Z}_2^4$, with $i=1,\ldots,8$.

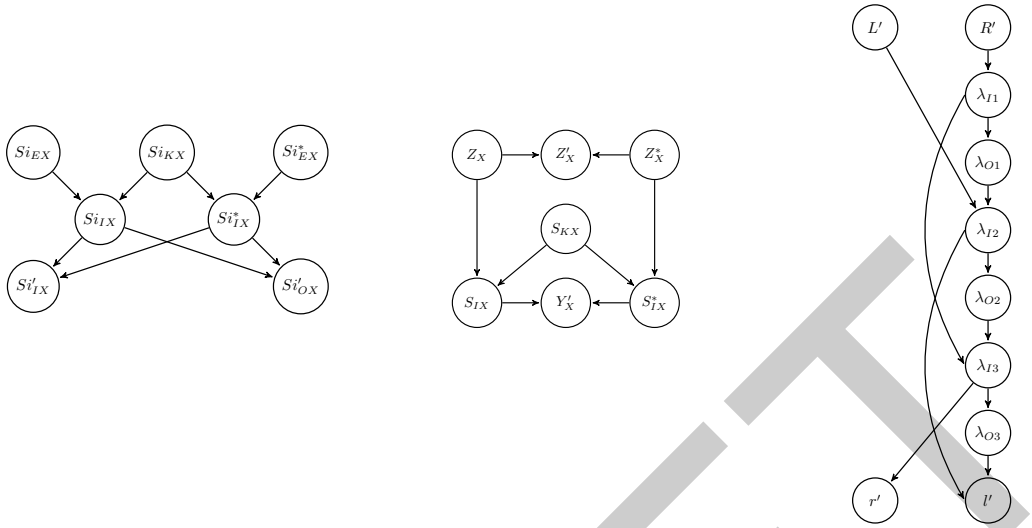
Many works in the literature aim to analyze S-Box. Authors of [6] and [7] propose an analysis of S-Box properties and consequently some possible design criteria in block ciphers context. On the basis of the properties discovered, many cryptanalysis methods were proposed in the literature to violate the S-Boxes. An algebraic approach is proposed in [8], which defines the set of criteria for determining the set of non-linear algebraic constraints, which describes the I/O relationship of the S-Boxes. Exploiting this set of constraints, the whole cipher is described as a system of multivariate non-linear equations. On the contrary, the author of [3] proposes a linear approximation of S-boxes and of the whole DES, which is valid with some probability; such method is an example of stochastic attack on the S-Boxes.

It has been shown that the distribution of the output of the S-Box is uniform if the input is unknown, but experimentally has been shown that the distribution of I/O differences is not uniform [4]. Taken two different inputs for a given S-Box and assuming that these two inputs are bounded by some known difference, then the probability distribution of the difference between the corresponding output of the S-Box is not uniform; such important property represents a strong system vulnerabilities, and underlies the differential cryptanalysis [4]. Authors trace differences through the transformations, discover where the cipher exhibits non-random behavior, and exploit such properties to recover the secret key.

3. Bayesian networks for differential cryptanalysis

The Bayesian Networks (BN) [9] are a formalism based on graph theory, expressing relationships of cause/effect among random variables. In the proposed approach we model the statistical distribution of I/O differences, discovered in [4], though a BN which allows performing a diagnostic inference to discover the key. The proposed BN, showed in Fig. 2(a), uses the original notation reported in [4]: at round X, Si_{EX}, Si_{EX}^* indicate the i-th block of six-bits of the output of the expansion function; Si_{KX} is the i-th six-bits block of the

subkey; Si_{IX}, Si_{IX}^{*} are two inputs to *i*-th S-Box; $Si_{IX}^{'}$ is the XOR between S-Box inputs; while $Si_{OX}^{'}$ is the XOR between S-Box outputs.



(a) (b) (c)

Fig. 2. (a) BN for the attack on the i-th S-Box. (b) BN for the attack on the i-th Feistel function. (c) BN for the attack on a 3-round DES.

Since the differential cryptanalysis is a chosen-plaintext attack, it is possible to assume to know the following evidence:

$$\Theta = \left\{ Si_{EX}, Si_{EX}^{*}, Si_{IX}^{'}, Si_{OX}^{'} \right\}, \tag{3}$$

thus, searching the key is equivalent to maximize the following likelihood:

$$p(Si_{KX} \mid \Theta). \tag{4}$$

Through a diagnostic inference it is possible to evaluate the eq.4. When leading more than one attack, the whole distribution is proportional to the product of the single distributions; thus, given the following set of evidences

$$\Psi = \left\{ \Theta_1, \Theta_2, \ldots, \Theta_M \right\}, \tag{5}$$

the likelihood can be evaluated as follows:

$$p(Si_{KX} \mid \Psi) = \eta \prod_{i=1}^{M} p(Si_{KX} \mid \Theta_i). \tag{6}$$

Eq.6 can be solved through a differential approach. Let us define

$$\Psi_j = \{\Theta_1, \Theta_2, \ldots, \Theta_j\}, \tag{7}$$

then, it follows that

$$p(Si_{KX} \mid \Psi_M) = \eta p(Si_{KX} \mid \Theta_M) p(Si_{KX} \mid \Psi_{M-1}). \tag{8}$$

The probability density functions of the proposed BN, necessary to perform the probabilistic inference, are expressed as follows:

$$\begin{aligned}
&p(Si_{EX}) = p(Si^*_{EX}) = p(Si_{KX}) = 1/2^6, \\
&p(Si_{IX} \mid Si_{EX}, Si_{KX}) = \delta(Si_{EX} \oplus Si_{KX} \oplus Si_{IX}), \\
&p(Si^*_{IX} \mid Si^*_{EX}, Si_{KX}) = \delta(Si^*_{EX} \oplus Si_{KX} \oplus Si^*_{IX}), \\
&p(Si'_{IX} \mid Si_{IX}, Si^*_{IX}) = \delta(Si'_{IX} \oplus Si_{IX} \oplus Si^*_{IX}), \\
&p(Si'_{OX} \mid Si_{IX}, Si^*_{IX}) = \delta(Si'_{OX} \oplus Si(Si_{IX}) \oplus Si(Si^*_{IX})),
\end{aligned} \tag{9}$$

where $\delta(\cdot)$ is the Kronecker delta and *Si(.)* is the *i*-th S-Box.

The proposed approach allows formalizing the attack to the whole Feistel function; nevertheless, since six-bit blocks obtained as output of the expansion function are not independent, it is not possible to generalize the BN show in Fig. 2(a). An alternative BN, built following the same method, is shown in Fig. 2(b), which adopts the following notation:

- Z_X, Z^*_X: inputs to the Feistel function;
- $Z'_X = Z_X \oplus Z^*_X$: difference between inputs;
- S_{KX}: 48-bit subkey;
- S_{IX}, S^*_{IX}: inputs to the S-Box;

Y'_X: permutation of the difference between outputs from the S-Box.

Attacking the Feistel function, in a chosen-plaintext context implies that it is possible to choose two inputs Z_X and Z_X^*, exploiting which it is possible to compute the input XOR Z_X', and to observe the difference between outputs Y_X'. Through the diagnostic inference it is possible to reduce the uncertainty about the 48-bit subkey.

The BN can be used also for a forward inference process, which extracts samples from the implicit distribution of Y_X' conditioned to Z_X'. In particular, it is possible to sample Y_X', starting from a 48-bit random number for S_{IX}, obtained through a random number generator [9], and by applying the following equation:

$$Y'_X = P(S(S_{IX}) \oplus S(S_{IX} \oplus E(Z'_X))). \tag{8}$$

The sampling technique can be used also for inferring the difference propagation inside the DES, while processing two input *P* and *P**. Let *P' = (L',R')* be the XOR between inputs *P* and *P**, explicitly decomposed in its left and right parts, *T' = (l',r')* be the XOR of cipher output, λ_{IX} be the XOR of inputs to the Feistel function at round *X*-th, λ_{OX} be the XOR of outputs from the Feistel function at round *X*-th. The propagation of differences can be modeled through a BN, as shown in Fig2(c) for a DES reduced to three round.

In order to attack a N-round DES, it is necessary to adopt the following algorithm:

- Get the value $\lambda_{I(N-1)}$ by sampling successive differences;
- Get the value $\lambda_{IN}=r'$;
- Get the value $\lambda_{ON} = l' \oplus \lambda_{I(N-1)}$;
- Build a subkey histogram by attacking the S-Boxes at last round using the BN in Fig. 2(a);
- Once the last round is broken, proceed with the previous one.

4. Conclusions and future work

This work demonstrated that the differential cryptanalysis of DES can be implemented through an alternative and novel approach based on Bayesian Networks. The proposed approach models a BN for attacking a single S-Box, and it can be extended for attacking the Feistel function, and finally the whole DES. When analyzing the number of pairs <plaintext, ciphertext> required and the computational complexity, the proposed approach is equivalent to the original formulation. Nevertheless the proposed novel point of view may pave the way for future promising developments. One of the most promising directions seems to be the exploitation of independences among different attack in a parallel implementation of the probabilistic inference. Moreover, it is possible to change the method adopted for the sampling phase, by performing an importance sampling that exploits the structure of the BN. Finally, we plan to evaluate alternative methods for performing efficient inference in Bayesian Networks, such as genetic algorithms [11], even in combination with parallelization [12].

References

[1] Daemen J, Rijmen V. The Design of Rijndael. Springer-Verlag New York, Inc.; 2002.
[2] Coppersmith D, Johnson DB, Matyas, SM. A proposed mode for triple-des encryption. IBM Journal of Research and Development. 1996;40(2):253-262.
[3] Matsui M. Linear Cryptanalysis Method for DES Cipher. In Advances in Cryptology - EUROCRYPT'93; Lecture Notes in Computer Science. 1994; 765: 386-397.
[4] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology. 1991; 4(1):3-72.
[5] National Institute of Standards and Technology. FIPS PUB 46-3: Data Encryption Standard (DES). 1999.
[6] Brickell EF, Moore JH, Purtill, MR. Structure in the S-boxes of the DES. In Proceedings on Advances in cryptology---CRYPTO '86; Springer-Verlag; 1987; 3-8.
[7] Dawson MH, Tavares SE. An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques - EUROCRYPT'91; 1991; Springer-Verlag; 352-367.
[8] Courtois NT, Bard GV. Algebraic Cryptanalysis of the Data Encryption Standard. Cryptography and Coding; Lecture Notes in Computer Science; 2007; 4887:152-169.
[9] Koller D, Friedman N. Probabilistic Graphical Models: Principles and Techniques – Adaptive Computation and Machine Learning. The MIT Press; 2009.
[10] Lo Re G, Milazzo F, Ortolani M. Secure random number generation in wireless sensor networks. 4th International Conference on Security of Information and Networks (SIN 2011); 2011; 175-182.
[11] Mengshoel OJ. Efficient Bayesian Network Inference: Genetic Algorithms, Stochastic Local Search, and Abstraction. 1999. Technical Report. University of Illinois at Urbana-Champaign, Champaign, IL, USA.
[12] Lo Presti G, Lo Re G, Storniolo P, Urso A. A Grid Enabled Parallel Hybrid Genetic Algorithm for SPN. Computational Science - ICCS 2004; Lecture Notes in Computer Science. 2004; 3036:156-163