"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

CONSIDERATIONS ON DIFFERENTIAL CRYPTANALYSIS ATTACKS ON LIGHTWEIGHT BLOCK CIPHERS

Florin MEDELEANU[1]
Marius ROGOBETE[2]
Ciprian RACUCIU[3]
[1]PhD. Cand. Eng. Ministry of National Defense, florinmed@yahoo.com
[2]Eng. Alstom GRID Romania
[3]PhD Prof. Eng. "Titu Maiorescu" University

Abstract: *The most part of symmetric block iterative algorithms are designed to be resistant to cryptanalytic attacks by using nonlinear elements, usually substitution boxes (S-box). Recently, new families of symmetric block iterative algorithms (e.g. lightweight block ciphers) were designed. These new classes are not using substitution boxes, but they have an increased number of rounds. The authors considered useful to compare the resistance of these two subclasses of block ciphers against differential cryptanalysis attack, having in mind that this attack, along with linear cryptanalysis attack, is one of the most important cryptanalytic attack used in evaluation of symmetric block encryption algorithms.*

Keywords: *AES, lightweight block cipher, differential cryptanalysis.*

INTRODUCTION

The Advanced Encryption Standard (AES) is nowadays the most widespread block cipher in commercial applications. It represents the state of art in block cipher design and provides an unparalleled level of assurance against all known cryptanalytic techniques, except for its round-reduced versions. It is true that AES (and other modern block ciphers) presents a highly algebraic structure, leading researchers to exploit it for novel algebraic attacks, but these tries have been unsuccessful as yet (except for academic reduced versions).

The best that one can hope for a cryptosystem is that all its encryption functions behave in unpredictable way (close to random), in particular we would like that it behaves in a way totally different from linear or affine maps. A sign of strength for AES is that nobody has been able to show that its encryption functions are any closer to linear maps than arbitrary random functions.

The term lightweight is used broadly to mean that an algorithm is suitable for use on some constrained platform. But the features that make an algorithm excel on an 8-bit microcontroller, say, do not necessarily imply that it can be realized by an extremely small circuit. It is preferred to have a less platform-dependent notion of what is meant by lightweight, and so some general discussion is needed.

The principal aim for a lightweight algorithm is to provide algorithms that (1) have very small hardware implementations, and at the same time (2) have software implementations on small, low-power microcontrollers, with minimal flash and SRAM usage.

The desire for low-area hardware designs means that there are favored simple, low complexity round functions, even if that means many rounds are required.

But a block cipher does not provide security by itself and different applications will likely have very different security requirements, and protocols must be developed in each specific instance to achieve the desired level of security. Also a block cipher is an extremely versatile cryptographic primitive, and security developers expect that any lightweight protocol can be based upon an appropriately-sized block cipher.

An obvious question for developers of lightweight applications is "Why not build security protocols around AES?" Indeed, AES has been suggested for general purpose and for lightweight use and given its stature it is recommended that AES algorithm should be used whenever appropriate. However, for the most constrained environments, AES is not the right choice: in hardware, for example, the emerging consensus in the academic literature is that area should not exceed 2000 gate equivalents, while the smallest available implementation of AES requires 2400.

BACKGROUND

Block ciphers form an important class of cryptosystems in symmetric key cryptography. These are algorithms that encrypt and decrypt blocks of data (with fixed length) according to a shared secret key.

To achieve the desired security, most modern block ciphers are iterated ciphers that typically incorporate sequences of permutation and substitution operations. In fact, according to the ideas that Shannon proposed in his seminal paper [6], the encryption process takes as input a plaintext and a random key and so proceeds through N similar rounds.

In each round (except possibly for a couple, which may be slightly different) the iterated ciphers perform a non-linear substitution operation (or S-box) on disjoint parts of the input that provides "confusion", followed by a permutation (usually a linear/affine transformation) on the whole data that provides "diffusion". A cryptosystem reaches "confusion" if the relationship between plaintext, ciphertext and key is very complicated.

The diffusion property consists of spreading the influence of all parts of the input (plaintext and key) to all parts of the ciphertext. The operations performed in a round form the round function. The round function at the p-th round ($1\leq p \leq N$) takes as inputs both the output of the ($p-1$)-th round and the subkey $k(p)$ (also called round-key). Any round key $k(p)$ is constructed starting from a master key k of some specified length, e.g. $k \in$ K (nowadays we have $2^{64} \leq |K| \leq 2^{256}$, where |K| represents the cardinality of the set K). The key schedule is a public algorithm (strictly dependent on the cipher) which constructs $N + 1$ subkeys ($k(0), \ldots, k(N)$).

DESCRIPTION OF SIMON

Simon is a family of lightweight block ciphers which are defined for word sizes n = 16, 24, 32, 48 and 64 bits. The key is composed of $m*n$-bit words for m = 2, 3, 4 (i.e. the key size $m*n$ varies between 64 and 256 bits) depending on the word size n. The block cipher instances corresponding to a fixed word size n (block size $2n$) and key size mn are denoted by Simon2n=mn and Speck2n=mn.

Block cipher Simon has a Feistel structure and its round function under a fixed round key k is defined on inputs x and y as:

$$R_k(x, y) = ((y \oplus f(x) \oplus k), x)$$

The function $f(x)$ is defined as:

$$f(x) = ((x{<}{<}{<}1) \land (x{<}{<}{<}8)) \oplus (x{<}{<}{<}2),$$

where the symbol Λ denotes the logical AND operation.

The round function of Simon is shown in Fig. 1.

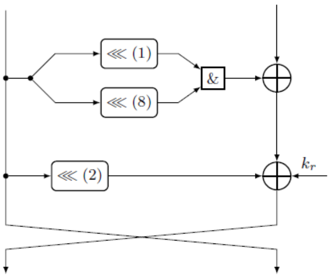
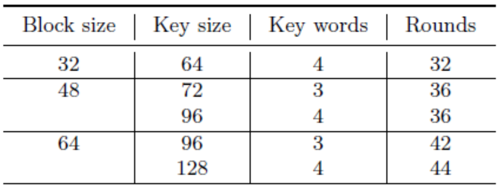


Fig. 1. SIMON round function

"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

The number of rounds, block size and key size of the block cipher are summarized in the table in Fig.2.



Block size	Key size	Key words	Rounds
32	64	4	32
48	72	3	36
	96	4	36
64	96	3	42
	128	4	44

Fig.2. Parameters for SIMON

4. EVALUATING THE DIFFERENTIAL EFFECT IN SIMON

The security of most block ciphers depends on substitution functions (S-boxes) which are (n,m)-functions. The resistance of the S-box to cryptographic attacks can be measured by evaluating certain properties of these functions. The two most important and powerful attacks on symmetric cryptosystems are differential and linear attacks and the respective cryptographic properties of these functions which measure the resistance against these two attacks are the nonlinearity and the differential uniformity. Since lightweight cryptographic algorithms are ARX ciphers, they do not have S-boxes. Instead they rely on basic arithmetic operations such as addition modulo n to achieve non-linearity. Computing full Differential Distribution Table (DDT) for the modular addition operation would require 4 x 2^{3n} bytes of memory and is therefore impractical for n > 16. To address this, in [1] partial DDT (pDDT) rather than the full DDT is computed. A pDDT contains (a fraction of) all differentials that have probability above a fixed probability threshold (hence the name – threshold search).

A property of Simon algorithm is that there are multiple trails satisfying a multiple round differential with the same input/output difference (differential effect). These trails start and end with the same input/output difference, but pass trough different values throughout intermediate rounds. An interesting property is that a multiple round differential is composed of multiple smaller subgraphs positioned at alternate levels. Each such subgraph represents a biclique. Clearly, the bigger the number and size of these bicliques, the differential effect would be stronger and hence the probability of the differential would be larger. Therefore, the ability to obtain good estimation of the probability of a given differential for Simon is intimately related to the ability to identify and characterize such complete bipartite subgraphs.

In order to understand the differential effect of Simon algorithm and the importance of the bipartite subgraphs, let's consider the pair of left and right input differences (Δ_i^L, Δ_j^R) = (11, 106) (hexadecimal values).

Through the non-linear component $f(x) = (x{<}{<}{<}1)\,\Lambda(x{<}{<}{<}8)$ of the round function, the difference $\Delta_i^L = 11$ propagates to a set of output differences. This set has the form ∇ = 000* 000* 00*0 00*0, where * can take values 0/1. Note that for some assignments of the * bits, the resulting difference may have zero probability (impossible input-output difference). For ∇ = {0122, 0102, 0120} three distinct output differences Δ_{i+1}^L from one round of Simon are produced. They are shown as the three lower level nodes in Fig. 3 and are obtained as ∇ ⊕ ((Δ_i^L<<<2) ⊕ Δ_i^R) = ∇ ⊕ (44) ⊕ Δ_i^R.

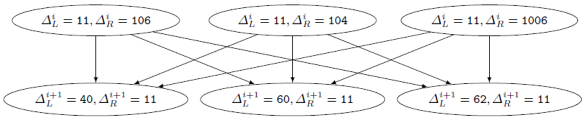

$\Delta_L^i = 11, \Delta_R^i = 106$
$\Delta_L^i = 11, \Delta_R^i = 104$
$\Delta_L^i = 11, \Delta_R^i = 1006$
$\Delta_L^{i+1} = 40, \Delta_R^{i+1} = 11$
$\Delta_L^{i+1} = 60, \Delta_R^{i+1} = 11$
$\Delta_L^{i+1} = 62, \Delta_R^{i+1} = 11$

Fig. 3. Bipartite subgraph in the differential (graph) of Simon32

Another node with the same input difference Δ_i^L to the round function, but with different right difference Δ_i^R = (11, 104) (see Fig. 3) produces a corresponding set of output differences ∇', which may or may not have common elements with ∇ in general. For example, in this case ∇' = {0100, 0120, 0122} produced by the node (11, 104). In either case though, ∇ and ∇' may still produce the same set of output differences (Δ_{i+1}^L , Δ_{i+1}^R). When this happens then a biclique is formed. This is shown in Fig. 3 where both ∇ and ∇' result in the same set of output differences (Δ_{i+1}^L , Δ_{i+1}^R) ∊ {(4, 11), (26, 11), (6, 11)}.

In general, when the sets ∇, ∇' produced from two different pairs of input differences have high (and possibly equal) probabilities, the complete subgraphs that are formed as a result, have thick edges (corresponding to high probability). Such subgraphs contribute to the clustering of differential trails in Simon.

Note that the described subgraphs may not be formed for all possible elements in ∇ of an arbitrary node since, as already mentioned, some of them may propagate with 0 probability through the non-linear component f. Furthermore, because the complete bipartite subgraphs depend on the input differences, they can not occur at arbitrary positions in the digraph. The frequent occurrence of such special subgraph structures in Simon in large numbers is the main cause for the strong differential effect observed experimentally using the tool for differential search.

Conclusions

An important problem today is the design of cryptographic algorithms that are both efficient and secure, have small memory footprint and are low-cost and easy to implement and deploy on multiple platforms. Finding an optimal compromise between these, often conflicting, requirements is a difficult area researched by the field of lightweight cryptography.

Also resistance against the two most powerful attacks on symmetric cryptosystems, differential and linear attacks, is important. Concerning specific attacks that are applied to lightweight ciphers, traditional attacks (for example differential attack) are combined with newer techniques (for example biclique attack).

Having in mind that the applications of lightweight cryptographic algorithms vary from mobile devices, through RFID tags to electronic locks, their importance is likely to continue increasing in the future and so the developing of various cryptanalytic attack against this type of ciphers.

Bibliography

[1] A. Biryukov and V. Velichkov. A Method for Automatic Search for Differential Trails in ARX Ciphers, 2013.

[2]R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers. The Simon and Speck families of lightweight block ciphers, 2013.

[3] A. Biryukov, A. Roy, and V. Velichkov. Differential Analysis of Block Ciphers SIMON and SPEC. 2014

[4] Daemen J. and Rijmen V., AES Proposal: Rijndael, NIST AES proposal, 1998.

[5] Daemen J. and Rijmen V., The design of Rijndael: AES - the Advanced Encryption Standard, Springer, 2002.

[6] Shannon C. E., Communication theory of secrecy systems, Bell System Tech. J. 28 (1949), 656–715.