Volume XXI 2018
ISSUE no.1
MBNA Publishing House Constanta 2018

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Border security Wireless Integrated Network Sensor attack resistance analysis by integral cryptanalysis of AES cipher

To cite this article: Florin Medeleanu, Ciprian Răcuciu, Dan-Laurenţiu Grecu and Narcis Antonie, Scientific Bulletin of Naval Academy, Vol. XXI 2018, pg. 123-128.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-18-I1-019

Border security Wireless Integrated Network Sensor attack resistance analysis by integral cryptanalysis of AES cipher

Florin Medeleanu[1], Ciprian Răcuciu[2], Dan-Laurențiu Grecu[2], Narcis Antonie[1]

[1] Military Technical Academy, Bucharest, George Coşbuc Bvd. 39-49, Romania
2 "Titu Maiorescu" University, Bucharest, Calea Văcăreşti 187, Romania
Corresponding author: florinmed@yahoo.com

Abstract. Wireless Integrated Network Sensor (WINS) make available monitoring and control capabilities for surveying the borders of a country. Applying these capabilities the illegal persons which cross the border by trespassing or unlawful activities which occur in a protected area can be easily identified. In order to achieve this objective, the protected area is split into a number of nodes. Each node communicates with each other and with the central node by the means of secured communication channels. In order to securely transmit the information to and from the nodes in a real system the cryptographic algorithm AES is often used. Integral cryptanalysis is an attack that makes use of chosen-plaintext and can subvert the security of cryptographic algorithm. This paper reports on analysis and results of integral cryptanalysis or square attack on a 4 round reduced version of the AES cipher (mini-AES).

Keywords: *border security, wireless integrated network sensor, cryptanalysis, square attack, block cipher, encryption, key recovery.*

1. Introduction

Wireless Integrated Network Sensor (WINS) project was started by Defence Advance Research Project Agency (DARPA) in US. On global scale WINS systems allow surveying and access route control of land, water and air resources for environment monitoring. WINS architecture includes sensors, data converters, signal processing, control functions and a communication network. WINS nodes are distributed at high density in the environment to be monitored. The structure of WINS system is depicted in Figure 1. Unfortunately the capabilities of such a system can be subverted by an attacker that eavesdrops, modifies or blocks the communication network. For this reason the communication network is protected using a cryptographic algorithm. The current standard in cryptography is AES algorithm. In this paper the security of the cryptographic algorithm (AES) against a specific attack – integral cryptanalysis is analyzed.

Daemen, Knudsen, and Rijmen designed in 1997 a new encryption algorithm which was published and described in a paper [1]. This new encryption algorithm, named SQUARE, was a predecessor of Rijndael [2], the future AES - FIPS 197. SQUARE, similar to other algorithms, was designed by cryptanalysis and used the wide trail strategy (for AES the authors used the same approach) in order to provide enough security measures to be safe against linear and differential cryptanalysis. However, since the beginning, the authors have noticed a property of this cipher which permitted to break six rounds of SQUARE algorithm. This new attack was based on input chosen-plaintext method. Initially SQUARE algorithm was designed with only six rounds, but due to this property, the authors had to add more rounds to the algorithm in order keep it secure against the new attack. Details about the new discovered attack were published along with details of the algorithm.

The attack was referred as the "Square attack", because it was applied initially on SQUARE algorithm, but was not appropriate to attack more than six rounds. The new attack inherits to some extent lots of similarities to differential and linear cryptanalysis. Due to this, and due to the diffusion level guaranteed by the design of the algorithm, the so-called wide trail strategy, the authors considered sufficient to add just two more rounds to the algorithm in order to neutralize this attack. Even though this attack was initially specific only to SQUARE algorithm, the equivalences of SQUARE with Rijndael and also with CRYPTON, allowed that the attack could certainly be used against these algorithms too. Adapted to Rijndael, the attack broke six rounds of the algorithm. The attack against Rijndael was almost the same as the original attack against SQUARE. With these facts in mind, the author of CRYPTON had enough proofs to infer that this type of attack could break at most six rounds of CRYPTON algorithm [3].

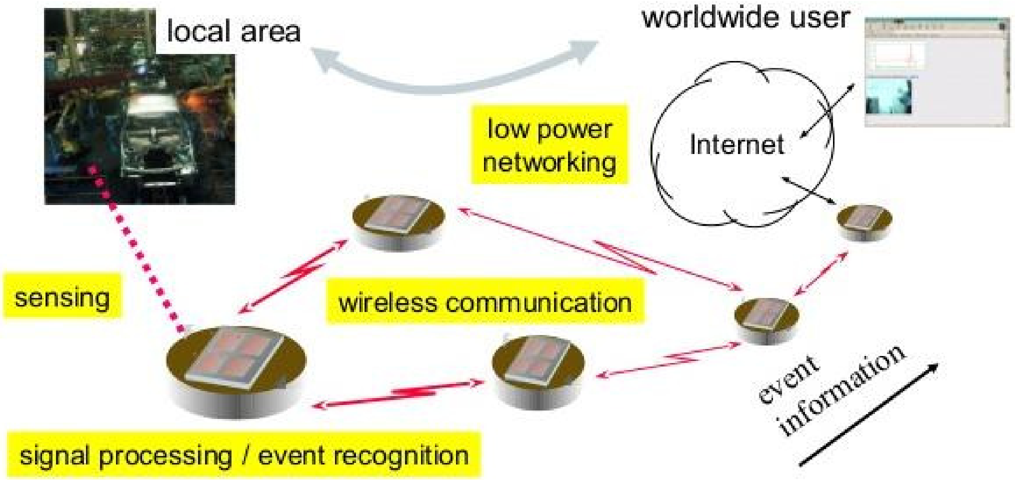

Figure 1. WINS system structure.

In order to generalize this attack to different algorithms than SQUARE, Lucks [4] adapted it to Twofish [5] algorithm. This is a Feistel type algorithm. As a consequence, Lucks changed the name of this generalized attack into "saturation attack". Using changes of the original SQUARE attack, other algorithms were attacked (Hierocrypt, Camellia, PES and IDEA). Knudsen and Wagner [9] unified the different procedures together in a single method, introduced the notion *integral cryptanalysis*, and specified the more effective higher-order integral attack.

2. Mini-AES algorithm

A lot of reduced versions of the AES algorithm have already been defined. In this paper we will take into consideration the version with 64 bit block length. We have chosen this variant of Mini-AES because is very similar to full version of AES, instead of bytes, this reduced version of AES uses nibbles (block of 4 bits). It's very intuitive to apply the results from the reduced version of Mini-AES to the full version of the same algorithm.

To encrypt a message with reduced version of the AES algorithm, the input message, named plaintext, is split in blocks of 64 bits. At any moment in time, just one input block is enciphered with reduced version of AES into ciphertext. The next input block is enciphered and the entire process continues till there is no more input plaintext to be processed. The reduced version of AES encryption process is done with a symmetric key of 64 bits length. Figure 2 describes the process of enciphering the input plaintext with reduced version of AES.

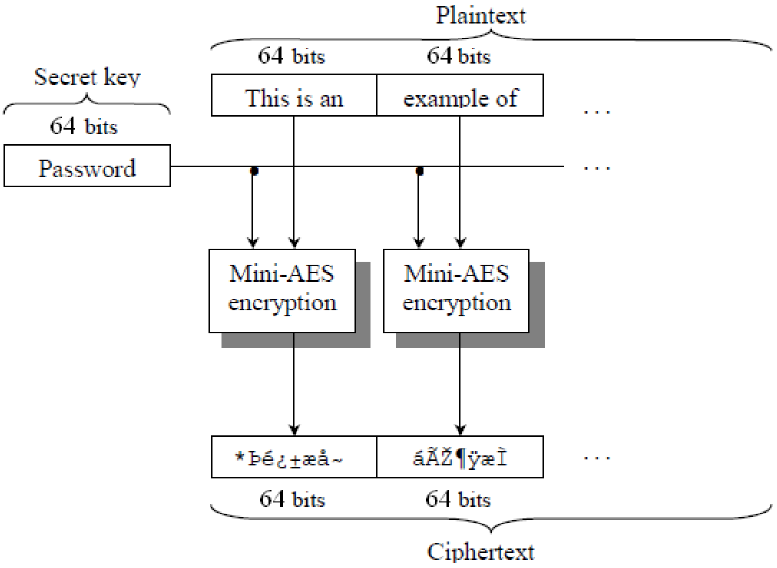

Figure 2. The encryption process of a plaintext message with Mini-AES.

In Table 1 the main variables of the reduced version of AES with 4 bits word size and standard AES with 8 bits word size are listed. The substitution values of S-box with dimension 4×4 are (in hex):

$$S = [0xD, 0xA, 0x1, 0x5, 0xC, 0xF, 0x9, \\ 0xE, 0x2, 0x3, 0xB, 0x7, 0x8, 0x0, 0x4, 0x6]. \tag{1}$$

The Galois field used in S-box construction is the extension field GF(2^4) defined with the base field GF(2)[x] and the characteristic polynomial $m(x)$. The characteristic polynomial was chosen at random as an irreducible polynomials. The state transformations for a round AddRoundKey$_i$, SubByte, ShiftRows and MixColumns are similar for the reduced version and for the original AES, but reduced as size. Particularly, for MixColumns transform, the coefficients used for Maximum Distance Separable matrix are the four LSB (least significant bits) of the original coefficients of AES Maximum Distance Separable matrix. Round constants used for the key expansion routine were chosen using a similar approach. The same number of rounds is used for the reduced version and the original AES version, also for different key sizes.

Table 1. Reduced and complete version AES parameters

Number of bits	Irreducible polynomial	State Size (16t bits)	Key Size (bits)
4	$1+x+x^4$	64	64-96-128
8	$1+x+x^3+x^4+x^8$	128	128-192-256

3. Integral cryptanalysis – Square attack

Square attack was born as a special designed attack for Square block algorithm [10]. The attack shares similarities with multiset [11], saturation [12] and integral cryptanalysis attacks [13, 14]. Each of these attacks operates with chosen-plaintext (CP).

A base notion of square attack is the Λ-set [10]. This is a multiset meaning a set with various multiple values. This set contains b text blocks of n-bit, with n being the block size and b usually a power of 2. The n-bit plaintext blocks are traced as t-bit words throughout the round operations. The relation between t and n is $t < n$. A Λ-set like this,

$$\{(0|4|7|3),(1|4|7|1),(3|4|7|2),(2|4|7|4), \\ (7|4|7|0),(4|4|7|7),(5|4|7|6),(6|4|7|5)\} \tag{2}$$

is a set with $b = 2^t = 8$ blocks of plain text, with n=12 bits wide. Vertical bar sign, |, represents concatenation.

Multiset attacks aim at the bijective operations of the algorithm. This method uses permutations (active words „*A*") to attack different permutations (Substitution-boxes). Also, algorithms that work with clean divided block of bits are especially targeted. A normal integral cryptanalysis attack starts with a Λ-set with only one active word. The Λ-set given in (2), there are two active word: the first and the last. The Λ-set is processed several rounds, having the effect that the "A" word looses step by step its pattern and transforming in "E" words (not permutations anymore but even number of values or arbitrarily number of pairs), then in "B" words (not even but balanced values), and finally in "?" words (unknown pattern).

Only the input plaintext can be influenced by the attacker. The words propagation through the rounds of the algorithm cannot be forced by the attacker. As effect, the detection and presence of square distinguisher holds with maximum probability (it is certain). The probabilistic or iterative construction of square distinguisher is not known, similar to differential or linear characteristic (these characteristics are normally built by putting together elemental characteristics).

The square distinguishers exploit particular transformations of the encryption round, because part of the input bits is constant (to a random fix value "P") as long as other input bits are specified to every existing value ("A").The first square attack [10] had order 1 and used only one active word with t-bit length (and the rest of t-bit words were passive i.e. to a constant value). Higher order square attacks (nth-order) make use of n t-bit active words (multi-active words) in the same time and the rest of the words passive. The input data required to deploy the attack is in proportion with the number of active word: 2^{tn} input chosen plaintexts (CP). In this paper we take into consideration this type of square attack, with only one 4-bit active word (nibble).

4. Practical Results

The first order square distinguisher is shown in Figure 3. This distinguisher covers 3.25 rounds of reduced version of AES. The initial location of "A" word does not influence the length of this distinguisher. We took into consideration for every round operation AddRoundKey, SubByte, ShiftRows and MixColumn as 0.25 part of a round. The reason for the spreading of "A", "P", "E" and "N" patterns is due to the construction of every pattern and how they transform throughout every other round operation.

In order to prove how the square attack works, we used round keys and plain text with the values given in Table 2.

Table 2. Round keys/ plain text used for square attack.

RK/PT	*Value (hex)*
RK_0	3C0B/E699/4E1B/1213
RK_1	3651/D0C8/9ED3/8CC0
RK_2	9E83/4E4B/9098/5C58
RK_3	51AC/1FE7/CF7F/9327
RK_4	804F/9FA8/50D7/C3F0
$PT_{1...16}$	$\mathcal{A}$000/0000/0000/0000
where	$\mathcal{A}$={0,1,2,3,4,5,6,7,8,9,A,B,C.D.E.F}

Plain text Λ-set used in our Square attack contains 16 plain texts which lead to a set of 16 cipher texts. For key recovery phase of the attack, 16 cipher texts will be partially decrypted by guessing the value of the last round key (RK_4). By partially decryption we mean trying every value of nibble, in total a set with 16 possible keys. MixColumn transformation is not used the last round - the fourth (similar to AES full cipher), which causes that the process of decryption actions on independent values of nibbles, because ShiftRow and NibbleSub act independently on every nibble. This fact means that guessing of key values can occur on nibble values (4 bits) and not on entire key value (48 bits). This observation simplifies the complexity of attack from 2^{48} to 2^{4}.

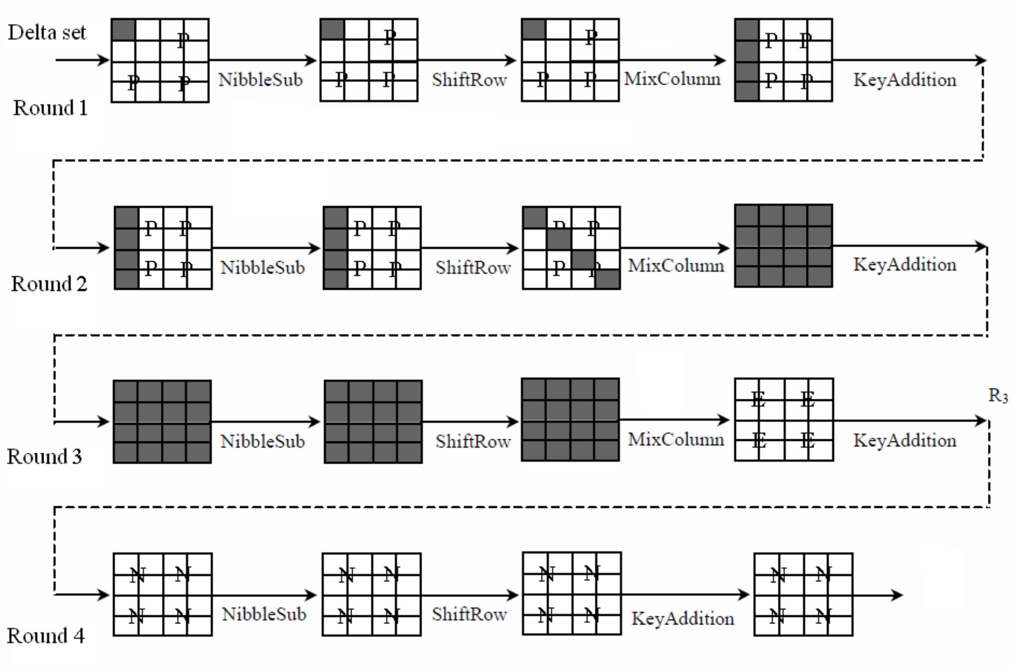

Figure 3. 1st-order square distinguisher

In Table 3 we show the values of cipher text (CT) set after 4 rounds. These values will be partially decrypted with 16 keys with values {0000/0000/0000/0000}, {1111/1111/1111/1111} ... {FFFF/FFFF/FFFF/FFFF}. The partially decrypted CT will be Xor-ed and for positions where the 0 result is obtained we keep the value of RK_4 as a possible correct value. These possible correct values of round key are stored in a table and used forward in the attack.

Table 3. Cipher text after 4 rounds.

Cipher text	*Value (hex)*	*Cipher text*	*Value (hex)*
CT_0	8714/A667/F703/ECCD	CT_8	7711/AE60/6635/4C7A
CT_1	0100/F890/0C51/8A8F	CT_9	FBE1/785D/177B/9235
CT_2	62A3/2551/9C85/EEC3	CT_{10}	4756/0AC6/F5C8/9732
CT_3	0922/3EB2/D773/9877	CT_{11}	271F/4C15/BB65/DC54
CT_4	41B0/AF69/3E08/B3B3	CT_{12}	24B2/0022/EB2C/3754
CT_5	7E5C/F04C/05EA/71CB	CT_{13}	8E18/8961/8FBD/8451
CT_6	0971/5058/C3D5/1454	CT_{14}	3B0D/5C1D/FFEB/04EA
CT_7	C50D/3110/4FA9/0E8A	CT_{15}	4F08/0477/76D2/FC01

After partially decrypting $CT_{0\ \ldots}\ CT_{15}$ and Xor-ing the results, we keep the values of the nibbles only for positions where the expected value "0" is obtained. For example, for the first position of guessed RK_4 nibble we obtained null Xor-ed value only for $RK_{4(1)}$={5, 8, E}. Of course, only one value is the correct one, but we cannot distinguish the right one. For this purpose we repeated the entire attack for a different Λ-set, for example $PT_{1\ldots16}$= $\mathcal{A}$111/1111/1111/1111, where $\mathcal{A}$={0,1,2,3,4,5,6,7,8,9, A,B,C,D,E,F}. For this Λ-set we try to obtain null Xor-ed value for the first partially decrypted nibble

only for already verified values $RK_{4(1)}$={5, 8, E}. Indeed, we obtained null Xor-ed value only for $RK_{4(1)}$={8}. This result confirms that the attack revealed the correct value of the round key.
Using the same procedure for every other nibble of RK_4, it is possible to obtain the entire value of RK_4.

5. Conclusions and future work

In this paper we verified the length of the first order distinguisher for Square attack, in a way similar to [15]. In fact we went straightforward and recovered the key for the fourth round. Having the fourth round key, the master key (RK_0) can be easily calculated. As a future work we proposed to verify the length of higher order distinguisher for Square attack (4^{th}, 8^{th} and 12^{th}) and also to recover the key.
A step forward would be to apply the Square attack on reduced round full AES version and to recover the key. In the sense that the full version of AES algorithm has 10, 12 or 14 rounds, the security of the algorithm is not endangered by this attack which can recover the key after 4 rounds. The remaining security margin, 6 to 8 rounds, is more than enough to guarantee that the AES algorithm is secure.

6. References

[1] J. Daemen, L. Knudsen, and V. Rijmen. *The block cipher SQUARE.* In Proceedings of the Fourth International Workshop on Fast Software Encryption (FSE 1997), volume 1267 of Lecture Notes in Computer Science, pages 149–165. IACR, Springer, January 1997.

[2] NIST. *Advanced Encryption Standard (FIPS PUB 197)*, November 2001. http:// www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[3] C.H. Lim. *A revised version of CRYPTON: CRYPTON v1.0.* In Proceedings of the Sixth International Workshop on Fast Software Encryption (FSE 1999), volume 1636 of Lecture Notes in Computer Science, pages 31–45. IACR, Springer, March 1999.

[4] S. Lucks. *The saturation attack - a bait for Twofish.* Proceedings of the 8th International Workshop on FSE, vol. 2355, pp. 187–205. IACR, Springer, April 2001.

[5] N. Ferguson, C. Hall, J. Kelsey, B. Schneier, D. Wagner, and D. Whiting. *Twofish: A 128- bit block cipher*, June 1998. http://www.schneier.com/paper-twofish-paper.pdf.

[6] P.S.L.M. Barreto, H.Y. Kim, J. Nakahara Jr, B. Preneel, V. Rijmen, and J. Vandewalle. *Improved SQUARE attacks against reduced-round HIEROCRYPT.* Proceedings of the 8th International Workshop on FSE (FSE 2001), vol. 2355, pp. 165–173. IACR, Springer, 2001.

[7] Y. He, S. Qing. *SQUARE attack on reduced Camellia cipher.* In Proceedings of the 3rd International Conference on Information and Communications Security (ICICS 2001), volume 2229 of Lecture Notes in Computer Science, pages 238–245. Springer, November 2001.

[8] P.S.L.M. Barreto, H.Y. Kim, J. Nakahara Jr, B. Preneel, and J. Vandewalle. *SQUARE attacks on reduced-round PES and IDEA block ciphers.* Cryptology ePrint Archive, Report 2001/068, August 2001. http://eprint.iacr.org/2001/068.

[9] L.R. Knudsen and D. Wagner. *Integral cryptanalysis (extended abstract).* In Proceedings of the 9th International Workshop on FSE, vol. 2365, pp.629– 632. IACR, Springer, February 2002.

[10] J. Daemen, L.R. Knudsen, V. Rijmen, *The Block Cipher SQUARE*, Fast Software Encryption, E. Biham,Ed., Springer-Verlag , LNCS 1267, 1997, 149–165.

[11] A. Biryukov, A. Shamir, *Structural Cryptanalysis of SASAS*, Adv. in Cryptology, Eurocrypt'01, B. Pfitzmann, Ed., Springer-Verlag, LNCS 2045, 2001, 394–405.

[12] S. Lucks, *The Saturation Attack – a Bait for Twofish*, Fast Software Encryption, M. Matsui, Ed., Springer-Verlag, LNCS 2355, 2001, 1–15.

[13] Y. Hu, Y. Zhang, G. Xiao, *Integral Cryptanalysis of SAFER+*, Electronic Letters, (35):17, Aug. 1999, 1458–1459.

[14] L.R. Knudsen, D. Wagner, *Integral Cryptanalysis*, Fast Software Encryption, J. Daemen and V. Rijmen, Eds., Springer-Verlag, LNCS 2365, 2002, 112–127.

[15] Jorge Nakahara Jr, Daniel Santana de Freitas, *Mini-ciphers: a reliable testbed for cryptanalysis?*, Dagstuhl Seminar Proceedings: Symmetric Cryptography 2009