2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

Discrete Lyapunov Exponent for Rijndael Block Cipher

Ljupco Kocarev[†], Paolo Amato[‡], Davide Ruggiero[‡], and Immacolata Pedaci[‡]

†Institute for Nonlinear Science
University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093–0402, USA
Email: lkocarev@ucsd.edu
‡STMicroelectronics
Soft Computing,Si-Optics & Post Silicon Technology Corporate R&D
Via Remo De Feo 1, 80022 Arzano (Napoli), Italy
Email: {paolo.amato; davide.ruggiero; immacolata.pedaci }@st.com

Abstract—The Rijndael block cipher, the winner of the Advanced Encryption Standard competition, is analyzed as a discrete time, discrete phase-space dynamical system. We compute its discrete Lyapunov exponent as well as the discrete Lyapunov exponents of the *ByteSub*, *ShiftRow* and *MixColumn* transformations, which are the main ingredients of the Rijndael block cipher. Our work shows that strong chaos-based cryptographic algorithms should be formed by repeated products of two simple transformations: one having perfect nonlinearity (and smaller value of discrete Lyapunov exponent) and one having the largest possible value of the discrete Lyapunov exponent (and being almost linear function).

1. Introduction

The research on network security has considerably grown in the last decade. There is a need for using cryptographic tools (algorithms, protocols, etc.) in order to ensure privacy in data transfer among users. Recently, new cryptographic techniques based on *chaos theory* have been developed [1, 2, 3, 4, 5, 6]. In this paper we use chaos theory in the analysis of asymptotic behavior of known encrypting algorithms originally designed without chaotic techniques. Mixing, and therefore chaotic, systems are proposed in cryptography by C. E. Shannon in [7].

Chaotic systems, when implemented on finite-state machines (digital computers), are, in fact, discrete-time dynamical systems acting on discrete phase-space. Owing to the discreteness, any dynamical trajectory in computer becomes eventually periodic, the effect well known in the theory and practice of pseudo-random number generators. The periodic approximations in dynamical systems are also considered in the ergodic theory [8], apparently without any relation to pseudo-chaos.

Recently, we have proposed a definition of finite-space (or discrete) Lyapunov exponent [9, 10]. It measures local (between neighboring points) average spreading of the discrete-time dynamical system. Let M be a cardinality of the discrete phase-space. We have also suggested a definition of pseudo-chaos in terms of finite-space Lyapunov exponent in a similar way as for continuous systems: the system is said to be pseudo-chaotic if its finite-space Lyapunov exponent approaches a positive number (or $+\infty$), when $M \to \infty$.

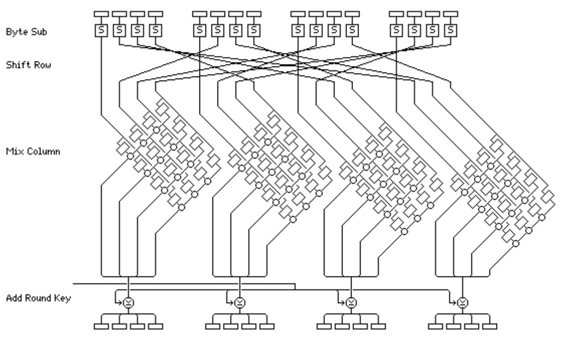

Figure 1: Diagram of Rijndael round.

In this paper we calculate discrete Lyapunov exponent for the Rijndael block cipher. In the following we give first a brief review of Rijndael block cipher. Then we analyze it as a dynamical system, and compute its Lyapunov exponent. Finally, we discuss possible applications of our approach for designing chaos-based encryption schemes.

2. Brief review of Rijndael

The Rijndael [11, 12] cipher was the winner of the AES competition and was designed by the researchers from Belgium. The cipher works for three block sizes: 128, 192, and 256 bits. Rijndael applies the Shannon product cipher concept and is not based on the Feistel structure. Cryptographic operations are based on arithmetic in $GF(2^8)$. In the following we assume that the block length is 128 bits. Figure 1 shows the structure of the Rijndael round.

The cipher applies the following transformations:

- *ByteSub* Transformation – an input block with 16 bytes is subject to a byte-by-byte transformation using the S-box.
- *ShiftRow* Transformation – the bytes of the input are

arranged into four rows and every row is rotated a fixed number of positions.

- *MixColumn* Transformation – the bytes of the input are arranged into four rows and every column is transformed using polynomial multiplication over $GF(2^8)$.
- *AddRoundKey* – the input block is XOR-ed with the round key.

3. Discrete Lyapunov exponent

Let us consider a map

$$F_M : \{0, 1 \ldots, M-1\} \to \{0, 1 \ldots, M-1\} . \tag{1}$$

We assume that the map F_M is $1:1$ and onto (bijection). Clearly, all trajectories of F_M are periodic; let α_j be a periodic orbit of F_M with period T_j. Since F_M is a bijection, it follows that $\cup_j \alpha_j = \{0, 1 \ldots, M-1\}$ and $\sum_j T_j = M$.

We define discrete Lyapunov exponent of the map F_M as

$$\lambda_{F_M} = \frac{1}{M}\left[\sum_{i=0}^{M-2} \ln \mid F_M(i+1) - F_M(i) \mid\right] \quad + \tag{2}$$

$$\frac{1}{M} \ln \mid F_M(M-2) - F_M(M-1) \mid , \tag{3}$$

where the distance between two elements of the set $\{0, 1 \ldots, M-1\}$ is the Euclidean distance between two integers $d_i = \mid F_M(i+1) - F_M(i) \mid$. We say that $i \pm 1$ are neighboring points of i. In the above equation all terms measure the divergence of two trajectories evolving in one iteration from two “slightly” different initial conditions: an initial point i and its neighbor $i+1$. Note that in the last term the neighbor of $M-1$ is the point $M-2$. Moreover, if we formally write $F_M(M) \equiv F_M(M-2)$ the last equation can be rewritten in more compact form in the following way:

$$\lambda_{F_M} = \frac{1}{M} \sum_{i=0}^{M-1} \ln \mid F_M(i+1) - F_M(i) \mid . \tag{4}$$

Thus, the Lyapunov exponent measures average spreading of the map F_M.

Let

$$\alpha_j = \{a_0^{(j)}, a_1^{(j)} = F_M(a_0^{(j)}), \ldots a_{T_j-1}^{(j)} = F_M(a_{T_j-2}^{(j)})\}$$

be a periodic orbit with period T_j; in another words let $a_0^{(j)} \neq a_1^{(j)} \neq \ldots \neq a_{T_j-1}^{(j)}$ and $F_M^{T_j}(a_0^{(j)}) = a_0^{(j)}$. We define the Lyapunov exponent of the map F_M for the periodic orbit α_j as

$$\lambda_{(F_M,\alpha_j)} = \frac{1}{T_j} \sum_{k=0}^{T_j-1} \ln \mid F_M(a_k^{(j)} + 1) - F_M(a_k^{(j)}) \mid . \tag{5}$$

Observe that the Lyapunov exponent of the map F_M can also be rewritten as a weighted sum of the Lyapunov exponents of all periodic orbits:

$$\lambda_{F_M} = \sum_j \frac{T_j}{M} \lambda_{(F_M,\alpha_j)} . \tag{6}$$

Clearly, $0 \leq \lambda_{F_M} \leq \ln(M-1)$. The map with null Lyapunov exponent is $F_M(x) = x$ for each $x \in \{0, 1, \ldots, M-1\}$. The set of all different maps F_M can be divided into equivalent classes, each class having same Lyapunov exponent.

We justify our definition of discrete Lyapunov exponent by showing that, for large classes of chaotic maps, the corresponding finite-space Lyapunov exponent approaches the Lyapunov exponent of a chaotic map when $M \to \infty$. The proof of this theorem can be found in [9].

Example 3.1 *The maps $F_M^{(i)}$ defined as*

$$F_M^{(i)}(x) = \begin{cases} x & if \quad 0 \leq x \leq i, \\ i+3 & if \quad x = i+1, \\ i+1 & if \quad x = i+2, \\ i+2 & if \quad x = i+3, \\ x & if \quad x \geq i+4, \end{cases} \tag{7}$$

have, for each $i = 0, 1, \ldots M-5$, same Lyapunov exponent: $\lambda_{F_M}^{(1)} = \ln 2/M$.

Example 3.2 *Let $M = 2m$ be an even number. We define P_M as*

$$P_M(x) = \begin{cases} m+k & if \quad x = 2k, \\ k & if \quad x = 2k+1, \end{cases} \tag{8}$$

where $k = 0, 1, \ldots m-1$. The Lyapunov exponent of this map is equal to

$$\lambda_{P_M} = \frac{m+1}{2m} \ln m + \frac{m-1}{2m} \ln(m+1).$$

The importance of this example is given by the following theorem, which is proven in [10].

Theorem 3.3 *For any permutation F_M of the set $\{0, 1, \ldots, M-1\}$ we have $\lambda_{F_M} \leq \lambda_{P_M}$.*

Example 3.4 *Let $M = 2m$. We define Q_M as*

$$Q_M(x) = \begin{cases} k & if \quad x = 2k, \\ M-1-k & if \quad x = 2k+1, \end{cases} \tag{9}$$

where $k = 0, 1, \ldots m-1$. The Lyapunov exponent of this map is equal to

$$\lambda_{Q_M} = \frac{1}{M} \ln(M-1)!.$$

We adopt the following definition of perfect nonlinearity (note that our definition is weaker than the usual one): F_M has a perfect nonlinearity if differences $|F_M(i+1) - F_M(i)|$, $i = 0, 1, \ldots, M-2$ take all possible values $1, 2, \ldots, M-1$. This example shows the existence of maps with perfect nonlinearity. For given M, there are $M-1$ classes of maps with perfect nonlinearity. For the discrete Lyapunov exponents of these classes, one has:

$$\lambda_{F_M}^{(k)} = \frac{1}{M}[\ln(M-1)! + \ln k],$$

where $k = 1, 2, \ldots M-1$. Note also that the permutation P_M, which has the maximum Lyapunov exponent, has very weak nonlinear properties: the differences $|F_M(i+1) - F_M(i)|$ take only two different values.

4. Rijndael as a dynamical system

Theory of dynamical systems aims to understand the asymptotic behavior of an iterative process. In another words, given a map $f : \mathcal{X} \mapsto \mathcal{X}$ and $x \in \mathcal{X}$, the theory hopes to understand the behavior of the set of the points $\{x, f(x), f(f(x)), \ldots\}$, called a trajectory of x.

By the assumption that plaintext X and cryptogam Y belong to the same domain, a block encryption algorithms can be written in form of transformations E_Z:

$$Y = E_Z(X), \tag{10}$$

where plaintext X, cryptogram Y and secret key Z are (array of) sequences of letters in finite alphabets $\mathcal{L}_X, \mathcal{L}_Y, \mathcal{L}_Z$, respectively, which are not necessarily equal to each other. When $\mathcal{L}_X = \mathcal{L}_Y$, as for Rijndael algorithm, it is meaningful to iterate the map E_Z on a given starting plaintext X and to consider the trajectory $\{X, E_Z(X), E_Z(E_Z(X)), \ldots\}$.

Rijndael works on 16 byte-blocks, and each byte is independently transformed with respect to the other blocks. Then the phase space is substantially the space $\{0, \ldots, 255\}^{16}$.

5. Discrete Lyapunov exponent of Rijndael dynamical system

In this section we consider the Rijndael algorithm as an iterative process, and compute its discrete Lyapunov exponent.

5.1. *ByteSub* transformation

A nonlinear transformation is essential part of every strong encryption algorithm. Nonlinear transformations are often implemented as lookup tables or S-boxes. A S-box with p input bits and q output bits is denoted with $p \to q$. The DES uses eight different $6 \to 4$ S-boxes. Byte level S-boxes ($8 \to 8$) are suited for software implementation on 8-bit processors.

ByteSub transformation $S(x)$ in the Rijndael algorithm is a byte-level S-box ($8 \to 8$) defined in the following way:

$$S(x) = \begin{bmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} x^{-1} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix},$$

where $x^{-1} \in GF(2^8)$ is the multiplicative inverse of x if $x \neq 0$ or zero if $x = 0$.

Let $f : L \to L$, $L = \{0, 1, \ldots, 255\}$ be the *ByteSub* transformation of the Rijndael algorithm. We have computed the discrete Lyapunov exponent of the map to be $\lambda_f = 4.01$. The discrete Lyapunov exponent of *ByteSub* transformation is slightly smaller that the corresponding value for the map with perfect nonlinearity and $M = 256$: $\lambda_{Q_M} = 4.54$. The reason for this is that our definition of perfect nonlinearity is somewhere weaker that one commonly accepted in cryptography. Nevertheless, the role of the *ByteSub* transformation in the Rijndael algorithm, similarly to any strong nonlinear transformation, is to mix in a nonlinear way the input information.

5.2. *ShiftRow* permutation

Let $a_{0,0}, \ldots, a_{0,3}, \ldots a_{3,0}, \ldots, a_{3,3}$ be 16 bytes (128 bits) of the the Rijndael algorithm. The *ShiftRow* permutation takes the input

$$\begin{aligned} a_0 &= (a_{0,0}, a_{0,1}, a_{0,2}, a_{0,3}) \\ a_1 &= (a_{1,0}, a_{1,1}, a_{1,2}, a_{1,3}) \\ a_2 &= (a_{2,0}, a_{2,1}, a_{2,2}, a_{2,3}) \\ a_3 &= (a_{3,0}, a_{3,1}, a_{3,2}, a_{3,3}) \end{aligned}$$

and returns $a_i >>> C_i$, $i = 0, 1, 2, 3$, where $a >>> C$ is the rotation of the sequence a of bytes to the right by C bytes. The values of C_i are $C_i = i$, $i = 0, 1, 2, 3$.

Rijndael works on 16 byte-blocks, and each byte is independently transformed with respect to the other blocks using the *ByteSub* transformation. The role of the *ShiftRow* permutation is just to permute all 16 bytes: it does not play role of a nonlinear map or a map with the maximum Lyapunov exponent, which measures the spreading factor. We have computed the Lyapunov exponent of the *ShiftRow* permutation to be 0.93, which is substantially smaller than the maximum one (for $M = 16$) 2.13. Note also that the differences $|F_M(i+1) - F_M(i)|$ for this map take only two different values: 3 and 13, again showing its weak nonlinear properties.

5.3. *MixColumn* transformation

In the Rijndael algorithm the *MixColumn* transformation is a transformation, which for given 4 input elements (bytes) outputs 4 elements (bytes), and can be represented by the following relation:

$$[y_i]_{4\times1} = [c_{i,j}]_{4\times4}[x_j]_{4\times1},$$

where the matrix $C = [c_{i,j}]_{4\times4}$ is chosen to be a *MixColumn* matrix, and addition and multiplication are defined over a finite field. For the Rijndael algorithm the *MixColumn* matrix, using hexadecimal representation of the matrix elements, is defined as

$$C = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 01 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}.$$

Multiplication in GF(2^8) is defined as multiplication of binary polynomials modulo an irreducible binary polynomial $m(x)$ of degree 8. For Rijndael, this polynomial is

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

or $'11B'$ in hexadecimal representation ($'1\ 0001\ 1011'$ binary).

The role of *MixColumn* transformation is to ensure largest possible spreading factor, and therefore should have maximum discrete Lyapunov exponent. This is indeed the case: we have found the Lyapunov exponent of the *MixColumn* transformation to be 21.49. Note that this map does not have strong nonlinear properties.

5.4. Discrete Lyapunov exponent of Rijndael

In addition to the analysis of the single transformations, the behavior of the whole Rijndael cipher has been studied.

We consider 16 bytes as a single block of length 128, which is represented as an integer. The computation of the Lyapunov exponent has been performed on 7000 iterations of the Rijndael map obtaining 87.04 as Lyapunov exponent value. The maximum value discrete Lyapunov exponents may have among all maps with $M = 2^{128}$ is 88.72.

6. Conclusions

In this work we have studied discrete Lyapunov exponent of the Rijndael block-cipher views as a dynamical system. We have computed its discrete Lyapunov exponent as well as the discrete Lyapunov exponent of the *ByteSub*, *ShiftRow* and *MixColumn* transformations. Our work indicated that strong chaos-based cryptographic algorithm should be formed by repeated products of two simple transformations: one having perfect nonlinearity (and smaller value of discrete Lyapunov exponent) and one having the largest possible value of the discrete Lyapunov exponent (and being almost linear function). Two questions which will be a subject of our future study are: what are the implications of our results to the Rijndael block-cipher and how to extend our results to the case of truly chaotic maps defined on the continuous phase space?

Acknowledgments

We are grateful to M. Sterjev for stimulating discussions. This research is supported in part by the NSF.

References

[1] G. Jakimovski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps," IEEE Trans. on Circuits and Systems, Part I, Vol. 48(2), 2001, pp. 163 – 169.

[2] L. Kocarev, "Chaos-Based Cryptography: a Brief Overview," (Invited paper), IEEE Circuits and Systems Magazine, Vol. 1(3), 2001, pp. 6 – 21.

[3] L. Kocarev and G. Jakimoski, "Unpredictable Pseudo-Random Bits Generated by Chaotic Maps," IEEE Trans. on Circuits and Systems, Part I, 2003.

[4] R. Tenny, L. S. Tsimring, L. Larson, and H. D. I. Abarbanel, "Using Distributed Nonlinear Dynamics for Public Key Encryption," Phys. Rev. Lett. **90**, 047903 (2003);

[5] R. Mislovaty, E. Klein, I. Kanter, and W. Kinzel, "Public Channel Cryptography by Synchronization of Neural Networks and Chaotic Maps," Phys. Rev. Lett. **91**, 118701 (2003);

[6] L. Kocarev, M. Sterjev, and P. Amato, "RSA encryption algorithm based on torus automorphism," Proceeding of ISCAS 2004, vol. IV, 2994, pp. 578 – 581.

[7] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Techn. J., Vol. 28, 1949, pp. 656–715.

[8] I.P. Cornfeld, S.V. Fomin and Ya. G. Sinai, *Ergodic Theory*. Springer Verlag, 1982.

[9] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudo-chaos," submitted for publication.

[10] L. Kocarev, J. Szczepanski, J. Amigo, C. Mitrovski, and P. Amato, "Discrete Chaos," submitted for publication.

[11] J. Daemen and V.Rijmen, "The Block Cipher Rijndael", in *Smart Card Research and Applications, LNCS 1820*, editors J.-J. Quisquater and B. Schneie, Springer-Verlag, 2000, pp. 288–296.

[12] J. Daemen and V. Rijmen, "Rijndael, the advanced encryption standard", Dr. Dobb's Journal, Vol. 26, March 2001, pp. 137–139