Discrete Lyapunov Exponent and Differential Cryptanalysis

G. Jakimoski and K. P. Subbalakshmi

***Abstract*—Partly motivated by the developments in chaos-based block cipher design, a definition of the discrete Lyapunov exponent for an arbitrary permutation of a finite lattice was recently proposed. We explore the relation between the discrete Lyapunov exponent and the maximum differential probability of a bijective mapping (i.e., an S-box or the mapping defined by a block cipher). Our analysis shows that "good" encryption transformations have discrete Lyapunov exponents close to the discrete Lyapunov exponent of a mapping that has a perfect nonlinearity. The converse does not hold.**

***Index Terms*—Block ciphers, chaotic maps, differential cryptanalysis, discrete chaos, Lyapunov exponent, maximum differential probability (DP).**

I. Introduction

RIGOROUSLY speaking, there is no chaos in a discrete phase space, and some of the chaotic properties are "lost" when the chaotic systems are studied using computer calculations. For instance, the aperiodicity of trajectories can not be captured by a computer model of the dynamical system, and the digital computers are incapable of showing the true long-time dynamics of some chaotic systems [1], [2]. However, due to the complexity of the studied phenomena, digital systems and computers have been often used in dynamical systems analysis, and vice versa, the chaotic behavior of digital systems and the applications of chaos in digital systems have been heavily addressed in the past years (e.g., [2]–[12]). Some of these applications of chaos such as compression, coding and encryption were recently used as a motivation to introduce the notion of discrete Lyapunov exponent [14]. In the case of a one-dimensional bijection $F: Z_M \rightarrow Z_M, Z_M = \{0, \ldots, M-1\}$, the discrete Lyapunov exponent is defined as

$$\lambda_F = \frac{1}{M} \sum_{i=0}^{M-1} \ln |F(c_i) - F(i)| \tag{1}$$

where c_i is $i+1$ if i is less than $M-1$, and $c_{M-1} = M-2$ (i.e., c_i is the neighbor of i). Analogous to its continuous counterpart, the discrete Lyapunov exponent tells us how far apart two neighboring points will get after one iteration of the map.

Differential cryptanalysis [15] is a general method of attacking block encryption algorithms. It exploits the predictability of the propagation of a chosen plaintext difference. The complexity of a differential cryptanalysis attack is determined by the maximum differential probability (DP): the higher the maximum DP the lower the complexity of the attack. In the case of a one-dimensional bijection $F: Z_M \rightarrow Z_M$, the maximum DP is defined as

$$\mathrm{DP}_F = \max_{\Delta x \neq 0, \Delta y} \frac{\#\{x \in Z_M | F(x + \Delta x) - F(x) = \Delta y\}}{M} \tag{2}$$

where '$+$' is addition modulo M, and '$-$' is addition with the inverse element.

We characterize the discrete Lyapunov exponent in terms of the maximum DP of a given map F. That is, we derive a lower bound and an upper bound on the discrete Lyapunov exponent of the map F given the size of the domain and the maximum DP of the map. We can use these bounds to identify a region where the discrete Lyapunov exponent of an encryption transformation with a given domain size M and good maximum DP (close to $2/M$) should belong.

The paper is organized as follows. In Section II, we derive a lower and upper bounds on the discrete Lyapunov exponent given the size of the domain and the maximum DP of the map. The security implications of the derived bounds are discussed in Section III. The paper ends with concluding remarks.

II. DP Characterization of the Discrete Lyapunov Exponent

Both, the maximum DP and the Lyapunov exponent are defined by the distribution of the output difference of a given map. While the discrete Lyapunov exponent is defined by the distribution of the output difference when the input difference is one, the maximum DP is a more general characteristic of the map, and it is defined by the distribution of the output difference for every nonzero input difference. We used this observation to provide the following bounds on the discrete Lyapunov exponent given the parameter M and the maximum DP.

Theorem 1: Let $F: Z_M \rightarrow Z_M$ $(Z_M = \{0, 1, \ldots, M-1\})$ be a bijection with $\mathrm{DP}_F \leq 1/2$. The following inequality holds for the discrete Lyapunov exponent λ_F of the map F

$$\rho \ln\left(\left\lfloor \frac{1}{\rho} \right\rfloor !\right) \leq \lambda_F \leq \rho \ln \frac{(M-1)!}{\left(M - \left\lceil \frac{1}{\rho} \right\rceil - 1\right)!} + \frac{1}{M}\ln(M-1)$$

where $\rho = 2\mathrm{DP}_F$.

Manuscript received August 28, 2006; revised November 20, 2006. This work was supported in part by the National Science Foundation under Grant NSF0627688. This paper was recommended by Associate Editor Z. Galias.

The authors are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030 USA (e-mail: goce.jakimoski@stevens.edu, ksubbala@stevens.edu).

Digital Object Identifier 10.1109/TCSII.2007.892214

Proof: We can rewrite the discrete Lyapunov exponent sum as

$$\lambda_F = \frac{1}{M}\sum_{\Delta y=1}^{M-1} n_{\Delta y}\ln\Delta y + \frac{1}{M}\ln|F(M-2)-F(M-1)|$$

where $n_{\Delta y} = \#\{x \in Z_M \setminus \{M-1\} | \Delta y = |F(c_x) - F(x)|\}$ is the number of occurrences of the output difference Δy (excluding the case $x = M-1$). The number of occurrences $n_{\Delta y}$ of any difference Δy is upper bounded by

$$\begin{aligned} n_{\Delta y} &= \#\{x \in Z_M \setminus \{M-1\} | F(c_x) - F(x) = \Delta y\} \\ &\quad + \#\{x \in Z_M \setminus \{M-1\} | F(c_x) - F(x) = -\Delta y\} \\ &\le 2\mathrm{DP}_F M = \rho M. \end{aligned}$$

Note that the sum $\sum_{\Delta y=1}^{M-1} n_{\Delta y}$ is equal to $M-1$ and constant for a given map. Hence, the discrete Lyapunov exponent is maximal when the number of occurrences of the largest differences is maximal. Similarly, the discrete Lyapunov exponent is minimal when the number of occurrences of the smallest differences is maximal. So, using the inequality

$$|F(M-2) - F(M-1)| \le M-1$$

and the fact that the number of occurrences $n_{\Delta y}$ is at most $\rho M = \lfloor \rho M \rfloor = \lceil \rho M \rceil$, we get

$$\begin{aligned} \lambda_F &\le \frac{1}{M}\sum_{\Delta y=M-\lceil 1/\rho \rceil}^{M-1} \rho M \ln\Delta y + \frac{1}{M}\ln(M-1) \\ &\le \rho\ln\frac{(M-1)!}{\left(M-\left\lceil\frac{1}{\rho}\right\rceil-1\right)!} + \frac{1}{M}\ln(M-1) \\ &\qquad\text{and} \\ \lambda_F &\ge \frac{1}{M}\sum_{\Delta y=1}^{\lfloor 1/\rho \rfloor} \rho M \ln\Delta y \ge \rho\ln\left(\left\lfloor\frac{1}{\rho}\right\rfloor !\right). \end{aligned}$$

■

The term $1/M\ln(M-1)$ in the upper bound is a result of the different definition of the neighbor of $M-1$ compared to the rest of the points. This term approaches zero when M goes to infinity, and often can be ignored for large values of M. For example, if we analyze a block cipher with block size 128, then the value of $1/M\ln(M-1)$ is $\approx 0.69 \times 2^{-121}$.

III. Security Implications of Discrete Lyapunov Exponent

The minimum achievable maximum DP of a given map $F : Z_M \to Z_M$ is $\mathrm{DP}_{\mathrm{opt}} = 2/M$ since there are M elements in Z_M and $M-1$ possible output differences. To simplify our analysis, we assume that M is a multiple of four.[1] In that case, we have

$$\left\lfloor\frac{1}{2\mathrm{DP}_{\mathrm{opt}}}\right\rfloor = \left\lceil\frac{1}{2\mathrm{DP}_{\mathrm{opt}}}\right\rceil = \frac{1}{2\mathrm{DP}_{\mathrm{opt}}} = \frac{M}{4}. \tag{3}$$

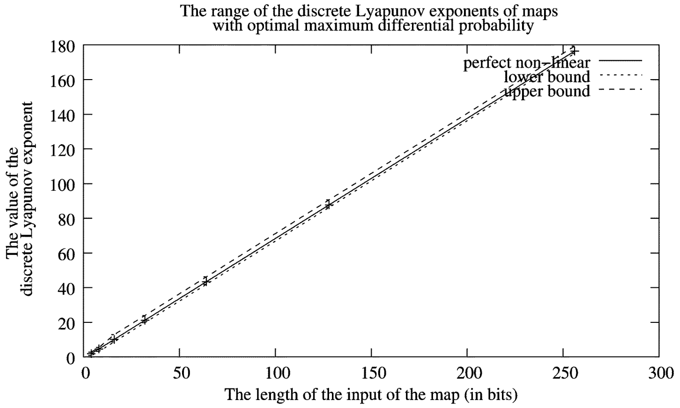

Fig. 1. Range of the discrete Lyapunov exponents of maps with optimal maximum DP. The lower and the upper bound of relation (4) tightly bound the discrete Lyapunov exponent of the perfect nonlinear maps too.

Using the bounds derived in the previous section, we see that *the discrete Lyapunov exponent for an optimal encryption mapping is in the following region:*

$$\frac{4}{M}\ln\left(\frac{M}{4}!\right) \le \lambda_F \le \frac{4}{M}\ln\frac{(M-1)!}{\left(\frac{3M}{4}-1\right)!} + \frac{1}{M}\ln(M-1). \tag{4}$$

Having an optimal maximum DP implies that for any nonzero input difference, the distribution of the output difference is close to uniform. A related concept, perfect nonlinearity, was defined in [14]. The map F has perfect nonlinearity if the differences $|F(i+1) - F(i)|, i = 0, 1, \ldots, M-2$ take all possible values $1, 2, \ldots, M-1$. The discrete Lyapunov exponent of a perfectly nonlinear map is

$$\lambda_{F_{\mathrm{non}}} = \frac{1}{M}\ln(M-1)! + \frac{1}{M}\ln|F(M-1) - F(M-2)|. \tag{5}$$

Using Stirling's formula,[2] it is not hard to see that for large M the lower and the upper bound in (4) are approximately $\ln(M/e) - 1.38$ and $\ln(M/e) + 1.86$ respectively, and the discrete Lyapunov of a perfectly nonlinear map is approximately $\ln(M/e)$. In other words, the good encryption mappings have discrete Lyapunov exponents close to the discrete Lyapunov exponent of a perfectly nonlinear map as depicted in Fig. 1. We can use this fact as a security test. Assume that F is the bijection defined by the block encryption algorithm for a given key. If one can determine the discrete Lyapunov exponent (see [16]), and the value of the discrete Lyapunov exponent is not close to the value of the discrete Lyapunov exponent of a perfectly nonlinear map, then there exist a differential whose probability is larger than $2/M$.

The next question that naturally comes up is whether a discrete Lyapunov exponent that is close to the discrete Lyapunov exponent of a perfectly nonlinear map implies good maximum DP. The answer is no. We demonstrate this using the perfectly nonlinear map given in [14]

$$\begin{aligned} &F_{\mathrm{non}}(x) \\ &= \begin{cases} k, & \text{if } x = 2k; \quad k = 0, \ldots, m-1 \\ M-1-k, & \text{if } x = 2k+1; \quad k = 0, \ldots, m-1 \end{cases} \end{aligned}$$

[1] Block ciphers operate on bit strings. So, the cardinality of the domains of the maps in use are powers of two.

[2] Stirling's formula $n! \approx \sqrt{2\pi n}\,(n/e)^n$ is a well-known formula that approximates $n!$ for large n.

where $M = 2m$. The discrete Lyapunov exponent of this map is $\lambda_{F_{\text{non}}} = 1/M \ln(M-1)!$ as pointed out in [14]. However, it is not hard to see that if the input difference is two, then the output difference is one (or minus one) in $m-1$ cases leading to a high DP $\text{DP}_{F_{\text{non}}} \geq (m-1)/M \approx 1/2$.

We end this section with the following generalization of our observation regarding the discrete Lyapunov exponent of maps with optimal maximal DP.

Corollary: Let $F : Z_M \rightarrow Z_M$, where $M = 2^m$, be a bijection with maximum DP $\text{DP}_F \leq 2^d/2^m \lll 1$. The following inequality holds for the discrete Lyapunov exponent λ_F of F

$$(m-d)\ln 2 - (1+\ln 2) \lessapprox \lambda_F \leq m \ln 2.$$

Proof: The upper bound follows trivially from the definition of discrete Lyapunov exponent. The lower bound is derived by replacing ρ with 2^{d+1-m} in the inequality of Theorem 1, and then using Stirling's formula to simplify the expression. The simplified expression is a good approximation even for relatively small values of $m-d$ (e.g., $m-d=5$ or 6.).

The previous result implies the following: if the discrete Lyapunov exponent of a given map is (significantly) lower than $(m-d)\ln 2$, then the maximum DP of the map is greater than $2^{-(m-d)}$. It is easy to show that the converse does not hold (e.g., using the aforementioned perfectly nonlinear map of [14]).

IV. Conclusion

We derive a relation between the maximum DP and the discrete Lyapunov exponent of a bijection. One can use this relation to determine, in some cases, whether a given block cipher is resistant to differential cryptanalysis or not.

References

[1] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurc. Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[2] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision," *Comput. Phys. Commun.*, vol. 153, no. 1, pp. 52–58, 2003.

[3] N. F. Pedersen and A. Davidson, "Chaos and noise rise in josephson junctions," *Appl. Phys. Lett.*, vol. 39, no. 10, pp. 830–832, 1981.

[4] C. A. Pickover, "Pattern formation and chaos in networks," *Commun. ACM*, vol. 31, no. 2, pp. 136–151, 1988.

[5] L. O. Chua and T. Lin, "Chaos in digital filters," *IEEE Trans. Circuits Syst.*, vol. 35, no. 6, pp. 648–658, Jun. 1988.

[6] T. Lin and L. O. Chua, "New class of pseudorandom generators based on chaos in digital filters," *Int J Circuit Theory Appl*, vol. 21, no. 5, pp. 473–480, 1993.

[7] G. Pérez and H. A. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, no. 11, pp. 1970–1973, 1995.

[8] K. Mischaikow and M. Mrozek, "Chaos in the lorenz equations: A computer-assisted proof," *Bull. Amer. Math. Soc.*, vol. 32, no. 1, pp. 66–72, 1995.

[9] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 45, no. 11, pp. 1129–1140, Nov. 1998.

[10] J.Černák, "Digital generators of chaos," *Phys. Lett. A*, vol. 214, pp. 151–160, 1996.

[11] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Mar. 2001.

[12] H. Berry, D. G. Pérez, and O. Temam, "Chaos in computer performance," *Chaos*, vol. 16, no. 1, 2006.

[13] M. Blank, "Discreteness and continuity in problems of chaotic dynamics," in *Translations of Mathematical Monographs*. Providence, RI: Amer. Math. Soc., 1997, vol. 161.

[14] J. Szczepanski, J. M. Amigo, and I. Tomovski, "Discrete chaos—I: Theory," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 6, pp. 1300–1309, Jun. 2006.

[15] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptolog.*, vol. 4, no. 1, pp. 3–72, 1991.

[16] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: From theory to practical algorithms," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 6, pp. 1341–1352, Jun. 2006.