Open access • Journal Article • DOI:10.1109/7384.963463

Chaos-based cryptography: a brief overview — Source link

Ljupco Kocarev

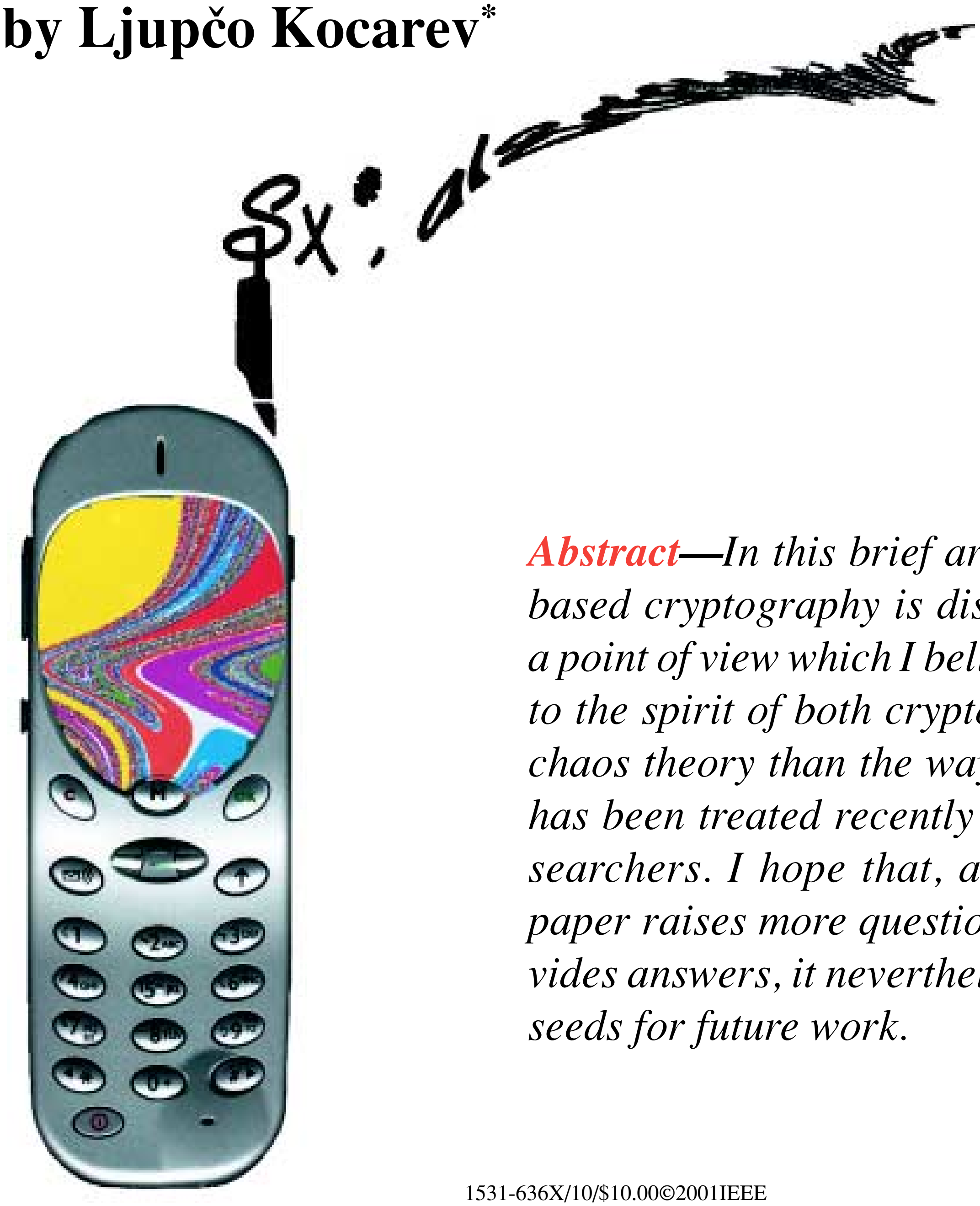
Institutions: University of California, San Diego

Published on: 01 Jan 2001 - IEEE Circuits and Systems Magazine (IEEE)

Topics: Butterfly effect, Chaos theory and Cryptography

Chaos-Based Cryptography: A Brief Overview

by Ljupčo Kocarev[*]



Abstract—*In this brief article, chaos-based cryptography is discussed from a point of view which I believe is closer to the spirit of both cryptography and chaos theory than the way the subject has been treated recently by many researchers. I hope that, although this paper raises more questions than provides answers, it nevertheless contains seeds for future work.*

1531-636X/10/$10.00©2001IEEE

Introduction

Over the past decade, there has been tremendous interest in studying the behavior of chaotic systems. They are characterized by sensitive dependence on initial conditions, similarity to random behavior, and continuous broad-band power spectrum. Chaos has potential applications in several functional blocks of a digital communication system: compression, encryption and modulation. The possibility for self-synchronization of chaotic oscillations [1] has sparked an avalanche of works on application of chaos in cryptography. An attempt only to mention all related papers on chaos and cryptography in this short presentation will result in a prohibitively long list; and, therefore, we refer the reader to some recent work [2]. Despite a huge number of papers published in the field of chaos-based cryptography, the impact that this research has made on conventional cryptography is rather marginal. This is due to two reasons:

- First, almost all chaos-based cryptographic algorithms use dynamical systems defined on the set of real numbers, and therefore are difficult for practical realization and circuit implementation.
- Second, security and performance of almost all proposed chaos-based methods are not analyzed in terms of the techniques developed in cryptography. Moreover, most of the proposed methods generate cryptographically weak and slow algorithms.

Cryptography is generally acknowledged as the best method of data protection against passive and active fraud [3]. An overview of recent developments in the design of conventional cryptographic algorithms is given in [4]. The main conclusion of the paper can be summarized in the following quote:

> *"It is quite clear that someone with a good understanding of present day cryptanalysis can design secure but slow algorithms with very little effort:*
>
> *For a block cipher, it is sufficient to define a round function based on a nonlinear operation (avoid linear rotations) and a simple mixing component (to spread local changes); add round keys in between the rounds (and at the beginning and the end of the cipher), which are derived in a complex way from the key (e.g., by using the block cipher itself with fixed round keys). If the number of rounds is 32, or even better 64, breaking this slow cipher will be very difficult. (Of course it is possible to follow this "recipe" and to come up with a weak cipher, but this will require some cryptographic skills!)."*

Unfortunately many researchers in chaos-based cryptography, while rushing to publish a novel cryptographic algorithm, do not follow the above recipe and come up, although without any cryptographic skills, with *both weak and slow ciphers*. For example, in an algorithm proposed in [5] each character of the message is encrypted as the integer number of iterations per-

* This work was supported in part by the ARO (grant DAAG55-98-1-0269, MURI Project "Digital Communication Devices Based on Nonlinear Dynamics and Chaos"), by the DOE (grant DE-FG03-95ER14516), and by ST Microelectronics.

The author is with the Institute for Nonlinear Science, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0402. E-mail: lkocarev@ucsd.edu.

formed in the logistic equation. This results in a weak and slow cipher. Indeed, while in conventional cryptographic ciphers the number of rounds (iterations) performed by an encryption transformation is usually less than 32, in [5] this number can be as large as 65536, and is always larger then 250. On the other hand the algorithm is also weak: it can be easily broken using known-plaintext attack [6].

The author of this note strongly believes that the research on chaos-based cryptography should be shifted from the *ad hoc* design of algorithms that are usually weak and slow, and therefore not comparable with conventional algorithms, toward better understanding of possible relationships between chaos and cryptography. Many fundamental concepts in chaos theory such as mixing, measure preserving transformations and sensitivity have been already applied for a long time in cryptography. Almost 15 years before the dawn of chaos, Shannon in his masterpiece wrote [7]:

> *"Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc. . . .*
>
> *In a good mixing transformation . . . functions are complicated, involving all variables in a sensitive way. A small variation of any one (variable) changes (the outputs) considerably."*

A deep relation between chaos and cryptography has not been established yet. An important difference between the two scientific areas lies in the fact that the systems used in cryptography work on a finite set, while those applied in chaos have meaning only on a continuum. The main aim of this short communication is to discuss possible connections between chaos and cryptography and to point out some directions for future research.

Preliminaries

We assume that the reader is familiar with chaos theory[†]. In order to make this paper self-contained we now briefly describe three most common cryptographic objects (called also primitives): block-encryption algorithms (private-key algorithms), pseudo-random number generators (additive stream ciphers) and cryptographic hash functions. The complete description of these primitives and their properties can be found in [4].

Block ciphers transform a relatively short string (typically 64 or 128 bits) to a string of the same length under control of a secret key. A block-encryption algorithm is usually written in the form of a mapping $x_{n+1} = E(x_n, z)$, $n = 0, \ldots, k-1$, where the plaintext x_0, the cryptogram x_k and the secret key z are sequences of letters in finite alphabets. The advantage of block ciphers is that they form a flexible tool that can be used in cryptography: they can be used to construct other primitives.

A pseudo-random number generator is a deterministic method, usually described with a mapping, to produce from a small set of "random" numbers, called the seed, a larger set of random-looking numbers called pseudo-random numbers. The pseudo-random

[†] *Editor's comment*: See "Nonlinear Dynamics of Discrete-Time Electronic Systems" by Orla Feely, March 2000 *IEEE CAS Newsletter*, http://www.nd.edu/~stjoseph/newscas.

number generator is cryptographically secure if, given the mapping that defines the generator and an arbitrary sequence of numbers generated by the generator, but not knowing the seed of the generator, it is hard to compute the next and the previous numbers in the sequence.

A one-way function H operates on an arbitrary-length pre-image message M and returns a fixed-length value, h, $h = H(M)$, such that given M it is easy to compute h, given h it is hard to compute M, and it is hard to find two different inputs with the same hash result. Note that the above definitions are only informal and to some level useless without defining the word "hard". This may be related to the question of when a cryptographic object is secure which at popular level is discussed in the section *Cryptography from an Information-Theory Point of View*. However, we should stress that primitives which are probable secure (based on some reasonable assumptions) are several orders of magnitude slower than the fastest algorithms currently in use.

Figure 1 summarizes similarities and differences between chaotic maps and cryptographic algorithms. Chaotic maps and cryptographic algorithms (or more generally maps defined on finite sets) have some similar properties: sensitivity to a change in initial conditions and parameters, random-like behavior and unstable periodic orbits with long periods. Encryption rounds of a cryptographic algorithm lead to the desired diffusion and confusion properties of the algorithm. Iterations of a chaotic map spread the initial region over the entire phase space. The parameters of the chaotic map may represent the key of the encryption algorithm. An important difference between chaos and cryptography is that encryption transformations are defined on finite sets, while chaos has meaning only on real numbers. Moreover, for the time being, the notions of cryptographic security and performance of cryptographic algorithms have no counterpart in chaos theory.

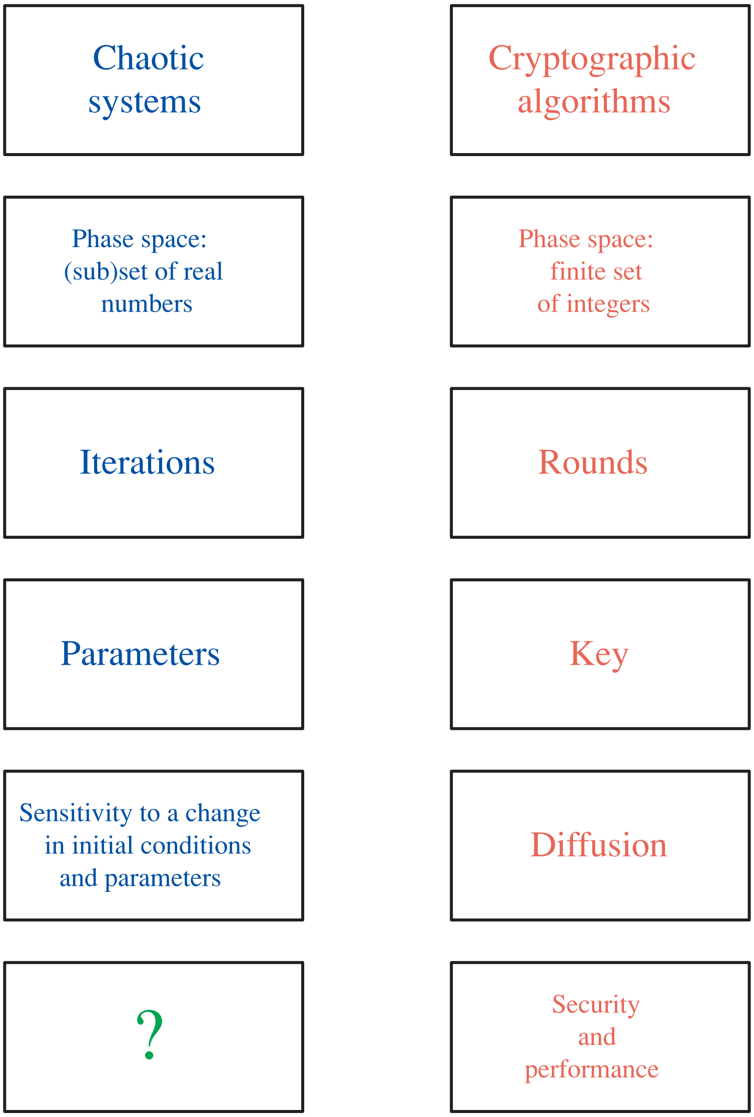
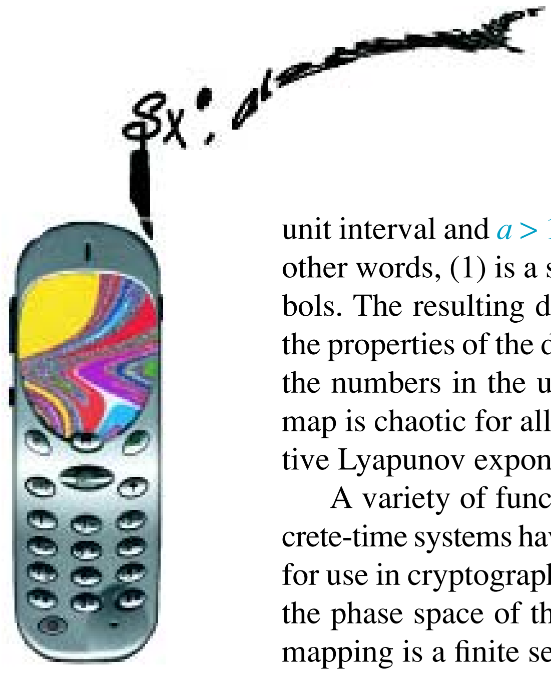

Chaotic systems
Cryptographic algorithms
Phase space: (sub)set of real numbers
Phase space: finite set of integers
Iterations
Rounds
Parameters
Key
Sensitivity to a change in initial conditions and parameters
Diffusion
?
Security and performance

Figure 1. Similarities and differences between chaotic systems and cryptographic algorithms.

We now illustrate with two simple examples the similarities and differences between chaotic systems and maps defined on finite sets. As an example of a chaotic map we consider the shift map,

$$x(t+1) = ax(t) \pmod 1 \tag{1}$$

where the phase space $X = [0, 1]$ is the



unit interval and $a > 1$ is an integer. In other words, (1) is a shift over a symbols. The resulting dynamics mirrors the properties of the digits in base a of the numbers in the unit interval. The map is chaotic for all $a > 1$ with positive Lyapunov exponent.

A variety of functions and/or discrete-time systems have been proposed for use in cryptography: in all of them the phase space of the corresponding mapping is a finite set of integers and all the parameters are integers. The simplest example is the discrete phase-space version of the shift map (1):

$$p(t+1) = ap(t) \quad (\text{mod N}) \tag{2}$$

where $a > 1$, N, and p are integers, and $p \in \{0, 1, \ldots, N-1\}$. If N is coprime to a the map (2) is invertible; note that the shift map (1) is not invertible for all a. All trajectories in finite phase space dynamical systems are eventually periodic. Therefore, one may introduce the *period functions* P_N to characterize the least period of the map F, that is F^{P_N} is identity and P_N is minimal, as a function of the system size N. As a rule, these functions are among the most complex objects found in discrete-time dynamical systems with finite set phase space. To show this we consider, as an example, the map (2), with $a = 2$. P_N has two extreme values, the smallest being $[\log \log N] + 1$, which occurs for $N = 2^k - 1$, and the largest $\text{N} - 1$, which occurs for prime values of N and for which 2 is a generator of the multiplicative group $U(N)$. However, the main question remains what is the typical value of P_N. The answer is unknown and is related to a class of number theoretical problems, centered around the so-called *Artin's conjecture* (see [8] and references therein). Computing typical values of some quantity calls for ergodic theory. This example shows the difficulties in developing an ergodic theory of finite phase space dynamical systems. On the other hand, the ergodic theory of the map (1) is much simpler.

The Lyapunov exponent (LE) of the system (2) is trivially equal to 0, because every orbit is eventually periodic and will repeat itself. Therefore, the central problem here is to estimate LE of a typical orbit for time not exceeding its period. The analysis of periodic orbits depends crucially on the ordering with which the orbits are considered. Two orderings, both corresponding to Lebesgue measure, are considered in the literature: ordering according to the system size N, and ordering according to the minimal period P_N and then lexicographically within the same period. In the case of the map (2), with $a = 2$, two different orderings lead to two opposite answers: ordering by system size yields logarithmic compressibility of information and zero finite-time LE (or lack of randomness) [9], while ordering by the minimal period leads to positive finite-time LE and randomness [8].

Choosing a Chaotic Map

Dynamical systems with chaos seem to be good candidates for encryption algorithms. Indeed, because

Two general principles which guide the design of practical algorithms are *diffusion* and *confusion*. Diffusion means spreading out of the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext. An extension of this idea is to spread the influence of a single key digit over many digits of ciphertext. Confusion means use of transformations which complicate dependence of the statistics of ciphertext on the statistics of plaintext.

block-encryption algorithms can be rewritten as discrete-time dynamical systems, $x_{n+1} = F(x_n)$ where the initial condition x_0 is plain-text to be encrypted, and the final state x_k is a ciphertext, then it is the property of the map being chaotic that implies "spreading out of the influence of a single plaintext digit over many ciphertext digits". To ensure a complicated structure of trajectories of the dynamical system proposed for an encryption algorithm, we postulate that, except being chaotic, the system should be mixing (more precisely K-mixing). Moreover, to ensure that the parameters of the system can be used as encryption keys, we postulate that the system has robust chaos, that is, the system is chaotic for a large set of parameters. We now explain the effect of K-mixing and robust chaos on encryption.

Two general principles which guide the design of practical algorithms are *diffusion* and *confusion*. Diffusion means spreading out of the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext. An extension of this idea is to spread the influence of a single key digit over many digits of ciphertext. Confusion means use of transformations which complicate dependence of the statistics of ciphertext on the statistics of plaintext. The mixing property of chaotic maps is closely related to the property of diffusion in encryption transformations (algorithms). The system $\mathbf{F}$ possesses the *mixing property* (or simply, is mixing), if for any two measurable sets A_1 and A_2, we have $\lim_{n \to \infty} \mu(\mathbf{F}^{-n} A_1 \cap A_2) = \mu(A_1)\mu(A_2)$ [10]. In other words, any set of initial conditions of nonzero measure will eventually spread over the whole phase space as the system evolves [10]. If we think of the set of possible (sensible) plaintexts as an initial region in the phase space of the map (transformation), then it is the mixing property (or in other terms, sensitivity to initial conditions) that implies "spreading out of the influence of a single plaintext digit over many ciphertext digits".

Mixing systems have also the following useful property [10]: if μ_0 is arbitrary measure (normalized and absolutely continuous with respect to μ), and $\mu_n = \mu_0(\mathbf{F}^{-n} A)$, then $\mu_n(A) \to \mu(A)$ for any measurable A. Thus we can say that in dynamical systems with the mixing property, any non-equilibrium distribution tends to an equilibrium. In other words, in the limit when the

Chaos-Based Cryptography: A Brief Overview

number of iterations tends to infinity, the statistics of the ciphertext (computed through the invariant measure) *do not depend* on the statistics of the plaintext (which correspond to the initial region in the phase space of the map).

A good encryption algorithm spreads also the influence of a single key digit over many digits of ciphertext. The keys of an encryption algorithm represent its parameters. Therefore, we should consider only such transformations in which both parameters and variables are involved in a sensitive way, that is "a small variation of any one" (variable, parameter) "changes the outputs considerably". In other words, a kind of "mixing property" should hold also in the parameter space of the map, if we would like to use chaotic maps as encryption algorithm. This implies that we consider only the maps for which chaos is persistent under small perturbations of parameters (keys).

A dynamical system is structurally stable when small C^1 perturbations yield a topologically equivalent system. In another words, a structurally stable or robust system retrains its qualitative properties under small perturbations. Robust or structurally stable chaotic attractors can, eventually, ensure the diffusion property in the key space. Algorithms based on non-robust systems may have weak keys. However, the majority of chaotic attractors are structurally unstable [11]. Therefore, one should take great caution in choosing chaotic maps. It is known that robust chaos cannot occur in smooth systems, while structurally stable chaos can occur in piece-wise smooth maps [12].

One should consider only systems that have robust chaos for a *large* set of parameters (keys). The entropy of a crypto-system is the measure of the size of the key-space and is usually approximated by $\log_2 K$, where K is the number of keys. Therefore, a larger parameter space of the dynamical system implies that its discretized version will have larger K.

Chaos from an Information-Theory Point of View

Chaos theory, as a branch of the theory of nonlinear dynamical systems, has brought to our attention a somewhat surprising fact: low-dimensional dynamical systems are capable of complex and unpredictable behavior. What is the origin of chaos in deterministic systems?

For simplicity we consider here a discrete-time dynamical system defined by iteration of the function $F: \mathcal{X} \to \mathcal{X}, \mathcal{X} \subseteq R^N$. The set of points $\{\boldsymbol{x}, F(\boldsymbol{x}), F^2(\boldsymbol{x}), \dots\}$ is called a trajectory (or orbit) of the initial condition $\boldsymbol{x}$. We assume that F has a chaotic attractor. Informally, an attractor is called chaotic if the motion on it is unpredictable: two nearby states on the attractor have different and unrelated behavior within the attractor.

The evolution of a deterministic system is completely determined by the vector field F and the initial condition $\boldsymbol{x}$. However, to specify completely the initial condition an infinite

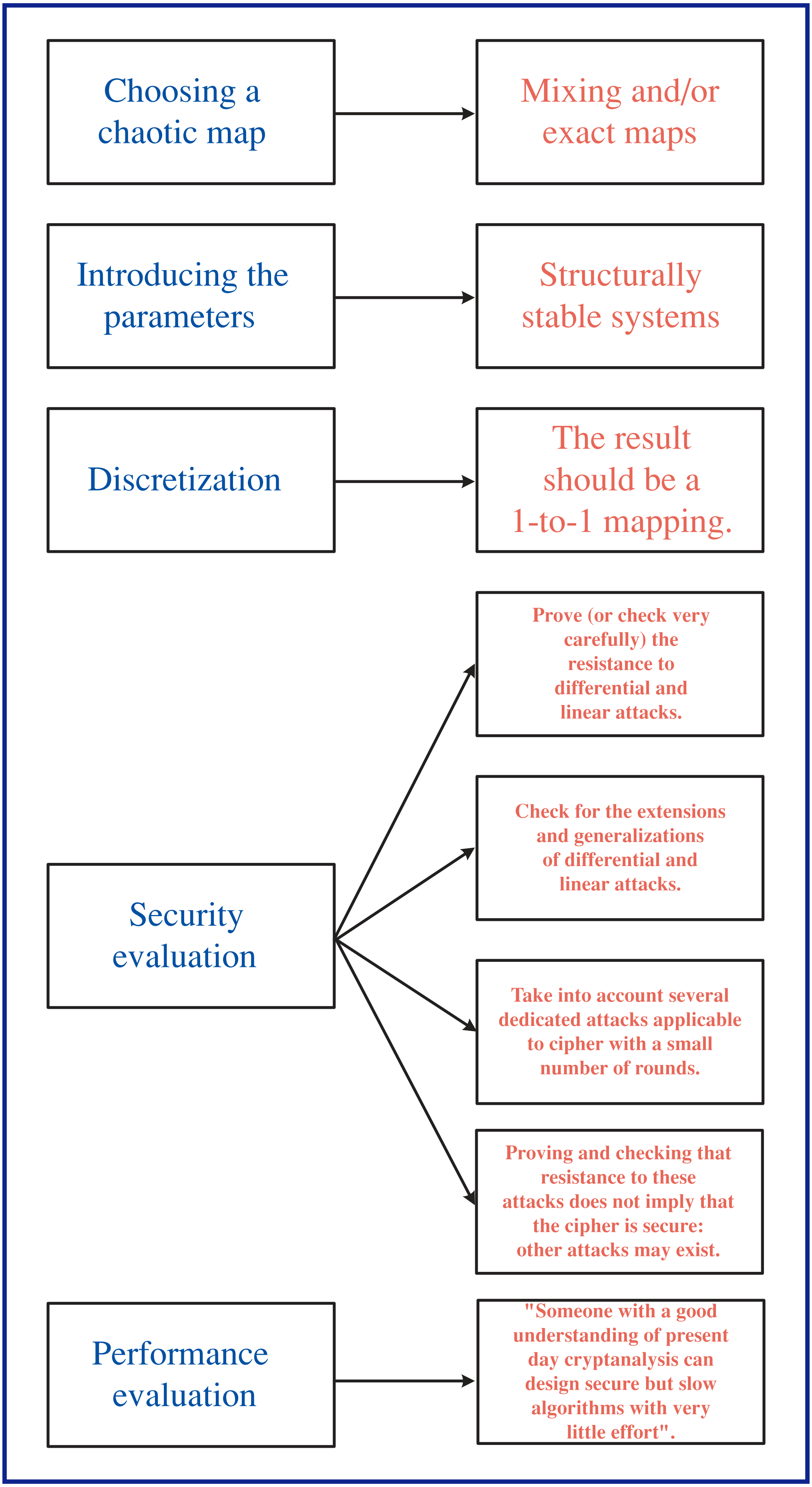

Choosing a chaotic map
Mixing and/or exact maps
Introducing the parameters
Structurally stable systems
Discretization
The result should be a 1-to-1 mapping.
Prove (or check very carefully) the resistance to differential and linear attacks.
Check for the extensions and generalizations of differential and linear attacks.
Security evaluation
Take into account several dedicated attacks applicable to cipher with a small number of rounds.
Proving and checking that resistance to these attacks does not imply that the cipher is secure: other attacks may exist.
Performance evaluation
"Someone with a good understanding of present day cryptanalysis can design secure but slow algorithms with very little effort".

Figure 2. A procedure for a design of a chaos-based block-encryption algorithm.

amount of information and a measuring system with an infinite precision are required, which are both intractable. What are the effects of a measuring system's finite precision? Measuring an initial (and future) state is equivalent to partitioning the state space into a finite number of regions, and observing the evolution in this macroscopic world. Any set of a finite number of disjoint regions which cover the state space is called a partition of the system. The process of partitioning the state space, assigning symbols to every region from the partition, and the resulting macroscopic dynamics are called symbolic dynamics.

If the system is chaotic, then different initial states belonging to the same region will produce different observations at some later time. From the viewpoint of our measuring system, identical macroscopic initial states evolve differently. A loss of determinism occurred, and transitions between the regions of the partition can only be specified by means of probabilities. Partitioning of the state space turns the deterministic chaotic system into an ergodic information source which can be analyzed in terms of information theory. The Kolmogorov-Sinai entropy (denoted by h_{KS}) is the measure of asymptotic rate of creation of information by iterating F. Systems with positive entropy are usually considered as chaotic. The unpredictability of chaotic trajectories is caused by exponential separation of nearby points. Unpredictability means uncertainty; therefore, one should expect that the entropy of a dynamical system is related to its positive Lyapunov exponents. This deep mathematical result (known as the Pesin theorem [13]) is rigorously proven only for so called Sinai-Ruelle-Bowen measure.

From the viewpoint of any measuring device, if the dynamical system produces unpredictable sequences, then the dynamical system is called chaotic. While the motion of the dynamical system in the continuous (microscopic) state space is deterministic, its motion in the partitioned (macroscopic) space is stochastic and the trajectories are sequences of symbols. On the basis of the knowledge of the past coarse-grained trajectory of the system we can predict its future macroscopic states only in probabilistic terms. Turning a deterministic chaotic system into an information source via partitioning of the state space is not in collision

Ljupčo Kocarev is associate research scientist at the Institute for Nonlinear Science at the University of California, San Diego. He has been working in all aspects of nonlinear sciences since 1986. He is now interested in relationships between chaos theory, coding theory, and cryptography. L. Kocarev has authored more than 60 journal articles in various international journals, including *Chaos: An Interdisciplinary Journal of Nonlinear Science*; *Chaos, Solitons, and Fractals*; *Geophysical Research Letters*; *International Journal of Bifurcation and Chaos*; *International Journal of Circuit Theory and Application*; *IEEE Transactions on Circuits and Systems, Part I: Fundamental Theory and Applications*; *IEEE Transactions on Circuits and Systems, Part II: Analog and Digital Signal Processing*; *IEICE Transactions on Fundamentals and Electronics, Communications and Computer Science*; *Journal of Applied Mathematics and Mechanics*; *Journal of Circuits, Systems and Computers*; *Journal of Physics A: Mathematical and General Physics*; *Journal of the Franklin Institute*; *Physica D*; *Physical Review E*; *Physical Review Letters*; and *Physics Letters A*.

The publication in 1949 by C. E. Shannon of the paper “Communication Theory of Secrecy Systems” [7] ushered in the era of *scientific secret-key cryptography*. Shannon provided a theory of secrecy systems almost as comprehensive as the theory of communication that he had published a year before. Indeed, he built his 1949 paper on the foundation of the 1948 one, which had established the new discipline of information theory [14].

with Shannon’s note [14] that a deterministic system cannot generate information. Actually, a chaotic system does not generate information, that is, its evolution is completely determined by its initial state. A chaotic system merely converts the information about its initial state into a form which is visible to the measuring system. Every letter in the coarse-grained trajectory, which is a sequence of letters, brings an additional amount of information about the initial state.

The word *random* in deterministic dynamical systems is linked to incompressibility of information: a trajectory of the system is termed random when the shortest program that generates it has (essentially) the same size as the trajectory itself. The trajectory of a point $\boldsymbol{x}$ is called random if its algorithmic complexity is positive. The following theorem is of essential significance in this case [15]: For chaotic systems the trajectories of almost all state points $\boldsymbol{x} \in \mathcal{X}$ are random and their algorithmic complexity is equal to the Kolmogorov-Sinai entropy h_{KS}. As a disturbing consequence, no finite computer program can produce or predict a chaotic trajectory, or in the language of Joseph Ford [16], for any additional bit of the initial state, a computer program can output only one additional bit about the chaotic trajectory.

Clearly, positive algorithmic complexity of almost all initial states does not suffice for the randomness of trajectories of a dynamical system; for example a dynamical system with a stable equilibrium would contradict such a conjecture. What is the source of the unpredictability and information generation of a chaotic behavior? The finite precision of any real measuring system and the sensitive dependence of a chaotic evolution to a change in initial states combine to an inability for long-term prediction of chaotic behavior.

Hopefully, this section resolves the juxtaposition of three seemingly contradictory terms: “random”, “deterministic” and “chaos”. Determinism of the defining equations implies existence and uniqueness of solutions, but it does not imply computability of solutions. Chaoticity of the behavior implies random trajectories that are not computable by any finite computer program. More on this relationship can be found in the inspired papers by Joseph Ford [16, 17].

Cryptography from an Information-Theory Point of View

Cryptography has come to be understood to be the science of secure communication. The publication in 1949 by C. E. Shannon of the paper “Communication Theory of Secrecy Systems” [7] ushered in the era of *scientific secret-key cryptography*. Shannon provided a theory of secrecy systems almost as comprehensive as the theory of communication that he had

However, Shannon's 1949 paper did not lead to the same explosion of research in cryptography that his 1948 paper had triggered in information theory. The real explosion came with the publication in 1976 by W. Diffie and M. E. Hellman of their paper, "New Directions in Cryptography" [18]. Diffie and Hellman showed for the first time that secret communication was possible without any transfer of a secret key between sender and receiver, thus establishing the turbulent epoch of *public-key cryptography*.

published a year before. Indeed, he built his 1949 paper on the foundation of the 1948 one, which had established the new discipline of information theory [14]. However, Shannon's 1949 paper did not lead to the same explosion of research in cryptography that his 1948 paper had triggered in information theory. The real explosion came with the publication in 1976 by W. Diffie and M. E. Hellman of their paper, "New Directions in Cryptography" [18]. Diffie and Hellman showed for the first time that secret communication was possible without any transfer of a secret key between sender and receiver, thus establishing the turbulent epoch of *public-key cryptography*. Moreover, they suggested that computational complexity theory might serve as a basis for future research in cryptography. Another line of research was established by A. C. Yao in 1982 [19] in such a way as to preserve the original Shannon's information-theory based approach to cryptography.

What is information? The amount of *randomness in a probability distribution* is measured by its entropy (or information) which for a discrete probability distribution P is

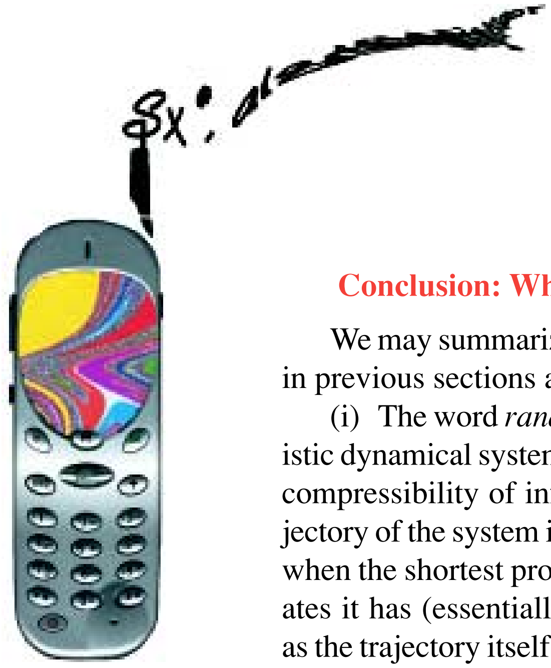
$$H(P) = -\sum p(x) \log p(x)$$

where x runs over the atoms of P. In a fundamental sense, the concept of information proposed by Shannon in his 1948 paper captures only the case when unlimited computing power is available. However, computational cost may play a central role in cryptography, and, therefore, the classical information theory may not provide a complete framework for the analysis of cryptographic algorithms. After Diffie and Hellman proposed the use of a trapdoor function as the cornerstone for a new form of cryptography, this deficiency was practically dramatized. Indeed, it may happen that although the ciphertext contains all the information about the plaintext, this information is *inaccessible*, and therefore cannot be efficiently computed. Thus, the question in the beginning of this paragraph should be replaced with: What is accessible information? Can two successful theories, namely Information Theory and Computational Complexity Theory, be combined to capture the notion of accessible information? A. C. Yao in 1982 provided the affirmative answer to this question. Yao proposed the definition of *computationally accessible* information and used it to discuss security for conventional cryptosystems, pseudo-random number generators, and trapdoor functions, subjects where information and computational complexity are closely intertwined.

The central question in cryptography is security. The basic properties characterizing a secure object are "randomness-increasing" and "computationally unpredictable". It is well known that, if one of the following objects exist—a secure pseudo-random number generator, a secure one-way function, and a secure block encryption algorithm—then all exist. The rigorous definitions for "randomness-increasing" and "computationally unpredictable" are far beyond the scope of this paper and we refer the reader to [19]. The following informal definitions of "randomness-increasing" and "computationally unpredictable" are adopted from Largarias [20] and Blum, Blum and Shub [21]. Without loss of generality, in the following we consider only pseudo-random number generators. A pseudo-random bit (or number) generator is a deterministic method (usually defined as a mapping $G : M_1 \rightarrow M_2$, where M_i are finite sets) to produce from a small set of random bits (called the seed) a larger set of random-looking bits (called pseudo-random bits). The notion of randomness-increasing is impossible in classical information theory because any deterministic mapping G applied to a discrete probability distribution P never increases entropy, i.e., $H(G(P)) \leq H(P)$. However, this may be possible when computer power is limited. Indeed, what may happen is that $G(P)$ may approximate a target distribution Q having a much higher entropy so well that, within the limits of computing power available, one cannot tell the distributions $G(P)$ and Q apart. If $H(Q)$ is much larger than $H(P)$, then we can say G is *computationally randomness-increasing*.

Yao [19] provided the basic insight on the nature of cryptographically secure objects: it is the notion of *computationally unpredictable*. The following informal definition of computationally unpredictable is due to Blum, Blum and Shub [21]. We say that a pseudo-random number generator is *polynomial-time unpredictable* if and only if for every finite initial segment of a sequence that has been produced by such a generator, but with any element deleted from that segment, a probabilistic Turing machine cannot, roughly speaking, do better in guessing in polynomial time what the missing element is, than by flipping a fair coin. Yao proved that a pseudo-random number generator is secure if and only if it is polynomial-time unpredictable.

The central unsolved question in the theory outlined above is whether a secure object exists. A major difficulty in settling the existence problem for this theory is summarized in the following heuristic unpredictability paradox [19]: *If a deterministic function is unpredictable, then it is difficult to prove anything about it, in particular, it is difficult to prove that is unpredictable*. Most of the results about unpredictability and cryptographic security follow from certain assumptions concerning the intractability of certain number-theoretical problems by probabilistic polynomial-time procedures. For example, the statement that the $x^2 \bmod N$ generator is unpredictable is proven under the so called quadratic residuacity assumption; see [21] for details.



Conclusion: What Is Next?

We may summarize our discussion in previous sections as follows.

(i) The word *random* in deterministic dynamical systems is linked to incompressibility of information: a trajectory of the system is termed random when the shortest program that generates it has (essentially) the same size as the trajectory itself. Determinism of the defining equations implies existence and uniqueness of solutions, but it does not imply *computability* of solutions. *Chaoticity* of the behavior implies random trajectories that are not computable by any finite computer program.

(ii) The amount of *randomness in a probability distribution* is measured by its entropy. A deterministic mapping applied to a discrete probability distribution never increases entropy. However, a *computationally randomness-increasing* deterministic mapping has the property that when computer power is limited it may increase the entropy of the distribution within the limits of computing power available. Equivalently we may say that this mapping generates *computationally unpredictable* sequences of numbers.

A deterministic mapping defined on a (sub)set of real numbers may have chaotic behavior; in this case the mapping is *computationally unpredictable*: a trajectory of the system is not computable by any finite computer program. A deterministic mapping defined on a finite set is always predictable: all its trajectories are eventually periodic. However, it may happen that when computer power is limited the mapping is *computationally unpredictable*: a probabilistic Turing machine cannot do better in guessing in polynomial time what is the next (previous) state of the trajectory, than by flipping a fair coin. *Whether and under what conditions these two different properties of being computationally unpredictable can be related to each other is a central problem of chaos-based cryptography*. The future impact chaos-based cryptography may have on conventional cryptography depends strongly on the successful solution of this problem. A good cryptographic algorithm offers an optimal trade-off between security and performance. Therefore, *another important problem in chaos-based cryptography is whether chaos can offer improvements to the performances of cryptographic algorithms*. In closing this paper, more detailed descriptions of the problems that are of importance for the future research on chaos-based cryptography will be offered.

- *Chaos and security*—Chaos is a necessary but not sufficient property of encryption algorithms. In accordance with Shannon's prescriptions [7], every encryption algorithm possesses properties of confusion, diffusion, mixing and sensitivity to changes in plaintext and secret key. This almost guarantees that an extension of the domain of an encryption algorithm from a lattice to a continuum will give rise to a chaotic map. We have done the domain ex-

What is information? The amount of *randomness in a probability distribution* is measured by its entropy (or information) which for a discrete probability distribution P is

$$H(P) = -\sum p(x) \log p(x)$$

where x runs over the atoms of P. In a fundamental sense, the concept of information proposed by Shannon in his 1948 paper captures only the case when unlimited computing power is available. However, computational cost may play a central role in cryptography, and therefore the classical information theory may not provide a complete framework for the analysis of cryptographic algorithms.

tension for the round function of the international data encryption algorithm (IDEA) [22, 23], and have numerically confirmed that the newly obtained map is chaotic. A linear interpolation between the points of the lattice was used to extend definition of the round function to the continuum. The other way around, if a nonlinear map is chaotic when defined on a continuum, then it will exhibit properties of confusion, diffusion, mixing, and sensitivity to changes in variables. However, in addition a good encryption algorithm must also be irreducible to any other (simpler) form which makes its cryptanalysis tractable. An excellent example is IDEA whose basic designing principle is the usage of three different algebraic groups: XOR, addition modulo 2^{16} and multiplication modulo $2^{16} + 1$. The groups are not mutually isomorphic, which Lai and Massey, the authors of IDEA, employ to prove that it is impossible to reduce IDEA to a simpler form [22, 23]. Therefore, sensitivity to changes in initial conditions and parameters, and the mixing property of a chaotic map do not guarantee that its discrete version is a good cryptoalgorithm. *It is a must that one proves its cryptographic security*. At present, the notion of cryptographic security has no counterpart in chaos theory, and the cryptographic security of a chaos-derived encryption algorithm can be checked only by means of crypto-tools.

Chaotic systems are characterized by positive Lyapunov exponent, positive entropy and positive algorithmic complexity. On the other hand, mappings and/or discrete-time systems that have been proposed for use in cryptography are defined on finite sets of integers. In such systems, the largest Lyapunov exponent and the complexity of an infinite sequence is trivially equal to 0, because every orbit is eventually periodic and will repeat itself. Therefore, the central problem here is to estimate the properties (LE, entropy, complexity and so on) of a typical orbit for time not exceeding its period. The questions one should try to answer are: What is the impact of these properties on the security of the cryptographic algorithms? When and under what conditions is a deterministic

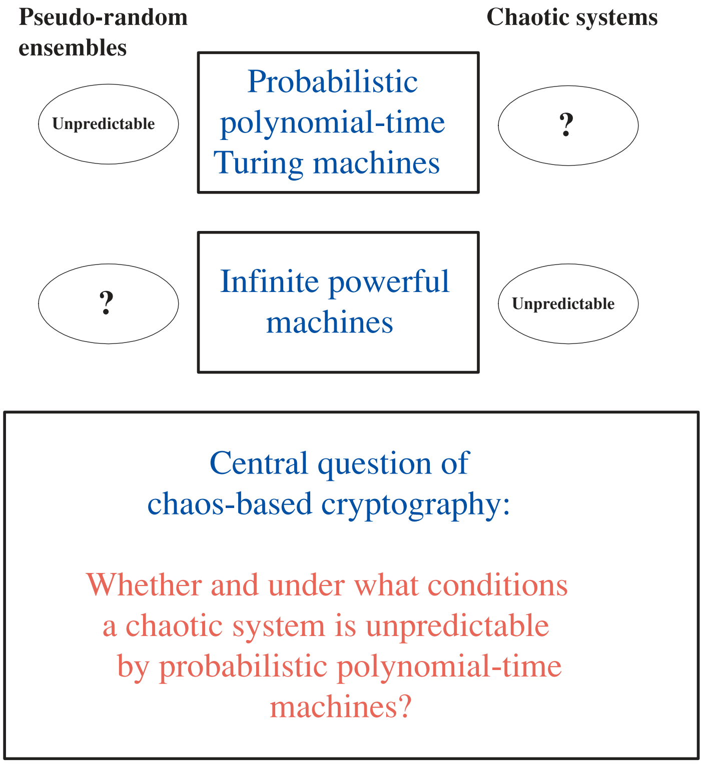

Pseudo-random ensembles
Chaotic systems
Unpredictable
Probabilistic polynomial-time Turing machines
?
?
Infinite powerful machines
Unpredictable
Central question of chaos-based cryptography:
Whether and under what conditions a chaotic system is unpredictable by probabilistic polynomial-time machines?

Figure 3. Pseudo-random ensembles are unpredictable by probabilistic polynomial-time machines, but may or may not be predictable by infinite powerful machines. Chaotic systems are unpredictable by infinite powerful machines (analog computers), but may or may not be predictable by probabilistic polynomial-time machines.

mapping computationally randomness-increasing? Can the property of being secure be expressed in terms of the known properties from chaos theory?

- *Chaos and performance*—A good cryptographic algorithm offers an optimal trade-off between security and performance. *"It is quite clear that someone with a good understanding of present day cryptanalysis can design secure but slow algorithms with very little effort"*. The properties of chaotic systems are asymptotic ones, however the cryptographic algorithms usually are built on very rapid diffusion and/or confusion properties.

One may numerically verify the diffusion property of an algorithm in a simple way: after how many iterations (rounds) is a small cloud of initial points (plaintext) spread uniformly through the whole space such that the average number of zeros (or ones) in the block of $2p$ bits is p. This number gives the strength of the diffusion property in an algorithm in a similar way that LEs measure the strength of the chaos in continuous systems. Do there exist measures for the confusion? What are the properties of chaotic systems relevant for the performance of cryptographic algorithms? Can chaos theory gain insight into the theory of designing cryptographic algorithms? The main questions to be addressed by a designer of cryptographic algorithms, including also chaos-based cryptographic algorithms, are: what is the most efficient way to design an algorithm for a particular environment, or, on which type of processor is a particular cipher more efficient than other ciphers?

- *A continuous model of cryptography*—A central assumption in computer science is that the Turing-machine model is an appropriate model of a digital computer and computer simulation. However, it was recently argued that another model of computation based on real numbers [24, 25] is also appropriate and in some cases more useful as a model of a computer. Both models are, of course, abstractions (The Turing machine employs a type of unbounded, infinite length, while it takes an infinite number of bits to represent a single real number). It seems to me that it is also appropriate, at least at the theoretical level, to consider a continuous (real-number) model for solving some of the problems in cryptography. This model when used in cryptography would be inherently connected to chaos theory.

Acknowledgement

The author is grateful to Prof. Chen, advisory editor of this magazine, for the opportunity he has been given to express some ideas about chaos-based cryptography. He would like to thank R. Chen, G. Maggio, T. Stojanovski and G. Jakimoski for helpful discussion.

References

[1] L. M. Pecora and T. L. Carroll, “Synchronization in Chaotic Systems”, *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[2] G. Jakimoski and L. Kocarev, “Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps”, to appear in *IEEE Transactions on Circuits and Systems—Part I*; L. Kocarev and G. Jakimoski, “Chaos and Cryptography: From Chaotic Maps to Encryption Algorithms” submitted for publication; N. Masuda and K. Aihara, “Cryptosystems with Discretized Chaotic Maps” submitted for publication.

[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition. New York: John Wiley & Sons, 1996.

[4] B. Preneel, V. Rijmen, and A. Bosselears, “Recent Developments in the Design of Conventional Cryptographic Algorithms”, *Lecture Notes in Computer Science*, vol. 1528, pp. 105–130, Springer - Verlag, Berlin, 1998.

[5] M. S. Baptista, “Cryptography with Chaos”, *Physics Letters A*, vol. 240, pp. 50–54, 1998.

[6] G. Jakimoski and L. Kocarev, “Analysis of Some Recently Proposed Chaos-Based Encryption Algorithms”, submitted for publication.

[7] C. E. Shannon, “Communication Theory of Secrecy Systems”, *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949.

[8] T. Kruger and S. Troubetzkoy, “Complexity, Randomness, Discretization: Some Remarks on a Program of J. Ford”, *Physica D*, vol. 105, pp. 97–104, 1997.

[9] B. V. Chirikov and F. Vivaldi, “An Algorithmic View of Pseudochaos”, *Physica*, D 129, pp. 223–235, 1999.

[10] I. P. Cornfeld, S. V. Fomin, and Ya. G. Sinai, *Ergodic Theory*. Berlin: Springer, 1982.

[11] J. Palis and F. Takens, *Hyperbolicity and Sensitive Chaotic Dynamics at Homoclinic Bifurcations*. Cambridge: University Press, 1993.

[12] S. Banerjee, J. A. Yorke, and C. Grebogi, “Robust Chaos”, *Physical Review Letters*, vol. 80, no. 14, pp. 3049–3052, 1998.

[13] D. Ruelle, *Chaotic Evolution and Strange Attractors*. Cambridge: University Press, 1989.

[14] C. E. Shannon, “A Mathematical Theory of Communication”, *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, July 1948.

[15] A. A. Brudno, “The Complexity of the Trajectories of a Dynamical System”, *Russian Mathematical Surveys,* vol. 33, no. 1, pp. 197–198, 1978.

[16] J. Ford, “What Is Chaos, That We Should be Mindful of It?”, in *The New Physics*, P.Davies, ed., Cambridge University Press, 1992.

[17] J. Ford, “How Random Is a Coin Toss?”, *Physics Today*, vol. 4, pp. 40–47, April 1983.

[18] W. Diffie and M. E. Hellman, “New Directions in Cryptography”, *IEEE Transactions on Information Theory*, vol. 22, pp. 644–454, 1976.

[19] A. Yao, “Theory and Applications of Trapdoor Functions”, *IEEE 23rd Symposium on Foundations of Computer Science,* pp. 80–91, 1982.

[20] J. C. Largaris, “Pseudo-Random Numbers”, in *Probability and Algorithms*, National Academy Press, pp. 65–85, 1992.

[21] L. Blum, M. Blum, and M. Shub, “A Simple Unpredictable Pseudo-Random Number Generator”, *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, 1986.

[22] X. Lai and J. L. Massey, “A Proposal for a New Block Encryption Standard”, *Advances in Cryptology - EUROCRYPT’ 90*, pp. 389–404, Springer-Verlag, Berlin, 1991.

[23] X. Lai, J. L. Massey, and S. Murphy, “Markov Ciphers and Differential Cryptanalysis”, *Advances in Cryptology - EUROCRYPT’ 91*, pp. 17–38, Springer-Verlag, Berlin, 1991.

[24] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and Real Computation*. New York: Springer-Verlag, 1998.

[25] J. F. Traub, “A Continuous Model of Computation”, *Physics Today*, pp. 39–43, May 1999.