Discrete chaotic cryptography (DCC).

New method for secure communication

Zbigniew Kotulski, Janusz Szczepański

Polish Academy of Sciences
Institute of Fundamental Technological Research
PL-00-049 Warszawa, Świętokrzyska 21, Poland
e-mail: zkotulsk@ippt.gov.pl, jszczepa@ippt.gov.pl

1. Summary

Cryptography is a permanent field of interest at all times. At present secret communication plays an increasing role in many fields of common life, like banking, industry, commerce, telecommunication etc. The basic idea of encryption is to modify the message in such a way that its content can be reconstructed only by a legal recipient. The message might be represented by a sequence of symbols from a finite alphabet. The process of encryption $e(M)$ can be regarded as a function or algorithm producing the cipher $C = e(M,k)$. By k we denote a set of parameters, often called a secret key. The inverse function to e is the decrypting d, which from the cipher C with the key k produces the plaintext: $M = d(C,k)$. In practice M, C and k can be understood as real numbers [11].

The earliest applications of chaotic systems in cryptography were connected with encrypting messages with the modulation of trajectories of continuous dynamical systems. These methods are strongly related to the concept of synchronisation of two chaotic systems and controlling chaos [6].

In the paper we propose a new method of constructing cryptosystems utilising discrete chaotic dynamical systems [5], [8]. Such systems seem to be good candidates for preparing the algorithms. During iteration, an initial condition of the chaotic dynamical system is being transformed in a very non-regular way. Therefore the encryption and decryption procedure is based on multiple inverse iteration and iteration of a certain two-dimensional chaotic system. We assume that one part of the initial condition is the message, the other one is the secret key. To ensure a complicated structure of trajectories of the dynamical system proposed as the algorithm, we postulate that except of being chaotic, the system should be ergodic or, preferably, mixing. These properties make that our cryptosystem is robust against any reasonable statistical attack and ensure the standard quality of the cryptosystem. The approach presented made it possible to construct cryptosystems and verify their safety by the methods of the theory of abstract dynamical systems. Thus, we have a very strong tool available.

In the paper we introduce two classes of chaotic dynamical systems which we apply for preparation of cryptographic algorithms. The first class is constructed in some abstract way, using some postulated functions. The second class has its source in investigations of very rarefied gases, so called reflection law models. In this case we assume that the key is introduced into the reflection law and the message is considered as the initial position of the particle.

Finally, we give some remarks on the implementation of the proposed encryption algorithm on digital computers with finite accuracy.

2. General remarks about cryptology

a. Cryptology

Cryptology is the branch of sciences (often considered as an art [3]) dealing with the theory of secure communication algorithms. The main field of interest of cryptology is to elaborate methods of save transmission of secret information and protecting stored data and also investigation of the power of the algorithms (and, if possible, methods of breaking them).

Cryptology has been of some interest at all times. Mostly it has been used in connection with military or diplomatic affairs and for instance in its early stages it was almost exclusively concerned with secretly written communications. With the development of an ever refined communication technology nowadays secret communication plays also an increasing role in commercial, industrial and banking communications. A typical secure communication problem nowadays might be to get access to classified data via the telephone line. It is due to the increasing importance of cryptology in economics nowadays that the research activities in the field and the search for new cryptographic methods still continues.

b. Cryptography

Cryptography is the process of transforming information (clear-text) into unintelligible form (cipher-text) so that it may be sent over insecure channels or it may be stored in insecure files. Cryptographic procedures, can also be used for personal identification, digital signature, access control etc..

c. Cryptosystem

Cryptosystem is a cryptographic algorithm, which is usually known, and which depends on some parameters called the key. With encryption (enciphering, coding) we can transform clear-text to a form which an outsider cannot interpret unless he knows the method and the (possible) key used in the process. Decryption (deciphering, decoding) is the inverse process in which encrypted data are translated to clear data. In other words, the basic idea of all encryption is to modify the message so, as to make it unintelligible to anyone but the intended recipient. The message M might be represented by a finite sequence of symbols from a finite alphabet. The process of encryption $e(M)$ can be regarded as a function or algorithm producing the ciphertext $C = e(M,k)$. Symbol k denotes a set of parameters and often is called the secret key. The inverse function to e is the decrypting d, which, from the cipher-text C with the secret key k, produces the plain-text: $M=d(C,k)$.

Thus, the cryptosystem is the two-way procedure:

encryption <==> decryption

3. Classification of cryptosystems.

The cryptosystems can be classified with respect to three following aspects:

a. Classification with respect to the structure of encryption algorithm.

a1. Stream ciphers

Stream cipher is the method in which a key generator produces a bit stream (the key stream) which enciphers the plain-text bit stream by simple modulo 2 addition. A stream cipher system thus hides the plain-text by changing the bits of it in a random-like way. An

interceptor, who does not know the key, will not know which bits have been changed (corresponding to the occurrence of "1" in the key stream), or which ones remain unchanged ("0" in the key stream). An ideal stream cipher would use a physical (true) random number generator as key generator. Since its output cannot be reproduced, however, decipherment would be impossible, unless the whole key stream, with the same length as the plain-text, is transported to the legitimate receiver via a safe channel. This procedure is often impractical, therefore mostly so-called pseudo-random number generators, with special properties, controlled by a relatively short key, have to be used instead as key generators. In practice, the following pseudo-random number generators are used: linear congruential and inverse congruential generators, feedback shift register generator and generators based on specific cryptographic algorithms (e.g. DES).

a2. Block ciphers

Unlike to the stream ciphers, where only one bit at a time is ciphered, in this case whole blocks of bits are treated simultaneously. In this case the plain-text information is hidden by the fact that, depending on the key, a cipher-text block can be deciphered to any combination of plain-text bits or to as many combinations as there are keys. If the keys are chosen with equal probability, then to the interceptor observing a cipher-text block, all the possible plain-text blocks are equally likely to have occurred.

Commonly used block ciphers: DES, IDEA, FEAL, etc.

b. Classification with respect to the method of distribution of the secret key.

b1. Private secret key

Traditional cryptography is based on the fact that the sender and receiver of a message knowing and using the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the cipher (to obtain the message). This method is known as secret key cryptography. The problem is getting the sender and receiver to agree on the secret key without anyone else finding out.

b2. Public key

The public key cryptography was invented in 1976 by W.Diffie and M.Hellman. In this system, each person gets a pair of keys, called the public key and private key. Each person's public key is published while the private key is kept secret. All communications involve only public key, and no private key is even transmitted.

Example - RSA (Rivest, Shamir, Adelman, 1977) public key cryptosystem [10].

It works as follows: take two large primes p and q, and find their product $n = pq$. Choose a number e, less than n and relatively prime to $(p-1)(q-1)$, and find its inverse $\bmod\ (p-1)(q-1)$, i.e. a number d such that $ed = 1 \bmod (p-1)(q-1)$. The public key is the pair (n,e), the private key is d. The secret factors p and q should be destroyed after calculation of d. Up to now there is not known an algorithm fast enough to compute d from (n,e), where n and e are at least of 100 digits long. If one could factor n into p and q, however, then one could obtain the private key d. Thus the entire security of RSA is predicted on the assumption that factoring is difficult.

How to use RSA? Let m be the message, we calculate the cipher-text c by $c = m^e \pmod n$. To decrypt, we compute $m = c^d \pmod n$, what recovers the original message m.

The other example of public key cryptosystem is „Elgamal cryptosystem", security of which is based on lack of the fast enough method of calculating logarithm of a natural number in the finite field.

c. Classification with respect to the methods of constructing the algorithm.

c1. Traditional methods

The main tools applied in cryptology are [11]:
- number theory
- algebra
- algebraic geometry (recently: elliptic curves over finite fields [7])
- combinatorics
- research for the systems with large complexity
- development of hardware and software.

Hardware improvement will continue inexorably, but it is important to realise that hardware improvement make cryptosystems more secure, not less. This is because a hardware improvement that allows an attacker to use a number of two digits longer than before will at the same time allow a legitimate user to use a key dozens of digits longer than before; a user can choose a new key a dozen digits longer than the old one without any performance slowdown. Thus although the hardware improvement does help the attacker, it helps the legitimate user much more.

c2. Methods utilising chaos

Last years a new approach of constructing cryptosystems based on application of the theory of chaotic dynamical systems has been developed.

The earliest applications of chaotic systems in cryptography were connected with encrypting messages with the modulation of trajectories of continuous dynamical systems. These methods are strongly related to the concept of synchronisation of two chaotic systems and controlling chaos. The state of art in this field is consistently presented in [6].

We propose a method of encryption of the plain-text using for construction of the algorithm n-th inverse iteration of some discrete chaotic dynamical system. The decryption algorithm is n-th iteration of the dynamical system taking the cipher-text as an initial point.

The idea of application of discrete dynamical system in cryptography was suggested by T.Habutsu,Y.Nishio, I.Sasase, S.Mori. The authors assumed some parameter of the tent map to be a secret key. Then the message (initial condition) was transformed by several inverse iterations of the map. This method works for the systems for which the map properties are strongly sensitive to small changes of the internal parameter playing the role of secret key. Trying to generalise this approach we face to the problem of finding if this property really takes places for certain dynamical systems. (Some weak points of this algorithm in the case of tent map were presented in [2]). Therefore it is worthily to construct a cryptographic algorithm using the essence of chaos i.e. exponential divergence of trajectories for different initial conditions. Our idea is to introduce the secret key into the initial condition of the discrete chaotic system.

A brief overview of applications of chaos in secure communications is announced in the following table:

Continuous Dynamical Systems	**Discrete Dynamical Systems**
Encryption of a message with modulation of trajectories Decryption of a ciphertext by synchronisation of two systems or filtration of the modulated trajectories Tools applied: - synchronisation of two chaotic systems - controlling chaos T.Caroll, L.Chua, L.Doerner, K.Eckert, C.Grebogi, K.Halle, S.Hayes, B.Huebinger, L.Kocarev, W.Martienssen, E.Ott, U.Parlitz, L.Pecora, J.York Book: T.Kapitaniak, *Controlling Chaos*	Encryption of a plaintext with *n*-th inverse iteration of a map Decryption of a ciphertext with *n*-th iteration of the map Tools applied: - chaos - ergodic theory Two approaches: - including the secret key into internal parameter of the map T.Habutsu, Y,Nishio, I.Sasase, S.Mori EUROCRYPT'91 - including the secret key into initial conditions Z.Kotulski, J.Szczepański - Ann.Physik 1997 K.Górski, A.Paszkiewicz, A.Zugaj

4. Discrete Chaotic Cryptography

Now we formulate the method of application of chaotic dynamical systems for secure communication more precisely. For completeness let us remind the fundamental definition.

A discrete dynamical system [9] is the couple (X, φ), where X is the state space with some structure, (for our purpose: an interval or Cartesian product of two intervals) and φ is a transformation from X to X, called the generator of the semigroup of iterations.

The idea of Discrete Chaotic Cryptography

Plain-text is some number $P \in (0, 1)$;

Secret key is some parameter k;

Encryption is the n-fold iteration of the inverse map φ^{-1} with the initial value P according to some (secret) rule of choices of the successive pre-images of φ^{-1};

Cipher-text C is a result of the encryption:

$$C = \varphi^{-n}(P) = \varphi^{-1}\left(\varphi^{-1}\left(\ldots \varphi^{-1}(P)\right)\right);$$

Decryption is calculation of the image of C under the n-th iteration of the map φ:

$$P = \varphi^{n}(C) = \varphi\left(\varphi\left(\ldots \varphi(C)\right)\right).$$

The secret key k can be introduced to the algorithm in the following way:

- into the initial condition [8]; $P := P_k$;
- into internal parameters of φ [5]; $\varphi := \varphi_k$.

To make the encryption procedure very complicated we assume the chaos property of dynamical systems used.

Chaos is the property of sensitive dependence of trajectories from the initial conditions. More precisely, the non-linear system is chaotic if it has positive Lyapunov exponents on some domain.

As an example consider a one dimensional dynamical system (I, φ), where φ is C^1. If at some point $x \in I$, $\lambda_x > 0$ (Lyapunov exponent) then

$$\forall \varepsilon > 0 \; \exists n_1, n_2 \; \exists U_{n_1, n_2} \ni x, \; \forall n_1 \le n \le n_2, \; \forall z_1, z_2 \in U_{n_1, n_2}$$

$$e^{(\lambda_x - \varepsilon) n} |z_1 - z_2| < |\varphi^n(z_1) - \varphi^n(z_2)| < e^{(\lambda_x + \varepsilon) n} |z_1 - z_2|.$$

where U_{n_1, n_2} is some neighbourhood of $x \in I$. The above expression means that the initial distance $|z_1 - z_2|$ between two arbitrary points z_1, z_2 (which are elements of the neighbourhood U_{n_1, n_2} of point x) after n iterations will increase at least $e^{(\lambda_x - \varepsilon) n}$ times.

Let us illustrate the idea of including the secret key into the initial condition by some elementary one-dimensional example.

An illustrative example

Let γ be a one-dimensional chaotic map with positive Lyapunov exponent λ:

$$\gamma: [0, 1] \to [0, 1]$$

and $P \in (0, 1)$ be the message to encrypt. Fix a natural number n (number of iterations) and choose the secret key $k \in (0, 1)$.

Let $\overline{C}$ be some selected pre-image of P under the map γ^n,

$$\overline{C} = \gamma^{-n}(P);$$

$$\gamma^n(\overline{C}) = \gamma^n(\gamma^{-n}(P)) = P.$$

Then, we calculate C, the ciphertext of P as

$$C = \overline{C} + k \pmod 1.$$

Decryption is the inverse operation, that is

$$P = \gamma^n(C - k).$$

A non-legal user tries to approximate the key *k* assuming some value of the secret key, say k_1 such that $\left|k - k_1\right| < 10^{-20}$. Then he calculates the value of plaintext $P_1 = \gamma^n\left(C - k_1\right)$.

For $n = 30$, $\lambda - \varepsilon \approx 1.558$ (what is a reasonable value for many dynamical systems), due to chaos we have:

$$\left|P - P_1\right| = \left|\gamma^n\left(C - k\right) - \gamma^n\left(C - k_1\right)\right| \geq e^{n(\lambda - \varepsilon)}\left|k - k_1\right| \approx 0.5$$

This shows how the chaos property preserves the system against the brute force attack (where the algorithm is tested with all possible secret keys).

However, cryptoanalysts use some more sophisticated attacks to break cryptosystems. To make the cryptosystem based on the chaos property more robust against statistical cryptoanalitycal attacks, we postulate some other important properties of the applied dynamical system, like ergodicity and mixing property. For cryptographic purposes we shall use dynamical systems with invariant measure equivalent to Lebesgue measure.

Ergodic properties - notation

We say that the measure μ is <u>invariant</u>, if and only if it satisfies

$$\forall A \in \sigma(X), \quad \mu(A) = \mu\left(\varphi^{-1}(A)\right).$$

We postulate that μ is equivalent to the Lebesgue measure, i.e.:

$$\forall A \in \sigma(X), \ \mu(A) = \int_A g(x)dx \,,$$

with its density function

$$0 < g_1 \leq g(x) \leq g_2 \,,$$

where g_1 is close to g_2.

We say that (X, φ) is <u>ergodic</u> if and only if it has only trivial invariant sets, i.e., if $\varphi(B) \subset B$ then $\mu(B) = 0$ or $\mu(B) = \mu(X)$.

The ergodicity implies that the state space cannot be nontrivially divided into several parts. Therefore if some trajectory starts from any point *x* it never localises in a smaller region. It means that the plain-text space which can correspond to a given cipher cannot be restricted to a "smaller" subspace (smaller then *X*). Thus, for the cipher-text *C* the corresponding plain-text *P* (during brute attack) must be searched for over all the state space *X*.

The system is <u>mixing</u> if the following condition is satisfied (we assume that $\mu(X) = 1$):

$$\lim_{n \to \infty} \frac{\mu\left(\varphi^{-n}(A) \cap B\right)}{\mu(B)} = \frac{\mu(A)}{\mu(X)} \,.$$

This property means that the part of *B* that after *n* iterations of φ will be contained in *A* is asymptotically proportional to the rate of *A* in *X* with respect to the measure μ. Thus for any cipher-text *C* all the possible plain-texts *P* (during brute attack) are μ-equiprobable.

Discrete Chaotic Cryptography - implementation 1

The idea of sensitive dependence on initial conditions (chaos) and ergodicity has its source in the theory of gases (*n*-particles models, Lorentz gas, Brownian motion). Therefore in the first cryptosystem we apply two-dimensional reflection law models [1], [12], [13]. This can be considered as an idealised model of a particle's movement in some environment (bounded domain). In the theory of gases two properties play a fundamental role: ergodicity that is the convergence of the average value over trajectory to the ensemble mean value and mixing, which guarantees the convergence from local non-equilibrium to equilibrium state. Analysing the behaviour of individual particles, assuming ergodicity or mixing, we go from any initial conditions of the particles to some macroscopic equilibrium state, where the particles are practically non-discriminable. Thus, using the reflecting system for encryption, we expect that the position of our particle, describing at its initial state the message being encrypted, after several reflections will take some non-predictable position and will not be statistically distinguishable from any other possible position, making the algorithm cryptographically secure.

In our cryptosystem, we take the initial condition of the first co-ordinate of the system (which describes the position of the particle on the boundary at the moment of reflection) as the plain-text and the initial condition of the second co-ordinate (representing the angle of reflection according to some reflection law) as the secret key. Both co-ordinates are iterated; the second, independently of the first (due to specific choice of the model), in a chaotic way; the first with some dependence on the second co-ordinate at each step. Under certain assumptions on the dynamical system, taking two initial conditions, we have an exponential divergence of their trajectories, depending on the distance of the initial conditions of both trajectories.

To precise our model we consider the motion of a free particle in a square. Describing it we use the co-ordinate system $\left(x_n, v_n\right)$, where x_n is the position of the particle at the boundary of the square at the moment of the *n*-th reflection and v_n is the angle from the tangent to the boundary at x_n to the velocity of the particle after reflection.

At the boundary the particle undergoes a reflection law:

$$T_D:(0,\pi)\to(0,\pi), \qquad T_D(v_{inc}) = v_{ref}$$

where v_{inc} is the angle of incidence and v_{ref} is the angle of reflection.

The movement of the particle is described by the following two-dimensional map

$$F_{T_D} : [0,\ L)\times(0,\ \pi) \longrightarrow [0,\ L)\times(0,\ \pi),$$

$$F_{T_D}\left(x_n, v_n\right) = \left(x_{n+1}, v_{n+1}\right).$$

Taking into account the geometry of the square, we come to the explicit formula:

$$F_{T_D}(P,k) = \left(S(P,k), T_D(k)\right).$$

In this model we take the initial value v_0 as a secret key:

$$k \equiv v_0 .$$

We se that the evolution of the second co-ordinate describes the evolution of the secret key.

To obtain the appropriate properties of the extended system F_{T_D} we put some conditions on the reflection law T_D.

Conditions on the reflection law

1. $T_D : (0,\ \pi) \to (0,\ \pi)$;

2. The interval $(0,\ \pi)$ can be divided into finite (or infinite countable) number of intervals $\Delta_1,\ \Delta_2,\ \ldots.$ such that

$$T_D\left(\Delta_i\right) = (0,\ \pi), \qquad i = 1,2,.....;$$

3. At each Δ_i the map T_D is of class C^2 and monotonic;

4. For some natural *s* and every *i* the following relationship is satisfied

$$\inf_{\Delta_i} \inf_{k \in \Delta_i} \left| \frac{dT_D^{(s)}(k)}{dk} \right| = \delta > 1,$$

where $T_D^{(s)}$ is the *s*-th iteration of the map T_D;

5. $$\sup_{\Delta_i} \sup_{k_1, k_2 \in \Delta_i} \frac{\left| \dfrac{d^2\, T_D(k_1)}{d\, k_1^2} \right|}{\left[\dfrac{d\, T_D(k_2)}{d\, k_2} \right]^2} = \rho < \infty .$$

Under the above conditions the map T_D is mixing and chaotic. Proceeding the inverse iterations and also closing the procedure with adequate maps (composition of non-linear map with an interval exchange transformation) we obtain that chaos (mixing, ergodicity) is transferred to the extended system F_{T_D}.

The next example of DDC system is constructed in some abstract way.

Discrete Chaotic Cryptography - implementation 2.

In the following cryptosystem we propose the algorithm using some abstract dynamical system. In the system the part decrypting a given ciphertext can be considered, in some sense, as a multiplicative perturbation of the chaotic dynamical system transforming the secret key.

More precisely, we construct a two-dimensional dynamical system (X, Φ) where X is the Cartesian product of two unit intervals and Φ is the map:

$$\Phi : [0,\ 1] \times [0,\ 1] \to [0,\ 1] \times [0,\ 1],$$

of the following form

$$\Phi(k, C) = [\phi(k), \chi(C, k)\phi(k)].$$

We interpret the first argument of Φ as the secret key and the second argument as the cipher-text. We assume that $\phi : [0,1] \to [0,1]$ is a chaotic and mixing map and χ is a transformation satisfying some special conditions [8]. To complete the model we apply in the encryption procedure a concentrating map proceeding the inverse iterations and also close the procedure with adequate spreading map. Under the above assumptions, in this system we have transferring of chaos (and also ergodicity and mixing property) from the subsystem ϕ to the whole system Φ. Thus we obtain the secure tool for encrypting the messages. The details of the model can be found in [8].

5. Final remarks.

In the paper we present a general method of constructing cryptosystems with application of discrete chaotic dynamical systems by utilisation of the essence of chaos (i.e. the sensitivity of the trajectories to small changes of initial conditions). Our approach made it possible to construct cryptosystems and verify their safety by methods of the theory of abstract dynamical systems. Since the theory is well developed and still extensively investigated, we have a very strong tool available.

A general theory of discrete chaotic cryptosystems is a kind of theoretical model. In practice, preparing concrete computer implementations, one should take into account the usual computational conditions [14]. Since numbers in numerical computations have finite representation, one must assume a size of computed values (key, plaintext, ciphertext) such that both the iterations and inverse iterations can be performed uniquely and such that one can obtain the required number of significant digits of plaintext in the decryption process. (This depends on the algorithm applied and computer used). To summarise, let us remark that the proposed algorithm is very fast. It requires only n iterations of some relatively simple maps, where the number n must be some compromise between safety of the method and accuracy of the computer arithmetic. Usually $20 \le n \le 100$.

References

1. H.Babovsky, *Initial and boundary value problems in kinetic theory. I. The Knudsen gas, II. The Boltzmann equation,* Transp.Theor.Stat.Phys., vol.**13**, Part I-pp.455-474, Part II-pp.475-498, (1984).
2. E.Biham, *Cryptoanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91*, EUROCRYPT'91, pp.532-534.
3. M.T.Boswell, S.D.Gore, G.P.Patil, C.Taille, The art. of computer generation of random variables, In: Handbook of Statistics, ed. C.R.Rao, vol.9, Elsevier Science Publishers 1993.
4. K.Górski, Z.Kotulski, A.Paszkiewicz, J.Szczepański, A.Zugaj, Application of discrete chaotic dynamical systems in cryptography - DCC method. (submitted).
5. T.Habutsu,Y.Nishio, I.Sasase, S.Mori, A secret key cryptosystem by iterating a chaotic map, EUROCRYPT'91, p.127
6. T.Kapitaniak, *Controlling Chaos, Theoretical and Practical Methods in Non-linear Dynamics*., Academic Press, London 1996.
7. N.Koblitz, A course in Number Theory and Cryptography, Springer-Verlag 1994
8. Z.Kotulski, J.Szczepański, *Discrete chaotic cryptography*, Annalen der Physik, vol.**6**, no.5, pp.381-394, (1997).
9. W.Perry, *Topics in Ergodic Theory,* Cambridge Univ. Press, Cambridge, (1981).
10. R.Rivest, Cryptography. Handbook of Theoretical Computer Science, Vol.A, Elsevier 1990.
11. B.Schneier, Applied Cryptography, Practical Algorithms and Source Codes in C, John Wiley, New York, 1996.
12. J.Szczepański, Z.Kotulski, On topologically equivalent ergodic and chaotic reflection laws leading to different types of particle motion, (submitted).
13. J.Szczepański, E.Wajnryb, *Do ergodic or chaotic properties of the reflection law imply ergodicity or chaotic behaviour of a particle's motion?,* Chaos, Solitons & Fractals, vol.**5**, no.1, pp.77-89, (1995).
14. R.Wieczorkowski, R.Zieliński, Computer Generators of Random Numbers, WN-T, Warsaw 1997.