CIRCUITS SYSTEMS SIGNAL PROCESSING
VOL. 24, NO. 5, 2005, PP. 497–517

DOI: 10.1007/s00034-005-2403-x

PUBLIC-KEY ENCRYPTION BASED ON CHEBYSHEV POLYNOMIALS*

L. Kocarev,[1] *J. Makraduli,*[2] *and P. Amato*[3]

Abstract. We propose public-key encryption algorithms based on Chebyshev polynomials, which are secure, practical, and can be used for both encryption and digital signature. Software implementation and properties of the algorithms are discussed in detail. We show that our ElGamal-like and RSA-like algorithms (when Chebyshev polynomials are employed) are as secure as the original ElGamal and RSA algorithms.

1. 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 pioneering work on chaos synchronization [1] led to several applications in communications, in which chaotic systems with continuous-value signals were used to transmit information. Several schemes have been developed which allow us to transform the information signal into a chaotic waveform on the transmitter side and to extract the information signal from the transmitted waveform on the receiver side. The most important among them are: chaotic masking, chaos shift keying, and chaotic modulation. In early days (from 1992 to 1996) the main research goal was to develop schemes in which a single chaotic system is used for both modulation

* Received February 15, 2005; revised May 30, 2005.

[1] Institute for Nonlinear Science, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0402, USA. E-mail: lkocarev@ucsd.edu

[2] Faculty of Electrical Engineering, Karpos II, Skopje, Macedonia. E-mail: janimak@sonet.com.mk

[3] STMicroelectronics, Soft Computing, Si-Optics & Post Silicon Technology, Corporate R&D Via Remo De Feo 1, 80022 Arzano (Napoli), Italy. E-mail: paolo.amato@st.com

and encryption. This approach eventually evolved into two distinct research areas: chaos-based modulation [2], [3] and chaos-based cryptography [4], [5].

In chaotic modulation, the digital information is mapped to inherently wide-band chaotic signals. Thus, chaotic modulation offers a novel solution to spread-spectrum communication. Two most promising approaches in chaos-based modulation have recently emerged. In the first approach, the unmodulated chaotic waveform is transmitted along with the modulated signal (transmitted reference scheme) either using a separate channel or using time division. One instance of this approach, so-called frequency-modulated differential chaos shift keying, was particularly studied in-depth by Kolumban, Kennedy, Kis, and Jako [2], [6]. In another approach, a chaotic reference is regenerated at the receiver with the help of synchronization. In [3] and [7] an example of such an approach is proposed, in which chaotic-time pulsed sequences are used instead of continuous-time waveform. Since the information about the state of the chaotic signal is contained entirely in the timing between pulses, the distortions that affect the pulse shape will not significantly influence the ability of the chaotic pulse generators to synchronize. This approach is known as chaotic pulse position modulation.

Cryptography is generally acknowledged as the best method of data protection against passive and active fraud [8]. An overview of recent developments in the design of conventional cryptographic algorithms is given in [8]. Three most common cryptographic objects are: block-encryption algorithms (private-key algorithms), pseudo-random number generators (additive stream ciphers), and public-key algorithms.

Block ciphers transform a relatively short string (typically 64, 128, or 256 bits) to a string of the same length under control of a secret key. Several block encryption ciphers based on chaotic maps have been proposed in the literature, in which a discretization (a process that describes the way a chaotic map is implemented in the computer) is not realized by rounding the chaotic map according to the computer arithmetic, but rather is constructed explicitly. Pichler and Scharinger [9] proposed cryptographic systems based on chaotic permutations constructed by explicitly discretizing the two-dimensional bakers map. Fridrich [10] extended their ideas to chaotic permutations on any size of two-dimensional lattices. Her permutations benefit from the expanding property along one axis, technically avoiding the contracting property along the other axis. The authors of [11] used two well-known chaotic maps, exponential and logistic, to construct a class of block encryption algorithms. In a recent paper [12], they analytically derived the lower bound of a number of active S-boxes in their algorithms, computed upper bounds for differential and linear probabilities, and therefore, proved the resistance of the algorithms proposed [11] to differential and linear attacks. Masuda and Aihara [13] considered a discrete version of the skew-tent map, which exploits important chaotic properties such as the sensitive dependence on initial conditions and the exponential information decay. They discussed the difference

between the discretized map and the original map, explaining the ergodic- and chaotic-like properties of the discretized map.

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. Chaotic systems may be used to generate pseudo-random numbers. For example, in a series of papers [14], the authors proposed a chaos-derived pseudo-random number generator. They numerically observed that the average cycle and transient lengths grow exponentially with the precision of implementation, and from this fact deduced that using high-precision arithmetic one can obtain pseudo-random number generators (PRNGs) which are still of cryptographic interest. Statistical properties of binary sequences generated by a class of ergodic maps with some symmetrical properties are discussed in [15]. The authors derived a sufficient condition for this class of maps to produce a sequence of independent and identically distributed binary random variables. However, the authors did not discuss the implementation of these maps on finite-state machines and the consequences this implementation may have on the randomness of the generated sequences. In a recent paper [16], the authors proposed a class of chaos-based pseudo-random bit generators.

Certain applications in cryptography require the use of a truly random number generator (RNG), which is a device which outputs a sequence of statistically independent and unbiased numbers. It is widely accepted that the core of any RNG must be an intrinsically random physical process. Thus, it is no surprise that the proposals and implementations of RNGs range from tossing a coin, to measuring thermal noise from a resistor and shot noise from a Zener diode or a vacuum tube, measuring radioactive decay from a radioactive source, and sampling a stable high-frequency oscillator with an unstable low-frequency clock, to mention only a few proposals. For chaos-based generators of truly random numbers, see, for example, [17], [18], [19], [20]. Papers [18], [19] are devoted to the analysis of the application of a chaotic piecewise-linear one-dimensional map as an RNG. Piecewise linearity of the map enables the authors to mathematically find parameter values for which a generating partition is Markov and the RNG behaves as a Markov information source, and then to mathematically analyze the information generation process and the RNG. The map is implemented in a 0.8μm standard complementary metal oxide semiconductor (CMOS) process utilizing switched current techniques.

Public-key algorithms [8], also called asymmetric algorithms, are designed so that:

(i) the encryption key is different from the decryption key;
(ii) the encryption key can be made public; and
(iii) the decryption key cannot, at least in any reasonable amount of time, be calculated from the encryption key.

There are many public-key algorithms; the three most widely used public-key cryptosystems are: RSA, ElGamal, and Rabin [8]. In this paper we propose public-key encryption algorithms using Chebyshev maps, which are both secure and practical, and can be used for both encryption and digital signature. This paper can be viewed as an extension of our previous work [21], [22], in which an ElGamal public-key algorithm was generalized for Chebyshev maps, defined on the set $[-1, 1]$, and implemented using floating-point arithmetic. In this paper, however, we implement our algorithms using integers. Thus, we propose ElGamal-like and RSA-like public-key algorithms using Chebyshev maps, which are well known examples of chaotic maps. Furthermore, our analysis of the periodic orbits in sequences of integers generated by Chebyshev maps is based on the arithmetic properties of toral automorphisms, another well-known class of chaotic maps.

This is the outline of the paper. In Section 2 we briefly discuss ElGamal and RSA public-key algorithms. Section 3 provides examples of chaotic maps. The core of this paper is Section 4. We first argue that public-key algorithms should always be implemented with integers, Section 4.1. Then in Section 4.2 we define modified Chebyshev polynomials and state two theorems which are of crucial importance for designing public-key algorithms. Section 4.3 presents a fast algorithm for computing Chebyshev polynomials. In Sections 4.4 and 4.5 we discuss ElGamal and RSA algorithms and their properties, respectively. We close our paper with Section 5. Readers who are only interested in applicative aspects of our work and do not want to understand in-depth mathematical aspects of this work, should restrict themselves to reading Sections 2–4. However, for readers who would like to follow the proof of our main theorem, Theorem 4.2, we present in Section 6 all the necessary background materials together with the proof of the theorem.

2. Public-key encryption

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" [23] ushered in the era of *scientific secret-key cryptography*. 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 [24]. The real explosion came with the publication, in 1976, by W. Diffie and M. E. Hellman of their paper, "New Directions in Cryptography" [25]. 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. In a public-key encryption system [8] Alice has a *public key* e and a corresponding *private key* d. In secure systems, the task of computing d given

e is computationally infeasible. The public key defines an encryption transformation E_e, while the private key defines the associated decryption transformation D_d. Bob, wishing to send a message m to Alice, obtains an authentic copy of Alice's public key e, uses the encryption transformation to obtain the cipher-text $c = E_e(m)$, and transmits c to Alice. To decrypt c, Alice applies the decryption transformation to obtain the original message $m = D_d(c)$.

Since 1976, numerous public-key algorithms have been proposed; the three most widely used public-key crypto-systems are: RSA, Rabin, and ElGamal. The security of the RSA system, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is based on the intractability of the integer factorization problem. In the Rabin public-key encryption scheme, the problem faced by a passive adversary is computationally equivalent to factoring. The security of the ElGamal public-key system is based on the intractability of the discrete logarithm problem. Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms. For this reason, public-key encryption is most commonly used in practice for encryption of small data items and/or for transport of keys, subsequently used for data encryption by symmetric-key algorithms.

Recall first the basic ElGamal algorithm. The ElGamal public-key algorithm can be viewed as Diffie–Hellman key agreement in key transfer-mode [8]. Consider a class of functions defined as $\pi_p(x) = x^p \pmod N$, where N is a prime number, x is a generator of the multiplicative group $\mathbb{Z}_N^*$, and $1 \leq p \leq N-2$. Any two functions π_p and π_q commute under composition:

$$\pi_p(\pi_q(x)) = \pi_{pq}(x). \tag{1}$$

The Diffie–Hellman key agreement protocol describes how Alice and Bob agree on their common secret key. Alice generates a number p, computes $y = \pi_p(x)$ and sends (x, y) to Bob. Bob creates a number q, computes $z = \pi_q(x)$ and sends z to Alice. The secret key, which can be shared by both Alice and Bob, is computed as follows. Alice computes the secret key k as $k = \pi_p(z)$. Bob computes the secret key k as $k = \pi_q(y)$.

In the ElGamal public-key scheme, Alice generates a large random prime N and a generator x of the multiplicative group $\mathbb{Z}_N^*$ of integers modulo N. She also generates a random integer $s \leq N-2$ and computes $A = x^s \pmod N$. Alice's pubic key is (x, N, A); Alice's private key is s. To encrypt a message m, Bob selects a random integer $r \leq N-2$, computes $B = x^r \pmod N$ and $X = mA^r \pmod N$, and sends the cipher-text $c = (B, X)$ to Alice. To recover the message m from c, Alice uses the private key s to recover m by computing $m = B^{-s}X \pmod N$. The decryption allows recovery of the original message because $B^{-s}mA^r \equiv x^{-rs}mx^{rs} \equiv m \pmod N$.

Recall now the RSA algorithm. Let $N = pq$ and $\phi = (p-1)(q-1)$, where p and q are two large random (and distinct) primes p and q. Alice selects a random integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$ and computes the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod\phi$. Alice's public key is (N, e); Alice's private key is d. To encrypt a message m, Bob computes $c =$

$m^e \pmod N$ and sends to Alice. To recover the message m from c, Alice should use the private key d to recover $m = c^d \pmod N$. Let $\pi_p(x) = x^p \pmod N$. The decryption in the RSA algorithm works for two reasons: the functions π_e and π_d commute under composition, and p is a periodic point of the function π_{ed} for every m: $m^{ed} \equiv m \pmod N$. The last follows from the following observation. Since $ed \equiv 1 \pmod \phi$, there exists an integer k such that $ed = 1 + k\phi$. Now, if $\gcd(m, p) = 1$, then by Fermat's theorem $m^{p-1} \equiv 1 \pmod p$. Raising both sides of this congruence to the power of $k(q-1)$ and then multiplying both sides by m yields $m^{ed} \equiv m \pmod p$. By the same argument $m^{ed} \equiv m \pmod q$. Finally, since p and q are distinct primes, it follows that $m^{ed} \equiv m \pmod N$.

3. Chaotic maps

3.1. Chebyshev maps

A Chebyshev polynomial map $T_p : R \to R$ of degree p is defined using the following recurrent relation:

$$T_{p+1}(x) = 2xT_p(x) - T_{p-1}(x), \tag{2}$$

with $T_0 = 1$ and $T_1 = x$. The first few Chebyshev polynomials are

$$\begin{aligned} T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1. \end{aligned}$$

One of the most remarkable properties of the Chebyshev polynomials is the *semigroup* property [26]:

$$T_r(T_s(x)) = T_{rs}(x). \tag{3}$$

An immediate consequence of this property is that Chebyshev polynomials commute under composition, i.e.,

$$T_s(T_r) = T_r(T_s). \tag{4}$$

The interval $[-1, 1]$ is invariant under the action of the map T_p: $T_p([-1, 1]) = [-1, 1]$. Thus, the Chebyshev polynomial restricted to the interval $[-1, 1]$ is the well-known chaotic map for all $p > 1$: it has a unique absolutely continuous invariant measure

$$\mu(x)\,dx = \frac{dx}{\pi\sqrt{1-x^2}},$$

with positive Lyapunov exponent $\lambda = \ln p$. For $p = 2$, the Chebyshev map reduces to the well-known logistic map.

For both ElGamal and RSA algorithms, property (1) is crucial for encrypting and decrypting the information. Now we address the following question: Are there

other functions with the semigroup property (1)? We consider only polynomials. Two polynomials, P and Q, are called permutable if $P(Q(x)) = Q(P(x))$ for all x. If we write $P \circ Q$ to indicate composition $P(Q(x))$, then P and Q are permutable if $P \circ Q = Q \circ P$. A sequence of polynomials, each of positive degree, containing at least one of each positive degree and such that every two polynomials are permutable, is called a *chain*. The Chebyshev polynomials $T_1(x), T_2(x), \ldots$, form a chain. The powers $\pi_j(x) \equiv x^j$, $j = 1, 2, \ldots$, form a chain as well. Suppose that $\lambda(x) = ax + b$, $a \neq 0$, so that $\lambda^{-1}(x) = (x - b)/a$. If P and Q commute, it is clear that $\lambda^{-1} \circ P \circ \lambda$ and $\lambda^{-1} \circ Q \circ \lambda$ also commute. We say that P and $\lambda^{-1} \circ P \circ \lambda$ are *similar*.

The answer to the above question for polynomials is given by the following theorem [26]: If P and Q commute, either both are iterates of the same polynomial or both are similar, with respect to the same λ, to either Chebyshev polynomials or powers. Thus, the sequences $\{T_j\}$ and $\{\pi_j\}$ are the only chains, up to similarities.

3.2. *Torus automorphisms*

In this section we briefly discuss some general properties of automorphisms of the two-dimensional torus. An automorphism of the 2-torus is implemented by a 2×2 matrix M with integer entities and determinant ± 1. The requirement that the matrix M has integer entities ensures that M maps torus into itself. The requirement that the determinant of the matrix M is ± 1 guarantees invertibility. Here we consider only strictly unimodular automorphisms, for which $\det M = 1$.

Let M be a 2-torus automorphism

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix} \pmod 1, \tag{5}$$

where $x, y \in [0, 1]$. Let k be a trace (which is an integer) of the automorphism M, $f(z) = z^2 - kz + 1$ its characteristic polynomial, and λ one of its roots (say, the largest one):

$$\lambda = \frac{k + \sqrt{k^2 - 4}}{2}.$$

It is well known that for $k > 2$ (we will consider only positive k) the automorphism M has strong chaotic properties and, in particular, it has a dense set of unstable periodic orbits. The detailed structure of periodic orbits of the 2-torus automorphisms has been studied by Percival and Vivaldi [27].

Periodic orbits of a toral automorphism consist of those points having rational coordinates $\xi = p_1/q_1, \eta = p_2/q_2$, p_i, q_i integers. Let p_i, q_i be co-primes (their greatest common divisor is 1) and let q be the least common multiple of q_1 and q_2. Clearing denominators, we let M act on Z^2, the lattice of integral vectors, and then take into account the periodicity of the torus by identifying points whose coordinates differ by multiplies of q, i.e., we consider the factor group Z^2/gZ^2. Thus, the dynamics of periodic orbits is dynamics over a finite set of integers.

The work [27] illustrated the close link existing between arithmetic in algebraic number fields and strongly chaotic dynamics. The main conclusions of [27] may be summarized as follows:

- A 2-torus automorphism has three different types of (periodic) orbit structure, according to the classification of rational primes: inert, split, and ramified primes [28].
- The orbits which correspond to inert primes are almost without structure. The split primes have two distinct ideal factors, which correspond to orbits confined to invariant sublattices. For this reason, two ideal orbits which exist on split prime lattices are the "most ergodic" orbits and, thus, equilibrium averages computed with them minimize statistical fluctuations.
- Both inert and split prime lattices are found infinitely often and, moreover, with the same frequency in both cases. These are consequences of Dirichlet's theorem on the existence of infinity many primes in any arithmetic progression [29].
- The ramified prime lattices support orbits which are exceptionally regular. However, there is only a finite number of ramified primes, so that this apparently contradictory phenomenon of regularity in chaos is in fact very rare.

4. Public-key encryption with Chebyshev polynomials

4.1. Floating-point arithmetic versus integer arithmetic

Chaotic systems are defined on real numbers. Any encryption algorithm which uses chaotic maps when implemented on a computer (finite-state machine) becomes a transformation from a finite set onto itself. Because of its wide dynamic range, the floating-point implementation seems to be the most appropriate for software realizations (implementation) of Chebyshev polynomials. However, there are three reasons for not using floating-point arithmetic in public-key encryption.

First, floating-point numbers are not uniformly distributed over any given interval of the real axis [30]. Furthermore, one may observe the existence of redundant number representations. Indeed, due to the normalized calculations in floating-point arithmetic, some floating-point numbers represent the same real signal value.

Second, noninvertibility of Chebyshev polynomials and their floating-point implementation imply a restriction on the length of the message. Indeed, the public-key encryption scheme proposed recently in [21], [22] can be viewed as a generalization of ElGamal public-key scheme using Chebyshev polynomials. We summarize the algorithm as follows. Alice generates a large integer s, selects a random number $x \in [-1, 1]$, and computes $T_s(x)$. Alice's public key is $(x, T_s(x))$, while her private key is s. Bob represents the message as a number $M \in [-1, 1]$,

generates a large integer r, and computes $T_r(x)$, $T_{rs} = T_r(T_s(x))$, and $X = MT_{rs}$. He sends the cipher-text $c = (T_r(x), X)$ to Alice. To recover plain-text M from c, Alice should use the private key s to compute $T_{sr} = T_s(T_r(x))$, and recovers M by computing $M = X/T_{sr}$. Let l_s, l_r, l_M be the lengths (in bits) of s, r, and M, respectively, and let N-bit precision arithmetic be used in a software implementation of the algorithm. Then $l_m \leq N - l_s - l_r$ [21], [22].

Third, the authors think that the most important reason is that there are no analytical tools for understanding the periodic structure of the periodic orbits in the floating-point implementation of chaotic maps (when implemented on a computer all chaotic maps are periodic: all trajectories are eventually periodic). On the other hand, when using integers one may hope that a possible link between number theory and chaos theory has been established, as in the case of the toral automorphisms, to understand the structure of the orbits.

4.2. Modified Chebyshev polynomials

In this section we use the following map, $T_p : \{0, 1, \ldots, N-1\} \to \{0, 1, \ldots, N-1\}$ defined as

$$y = T_p(x) \pmod N, \tag{6}$$

where x and N are integers, to extend ElGamal and RSA public-key algorithms to Chebyshev maps. We call (6) a modified Chebyshev polynomial.

The modified Chebyshev polynomials can replace powers in ElGamal and/or RSA public-key algorithms only if they commute under composition and if one can compute the period of their orbits. The following two theorems show that these properties hold for modified Chebyshev polynomials.

Theorem 4.1. *Modified Chebyshev polynomials commute under composition, that is,*

$$T_p\left(T_q(x) \pmod N\right) \pmod N = T_{pq}(x) \pmod N.$$

Theorem 4.2. *Let N be an odd prime and let $x \in Z$ such that $0 \leq x < N$. Then the period of the sequence $T_n(x) \pmod N$, for $n = 0, 1, 2 \ldots$, is a divisor of $N^2 - 1$.*

The first theorem can easily be verified; the proof of the second theorem is given in the Appendix.

We now present an example. Several trajectories of the map (6), when $N = 19$,

Table 1. Periods of the sequences $\{T_n(x) (\mathrm{mod}\, 19)\}_{n\geq 0}$ for each $x = 0, 1, 2, \ldots, 18$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Period	4	1	5	20	20	18	18	5	18	3	6	9	10	9	9	20	20	10	2

are given below:

$x = 0,\ 1, 0, 18, 0, 1, 0, 18, 0, \ldots,$
$x = 1,\ 1, 1, 1, 1, \ldots,$
$x = 2,\ 1, 2, 7, 7, 2, 1, 2, 7, 7, 2, \ldots,$
$x = 3,\ 1, 3, 17, 4, 7, 0, 12, 15, 2, 16, 18, 16, 2, 15, 12, 0, 7, 4, 17, 3, \ldots,$
$x = 4,\ 1, 4, 12, 16, 2, 0, 17, 3, 7, 15, 18, 15, 7, 3, 17, 0, 2, 16, 12, 4, \ldots,$
$x = 5,\ 1, 5, 11, 10, 13, 6, 9, 8, 14, 18, 14, 8, 9, 6, 13, 10, 11, 5, \ldots.$

The periods of all trajectories of the map (6), with $N = 19$, are listed in Table 1. They are always divisors of $18 \times 20 = 2^3 3^2 5$. One can easily show that for any odd prime N the periods of the trajectories starting from the initial points $x = 0$, $x = 1$, and $x = N - 1$ are always 4, 1, 2, respectively.

4.3. Software implementation

In a public-key algorithm encryption, decryption, signing, and verifying signatures all involve multiplying with a large number. We now present an algorithm for computing $T_p(x) \,(\mathrm{mod}\, N)$ when N and p are large numbers. Equation (2) can be rewritten as

$$\begin{bmatrix} T_p \\ T_{p+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{p-1} \\ T_p \end{bmatrix} = A \begin{bmatrix} T_{p-1} \\ T_p \end{bmatrix}, \tag{7}$$

or, after some algebra, as

$$\begin{bmatrix} T_p \\ T_{p+1} \end{bmatrix} = A^p \begin{bmatrix} T_0 \\ T_1 \end{bmatrix}. \tag{8}$$

Matrix exponentiation can be done effectively by the *square and multiply* algorithm. Using notation

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

the pseudo-algorithm for calculating the matrix exponent A^p is

$$
\begin{aligned}
&A^p = I;\\
&for(i = p.numBits(); i > 0; i--)\\
&\{\\
&\qquad A^p = \left(A^p\right)^2;\\
&\qquad if(p.bitAt(i) == 1)\\
&\qquad\qquad A^p = A^p A;\\
&\}.
\end{aligned}
$$

Bit positions are enumerated starting at 1. The algorithm represents the matrix version of the number exponentiation algorithm that is used in the commercial asymmetric encryption algorithms.

The $T_p(x) \pmod N$ calculation speed is tested on an Intel Pentium 1700 MHz processor with 512 MB RAM, using equation (8). The test includes Java [31] and GNU multiple precision library [32] implementation. For N and p of order 1024 bits, calculating $T_p(x) \pmod N$ takes

$$
\begin{aligned}
\text{Java} &: \sim 700 \text{ ms}\\
\text{GMP} &: \sim 70 \text{ ms}.
\end{aligned}
$$

4.4. ElGamal public-key encryption with Chebyshev polynomials

The ElGamal public-key encryption scheme can be viewed as a Diffie–Hellman key agreement in key transfer-mode [8]. Its security is based on the intractability of the discrete logarithm-problem and the Diffie–Hellman problem. The basic ElGamal and generalized ElGamal encryption schemes are described in [8]. Here we generalize the ElGamal encryption scheme for Chebyshev polynomials.

(1) *Description of the algorithm.* The ElGamal public-key cryptographic system consists of two algorithms: an algorithm for key generation and an algorithm for encryption.

Algorithm for key generation.
Alice should do the following:

1. Generate a large random prime N and an integer x such that $x < N$.
2. Generate a random integer $s < N$ and compute $A = T_s(x) \pmod N$.
3. Alice's pubic key is (x, N, A); Alice's private key is s.

Algorithm for ElGamal public-key encryption.

1. Encryption. To encrypt a message m, Bob should do the following:
   (a) Obtain Alice's authentic public key (x, N, A).
   (b) Represent the message as an integer m in the range $\{0, 1, \ldots, N-1\}$.
   (c) Select a random integer $r < N$.
   (d) Compute $B = T_r(x) \pmod N$ and $X = mT_r(A) \pmod N$.
   (e) Send the cipher-text $c = (B, X)$ to Alice.
2. Decryption. To recover the message m from c, Alice should do the following:
   (a) Use the private key s to compute $C = T_s(B) \pmod N$.
   (b) Recover m by computing $m = XC^{-1} \pmod N$.

Proof that decryption works. This follows from the fact that

$$T_s(B) = T_s(T_r(x)) = T_r(T_s(x)) = T_r(A).$$

(2) *Example.* We now present an example with artificially small parameters.

Key generation. Alice chooses the prime $N = 1749940627$, integers $x = 25749480$ and $s = 7207480595$, and computes $A = 173359085$. Alice's public key is $(N = 1749940627, x = 25749480, A = 173359085)$, while her private key is $s = 7207480595$.

Encryption. To encrypt a message $m = 11223344$, Bob chooses an integer $r = 6431562606$ and computes $B = 1399079193$ and $X = 878048528$. He sends the cipher text $c = (B, X) = (1399079193, 878048528)$ to Alice.

Decryption. To recover the message m from c, Alice computes $C = 1376040233$ and $m = 11223344$.

(3) *Security.* If $x > 1$, the Chebyshev polynomial $T_n(x)$ can be written as

$$T_n(x) = \cosh(n \cosh^{-1}(x)).$$

Thus, if $y = T_n(x) \pmod N$, then, after some algebra, we find $n = \log_{x+\sqrt{x^2-1}} (y + \sqrt{y^2-1})$. In the case where both square roots, $\sqrt{x^2-1}$ and $\sqrt{y^2-1}$, exist in GF(N), one has a conventional discrete log problem. On the other hand, if at least one of the square roots exists in the quadratic extension field GF(N^2), this leads to a quadratic extension field generalization of the discrete log problem. Thus, the security of our modified ElGamal public-key algorithm is the same as the security of the original ElGamal algorithm.

4.5. RSA public-key encryption with Chebyshev polynomials

The RSA cryptosystem, named after its inventors, R. Rivest, A. Shamir, and L. Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem. This section describes the generalization of an RSA encryption scheme for Chebyshev polynomials. As in the case of an RSA cryptosystem, our system can be used for both encryption and digital signature and its security is based on the intractability of the integer factorization problem.

(1) *Description of the algorithm.* The RSA public-key cryptographic system consists of two algorithms: an algorithm for key generation and an algorithm for encryption.

Algorithm for key generation.
Alice should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $N = pq$ and $\phi = (p^2 - 1)(q^2 - 1)$.
3. Select a random integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. Alice's public key is (N, e); Alice's private key is d.

Algorithm for encryption.

1. Encryption. To encrypt a message m, Bob should do the following:
   (a) Obtain Alice's authentic public key (N, e).
   (b) Represent the message as an integer in the interval $[1, N - 1]$.
   (c) Compute $c = T_e(m) \pmod{N}$ and send to Alice.
2. Decryption. To recover the message m from c, Alice should do the following:
   (a) Use the private key d to recover $m = T_d(c) \pmod{N}$.

The integers e and d in RSA key generation are called the *encryption exponent* and the *decryption exponent*, respectively, while N is called the *modulus*.

Proof that decryption works. – It was shown in Section 4.2 that if p is an odd prime number and $0 \leq g < p$, then the period of the sequence $T_n(g) \pmod{p}$, $n = 0, 1, \ldots$, is a divisor of $p^2 - 1$. Since $ed \equiv 1 \pmod{\phi}$, there exists an integer k such that $ed = 1 + k\phi$. Thus, we find

$$T_d(T_e(x)) \equiv T_{de}(x) \equiv T_{1+k\phi}(x) \equiv T_1(x) \equiv x \pmod{p}.$$

By the same argument,

$$T_d(T_e(x)) \equiv T_{de}(x) \equiv T_{1+k\phi}(x) \equiv T_1(x) \equiv x \pmod{q}.$$

Finally, since p and q are distinct primes, we may use the Chinese remainder theorem to show that

$$T_d(T_e(x)) \equiv T_{de}(x) \equiv T_{1+k\phi}(x) \equiv T_1(x) \equiv x \pmod{N}.$$

(2) *Example.* We now present an example with artificially small parameters.

Key generation. Alice chooses the primes $p = 21787$ and $q = 3793$ and computes $N = 82638091$ and $\phi = 6829053595064064$. Alice chooses $e = 65537$ and, using the extended Euclidean algorithm, finds $d = 2150406320724737$. Alice's public key is the pair $(N = 82638091, e = 65537)$, while her private key is $d = 2150406320724737$.

Encryption. To encrypt a message $m = 11223344$, Bob computes

$$c = T_{65537}(11223344) \pmod{82638091} = 12355612.$$

Decryption. To decrypt c, Alice computes

$$T_d(c) \pmod{N} = T_{2150406320724737}(12355612) \pmod{82638091} = 11223344.$$

5. Conclusion

In this paper we have proposed public-key encryption algorithms using Chebyshev polynomials, which are both secure and practical and can be used for both encryption and digital signature. We have shown that ElGamal and RSA algorithms can be extended for Chebyshev polynomials. A fast algorithm for computing Chebyshev polynomials is suggested. The public-key algorithms and their properties depend, in a crucial way, on the properties of the discretized versions of two well-known chaotic maps: Chebyshev maps and toral automorphisms.

6. Appendix

6.1. Ideal theory in quadratic fields

In this Appendix we briefly summarize the ideal theory in quadratic fields, following [28], [29].

Quadratic integers. The solutions of the linear equations with integral coefficient, $ax + b = 0$, form the field of rational numbers. If the leading coefficient is equal to 1, $a = 1$, the solutions are integers. Following Dedekind, quadratic irrationals are defined as the solutions of quadratic equations with integral coefficients, whereas quadratic equations whose leading coefficient is 1 yield *quadratic*

integers. Thus $(1 + \sqrt{5})/2$ and $2i$ are quadratic integers, since they satisfy the equations $x^2 - x - 1 = 0$ and $x^2 + 4 = 0$, respectively. Quadratic integers coincide with the eigenvalues of 2×2 integral matrices. Sometimes, when the possibility of confusion arises, ordinary integers will be called *rational* integers.

Norm, units, and primes. By analogy with complex conjugates, we define the conjugate of a quadratic irrational $z = (a + b\sqrt{D})/c$ as $z' = (a - b\sqrt{D})/c$. The number $zz' = N(z)$ is called the *norm* of z. Then $N(z) = N(z')$ and $N(zv) = N(z)N(v)$. We shall be interested exclusively in real fields, where the norm of the number has nothing to do with its actual magnitude, and can even be negative. The norm of a quadratic integer is a rational integer.

The divisors of all rational integers are just 1 and -1, which are called *units*. The units of a quadratic field are precisely those quadratic integers of the field having unit norm. In real fields there is an infinity of units, forming a cyclic multiplicative group. So every unit can be expressed as a power of the generator of the group, which is called the *fundamental unit*. For instance, the golden mean $(1 + \sqrt{5})/2$ and $2143295 + 221064\sqrt{94}$ are fundamental units in their respective fields.

A quadratic integer z that is not a unit is called a prime if a factorization $z = uv$ is possible only when one of the two factors is a unit. For instance, $z = 2 + \sqrt{7}$ is a prime. Then one would hope that any integer can be factored in essentially only one way as a product of primes. The richness and difficulty of the arithmetic of quadratic integers depends largely on the fact that unique factorization generally fails.

Quadratic residues. The values of a for which the congruence in x,

$$x^2 \equiv a \pmod{p}, \tag{9}$$

is solvable are called *quadratic residues* of the odd prime p. The quadratic residue character is denoted by the Legendre symbol $(\frac{a}{p})$ [also written (a/p)], where

$$\left.\begin{array}{lll} (a/p) = 1, & \text{if} & x^2 \equiv a \pmod{p} \text{ solvable and } (a, p) = 1, \\ (a/p) = 0, & \text{if} & (a, p) = p, \\ (a/p) = -1, & \text{if} & x^2 \equiv a \pmod{p} \text{ unsolvable.} \end{array}\right\} \tag{10}$$

Thus, $[1 + (a/p)]$ is the number of solutions to equation (9) for any a.

Modules. We define a *module* as a set of quantities closed under addition and subtraction. Thus, when a module contains an element ξ, it contains $0(= \xi - \xi)$ as well as negatives $-\xi(= 0 - \xi)$ and integral multiples ($\xi + \xi$ written as 2ξ, $\xi + \xi + \xi$ written as 3ξ, etc.). We shall use capital letters $\mathcal{M}, \mathcal{N}, \mathcal{D}$, etc., to denote modules. We consider combinations of a finite set of vectors V_i,

$$u = x_1 V_1 + x_2 V_2 + \cdots + x_s V_s, \tag{11}$$

where the x_i range over all integers. The set of those u forms a module $\mathcal{M}$ and

the vectors V_i are called a *basis* of the module, written

$$\mathcal{M} = [V_1, V_2, \ldots, V_s].$$

Field. A field is a set of quantities taken from the complex numbers closed under the rational operations, namely addition, subtraction, multiplication, and division (excluding division by zero). In quadratic number theory, the field we consider is taken to be the set of surds $(a + b\sqrt{D})/c$ for a, b, c integral, D fixed and not a perfect square, and $c \neq 0$. It can be seen that addition, subtraction, multiplication, and division of such quantities lead to quantities of the same form. This field is written symbolically as $R(\sqrt{D})$, meaning that the set of surds is *generated* by adjoining $\sqrt{D}$ to the rationals. The field $R(\sqrt{D})$ is called a field over rationals. We now extract from D its (positive or negative) square-free kernel D_0, so that $D = m^2 D_0$. Note that $\sqrt{D}$ and $\sqrt{D_0}$ generate the same field. We define

$$\omega_0 = \begin{cases} \sqrt{D_0}, & \text{if } D_0 \not\equiv \pmod 4, \\ (1 + \sqrt{D_0})/2, & \text{if } D_0 \equiv \pmod 4. \end{cases} \tag{12}$$

Thus, the basis of quadratic integers in $R(\sqrt{D})$ is $[1, \omega_0]$. This module is designated by the symbol

$$\mathcal{D} = [1, \omega_0].$$

For example, the basis of $R(\sqrt{2})$ is $[1, \sqrt{2}]$, the basis of $R(\sqrt{5})$ is $[1, (1+\sqrt{5})/2]$, while $R(\sqrt{8})$ has the same basis as $R(\sqrt{2})$. In general, the field $R(\sqrt{m^2 D_0})$ is independent of m, and so is $\mathcal{D}$ and its basis.

The rational integer d, defined as

$$d = \begin{cases} D_0, & \text{if } D_0 \equiv \pmod 4, \\ 4D_0, & \text{if } D_0 \not\equiv \pmod 4, \end{cases} \tag{13}$$

is called a *field discriminant*. All numbers sharing the same discriminant d form a field.

Integral domain. A set of quantities taken from complex numbers which is closed under addition, subtraction, and multiplication (ignoring division) is called a *ring*. If a ring contains the rational integers, it is called an *integral domain*. The quadratic integers of a fixed field $R(\sqrt{D_0})$ form a domain which we call $\mathcal{D}$.

If the integral domain $\mathcal{D}$ of all quadratic integers of $R(\sqrt{D})$ contains an integral domain $\mathcal{D}^*$ which does not consist wholly of rationals, then $\mathcal{D}^*$ is characterized by some fixed positive rational integer n as the set of integers of $\mathcal{D}$ which are congruent to a rational integer modulo n. The integral domain $\mathcal{D}^*$ corresponding to n is written $\mathcal{D}_n$. Thus $\mathcal{D}_1 = \mathcal{D}$. Note also that $\mathcal{D}_n = [1, n\omega_0]$.

Ideals. We start with $\mathcal{D}_n$, a quadratic integral domain. We define an *ideal* $\mathcal{A}$ in $\mathcal{D}_n$ as a module in $\mathcal{D}_n$ with a special property that if $\alpha, \beta \in \mathcal{A}$ and $\xi \in \mathcal{D}_n$, then $\alpha \pm \beta \in \mathcal{A}$ (property valid for modules) and $\alpha\xi \in \mathcal{A}$ (property distinguishing

ideals). Starting with α, a fixed element of $\mathcal{D}_n$, we define the *principal ideal* in $\mathcal{D}_n$,

$$\mathcal{A} = (\alpha)$$

as the set of $\alpha\xi$ where $\xi \in \mathcal{D}_n$. The ideal (1) is called the *unit* ideal. We define the *sum* of ideals as the ideal $\mathcal{A} + \mathcal{B} = \{\alpha + \beta\}$, where $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$. We next define the *product* of two ideals $\mathcal{A}$ and $\mathcal{B}$ as the ideal $\mathcal{C}$ "generated by all products" $\alpha\beta$. We now say *ideal* $\mathcal{A}$ *divides ideal* $\mathcal{C}$ in $\mathcal{D}_n$ (or $\mathcal{A}|\mathcal{C}$ if and only if an ideal $\mathcal{B}$ exists in $\mathcal{D}_n$ for which $\mathcal{C} = \mathcal{A}\mathcal{B}$).

An *indecomposable ideal* in $\mathcal{D}_n$ is an ideal $\mathcal{Q}$ in $\mathcal{D}_n$ other than the unit ideal, which has no ideal in $\mathcal{D}_n$ as a divisor other than $\mathcal{Q}$ and $\mathcal{D}_n$. The integral domain $\mathcal{D}_1$ has unique factorization into indecomposables if and only if all ideals are principals.

A *prime ideal* in $\mathcal{D}_n$ is an ideal $\mathcal{P}$ in $\mathcal{D}_n$ other than the unit ideal, with the property that for any two ideals in $\mathcal{D}_n$, $\mathcal{A}$ and $\mathcal{B}$, if $\mathcal{P}|\mathcal{A}\mathcal{B}$, then $\mathcal{P}|\mathcal{A}$ or $\mathcal{P}|\mathcal{B}$. Every prime ideal $\mathcal{P}$ belongs to a rational prime p determined uniquely by $\mathcal{P}|(p)$.

The rational prime p factors in the quadratic field $R(\sqrt{D})$ (D is a square-free integer), according to the following rules based on d, the discriminant of the field, and (d/p), the Kronecker symbol,

$$\left.\begin{array}{lll} (p) = (p) & \text{or } p \text{ is inert (does not factor) if and only if} & (d/p) = -1, \\ (p) = \mathcal{P}_1\mathcal{P}_2 & \text{or } p \text{ splits into two different factors if and only if} & (d/p) = 1, \\ (p) = \mathcal{P}^2 & \text{or } p \text{ ramifies if and only if} & (d/p) = 0. \end{array}\right\} \tag{14}$$

6.2. *Dynamics and arithmetics*

In this section we briefly summarize the arithmetic properties of toral automorphisms, following [27]. Consider the dynamics of the following map:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & k \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}, \tag{15}$$

where x, y, k are integers and N, is prime. We further assume that $0 < x_0, y_0 < N$, and $2 < k < N$.

Let us consider a fixed value of the trace k, and let

$$\lambda = \frac{k + \sqrt{k^2 - 4}}{2}$$

be the eigenvalue of the matrix in equation (15). This determines an integral domain $\mathcal{D}_1$ to which the eigenvalue belongs. Let d be the field discriminant, i.e., let $d = D_0 \equiv \pmod 4$ or $d = 4D_0 \not\equiv \pmod 4$ where D_0 is the square-free kernel of $k^2 - 4$.

Consider now the unit ideal in $\mathcal{D}_1$ (i.e., $\mathcal{D}_1$ itself): $\mathcal{D}_1 = (1) = [1, \omega_0]$ where ω_0 is given by equation (12). Multiplying this ideal by λ we obtain the same ideal,

but with a different basis. Its elements are integral linear combinations of the basis elements 1 and ω_0 given by the equation

$$\lambda[1, \omega_0] = [m_{11} + \omega_0 m_{21}, m_{12} + \omega_0 m_{22}],$$

where the numbers m_{ij} are rearranged as a matrix

$$M' = \begin{bmatrix} m_{11} & m_{21} \\ m_{12} & m_{22} \end{bmatrix}. \tag{16}$$

Since λ is a unit of norm $+1$, the matrix M' is strictly unimodular (its determinant is equal to $+1$). We now identify the point $(x, y) \in Z^2$ with $z = x + y\omega_0$, i.e., z is a quadratic integer in the ideal (1). From (16) one obtains

$$\lambda z = \lambda x + \lambda y \omega_0 = x' + y'\omega_0.$$

One can see that multiplication by λ corresponds to the action of the transpose M of M' on Z^2: $M(x, y) = (x', y')$. In constructing the matrix M from (16), we have used the largest solution λ of the equation $\lambda^2 - k\lambda + 1 = 0$. This choice is not restrictive, since the smallest solution λ', which is conjugate to λ, would just correspond to the inverse matrix M^{-1}, as is easily verified. Note also that one can derive an explicit expression for M. Let $k^2 - 4 = m^2 D_0$ and let D_0 be a square-free kernel. Thus, for k odd, M reads

$$M = \begin{bmatrix} h & (h^2 + mh - 1)/m \\ m & h + m \end{bmatrix},$$

where $h = (k - m)/2$, while for k even, M reads

$$M = \begin{bmatrix} h & (h^2 - 1)/m \\ m & h \end{bmatrix},$$

where $h = m/2$.

We now determine, for each value of k, the properties of the orbits generated by M, a task which is greatly simplified by our choice of identifying Z^2 with the unit ideal in $\mathcal{D}_1$. Then, one can determine the properties of the orbits generated by other 2×2 matrices with integer entries and determinant $+1$. It turns out, however, that the orbit structure depends to a great extent on the eigenvalue λ alone, which depends only on one parameter, the trace k.

In order to take into account the periodicity of the torus, we use a "two-dimensional" modular arithmetic, identifying quadratic integers which differ by elements of the ideal $(N) = [N, N\omega_0]$. In other words, we identify the points of square lattices with side N. To do so, we need a generalization of the concept of congruence, since if $z = x + y\omega_0$ both x and y must be taken modulo N. We say that two quadratic integers v, z are congruent module an ideal $\mathcal{A}$, and write $v \equiv z \,(\mathrm{mod}\, \mathcal{A})$, if $v - z$ is contained in $\mathcal{A}$.

The period of an orbit through the point (x, y) is given by the smallest integer T satisfying the congruence

$$\lambda^T z \equiv z \,(\mathrm{mod}\, (N)), \qquad z = x + y\omega_0.$$

Note that since λ is a unit, $(\lambda)\mathcal{A} = \mathcal{A}$ for any ideal $\mathcal{A}$; thus, $\mathcal{A}$ is an invariant sublattice of Z^2. On the other hand, since one performs arithmetic modulo (N), the only invariant ideals on the torus are divisors of (N). To perform the ideal factorization of (N) (if N is an integer), we first determine its rational prime factors, $N = p_1 p_2 \dots p_n$, where p_i are rational primes. This corresponds to the ideal factorization $(N) = (p_1)(p_2)\dots(p_n)$. However, in our case, N is a prime number. In the following, an orbit which belongs to some ideal factor of (N) different from (1) will be called an *ideal orbit*, otherwise we shall speak of a *free orbit*. Bellow we state some results, which are proved in [27].

1. If $(d/N) = -1$, (N) is inert. All orbits are free and have the same period T, which is a divisor of $N+1$. If $T = (N+1)/m$, then there are $m(N-1)$ free orbits.
2. If $(d/N) = -1$, (N) splits. All orbits have the same period T, which divides $N-1$. If $T = (N-1)/m$, then there are $m(N-1)$ free orbits and $2m$ ideal orbits.
3. If $(d/N) = -1$, (N) ramifies. The periods of orbits are computed as follows. Let $\lambda = (k + b\sqrt{D_0})$ (with k and b both even if $D_0 \not\equiv 1 \pmod 4$). We have two cases:

   3(a). If $k \equiv 2 \pmod N$, there are $N-1$ ideal fixed points and $N-1$ free orbits of period N.

   3(b). If $k \equiv -2 (\mathrm{mod} N)$, there are $(N-1)/2$ ideal orbits of period 2 and $(N-1)/2$ free orbits of period $2N$.

6.3. Proof of Theorem 4.2

In this section we give a proof of Theorem 4.2. Consider the following matrix:

$$C = \begin{bmatrix} 0 & 1 \\ -1 & 2g \end{bmatrix}.$$

We write $\lambda = g + \sqrt{g^2 - 1}$ for its largest eigenvalue. Let $g^2 - 1 = m^2 D_0$, where D_0 is a square-free kernel. We define an integer d as follows:

$$d = \begin{cases} D_0, & \text{if } D_0 \equiv \pmod 4, \\ 4D_0, & \text{if } D_0 \not\equiv \pmod 4. \end{cases}$$

The proof of Theorem 4.2 follows directly from the following theorem:

Let N be an odd prime and let $g \in Z$ be such that $0 \le g < N$. Let T be the period of the sequence $T_n(g) \pmod N$ for $n = 0, 1, 2 \dots$. Then:

(i) *if $x^2 \equiv d \pmod N$ is solvable, then T is a divisor of $N-1$; otherwise*
(ii) *if $x^2 \equiv d \pmod N$ is unsolvable, then T is a divisor of $N+1$.*

The proof of this theorem, however, follows from the results of the previous Section 6.2 if $g \geq 2$. We need only to consider the cases $g = 0$ and $g = 1$. As mentioned in Section 4.2 the periods of the trajectories starting from the initial points $g = 0$ and $g = 1$ are always 4 and 1, respectively. Thus, for all odd primes N, the period of the sequence $T_n(g) \pmod N$ is a divisor of $N^2 - 1$.

References

[1] L. M. Pecora and T. L. Carroll, Synchronization in chaotic systems, *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[2] G. Kolumban, M. P. Kennedy, G. Kis, and Z. Jako, FM-DCSK: A novel method for chaotic communications, *ISCAS '98. Proceedings of the 1998 IEEE International Symposium on Circuits and Systems*, vol. 4, pp. 477–480, 1998.

[3] M. Sushchik, N. Rulkov, L. Larson, L. Tsimring, H. Abarbanel, K. Yao, and A. Volkovskii, Chaotic pulse position modulation: A robust method of communicating with chaos, *IEEE Commun. Lett.*, vol. 4, no. 4, pp. 128–130, 2000.

[4] L. Kocarev, Chaos-based cryptography: A brief overview, *IEEE Circuits Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[5] F. Dachselt and W. Schwarz, Chaos and cryptography, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 48, no. 12, pp. 1498–1509, 2001.

[6] M. P. Kennedy, G. Kolumban, G. Kis, and Z. Jako, Performance evaluation of FM-DCSK modulation in multipath environments, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 47, no. 12, pp. 1702–1711, 2000.

[7] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, Digital communication usnig chaotic pulse position modulation, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 48. no. 12, pp. 1436–1444, 2001.

[8] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1997.

[9] F. Pichler and J. Scharinger, Finite dimensional generalized Baker dynamical systems for cryptographic applications, *Lect. Notes in Comput. Sci.*, vol. 1030, pp. 465–476, 1996.

[10] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Internat. J. Bifur. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[11] G. Jakimoski and L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 48, no. 2, pp. 163–169, 2001.

[12] G. Jakimoski and L. Kocarev, Differential and linear probabilities of a block-encryption cipher, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 50, no. 1, pp. 121–123, 2003.

[13] N. Masuda and K. Aihara, Cryptosystems with discretized chaotic maps, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 49, no. 1, pp. 28–40, 2002.

[14] R. A. J. Matthews, On the derivation of a 'chaotic' encryption algorithm, *Cryptologia*, vol. 13, pp. 29–42, 1989; D. D. Wheeler, Problems with chaotic cryptosystems, *Cryptologia*, vol. 13, pp. 243–250, 1989; D. D. Wheeler and R. A. J. Matthews, Supercomputer investigations of a chaotic encryption algorithm, *Cryptologia*, vol. 15, no. 2, pp. 140–152, 1991.

[15] T. Kohda and A. Tsuneda, Statistics of chaotic binary sequences, *IEEE Trans. Inform. Theory*, vol. 43, pp. 104–112, 1997.

[16] L. Kocarev and G. Jakimoski, Pseudorandom bits generated by chaotic maps, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 50, no. 1, pp. 123–126, 2003.

[17] C. S. Petrie and J. A. Connelly, A noise-based IC random number generator for applications in cryptography, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 47, no. 5, pp. 615–621, 2000.

[18] T. Stojanovski and L. Kocarev, Chaos-based random number generators-part I: Analysis, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 48, no. 3, pp. 281–288, 2001.

[19] T. Stojanovski, J. Pihl and L. Kocarev, Chaos-based random number generators PART II: Practical realization, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 48, no. 3, pp. 382–385, 2001.

[20] A. Gerosa, R. Bernardini, and S. Pietri, A fully integrated chaotic system for the generation of truly random numbers, *IEEE Trans. Circuits Systems I: Fund. Theory Appl.*, vol. 49, no. 7, pp. 993–1000, 2002.

[21] L. Kocarev and Z. Tasev, Public-key encryption based on Chebyshev maps, *2003 IEEE International Symposium on Circuits and Systems*, May 25–28, 2003, Bangkok, Thailand, ISCAS 2003, accepted for publication.

[22] L. Kocarev, Z. Tasev, and J. Makraduli, Public-key encryption and digital-signature schemes using chaotic maps, *16th European Conference on Circuits Theory and Design*, September 1–4, 2003, Krakow, Poland, ECCTD 2003, accepted for publication.

[23] C. E. Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[24] C. E. Shannon, *Bell Syst. Tech. J.*, vol. 27, no. 379, 1948; vol. 27, no. 623, 1948.

[25] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory*, vol. 22, pp. 644–654, 1976.

[26] T. J. Rivlin, *Chebyshev Polynomials*, Wiley, New York, 1990.

[27] I. Percival and F. Vivaldi, Arithmetical properties of strongly chaotic motions, *Physica D*, vol. 25, nos. 1–3, pp. 105–130, 1987.

[28] H. Cohn, *A Second Course in Number Theory*, Wiley, New York, 1962.

[29] H. Hasse, *Number Theory*, Springer-Verlag, Berlin, 2002.

[30] D. E. Knuth, *The Art of Computer Programming*, vol. 2, Addison Wesley, Reading, MA: 1998.

[31] http://java.sun.com

[32] www.swox.com/gmp/