Pseudorandom Sequences obtained from Expansions of Irrational Numbers *

Hossein Ghodosi
Chris Charnes
Josef Pieprzyk
Rei Safavi-Naini

Department of Computer Science
Center for Computer Security Research
University of Wollongong
Wollongong, NSW 2500, AUSTRALIA

e-mail: [hossein/chris/josef/rei]@cs.uow.edu.au

August 2, 1995

Abstract

The main challenge in stream cipher design is to produce sequences that appear random. A number of keystream generators have been proposed and considered in the literature (several of those have been broken). The common characteristic of these keystream generators is that the obtained sequences are periodic.

This paper proposes a novel method for the generation of pseudorandom sequences. The method is based on the expansion of irrational numbers. In contrast to previous methods, our method produces non-periodic sequences.

It will be shown that binary sequences obtained from the expansions of irrational numbers behave randomly. In other words, the output sequences are indistinguishable from the truly random sequences. The advantages of our method, in contrast to the truly random generators (like tossing a coin), is that the sequences can be reproduced. The output of this pseudorandom generator is provably unpredictable provided the attacker does not know the secret seed.

1 Introduction

The operational disadvantages of perfectly secure stream cipher cryptosystems, which apply truly random sequences as the keystream, have led to the development of practically secure stream cipher systems [11]. The strength of such stream cipher cryptosystems, as practical secure cryptosystems, depends on the security of the keystream. Therefore, the main challenge in stream cipher design is to produce sequences that appear random. Since such sequences are

*Support for this project was provided in part by the Australian Research Council under the reference number A49530480

not truly random they are called *pseudorandom* sequences. Classical pseudorandom generators are deterministic algorithms with well known mathematical structures that output numbers or binary strings which "appear" random.

Statistical tests provide a useful tool for testing the quality of pseudorandom generators. Golomb [5] formulated three postulates that a binary periodic sequence should satisfy in order to be regarded as a *pseudo-noise* sequence. It has been shown that *m-sequences*, which are produced by linear feedback shift registers (LFSRs), can satisfy these properties. However, they are predictable and hence weak from a cryptographic point of view. For a system to be secure the keystream must be unpredictable, which means that knowing a part of the sequence should not enable a cryptanalyst to generate the whole sequence.

A number of keystream generators have been proposed in the literature, several of those have been broken (for example see [8], [12], [13], [15], and [4]). A number of keystream generators commonly used in stream ciphers are obtained by applying *non-linear* transformations to m-sequences. Some other keystream generators are developed based on combinations of LFSRs. The common characteristic of these keystream generators is that they produce periodic sequences. Although the period of the sequence is long, and in practice the whole sequence will not be generated, it does make the sequence vulnerable (the computational complexity of some cryptanalytic algorithms depends on the number of the register cells which are applied in the generator).

In this paper we propose a novel method for the generation of binary pseudorandom sequences as keystreams. The method is based on the expansion of irrational numbers. In contrast to conventional keystream generators our method produces non-periodic sequences.

The organization of the paper is as follows. In Section 2, some basic concepts are considered. Pseudorandomness of binary sequences obtained from the expansion of irrational numbers is considered in Section 3. Section 4 discusses the linear complexity of the sequences. Section 5 describes Cantor's diagonal method for generation of transcendentals. The KLL algorithm for algebraic number identification is discussed in Section 6. In Section 7, two pseudorandom generators of transcendentals are proposed.

2 Preliminaries

Let $S = s_1, s_2, s_3, \ldots$, be a binary sequence. The *period* of the sequence S is the smallest of p if $s_{i+p} = s_i$ for all $i > 0$. A *run* of length k starts at position t if $s_{t-1} \neq s_t = s_{t+1} = \ldots = s_{t+k-1} \neq s_{t+k}$. Two different types of runs exist [16]; a *block* of length k ($0\overbrace{11\cdots11}^{k}0$), and a *gap* of length k ($1\overbrace{00\cdots00}^{k}1$).

2.1 Randomness Postulates

In a sense, no finite sequence is ever truly random [5]. The most familiar example of a random binary sequence arises from tossing a perfect coin repeatedly, assigning 0 and 1 to the two possible outcomes. Golomb's randomness postulates for binary periodic sequences are as follows [5]:

1. If the period p is even, then the number of ones is equal to the number of zeros, otherwise the number of ones is one more than the number of zeros.

2. The frequency of runs of length k in a period is $\frac{1}{2^{k-1}}$. Moreover, half of the runs of a certain length are blocks and the other half are gaps.

3. The autocorrelation function $AC(k)$ has two values for a period p. Explicitly:

$$AC(k) = \frac{1}{p}\sum_{i=1}^{p} s_i s_{i+k} = \begin{cases} 1 & \text{for} k = np \\ \frac{-1}{p} & \text{otherwise} \end{cases}$$

where 0's of the sequence are replaced by 1's and 1's by -1's ($s_i s_j$ denote the multiplication of two bits s_i and s_j).

In [5] m-sequences are defined and necessary conditions for generating such sequences are proposed. It has been shown that m-sequences meet Golomb's randomness postulates in a satisfactory way. But, the main weakness of m-sequences is that they are very predictable. In fact knowledge of $2n$ consecutive bits of an m-sequence, which is produced by n cell registers, enables the cryptanalyst to determine the whole sequence [16].

2.2 Real Numbers

The decimal representation of a real number is finite or periodic if and only if the number is rational. By contrast the decimal representation of every irrational number is infinite and non-periodic. In this paper, when we talk about the expansion of an irrational number, we mean the fractional part of it. For example, the decimal expansion of $\sqrt{2}$ is $41421\cdots$. In other words, instead of $\sqrt{2}$, we consider the irrational number $\sqrt{2} - 1$ (later we will see the justification of this transformation).

In [9] it is shown that for any natural number m which is not the *d-th* power of an integer, $\sqrt[d]{m}$ is irrational. In general, real numbers which satisfy the equation of the form

$$a(x) = a_0 + a_1 x + \ldots + a_d x^d = 0$$

with integral coefficients, are either integers or irrational. Such numbers are called *algebraic* numbers. On the other hand, there are irrational numbers, which satisfy no such equations. Such irrational numbers are called *transcendental* numbers.

Definition 2.1 *A set S of real numbers is said to have the measure zero if it is possible to cover the points of S with a set of intervals of arbitrary small total length.*

As an example, the set of natural numbers has the measure zero. When the integer 1 is enclosed in the interval $(1 - \frac{\varepsilon}{2}, 1 + \frac{\varepsilon}{2})$, the integer 2 in the interval $(2 - \frac{\varepsilon}{4}, 2 + \frac{\varepsilon}{4})$, $\cdots$, and in general the integer n in the interval $(n - \frac{\varepsilon}{2^n}, n + \frac{\varepsilon}{2^n})$, the natural numbers are covered by intervals of total length $\varepsilon + \frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \cdots = 2\varepsilon$, which can be made arbitrarily small.

Definition 2.2 *We say that almost all real numbers in an interval have a certain property P if the set of real numbers (or points) lacking the property P has the measure zero.*

Definition 2.3 *A set is said to be countable (or denumerable) if it can be put in one-to-one correspondence with the natural numbers.*

3 Pseudorandom Binary Sequences from Expansions of Irrational Numbers

The question of when an infinite sequence of bits is random has been raised for a long time, and various reasonable definitions have been provided. The classical definitions of random sequences are similar to Golomb's randomness postulates. In several applications related to computer

science one would like a notion of randomness that implies some kind of unpredictability. The importance of this for cryptography as well as complexity theory is discussed in [14] and [17].

In this section we will show that sequences obtained from the *binary expansions* of irrational numbers pass the next bit test. Given a generator g and the first k output bits of the generator $s_1, s_2, \cdots, s_k$ (the input seed is kept secret [1]), it is not feasible computationally to predict $(k+1)-th$ bit of the output string, then g passes the next bit test.

Lemma 3.1 *Let $S = s_1 s_2 \cdots$ be a sequence of length (or period) n. Then there exists a sequence $T = t_1 t_2 \cdots t_k$, $k < n$, which is not a subsequence of the sequence S.*

Proof: Let k be the smallest natural number such that $n < 2^k$. Since k bits can represent 2^k different states of length k, there are states (sequences) of length at least k which have not occurred in S. □

Lemma 3.2 *There is at least one irrational number in whose binary expansion the finite binary sequence $S = s_1 s_2 \cdots s_k$ occurs.*

Proof: Let T be a sequence of length l which has not occurred in the sequence S (lemma 3.1). Extending S to $S \parallel T \parallel S \parallel T \parallel T \parallel S \parallel T \parallel T \parallel T \cdots$ gives an infinite and non-periodic sequence and thus is the binary expansion of an irrational number ($S \parallel T$ denotes the concatenation of two binary sequences S and T). □

Theorem 3.1 *There are infinitely many irrational numbers in whose binary expansions the finite binary sequence $S = s_1 s_2 \cdots s_k$ occurs.*

Proof: Assume that there are a finite number M of irrational numbers whose binary expansions contain the sequence S. Extending S by just one bit gives two different sequences $S \parallel 0$ and $S \parallel 1$. Thus extending S by i bits gives 2^i different finite length sequences (each of length $k+i$). We choose an i such that $2^i > M$. Hence there is a finite length sequence which can not appear in the binary expansion of any irrational number, a contradiction to the lemma 3.2. □

Since there is a one-to-one and onto mapping from the real numbers to the unit interval [0, 1], it is more convenient to use this interval to represent the irrational numbers. Thus the binary expansion of an irrational number α can be considered as $0.\alpha_1\alpha_2\alpha_3\cdots$. We show that the binary expansion of irrational numbers passes the next bit test.

Theorem 3.2 *Binary expansion of irrational numbers passes the next bit test.*

Proof: Let $\alpha_1, \alpha_2, \cdots, \alpha_k$ be the first k bits of the binary expansion of an irrational number and let the rational number $b = 0.\alpha_1\alpha_2\cdots\alpha_k$ be an approximation of all irrational numbers whose binary expansions begin with sequence $\alpha_1, \alpha_2, \cdots, \alpha_k$ (there are infinitely many of such irrational numbers). It is clear that those irrational numbers, which produce zero as the next bit belong to the interval $D_0 = (b, b + 2^{-(k+1)})$. Let $\gamma = \alpha_1, \alpha_2, \cdots, \alpha_k, 0, \cdots$ be one of such irrational numbers. No matter what the bits following 0 are, the value of this irrational number is greater than b but less than $b + 2^{-(k+1)}$ and hence $\gamma \in D_0$.

[1] In our method the irrational number is kept secret.

On the other hand, irrational numbers of the interval D_0 will generate the sequence $\alpha_1, \alpha_2, \cdots, \alpha_k, 0$. Because for any irrational number $\beta \in D_0$ the irrational number $(\beta - b) < 2^{-(k+1)}$ has the expansion $0.\overbrace{00\cdots0}^{k+1}\cdots$ (but not all zeros because it is an irrational number). Hence the binary expansion of β is of the form:

$$\alpha_1, \alpha_2, \cdots .\alpha_k, 0, \cdots + 0.\overbrace{00\cdots0}^{k+1}\cdots = \alpha_1, \alpha_2, \cdots, \alpha_k, 0, \cdots.$$

This proves that D_0 is the set of irrational numbers of the form $\alpha_1, \cdots, \alpha_k, 0, \cdots$ Similarly, it can be shown that all irrational numbers which generate one as the next bit are belong to the interval $D_1 = (b + 2^{-(k+1)}, b + 2^{-k})$, and conversely.

We assume that the set of real numbers with initial sequence $\alpha_1, \alpha_2, \cdots, \alpha_k$ is uniformly distributed. Then the probability that α_{k+1} be zero, given the knowledge of $\alpha_1, \alpha_2, \cdots, \alpha_k$, is the measure of the set D_0, which is $\frac{1}{2^{k+1}}$. Likewise, the probability that α_{k+1} be one is $\frac{1}{2^{k+1}}$. Hence the probability of either bit occurring is the same. □

4 Linear Complexity of Sequences

A powerful tool to attack a stream cipher system is to use the efficient synthesis procedure, proposed by Berlekamp-Massey [7], to find the shortest LFSR that is able to generate a given sequence. The algorithm processes a given sequence, $S = s_1, s_2, \cdots, s_n$, starting from s_1. In processing the element s_i the algorithm determines the shortest LFSR, and its corresponding characteristic polynomial, that is able to produce $s_1, s_2, \cdots, s_i$; thus at the end of the algorithm the shortest LFSR, and its corresponding characteristic polynomial, that can produce the sequence $S = s_1, s_2, \cdots, s_n$ will be determined. This length, *the length of the shortest LFSR that is able to produce a given sequence* is called the *linear complexity* of the sequence. The expected linear complexity, of a randomly selected sequence, is close to $\frac{n}{2}$, where n is the length of the sequence [11].

The most frequently cited example criticizing linear complexity measure is that of the sequence of length n with repeated zeros followed by one. This has the maximum linear complexity, which is equal to the length of the sequence. Rueppel compares the linear complexity profiles of an m-sequence of length 31, associated with the characteristic polynomial $f(x) = 1 + x^2 + x^5$, and the linear complexity profile of a sequence obtained by 31 tosses of a fair Swiss coin and concludes that a *typical* random sequence will have a linear complexity profile closely following the $\frac{n}{2}$ line. We will prove that the linear complexity profile of every unpredictable sequence follows the $\frac{n}{2}$ line.

Theorem 4.1 *If a sequence satisfies the next bit test, then its linear complexity profile follows closely the $\frac{n}{2}$ line.*

Proof: Let L be the value of the linear complexity in processing the element s_{i-1} of the sequence $S = s_1, s_2, \cdots, s_n$. If s_i is constructible by the characteristic polynomial, which is developed in processing of the s_{i-1}th element, then the linear complexity will not change. Otherwise, if $L < \lceil \frac{i}{2} \rceil$ then the linear complexity jumps to a position over the $\frac{n}{2}$ line ($\lceil a \rceil$ denotes the smallest integer equal to or greater than a). The amount of jump depends on $L - \lceil \frac{i}{2} \rceil$. For example, if $L = \lceil \frac{i}{2} \rceil - b$, then the jump will be equal to $2b$. Therefore, the maximum number of jumps will occur in the linear complexity profile of sequences which pass the next bit test, and hence, their linear complexity profile closely will follow the $\frac{n}{2}$ line. □

Corollary 4.1 *The linear complexity profile of binary sequences obtained from the binary expansion of randomly chosen irrational numbers follows closely the* $\frac{n}{2}$ *line.*

5 Cantor's Diagonal Method

In [6] a method is given for generating transcendental numbers. It is shown that Cantor's *diagonal* method is constructive and a computer program can be written to generate the digits of transcendental numbers. The diagonal method can generate n digits of a transcendental in $O(n^2 log^2 n log log n)$ steps. As the complexity of the diagonal method is less than $O(n^3)$, we can say that it is efficient enough for some applications which do not require a large volume of digits. In terms of Complexity Theory [3], the problem of transcendental number generation belongs to the class **P**.

The algorithm used in [6] to to generate transcendentals, is based on Cantor's proof of the two following theorems.

Theorem 5.1 *Given any sequence of real numbers and any interval* (α, β)*, one can determine a number* γ *in* (α, β) *that does not belong to the sequence. Hence, one can determine infinitely many such numbers* γ *in* (α, β)*.*

Theorem 5.2 *The collection of all algebraic reals can be written as an infinite sequence.*

Let $b = b_1, b_2, b_3, \cdots$ be a sequence of all algebraic reals in the interval $[0, 1]$.
Cantor's diagonal method generates the digits of a transcendental γ in $[0, 1]$ as follows.
Let $b(n)$ denote the n-th digit of b, where b is the binary representation of an algebraic real. The diagonal number of the sequence $b_1, b_2, b_3, \cdots$ of binary representations to be the real number whose binary representation d is obtained by the following rule:

$$\gamma(n) = \begin{cases} 0 & \text{if } b_n(n) = 0; \\ 1 & \text{if } b_n(n) = 1. \end{cases}$$

The digits generated by Cantor's diagonal method depend on the initial enumeration of the algebraics. Since there are $2^{\aleph_0}$ transcendental numbers and $2^{\aleph_0}$ enumerations of the algebraic numbers, all transcendentals can be generated by Cantor's diagonal method ($\aleph_0$ is the cardinality of the natural numbers).

Note that to generate different transcendentals, one needs to permute the sequence $b_1, b_2, b_3, \cdots$ of all algebraic numbers. This makes the algorithm impractical in stream cipher systems since the receiver must know this permuted version prior to the start of the communication.

To use transcendentals in stream cipher systems we require a generation method which can efficiently be indexed. That is, an algorithm that takes a finite length input and produces an arbitrary transcendental number. However this is not possible as any such method can only generate a subset of transcendentals. This consideration restricts us to subsets of irrational numbers that are efficiently indexable.

6 Weak Irrational Numbers

Algebraic numbers form a subset of irrationals that can be efficiently indexed using coefficients of their minimal polynomials. However, the resulting sequences are not secure.

An algebraic irrational can be randomly generated by random selection of a minimal polynomial $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ which uniquely defines the irrational α. The security

parameters of a such generator would be described by the pair (d, H) where d is the degree of $a(x)$ and H is the height of $a(x)$ i.e. all coefficients a_i $(i = 1, \ldots, d)$ are selected from the set of integers from the interval $[-H, H]$. Kannan, Lenstra and Lovász have shown in [10] that algebraic numbers can be identified.

They use the LLL-algorithm [1] to determine efficiently the minimal polynomial $a(x)$ of an algebraic irrational α from its approximation $\bar{\alpha}$. More precisely, their method (the KLL attack) identifies (in polynomial time) the polynomial $a(x)$ given $O(d^2 + d \log H)$ bits of the binary expansion of the algebraic number. As we have to assume that both parameters d and H are known to potential cryptanalysts, the binary expansions of algebraic irrationals are not secure pseudorandom sequences.

The technique described in [10] of determining an algebraic number from its approximation extends to certain classes of transcendental numbers. Examples of such numbers are: $cos^{-1}(\alpha)$, $sin^{-1}(\alpha)$ and $log(\alpha)$ where α is an algebraic irrational. This follows from Theorem 2.3 of [10]. We examine closely the hypothesis of this theorem.

Central to Theorem 2.3 of [10], is the assumption that there is a complex valued *approximable* function f which satisfies the *uniform Lipschitz condition*, for the precise definitions see [10]. Examples of such functions are: $sin(z)$, $cos(z)$. Kannan et al. have extended their algorithm to this setting. Their Theorem 2.3 asserts that there is an (efficient) algorithm which takes as input such a function f, parameters (d,H), a complex number $\bar{\beta}$, and outputs a complex number β which is approximated by $\bar{\beta}$, and an algebraic number $f(\beta)$ of degree at most d and height at most H. The assertion about the transcendental numbers $cos^{-1}(\alpha)$, etc., follows from this theorem.

7 Transcendentals Immune to KLL Attack

To avoid the KLL attack we should choose transcendental numbers not of the type $f^{-1}(\beta)$, where f and β satisfy the above conditions. We will consider two classes of transcendental numbers which seem suitable for cryptographic applications.

Class 1 - Simple exponentiation. Consider irrationals of the following form α^β, where $\alpha \neq 0, 1$ and β is a real quadratic irrational. They are known to be transcendental, see [2]. In particular $2^{\sqrt{2}}$, $2^{\sqrt{5}}$ are transcendental. Moreover transcendental numbers of the type α^β cannot be determined with the help of Theorem 2.3 of [10] as long as α and β are not revealed. Hence we propose to use the binary expansions of numbers of the form α^β, as (secure) pseudorandom sequences. Both α and β are kept secret and create a seed of the pseudorandom number generator.

Class 2 - Composite exponentiation. For our second class we require a theorem of Baker [2]. It is proved in [2], that numbers of the form $\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$, such that: the $\alpha_i \neq 0, 1$ and β_i are algebraic, and $1, \beta_1, \ldots, \beta_n$ are linearly independent over the rationals, are transcendental. The simplest numbers of this type have the form $\alpha_1^{\beta_1} \alpha_2^{\beta_2}$, where $\beta_1 = \sqrt{m}$, $\beta_2 = \sqrt{n}$, m, n natural non-square numbers. We take these as our second source. It is easy to show that if mn is a non-square, then $1, \beta_1, \beta_2$ are linearly independent over the rationals. Hence for such β_i, $\alpha_1^{\beta_1} \alpha_2^{\beta_2}$ is transcendental. An example of these numbers is $2^{\sqrt{2}} 3^{\sqrt{3}}$. Clearly, numbers $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ are secret and constitute a seed of the pseudorandom number generator.

7.1 Security Considerations

The class 1 transcendentals uses two index functions. The first one $I_\alpha : \{0,1\}^{n_\alpha} \to \mathcal{A}$ assigns an irrational $\alpha \in \mathcal{A}$ for a binary string of length n_α. The second one $I_\beta : \{0,1\}^{n_\beta} \to \mathcal{B}$ assigns an irrational $\beta \in \mathcal{B}$ for a binary string of length n_β. Both index functions are one-to-one. We can apply the KLL algorithm to identify the transcendental $T = \alpha^\beta$ in the following way. We will randomly select $\alpha' \in \mathcal{A}$ and calculate

$$\beta' = \log_{\alpha'} T \ .$$

The KLL algorithm is used to determine β'. This analysis is successful if $\alpha' = \alpha$ as the KLL will give the correct irrational algebraic number from the approximation of β. The complexity of the algorithm is $O(2^{n_\alpha - 1} p_{KLL}(n_\beta))$ where $p_{KLL}(n_\beta)$ is the time complexity function for the KLL algorithm to identify the algebraic number β.

Proposition 7.1 *Parameters α and β of the class 1 of transcendentals can be identified by an algorithm of the time complexity function*

$$p_{class1}(n) \leq O(2^{n_\alpha - 1} p_{KLL}(n_\beta)) \ .$$

Cryptanalysis of the class 2 transcendentals seems to be more complex then for the class 1 ones.

7.2 Efficiency of Computing the Generators

For simple exponentiation generators, we have $t = \alpha^{\sqrt{m}}$, m non-square integer and α algebraic $\neq 0, 1$. So $t = \exp(\sqrt{m} \ln \alpha)$. Thus in the case that α is an integer, we can obtain the decimal expansion of t and the binary expansion by standard numerical methods. For composite exponentiation generators, $t = \alpha_1^{\sqrt{m}} \alpha_2^{\sqrt{n}}$, and if α_1, α_2 are integers, the decimal expansion of t is the product of two decimal expansions of generators of the first type.

8 Conclusion

In order to generate pseudorandom sequences, which can be used as keystreams in stream cipher cryptosystems, we propose the binary expansion of irrational numbers. We have shown that the binary sequences obtained from binary expansions of irrational numbers are unpredictable.

Cantor's diagonal method can be used to generate transcendentals. The input for this method is a sequence of all algebraic reals. To generate an arbitrary transcendental, the sequence of all algebraic reals has to be permuted. The seed for the pseudorandom number generator based on Cantor's method, would be a permutation which acts on the sequence of all algebraic reals. In general, one can expect that the description of such permutations is equivalent to the generation of transcendentals. Therefore, Cantor's diagonal method, although efficient for a fixed permutation of all algebraic reals, is not suitable for cryptographic applications.

Attempts of designing of pseudorandom number generators based on algebraic reals are doomed to fail. The KLL attack efficiently identifies the algebraic real from its approximation. Also some generators which are derived from algebraic reals are susceptible to the KLL attack.

We have proposed two pseudorandom number generators. Both produce transcendentals and both are immune against the KLL attack.

ACKNOWLEDGMENTS

The first author would like to thank the University of Tehran for financial support of his study.

References

[1] H.W. Lenstra A.K. Lenstra and L. Lovász. Factoring Polynomials with Rational Coefficients. *Math. Ann.*, 261:513–534, 1982.

[2] A. Baker. *Transcendental Number Theory.* Cambridge University Press, 1975.

[3] M.R. Garey and D.S. Johnson. *Computers and Intractability.* Freeman, San Francisco, USA, 1979.

[4] J. Dj. Golić. Intrinsic Statistical Weakness of Keystream Generators. In *Advances in Cryptology - Proceedings of ASIACRYPT '94, Ed. J. Pieprzyk and R. Safavi-Naini, Lecture Notes in Computer Science, Vol. 917*, pages 91–103. Springer-Verlag, 1995.

[5] S.W. Golomb. *Shift Register Sequences.* Holden-Day, San Francisco, USA, 1967.

[6] R. Gray. Georg Cantor and Transcendental Numbers. *The American Mathematical Monthly*, 101(9):819–832, November 1994.

[7] J.L. Massey. Shift-Register Synthesis and BCD Decoding. *IEEE Trans. on Inform. Theory*, IT-15(1):122–127, January 1969.

[8] W. Meier and O. Staffelbach. Correlation Properties of Combiners with Memory in Stream Ciphers. In *Advances in Cryptology - Proceedings of EUROCRYPT '90, Ed. I.B. Damgård, Lecture Notes in Computer Science, Vol. 473*, pages 204–213. Springer-Verlag, 1990.

[9] I. Niven. *Irrational Numbers.* Mathematical Association of America, USA, 1956.

[10] A.K. Lenstra R. Kannan and L. Lovász. Polynomial Factorization and Nonrandomness of Bits of Algebraic and Some Transcendental Numbers. *Mathematics of Computation*, 50(181):235–250, January 1988.

[11] R.A. Rueppel. New approaches to stream ciphers. In *PhD Thesis to Swiss Federal Institute of Technology, Zurich*, 1984.

[12] R.A. Rueppel. Correlation immunity and the summation combiner. In *Advances in Cryptology - Proceedings of CRYPTO '85, Ed. H.C. Williams, Lecture Notes in Computer Science, Vol. 218*, pages 260–272. Springer-Verlag, 1986.

[13] R.A. Rueppel. Stream ciphers. In *Contemporary Cryptology - The Science of Information Integrity.* IEEE Press, New York, 1992.

[14] A. Shamir. On the Generation of Cryptographically Strong Pseudo-Random Sequences. In *Proc. 8th International Colloquium on Automata, Languages and Programming*, 1981.

[15] T. Siegenthaler. Correlation Immunity of Nonlinear Combining Functions for Cryptographic Applications. *IEEE Trans. on Inform. Theory*, IT-30:776–780, 1984.

[16] Henk C.A. Van Tilborg. *Introduction to Cryptology.* Kluwer Academic, USA, 1988.

[17] A.C. Yao. Theory and Applications of Trapdoor Functions. In *the 23rd IEEE Symposium on the Foundations of Computer Science*, pages 80–91, 1982.