UNIVERSITY OF NIŠ
The scientific journal **FACTA UNIVERSITATIS**
Series: **Mechanics, Automatic Control and Robotics** Vol.2, No 10, 2000 pp. 1393 - 1402
Editor of series: Katica (Stevanovi}) Hedrih, e-mail: katica@masfak.masfak.ni.ac.yu
Address: Univerzitetski trg 2, 18000 Niš, YU, Tel: +381 18 547-095, Fax: +381 18 547-950
http:// ni.ac.yu/Facta

ON CRYPTOGRAPHIC APPROACHES FOR SECURITY OF INFORMATION TECHNOLOGIES *

UDC 003.26:687.188:681.3.074(045)

Miodrag J. Mihaljević, Zoran M. Marković

Mathematical Institute, Serbian Academy of Science and Arts, 11001 Belgrade, Yugoslavia
E-mail: miodragm@turing.mi.sanu.ac.yu

Abstract. *Cryptographic approach for security of information technologies is addressed. Main facts about cryptology, a part of which is cryptography are summarized, and two examples related to methods for construction and analysis of certain basic cryptographic elements are presented. Finally, the main open problems are pointed out.*

Key words: *information technologies, security, cryptology, cryptography, cryptanalysis, cellular automata, iterative decoding techniques.*

1 Introduction

Security issue is one of the hottest topics in the information technologies (IT) (see [1], [2] and [3], for example), and particularly this is due to extensive development of the *e-commerce*, [1].

An information security service is a method to provide some specific aspect of security. For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service. Breaking an information security service implies defeating the objective of the intended service.

Information security is much broader issue than cryptography, but it is essential to note that without cryptography it is not possible to ensure high level of security.

Main goals of the paper are the following: (i) to point-out cryptographic methods as the most important ones for the IT security issue; (ii) to illustrate some of the cryptographic approaches by two examples.

This paper is far from an overview of the cryptographic approaches, and intention of the authors was to provide a non-specialist reader with some, hopefully, interesting information and motivation for more detailed consideration of the topic. Also, it is interesting to note that according to [4], cryptography is one of the major

Received September 04, 2000
* This research was supported in part by the Science Fund of Serbia, through the Mathematical Institute, Serbian Academy of Science and Arts.

topics in contemporary mathematics. Namely, at the begining, cryptography was more an art or a craft than a science, although based on some methods and techniques of the number theory. But the second half of the 20th century witnessed a veritable explosion of cryptology, which now employs a growing number of diverse mathematical fields and influences their development. While probability theory and statistics are now a foundation of many cryptographic methods (as illustrated in 3.2. below), cryptography influenced, for example, the introduction of stochastic methods into classical mathematics: stochastic proofs, which demonstrate something with high probability but not with certainty (e.g., in connection with primality testing), were quite a novelty for the mathematical world. Similarly for many other fields of mathematics, their results are used in cryptology, but also the new research is driven by the cryptological interest. This might not be so surprising for the fields which are bordering on computer science, like recursion theory, computational complexity, formal languages or finite automata (an example is given in 3.1.). But the same is true, for example, for large parts of algebra, like semigroups, finite fields (see 3.1.) or parts of algebraic geometry. The new field of quantum computing is generally expected to have its first practical application just in the domain of cryptography (for the secure distribution of keys, for example). A whole new field of protocols has emerged in cryptology, presently connected to mathematical logic and the theory of games but still awaiting an adequate mathematical treatment. In short, cryptology will be a driving force in the next century for many branches of mathematics, both as a field of applications and a source of challenging new problems.

The paper is organized as the following. Section 2 summarize main facts about cryptology, a part of which is cryptography. Section 3 presents two examples related to methods for construction and analysis of certain basic cryptographic elements. Concluding remarks, including some open problems are given in Section 4. Proofs of the lemmas and the theorem are given in the Appendix.

2 Cryptology

Simply speaking cryptology is the study of cryptography and cryptanalysis. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptanalysis is the study of mathematical techniques for attempting to defeat cryptographic techniques, and more generally, information security services. Accordingly, a main goal of cryptography is to deal with constructions of the systems for the IT security, and main goal of cryptanalysis is to deal with breaking of the given systems for the IT security. Cryptanalysis is also important for security evaluation and establishing the principles for design of secure cryptographic methods.

Main goal of cryptography is to give adequate methods for the following four IT security objectives that form a framework upon which the others can be developed.

a) *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. Secrecy and privacy are terms synonymous with confidentiality.

b) *Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation (such as insertion, deletion and substitution) by unauthorized parties.

c) *Authentication* is a service related to identification of entities and information itself. Two parties entering into a communication should identify each other, and information delivered over a channel should be authenticated as well. Accordingly, this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data authentication.*

d) *Non-repudiation* is a service which prevents an entity from denying previous commitments or activities. When disputes arise due to an entity denying that certain action were taken, non-repudiation service should resolve the dispute.

Cryptographic primitives can be defined as the basic cryptographic tools used to provide information security. Roughly speaking, cryptographic primitives can be classified as the following:

- symmetric key or secret key cryptographic primitives based on an underlying parameter, named key, which must be secret; this class of primitives include the following ones:
  - symmetric-key ciphers: stream and block ciphers
  - message authentification codes (MACs)
  - signatures
  - pseudorandom sequences
  - identification primitives;
- asymmetric key or public key cryptographic parameters based on two underlying parameters - keys where one should be public and the other should be secret; this class of primitives include the following ones:
  - public-key ciphers
  - signatures
  - identification primitives;
- unkeyed cryptographic primitives which do not require any secret parameter; this class of primitives includes the following ones:
  - hash functions
  - one-way permutations
  - random sequences.

A cryptosystem is a general term referring to a set of cryptographic primitives used to provide information security services.

3 Two Examples

This section presents two illustrative examples of the cryptographic techniques: an approach for construction of the cryptographic primitives, and an approach for security examination of certain cryptographic primitives for stream ciphers.

3.1 An approach for the constructions

A large number of cryptographic primitives are based on the finite state machine concept. In this section we point out a particular class of finite state machines. A well

known and widely used class of finite state machines are linear feedback shift registers; the intention of this section is to present another class of finite state machines known as the linear cellular automata which recently appeared as an interesting alternative.

Generally speaking, a linear finite state machine (LFSM) is a realization or an implementation of a certain linear operator. Linear feedback shift register (LFSR) and Linear Cellular Automaton (CA) are particular LFSMs. Following [7] this section summarizes the main characteristics of the CA over GF(q), assuming q is a power of a prime (for the background see also [5] and [6]).

A null-boundary linear hybrid cellular automaton is a LFSM composed of an one-dimensional array of n cells with the following characteristics. Each cell consists of a single memory element capable of storing a member of GF(q), and a next-state computation function. Here, we assume that communication between cells is only with the nearest-neighbor, so that each cell is connected to only its left and right neighbors. The leftmost and rightmost cells behave as though their left and right neighbors, respectively, are in state 0, and this make the CA null-boundary. At each time step t, cell i has a state $s_i^{(t)}$ (that is a member of GF(q)). The next-state function of a cell is its updating rule, or just rule. A linear CA employs linear next-state functions. If in a CA the same rule is applied to all cells, then the CA is called a uniform CA; otherwise it is called a hybrid CA.

For time step $t+1$, each cell i computes its new state $s_i^{(t+1)}$, using its next-state function f_i. In a CA, this function can depend only on the information available to the cell, and in the here considered case, it is the states of cells $i-1$, i, and $i+1$ at the time t. Since we require that f_i be linear,

$$s_i^{(t+1)} = f_i(s_{i-1}^{(t)}, s_i^{(t)}, s_{i+1}^{(t)}) = c_i s_{i-1}^{(t)} + d_i s_i^{(t)} + b_i s_{i+1}^{(t)},$$

and b_i, d_i, and c_i are constants from GF(q) characterizing the particular machine. The multiplication and addition operations are performed in the field GF(q). The number of possible functions f_i is the number of choices for b_i, d_i, and c_i, which is q^3. Hence, the number of rule configurations for an n-cell CA is $(q^3)^n = q^{3n}$.

We define the state of a CA at time t to be the n-tuple formed from the states of the individual cells, $s^{(t)} = [s_1^{(t)}, ..., s_n^{(t)}]$. The next-state function of the CA is computed as $s^{(t+1)} = f(s^{(t)})$,

$$s^{(t+1)} = [f_1(0, s_1^{(t)}, s_2^{(t)}), ..., f_i(s_{i-1}^{(t)}, s_i^{(t)}, s_{i+1}^{(t)}), ...] \ .$$

Since each f_i is a linear function, f is also a linear function, mapping n-tuples to n-tuples. Linearity implies that f has an $n \times n$ matrix formulation A, so that the previous expression can be rewritten as a matrix-vector product

$$s^{(t+1)} = f(s^{(t)}) = A s^{(t)} \ ,$$

where A is the transition matrix for the CA, and the product is a matrix-vector multiplication over GF(q).

Because the CA communication is restricted to nearest-neighbor, the matrix A is tridiagonal. The subdiagonal contains the multipliers on the left inputs of the cells;

likewise, the super-diagonal contains the right-input multipliers. The main diagonal consists of the self-input multipliers, and the rest of the matrix is 0:

$$A = \begin{bmatrix} d_1 & b_1 & 0 & \dots & 0 & 0 \\ c_2 & d_2 & b_2 & \dots & & 0 \\ 0 & c_3 & d_3 & \dots & & \cdot \\ & \cdot & \cdot & \dots & & \cdot \\ 0 & & & \dots & d_{n-1} & b_{n-1} \\ 0 & 0 & \dots & \dots & c_n & d_n \end{bmatrix} \quad (1)$$

The next state of cell i is the product of the ith row of A and $s^{(t)}$,

$$s_i^{(t+1)} = A_i \cdot s^{(t)} = c_i s_{i-1}^{(t)} + d_i s_i^{(t)} + b_i s_{i+1}^{(t)} \ .$$

An important CA characteristic relevant for cryptographic applications is the cycle length of its sequence of states. A CA has a maximum length cycle if the sequence of states $s^{(0)}$, $s^{(1)}$, $s^{(2)}$, ... , $s^{(0)}$ includes all $q^n - 1$ nonzero states for any nonzero starting state $s^{(0)}$.

Let the transition matrix of an LFSM be denoted A_{LFSM}. The characteristic polynomial of the LFSM is defined to be:

$$|xI - A_{LFSM}| \ ,$$

where x is an indeterminate, and I is the identity matrix with the same dimension as A_{LFSM}. The characteristic polynomial is primitive if and only if the LFSM has a maximal length cycle.

For more details on CAs see [9], [7] and [10], for example.

CA based constructions of certain cryptographic primitives are discussed in a number of papers (see [8], [12], [11], [19] and [20]). Particularly, recently a CA based construction of a keystream generator for stream ciphers and a cryptographic hash-function are proposed in [19] and [20], respectively.

3.2 An approach for the cryptanalysis

As an example of the methods for cryptanalysis (or security evaluation) of cryptographic primitives this section presents some results relevant for the cryptanalysis of certain keystream generators for stream ciphers. These results are of interest for the cryptanalytic approach known as "fast correlation attack" (see [3], for example) considered in a number of papers including [14], [25], [23] and [17]. This cryptanalytic approach is based on the iterative decoding techniques (see [13] and [18], for example).

Formally speaking, the problem under consideration is convergence analysis of the recursion specified by Definition 1.

Definition 1: The self-composition of the relevant Bayes error probability is defined as the recursion

$$P^{(l)} = P^{(l-1)} - f(P^{(l-1)}), \quad l = 1, 2, \dots \quad (2)$$

where $P^{(0)} = p \leq 0.5$ and $f(P)$ on $[0, 0.5]$ is given by

$$f(P) = \sum_{\mathbf{s}:\, q(P,\mathbf{s})>1} \Pr(\mathbf{S} = \mathbf{s}) \frac{q(P,\mathbf{s}) - 1}{q(P,\mathbf{s}) + 1}, \tag{3}$$

$q(P, \mathbf{s})$ is given by

$$q(P,\mathbf{s}) = \frac{P}{1-P} \prod_{w=1}^{n-1} \left(\frac{1 + (1-2P)^w}{1 - (1-2P)^w} \right)^{J - 2s_i(w)}, \tag{4}$$

n, J, p are certain parameters, and $\Pr(\mathbf{S} = \mathbf{s}) > 0$.

According to [16], we now give several lemmas and a theorem yielding the necessary and sufficient conditions for (2) to converge to zero. The proofs are given in the Appendix.

First note that $f(P)$ is a continuous nonnegative function on the segment $[0, 0.5]$ such that $f(0) = f(0.5) = 0$.

Lemma 1: The recursion (2) converges to 0 if and only if

$$f(P) > 0, \quad P \in (0, p]. \tag{5}$$

Lemma 2: For each $P \in (0, 0.5)$, we have that $f(P) > 0$ if and only if $q(P, \mathbf{0}) > 1$ where $\mathbf{0} = [0]_{w=1}^{n-1}$. Otherwise, $f(P) = 0$.

Lemma 3: Let $Q(P)$ be a function defined for $P \in (0, 0.5]$ by

$$Q(P) = \frac{P}{1-P} \prod_{w \in \Omega} \left(\frac{1 + (1-2P)^w}{1 - (1-2P)^w} \right)^{J(w)}. \tag{6}$$

Then, for $\Omega = \{1\}$ and $J(1) = 1$, we have $Q(P) = 1$, $P \in (0, 0.5]$. For $\Omega = \{1\}$ and $J(1) > 1$, we have $Q(P) > 1$, $P \in (0, 0.5)$, and $Q(0.5) = 1$. Finally, for $\Omega \neq \{1\}$, a critical value $P_0 \in (0, 0.5)$ exists such that $Q(P) > 1$ for $0 < P < P_0$, $Q(P_0) = 1$, $Q(P) < 1$ for $P_0 < P < 0.5$, and $Q(0.5) = 1$.

Theorem 1: The self-composition of the Bayes error probability converges to 0 for $0 < p < P_0$, and is in every iteration step equal to p for $P_0 \leq p \leq 0.5$. The critical value P_0 is equal to the unique value of $P \in (0, 0.5)$ such that

$$\frac{P}{1-P} \prod_{w \in \Omega} \left(\frac{1 + (1-2P)^w}{1 - (1-2P)^w} \right)^{J(w)} = 1 \tag{7}$$

if $\Omega \neq \{1\}$. For $\Omega = \{1\}$ and $J(1) > 1$, $P_0 = 0.5$, and for $\Omega = \{1\}$ and $J(1) = 1$, $P_0 = 0$.

4 Concluding Remarks

Security issue related to IT is one of the most important topics. Accordingly, this paper points-out cryptographic methods as the most important ones for the IT security issue, and illustrates some of the cryptographic approaches by two examples. The examples are related to an approach for construction of the cryptographic primitives, and an approach for security examination of certain cryptographic primitives for stream ciphers.

Finally, we can say that main, still open problems in cryptology include the following: (i) construction of the basic cryptographic elements (cryptographic primitives) suitable for high-speed implementations and with a desired level of the cryptographic security; (ii) developing methods for the security evaluation of cryptographic algorithms.

Appendix

Proof of Lemma 1: Since $f(P)$ is a nonnegative function not greater than P, the sequence $\{P^{(l)}\}_{l=1}^{\infty}$ is nonnegative and nonincreasing and, hence, it converges to a limit $P^* \in [0,p]$ such that $f(P^*) = 0$, that is, to a fixed point of the function $P - f(P)$. It follows that $P^* = 0$ if and only if (5) is true.

Proof of Lemma 2: Except in the degenerate case, according to (4), we obtain that for all $\mathbf{s} \neq \mathbf{0}$

$$q(P,\mathbf{0}) \; > \; q(P,\mathbf{s}), \quad P \in (0,0.5). \tag{8}$$

On the other hand, $\Pr(\mathbf{S} = \mathbf{s}) > 0$ for all $\mathbf{s}$. Therefore, in view of (3), it follows that the necessary and sufficient condition for $f(P) > 0$ is that a value of $\mathbf{s}$ exists such that $q(P,\mathbf{s}) > 1$. However, (8) implies that this is equivalent to $q(P,\mathbf{0}) > 1$.

Proof of Lemma 3: First note that $Q(P)$ is a positive and continuous function such that $Q(0.5) = 1$. Its first derivative on (0. 0.5)

$$Q'(P) \; = \; Q(P) \left(\frac{1}{P(1-P)} - \sum_{w \in \Omega} \frac{4J(w)w(1-2P)^{w-1}}{1-(1-2P)^{2w}} \right) \tag{9}$$

after a substitution $P = (1-x)/2$ becomes

$$Q'\left(\frac{1-x}{2}\right) \; = \; \frac{4Q(\frac{1-x}{2})}{|\Omega|(1-x^2)} F(x) \tag{10}$$

where for any $x \in (0,1)$

$$F(x) \; = \; \sum_{w \in \Omega} \left(1 + \frac{|\Omega| J(w) w (x^{w+1} - x^{w-1})}{1-x^{2w}} \right), \tag{11}$$

and $|\Omega|$ denotes the cardinality of Ω. The zeros of $Q'((1-x)/2)$ on $(0,1)$ are thus determined by $F(x)$. So, we proceed by analyzing $F(x)$.

When $\Omega = \{1\}$ and $J(1) = 1$, $F(x) = 0$ for all $x \in (0,1)$, meaning that $Q(P) = 1$, $P \in (0, 0.5]$. When $\Omega = \{1\}$ and $J(1) > 1$, $F(x) < 0$ for all $x \in (0,1)$. Since $Q(P) > 0$, $P \in (0, 0.5)$, it then follows that when $\Omega = \{1\}$ and $J(1) > 1$, $Q(P)$ is a decreasing function on $(0, 0.5]$ such that $Q(0.5) = 1$, as desired.

Assume now that $\Omega \neq \{1\}$. The first derivative of $F(x)$ on $(0,1)$ is

$$F'(x) \;=\; \sum_{w\in\Omega} -\frac{|\Omega|J(w)wx^{w-2}}{(1-x^{2w})^2}\left((w-1)-(w+1)(x^2-x^{2w})-(w-1)x^{2w+2}\right). \tag{12}$$

According to (12), we now analyze the following function on $(0,1)$, for any $w \in \Omega\backslash\{1\}$:

$$\Phi_w(x) \;=\; (w-1)-(w+1)(x^2-x^{2w})-(w-1)x^{2w+2}. \tag{13}$$

The first derivative of $\Phi_w(x)$ is

$$\Phi'_w(x) \;=\; 2(w+1)x\left(-1+wx^{2w-2}-(w-1)x^{2w}\right). \tag{14}$$

Consequently, for any $w \in \Omega \setminus \{1\}$, define the following function on $(0,1)$:

$$\phi_w(x) \;=\; -1+wx^{2w-2}-(w-1)x^{2w}. \tag{15}$$

The first derivative of $\phi_w(x)$ is

$$\phi'_w(x) \;=\; 2w(w-1)x^{2w-3}\left(1-x^2\right). \tag{16}$$

According to (16), $\phi'_w(x)$, $x \in (0,1)$, is a positive function, for each $w \in \Omega \setminus \{1\}$. In view of the fact that $\phi_w(0+) = -1$ and $\phi_w(1-) = 0$, we then obtain that $\phi_w(x)$, $x \in (0,1)$, is a negative increasing function, for each $w \in \Omega \setminus \{1\}$. So, according to (15) and (14), $\Phi'_w(x)$, $x \in (0,1)$, is a negative function, for each $w \in \Omega \setminus \{1\}$. On the other hand, using (13) we get $\Phi_w(0+) = w-1$ and $\Phi_w(1-) = 0$, so that $\Phi_w(x)$ is a positive function on $(0,1)$, for each $w \in \Omega \setminus \{1\}$.

Further, by (12) it follows that $F'(x)$ is a negative function on $(0,1)$. Since from (11) we obtain that $F(0+) = |\Omega|$ and $F(1-) = -\infty$, it then follows that $F(x)$ has exactly one zero on $(0,1)$. Using (10) and the fact that $Q(P) > 0$, $P \in (0, 0.5)$, we thus obtain that $Q'(P)$ has exactly one zero, P^*, on $(0, 0.5)$, and that $Q'(P)$ is a negative function for $0 < P < P^*$, and a positive one for $P^* < P < 0.5$.

Finally, from $Q(0+) = \infty$, $Q(0.5) = 1$, and the established characteristics of $Q'(P)$ it follows that for $\Omega \neq \{1\}$, a point $P_0 \in (0, 0.5)$ exists such that $Q(P) > 1$ for $0 < P < P_0$, $Q(P_0) = 1$, $Q(P) < 1$ for $P_0 < P < 0.5$, and $Q(0.5) = 1$, as desired.

Proof of Theorem 1: For $\Omega = \{1\}$ and $J(1) = 1$, the proof is trivial. For $\Omega \neq \{1\}$ or $\Omega = \{1\}$ and $J(1) > 1$, the existence of P_0 is established by Lemma 3. It then follows that $Q(P) > 1$ for any $0 < P < P_0$. By Lemma 2, $Q(P) > 1$ implies that $f(P) > 0$, $0 < P < P_0$. Finally, by Lemma 1, the self-composition converges to 0 if $0 < p < P_0$.

On the other hand, in view of Lemma 2, we have that $f(P) = 0$ for $P_0 \leq P \leq 0.5$, so that (2) implies that the Bayes error probability equals p in every iteration step if $P_0 \leq p \leq 0.5$.

References

[1] M. H. Sherif, *Protocols for Secure Electronic Commerce.* Boca Raton: CRC Press, 2000.

[2] M. Rozenblit, *Security for Telecommunications Network Management.* New York: IEEE Press, 2000.

[3] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography.* Boca Raton: CRC Press, 1997.

[4] V. I. Arnold, "Polymathematics: Is mathematics a single science or a set of arts", in *Mathematics: Frontiers and Perspectives*, Eds. V. Arnold, M. Atiyah, P. Lax, and B. Mazur, AMS Press, pp. 403-416, 2000.

[5] S. Wolfram, *Cellular Automata and Complexity.* Reading MA: Addison-Wesley, 1994.

[6] P.P. Chaudhuri, D.R. Chaudhuri, S. Nandi and S. Chattopadhyay, *Additive Cellular Automata: Theory and Applications.* New York: IEEE Press, 1997.

[7] K. Cattell and J.C. Muzio, "Analysis of one-dimensional linear hybrid cellular automata over GF(q)", *IEEE Trans. Computers*, vol. 45, pp. 782-792, 1996.

[8] S. Wolfram, "Cryptography with Cellular Automata", *Lecture Notes in Computer Science*, vol. 218, pp. 429-432, 1985.

[9] A.K. Das, A. Ganguly,A. Dasgupta, S.Bhawmik, and P. Pal Chaudhuri, "Efficient characterization of cellular automata", *IEE Proc. Pt. E*, vol. 137, pp. 81-87, Jan. 1990.

[10] K. Cattell and J.C. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata", *IEEE Transactions on Computer-Aided Design*, vol. 15, pp. 325-335, March 1996.

[11] S. Nandi, B.K. Kar and P. Pal Chaudhuri, "Theory and applications of cellular automata in cryptography", *IEEE Transactions on Computers*, vol. 43, pp.1346-1357, Dec. 1994.

[12] W. Meier and O. Staffelbach, "Analysis of pseudo random sequences generated by cellular automata", *Lecture Notes in Computer Science*, vol. 547, pp. 186-189, 1992.

[13] R. G. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. IT-8, pp. 21-28, Jan. 1962.

[14] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *Journal of Cryptology*, vol. 1, pp. 159-176, 1989.

[15] M. Mihaljević, M.P.C. Fossorier and H. Imai, "An algorithm for cryptanalysis of certain keystream generators suitable for high-speed software and hardware implementations", *IEICE Transactions on Fundamentals*, vol. E84-A, Jan. 2001.

[16] M. Mihaljević and J. Golić, "A method for convergence analysis of iterative probabilistic decoding", *IEEE Transactions on Information Theory*, vol. 46, Sept. 2000.

[17] M. Mihaljević, M.P.C. Fossorier and H. Imai, "A low-complexity and high-performance algorithm for the fast correlation attack", to appear in *Lecture Notes in Computer Science*,

[18] M. Fossorier, M. Mihaljević and H. Imai, "Reduced complexity iterative decoding of Low Density Parity Check codes based on Belief Propagation", *IEEE Transactions on Communications*, vol. 47, pp. 673-680, 1999.

[19] M. Mihaljević and H. Imai, "A family of fast keystream generators based on programmable linear cellular automata over GF(q) and time variant table", *IEICE Transactions on Fundamentals*, vol. E82-A, pp. 32-39, Jan. 1999.

[20] M. Mihaljević, Y. Zheng and H. Imai, "A family of fast dedicated one-way hash functions based on linear cellular automata over GF(q)", *IEICE Transactions on Fundamentals*, vol. E82-A, pp. 40-47, Jan. 1999.

[21] M. Mihaljević, "An improved key stream generator based on the programmable cellular automata", *Lecture Notes in Computer Science*, vol. 1334, pp. 181-191, 1997.

[22] M. Mihaljević, "Security examination of a cellular automata based pseudorandom bit generator using an algebraic replica approach" *Lecture Notes in Computer Science*, vol. 1255, pp. 250-262, 1997.

[23] M. Mihaljević and J. Golić, "A comparison of cryptanalytic principles based on iterative error-correction", *Lecture Notes in Computer Science*, vol. 547, pp. 527-531, 1992. (reprinted in *Lecture Notes in Computer Science*, vol. 1440, 1999)

[24] J. Golić and M. Mihaljević, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance", *Journal of Cryptology*, vol. 3, pp. 201-212, 1991.

[25] M. Mihaljević and J. Golić, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence", *Lecture Notes in Computer Science*, vol. 453, pp. 165-175, 1990.

[26] J. Golić abd M. Mihaljević, "Minimal linear equivalent analysis of a variable memory binary sequence generator", *IEEE Transactions on Information Theory*, vol. 36, pp. 190-192, Jan. 1990.

O KRIPTOGRAFSKIM PRISTUPIMA ZA BEZBEDNOST U DOMENU INFORMACIONIH TEHNOLOGIJA

Miodrag J. Mihaljević, Zoran M. Marković

U ovom radu se razmatra kriptografski pristup za ostvarivanje bezbednosti u domenu informacionh tehnologija. Prvo se rezimiraju osnovni stavovi o kriptologiji, čiji je sastavni deo kriptografija. Ističe se da su kriptografske tehnike neophodne za ostvarivanje visokog stepena bezbednosti (iako one same nisu i dovoljne za izgradnju kompletne bezbednosti). Zatim se kroz dva primera ilustruju neke tehnike od interesa za kriptografske metode. Prvi primer ukazuje na jedan pristup za konstrukciju osnovnih kriptografskih algoritama (kriptografskih primitiva), a drugi primer ukazuje na jednu tehniku za analizu nekih kriptografskih primitiva (generatora pseudoslučajnih nizova). Na kraju se ukazuje na dva ključna otvorena problema vezana za kriptografske metode.