BABEŞ-BOLYAI UNIVERSITY

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

Security in Networks and in Wireless Technologies

PhD Thesis Summary

Scientific Supervisor:

Prof. Univ. Dr. Florian M. Boian

PhD Student:

Bogdan Crainicu

Cluj Napoca, 2015

Contents of the Thesis

Keywords

randomness, algorithmic probability, algorithmic information theory, random sequence/stream, pseudorandom number generator, stream encryption algorithm, *RC*4, *KSA*, *RC*4*m*, *KSAm*, initialization vector *IV*, invariance weakness, *IV* weakness, distinguisher, $\text{distinguisher}_{\text{indicator}}$, corellation, $\text{corellation}_{\text{distinguisher}}$, correlation on pattern, $\text{distinguisher}_{\text{strong}}$, $\text{distinguisher}_{\text{weak}}$, X_N-uncertain state, X_N-weak-uncertain key.

List of publications

1. [CRA05] **Crainicu, B.**, "An Overview of the IPsec Extensions Header – AH (Authentication Header and ESP (Encapsulating Security Payload)", *Education/Training and Information/Communication Technologies – RoEduNet'05*: Proceedings of the 4th International Conference RoEduNet Romania: Târgu Mureş – Sovata, 20-22 May 2005, Editura Universităţii "Petru Maior" din Târgu Mureş, 2005, ISBN 973-7794-29-X, pp. 245-254.

2. [CRAI05] **Crainicu, B.**, "Web Security: Secure Socket Layer and Transport Layer Security", *Interdisciplinarity in Engineering: Proceedings of the Scientific Conference Inter-Ing 2005*: Târgu Mureş, "Petru Maior" University, Faculty of Engineering, 10-11 November 2005, Editura Universităţii "Petru Maior" din Târgu Mureş, 2005, ISBN 973-7794-41-9, pp. 787-800.

3. [CM06] **Crainicu, B**., Măruşteri, M., "PGP Cryptographic Keys and Key Rings", *Proceedings of the 5th RoEduNet IEEE International Conference*: Sibiu, 1-3 June 2006, Romania, Editura Universităţii "Lucian Blaga" din Sibiu, 2006, ISBN (10) 973-739-277-9, (13) 978-973-739-277-0, pp. 138-141.

4. [CRA08] **Crainicu, B.**, "Wireless LAN Security Mechanisms at the Enterprise and Home Level", *Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics*, Springer Netherlands, ISBN978-1-4020-8736-3 (Print), 978-1-4020-8737-0 (Online), 2008, pp. 305-310.

5. [CI08] **Crainicu, B.**, Iantovics, B.L., "Cryptanalysis of KSAm-like Algorithms", *First International Conference on Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing. CANS 2008*, Published by IEEE Computer Society, 2008, IEEE Computer Society Order Number P3621, ISBN 978-0-7695-3621-7, Library of Congress Number 2009900732, pp. 130-148.

6. [CRI08] **Crainicu, B.**, Iantovics, B., "On A New RC4 Key Scheduling Algorithm", *Proceedings of the International Conference Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing, CANS 2008*, 8-9 November, Târgu Mureş, 2008, Editura Universităţii "Petru Maior" Târgu-Mureş, 2008, ISSN 2065-0426, pp. 16-25.

7. [CRA09] **Crainicu, B.**, "A Local Search Approach for Recovering an Internal State of RC4 Stream Cipher", *11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2009*, Timisoara, Romania, September 26-29, 2009.

8. [CB10] **Crainicu, B.**, Boian, F., "KSAm – An Improved RC4 Key-Scheduling Algorithm for Securing WEP", *Novel Algorithms and Techniques in Telecommunications and Networking,* Springer Netherlands, 2010, ISBN 978-90-481-3661-2 (Print), ISBN 978-90-481-3662-9 (Online), pp. 391-396.

9. [CRB10] **Crainicu, B.**, Boian, F., M., "Some Combinatorial Aspects of the KSAm-like Algorithms Suitable for RC4 Stream Cipher", *Studia Universitatis Babes-Bolyai*, Series Informatica, Volume LV, Number 1, 2010, ISSN 1224-869x (paper version), ISSN 2065-9601 (online version), pp. 105-114.

10. [CE11] **Crainicu,B.**, Enăchescu, C., "A Metaheuristic Tabu Search Approach for Internal State Reconstruction of RC4", Proceedings *of 10th RoEduNet IEEE International Conference*, Iaşi, Romania, 23-25 June 2011, Published by Stef, 2011, ISSN 2247-5443, pp. 164-167.

11. [CI11] **Crainicu,B.**, Iantovics, B., "An Agent-based Security Approach for Intrusion Detection Systems", *7th International Workshop on Grid Computing for Complex Problems*, *GCCP2011*, Bratislava, Slovakia, October 24 - 26, 2011, Institute of Informatics, Slovak Academy of Sciences, ISBN 978-80-970145-5-1, pp. 126-133.

12. [CRA14] **Crainicu, B**., "On Invariance Weakness in the KSAm Algorithm", *8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014*, 9-10 October 2014, Tirgu-Mures, Romania, Elsevier, ISSN 2212 – 0173, pp. 850-857.

13. [IC08] Iantovics, B., L., **Crainicu, B**., "Complex Mobile Multiagent Systems", *First International Conference on Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing. CANS 2008*, Published by IEEE Computer Society, 2008, IEEE Computer Society Order Number P3621, ISBN 978-0-7695-3621-7, Library of Congress Number 2009900732, pp. 21-30.

14. [IAC08] Iantovics, B., L., **Crainicu, B.**, "Security in Mobile Multiagent Systems", *Proceedings of the International Conference Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing, CANS 2008*, 8-9 November, Târgu Mureş, 2008, Editura Universităţii "Petru Maior" Târgu-Mureş, 2008, ISSN 2065-0426, pp. 183-191.

15. [IM10] Iantovics, B., L., Marusteri, M., Kountchev, R., Zamfirescu, C., B., **Crainicu, B.**, "Intelligent CMDS Medical Agents with lerning Capacity", *Proceedings of the International Conference on Virtual learning. ICVL 2010*, October 29-October 31, 2010, Targu Mures, Romania, Bucharest University Press, 2010, ISSN 1844-8933, pp. 325-331.

16. [IC13] Iantovics, B., L., **Crainicu, B,** "Sisteme multiagent: o abordare modernă în inteligenţa artificială**",** Editura Universităţii "Petru Maior, ISBN 978-606-581-099-0, 2013.

17. [IC14] Iantovics, B., L., **Crainicu, B.**, "A Distributed Security Approach for Intelligent Mobile Multiagent Systems", *Advanced Intelligent Computational Technologies and Decision Support Systems, Studies in Computational Intelligence*, Volume 486, Springer International Publishing, 2014, ISBN 978-90-481-3661-2 (Print), ISBN 978-90-481-3662-9 (Online), pp 175-189.

18. [MCS061] Măruşteri, M., **Crainicu, B.**, Şchiopu, A., "ROBIOCLUSTER – an open source platform for HPC (high performance computing)/Linux clusters in the biomedical field", *Integrating Biomedical Information: From eCell to ePatient, Proceedings of the European Federation for Medical Informatics, Special Topic Conference*, April 6-8, 2006, Timişoara, Romania, Akademische Verlagsgesellschaft Aka GmbH, Berlin, ISBN 3-89838-072-6 (Aka), ISBN-10 1-58603-614-9 (IOS Press), ISBN-13: 978-1586036140 (IOS Press), ISBN 973-625-303-1 (Editura Politehnica), 2006, pp. 174-177.

19. [MCS062] Măruşteri, M., Ş., **Crainicu, B.**, Şchiopu, A., "New trends in Open Source Educational Platforms – The ROSLIMS Linux Live CD Paradigm", *Proceedings of the 5th RoEduNet IEEE International Conference*: Sibiu, 1-3 June 2006, Romania, Editura Universităţii "Lucian Blaga" din Sibiu, 2006, ISBN (10) 973-739-277-9, (13) 978-973-739-277-0, pp. 82-86. *Acta Universitatis Cibiniensis*, Vol. LV, Technical Series, Editura Universităţii "Lucian Blaga" din Sibiu, 2007, ISSN 1583-7149, pp. 136-140.

20. [MCS063] Măruşteri, M., **Crainicu, B.**, Şchiopu, A., *ROSLIMS Linux Live CD – all-in-one cross platform solution for running biomedical software*, Integrating Biomedical Information: From eCell to ePatient, Proceedings of the European Federation for Medical Informatics, Special Topic Conference, April 6-8, 2006, Timişoara, Romania, Akademische Verlagsgesellschaft Aka GmbH, Berlin, ISBN 3-89838-072-6 (Aka), ISBN-10 1-58603-614-9 (IOS Press), ISBN-13: 978-1586036140 (IOS Press), ISBN 973-625-303-1 (Editura Politehnica), 2006, pp. 178-181.

Original contributions / Results of the research

1. An unified formal model of sinchronous and asynchronous stream encryption algorithm, *AlgStream*(S_0, S, k, F_0, F, f, *crypt*, Z, M, C), based on the definition of a keystream generator $G(S_0, S, k, F_0, F, f, Z)$, that integrates the components: the component that initializes and modifies an internal state vector, using an initial secret key k or a secret seed k_s (*component*_1), the component that produces the secret keystream (*component*_2), and the component that perform the encryption task (*component*_3). (Section 4.3.)
2. Definition of the internal state size of a keystream generator implementat by an autonomous finite state machine.
3. A general known-plaintext attack model against stream encryption algorithms, *ModelAtacB*, which takes into account the highest degree of vulnerability of the encryption algorithm, established by the maximum amount of information to which an attacker may legitimately or illegitimately gain access. (Section 4.3.2.)
4. An attack method against the *RC*4 stream encryption algorithm, *TabuStateTable* (*TST*), which tries to reconstruct the initial state table *S* based on the approaches of the *Knudsen* attack, the tree representation and the general conditions defined in *Tomašević* attack, using a Tabu search strategy. The obtained results are superior to those of the *Knudsen* and *Tomašević* attacks. (Section 5.3.7.2.)
5. A key scheduling algorithm for the *RC*4 stream encryption algorithm, *KSA modified* (*KSAm*), which invalidate the *Fluhrer-Mantin-Shamir* invariance weakness of the original *KSA*, cancels the *IV* weakness by destroying the *Fluhrer-Mantin-Shamir* resolved condition**,** provides protection against *Ohigashi-Shiraishi-Morii* and *Klein/PTW* attacks in the *WEP* mode of operation, causes the inefficiency of the *Roos* weak keys and significantly reduces the *Mantin-Shamir* statistical bias of the keystream's second output *Z*. (Sections 6.1., 6.2., 6.3.3., 6.3.4.)
6. A general model of algorithmic approach for determining the mappings between bits of the secret key *K* and identifiable patterns from the initial permutation *S*, a model which can be used to test any *Scrambling* mechanism (e.g. *KSA*/*KSAm*) applied to a permutation which interchanges at every step the values of two entries based on two indices. (Section 6.2.4.)

7. A cryptanalysis model of the permutation's state *S* related to a stream encryption algorithm, based on the knowledge of the permutation's initial internal state *S*, the probability of preserving the permutation's initial internal state *S* and the probability of (*b*)-*conserving* the permutation *S* following the sequence of some permutation's *Scrambling* cycles of the values of the permutation's elements *S*. (Section 6.2.5.)

8. Definition of the concepts: *distinguisher*, $distinguisher_{indicator}$, $correlation_{general}$, $correlation_{distinguisher}$, *correlation on pattern*, *pattern associated to the output sequence*. Definition of a distinguishers class for stream encryption algorithms. Based on the distinguishers' values, designing attack mechanisms against the internal state related to stream encryption algorithms, with practical implementation and testing on *RC*4*m*. (Sections 6.3.1., 6.3.2.)

9. Definition of the correlation factor rc concept with the aim of redefining the concepts of *a-state* and *b-predictiveness* from [MS02], so as to be taken into account the correlations with the initial states, and of modeling the identification's process of the distinguishers based on predictive states from the statistic point of view. Correlation factor becomes a very useful element of cryptanalysis in the context where the initial secret state of a pseudorandom generation algorithm is obtained from a sequence of different cycles based on different constraints and a secret key – *RC*4*m* is such a case because of the *KSAm* algorithm which contains two different *Scrambling* sequences. (Section 6.3.3.)

10. Definition of the $distinguisher_{strong}$ and $distinguisher_{weak}$ concepts as criptanalysis tools for $S_i \rightarrow s_i$ and/or $S_i \rightarrow T_i$ correlations. (Section 6.3.3.)

11. Definition of the a_m-*state* and r_c-*b-predictive state* concepts, and identification of the distinguishers for the a_m-*states* which are r_c-*b-predictive*.

12. Determination of the advantage coefficient or distinguishing coefficient between a *RC*4/*RC*4*m* sequence and a pseudorandom one. (Section 6.3.4.)

13. Establishing the performance of the attack of the $distinguishers_{indicator}$'s / $distinguishers_{strong}$'s and $distinguishers_{weak}$'s identification from the set of the $distinguishers_{weak}$, based on *fortuitous states* and correlation factor r_c. (Section 6.3.4.)

14. Definition of the X_N-*uncertain* state and of the X_N-weak-uncertain key class which allow the identification and analysis of the most unlikely permutation *S*. (Section 6.3.5.)

I wish to particularly thank the scientific coordinator, Prof. Dr. Mircea Florian Boian for his openness, availability and invaluable support throughout the period of conception and elaboration of this thesis.

I address my sincere thanks to Prof. Dr. Călin Enăchescu for his encouragement and help during these years.

I thank to my family for the enormous support that they offered.

At the same time, I wish to thank colleagues from the Department of Computer Science of the "Petru Maior" University of Târgu-Mureș, and colleagues from the Faculty of Mathematics and Computer Science of the " Babes-Bolyai" University of Cluj-Napoca, for their constructive opinions and suggestions .

Summary

The PhD thesis "*Security in Networks and in Wireless Technologies*" is based on the analysis of the principles and mechanisms underlying stream protocols and encryption algorithms, as a component of symmetric cryptography. Bearing in mind that stream encryption algorithms are intrinsically linked to generators of random numbers/sequences and pseudo-random, besides detailing notions, model and the necessary formalisms for building stream cryptographic systems, thesis contains a summary of the basic concepts that define the randomness concept from the perspective of classical probability theory, Shannon's information theory and, in particular, algorithmic probability, and algorithmic information theory, presenting the main algorithmic approach of randomness. In cryptographic terms, the randomness concept is the central element in the design of (pseudo)random number generators that produce encryption keystream or the final encryption key within the sequential ciphers.

The comparison between stream and block ciphers, the efficiency metric of the encryption process must be defined very clearly. The paper [PP10] specifies that for software-optimized stream ciphers, efficiency means fewer processor cycles are needed to encrypt a bit, and for hardware-optimized stream ciphers, efficiency means that fewer hardware gates are needed to encrypt at he same data rate. Analysis of the efficiency of the encryption process must not neglect the fact that the mode of operation of certain block ciphers are converted into synchronous stream ciphers (for example, operating modes *CTR – Counter* and *OFB – Output feedback*).

Besides the advantages deriving from implementation simplicity and high speed encryption, stream ciphers are linear in time and and constant in space, and, an aspect not neglected, the propagation of errors is very low — an error occurred during encryption of a byte or symbol does not affect the encryption of bytes or symbols which follows (synchronous stream cipher), or an error in the encrypted text affects at most t bytes or symbols in decrypted plaintext (asynchronous stream cipher); thus, the stream ciphers are very useful where the transmission errors occur with high probability. Stream ciphers exhibit two major disadvantages: low diffusion due to the fact that the information in a byte or symbol in the plaintext is contained in a single byte or symbol of the encrypted text, and, compared to block ciphers, an attacker who broke the algorithm can easily insert forged text what seems authentic.

One of the most popular and most used stream ciphers are: *A*5/1, *CryptMT*, *ISAAC*/*ISAAC*+, *Rabbit*, *RC*4, *Scream*, *SEAL*, *SNOW*, *Trivium*, *Turing*, *VEST*.

The thesis focuses on analysis of stream cipher *RC*4 (*Rivest Cipher* 4 or *Ron's Code* 4), showing the main cryptanalytic results occurring in the literature, with a particular focus on vulnerabilities discovered in the key scheduluing component, from the point of view of both algorithm architecture, as well as from that of its modes of operation. *RC*4 is regarded as one of the fastest encryption algorithms at software level, and it is still the most used stream cipher, being found in widespread cryptographic implementations: *SSL/TLS*, *IPsec-ESP* (*Encapsulating Security Payload*), *Kerberos*, *RDP* (*Remote Desktop Protocol*), *Microsoft Point-to-Point Encryption*, *SSH* (*Secure Shell*), *SASL* (*Simple Authentication and Security Layer*) etc. Studies and researches carried out in the course of time on *RC*4 algorithm have revealed the fact that critical vulnerabilities arise not primarly from its architecture, but especially in the way it is implemented in the various operating modes. Surely, the most eloquent example is *WEP* (*Wired Equivalent Privacy*), a protocol now considered extremely vulnerable to wireless transmissions [CRA08]. Starting from cryptanalysis of Fluhrer, Mantin and Shamir [FMS01], Klein in [KLA08] and Tews, Weinmann and Pyshkin in [TW08] implement a practical attack that allows recovery of 95% of a 104-bits *WEP* key by capturing at least 85000 packages which shares the same *IV*s (*Initialization Vectors*). However, the success of the attack speculates the faulty use of the nonsecret 24-bits *IV*s (a size too small), which is concatenated with 104-bits secret key to form a a secret 128-bits seed that becomes the input data for the pseudorandom number generator *WEP PRNG*; *WEP PRNG* generates then a sequence of pseudorandom bytes, the keystream, used for message encryption. How it was natural, the industry has reacted quickly, but removal of proven vulnerabilities of the *WEP* protocol was realized with substantial costs: instead of changing the mode of operation of the *RC*4 algorithm, it was chosen to replace it with the *AES* block cipher (*Advanced Encryption Standard*), together with changing the algorithm for *MIC* (*Message Integrity Check*), resulting the *WPA2* mechanism (*Wi-Fi Protected Access II*), process that required complete replacement of existing hardware that does not have support for *AES*. In this context, the thesis suggests at least a solution that strengthens considerably the level of security offered by the *WEP* protocol.

If the *IV* is kept in the *RC*4 mode of operation, cryptologists are unanimously agreed that the enforcement of strict security conditions to these *IV*s (unrepeatability, randomness, increased size), combined with the use of a minimum 256-bits secret key size and removing the first 256 bytes (minimum) of the keystream, basically determines the impenetrability of the RC4 cipher.

In these circumstances, taking into account the statistical properties of the generator which it incorporates, combined with its high operating/encryption speed, the *RC*4 architecture can still remains an important option for stream encryption, especially in wireless transmissions in which distribution and mobility of the nodes is high, and in mobile multiagent systems [IC08], [IAC08], [IC14], [CI11], [IM10].

The thesis proposes an improved mechanism for key scheduling algorithm, *KSAm* (*Key Scheduling Algorithm modified*) for *RC*4 stream cipher and a new attack method against *RC*4 that aims to reconstruct the initial secret state table. Advancing new formal models of cryptanalysis (methods of cryptanalytic attack) against key scheduling algorithm which is based on the sequential modification of two values from a vector that represents the internal state of the stream encryption algorithm, models tested on *RC*4 and *RC*4*m* (*RC*4 cipher with *KSAm* as key scheduling algorithm). A set of successful attacks against *RC*4 are tested against *RC*4*m* as well, the results of these tests demonstrating the viability of the proposed *KSAm* mechanism.

The thesis is divided into 6 chapters and 2 annexes.

Chapter 1, Randomness. Random sequences/streams, includes a summary of the concept of randomness. This concept is a fundamental component of cryptography, in particular in the study and design of stream cryptographic algorithms. For this reason, starting from the classical probability theory and Shannon's information theory, the chapter focuses on the detailed synthesis of the notion of randomness from the perspective of algorithmic probability and algorithmic information theory.

The property of randomness assigned to a phenomenon/process/event/system /behavior is directly related to a set of other interdependent concepts as chance, entropy, (un)predictability, stochasticity, (in)determinism, chaos/disorder, hazard, uncertainty, (un)typicality, that allow to create a framework for defining, more or less complete, the property of randomness. Logically, the property of randomness implies lack of predictability, coherence, determinism, order, elements' correlation within within a sequence of characters/symbols/numbers/bits/steps. Any process/phenomenon which cannot be predicted should be treated in terms of randomness. According to [EAG05], one cannnot equate the randomness and unpredictability (although one of the mathematical approaches of randomness is from the perspective of unpredictability), the property of randomness being a special case of the concept of unpredictability of a process or phenomenon; therefore, it can be asserted that the property of randomness is unquestionably unpredictable. However, regardless of the analysis approaches of randomness (stochastic/unpredictable, chaotic/incompressible, typical), the challenge, from the mathematical

point of view, is extremely high in terms of formalization/definition, or of attempt to formalize/define the concept of randomness.

The requirement that results of a random phenomenon/process/event cannot be integrated into any deterministic structure does not mean that such a structure does not exist, just that, at least, it was not found – hence starts the doubt about the real existence of randomness. This aspect, combined with the notion of appearance through which a sequence of numbers/bits which ”seems” to be random for an algorithm/adeversar, may ”not” appear random for another algorithm/opponent, leads to the need of formulating different algorithmic approaches for randomness, constructed above the previous intuitive definitions in the form of supersets of parameterized specifications that finally allow establishing of some formal definitions for randomness.

Muchnik, Semenov and Uspensky outlined in [MSU98] the axis of intuitive approach for randomness, indicating that the pairing of randomness with sequences depends on the probabilistic model chosen and agreed in advance – a sequence for which it has defined in advance a measure (metric) for randomness must be declared random or nonrandom based on that measure (metric). From this point it has to start for an algorithmic, granular definition of the concept of randomness.

Li and Vitanyi outlined in [LIV08] that the classical probability theory cannot cover the concept of randomness for individual sequences, it can only express the properties' probabilities associated with the results of a random event/process, i.e. the properties' probabilities of the complete set of sequences for a particular distribution, being unable to define what it means for an individual sequence to be random.

Furthermore, the classical probability theory does not provide the tools to question the result of an event after it has occurred – the only option available is to exclude in advance the ”inequity” of the possible result by taking measures more or less restrictive [VIT01]. Chaitin writes in [CHAG75] that although the notion of randomness can be precisely defined and, moreover, can be measured, the classical probability theory is not able to determine whether a given individual number is random or nonrandom. Therefore, Chaitin suggests that a much more sensitive definition is necessary for randomness. To solve this problem, i.e. providing mathematical components that allow the definition of the property of randomness, consists in using the probability measure function, which specifies the probability to observe any event from an experiment whose result is uncertain, representing the fundamental notion of the modern probability theory, whose axiomatic were established by Kolmogorov in 1933 [KOL56].

From the point of view of information theory, the entropy of a random variable, defined by Shannon in [SHA48], in the context of the probability distribution of the variable in question, constitutes a measure of relativity/insecurity/indeterminism/uncertainty/disorder – Shannon defines entropy as a measure of information distribution. Shannon presents in [SHA48] connection between thermodynamic entropy and information theory entropy, suggesting that it is possible to measure the information content of a message and how to correctly convey a message correctly in the presence of noise.

The Shannon entropy is actually a functional mapping between random variables (distributions of random variables) and real numbers. The main interpretation of the Shannon entropy is to establish the number of bits needed for the representation/coding of the random variables' values. One of the important Shannon's observations is that semantic aspects of a message are irrelevant to the engineering process of handling the message. According to information theory formulated by Shannon, a set of possible messages is assigned a quantity of information, which represents the number of bits needed to consider all the possibilities of representation of messages (it is assumed that all messages are equal). Therefore, messages can be handled as a whole, using this number of bits. But Shannon does not make any indication about the number of bits required for handling/transmission of an individual message from that set/ensemble. The examples presented in the literature [GV03], [GW04] reveals that some strings of bits (representations of messages) can be compressed, but with the risk of iregularities occurence which means the removal of the property randomness for the (compressed) string of bits. Instead, if any element of regularity is missing, it becomes extremely difficult to represent large numbers. The conclusion that emerges is the need to have a measure of information which, in contrast to the approach of Shannon, to not rely on probabilistic assumptions and to take into account the fact that the strings that contain regularity elements are collapsible [GV03], [GW04]. Therefore, it must found/defined this measure applicable to both the information content of individual finite object (finite binary string) and the amount of information held by a finite object with respect to another finite object [KOL65].

Thus, the classical probability theory and information theory defined by Shannon cannot provide a rigorous definition of the property of randomness. Shannon's information theory measures probabilities within a system of events, where a lot of possible results occure, but it cannot analyze a single event extracted and isolated from the system.

If the (intuitive) definitions of the property of randomness are clearly formulated, logically and conceptually, difficulties that arise are related to precise establishing the measures/metrics

associated with the property of randomness (probabilistic model selection, according to [MSU98]), on the one hand, and in validating the nondeterministic template of random sequence, on the other hand; actually, response should be given to the the question: what are the mathematical measures/metrics which determine that a sequence is random?

Thus, formalizing the definition given for the property of randomness and for random sequence, from algorithmic perspective, consists in establishing/defining the measures/metrics for the property of randomness, creating related tests based on these measures/metrics, and imposing the condition of passing/meeting the respective tests.

Solomonoff proposes and develops in [SOL60], [SOL164], [SOL264], [SOL78], [SOL97] the notion of algorithmic probability, which allocates to an object a priori probability with universal value. Having theoretical applicability in important areas (artificial intelligence, analysis of the time complexity of algorithms, theory of inductive inference) and facilitating a superior understanding of the property of randomness, the most important shortcoming of the algorithmic probability lies in the fact that it is not calculable in practice and can be only approximated.

Algorithmic Information Theory (*AIT*) is based on the concept of Solomonoff's algorithmic probability, fundamental results in this field were obtained by Lomogorov [KOL65] and Chaitin [CHA66], [CHA69], [CHA74], [CHAG75], [CHA75], [CHA76], [CHAG76], [CHAG77].

In the paper [KOL65], Kolmogorov defines the concept of information from combinatorial, probabilistic and algorithmic perspectives. Within combinatorial approach, Kolmogorov characterizes the entropy using language alphabets and set of elements. To address the probabilistic approach, Kolmogorov analyses random variables, with a certain probability distribution. In the algorithmic approach, relying on recursive functions, Kolmogorov suggests a method of efficient describing the length $l(s) = n$ of a string s, on $log_2\ n + log_2\ log_2\ n + log_2\ log_2\ log_2\ n$ + ... bits, continuing recursively to the last positive term, method which allows to describe the amount of information [ZAW].

AIT can be considered as information theory (the theory of information content) of an individual object, and treats, based on computational theory, the links between information, computing and randomness. By combining information theory with computational theory, *AIT* creates the concept of information whitin an individual object or (algorithmic) complexity of an individual object, and, further, of the randomness assigned to individual objects, elements that cannot be found in the Shannon's information theory. If the Shannon's information theory measures only the amount of information, the algorithmic part of *AIT* measures the content of information using algorithms (programs).

Both Shannon's information theory and algorithmic information theory start with the idea that the amount of information about a phenomenon can be measured by the minimum number of bits needed to describe the observation [GW08]. But whereas Shannon's theory considers description methods that are optimal relative to some given probability distribution, *AIT* takes a dfferent, nonprobabilistic approach: any computer program that first computes (prints) the string representing the observation, and then terminates, is viewed as a valid description – the amount of information in the string is then de_ned as the size (measured in bits) of the shortest computer program that outputs the string and then terminates [GW08]. Thus, a first deinition of the algorithmi complexity of a string (object) is determined by the length of the shortest program or set of algorithms that describes or outputs that string (object) on a universal Turing machine.

Starting from the concept of algorithmic probability invented by Solomonoff several approaches have been proposed to formalize the property of randomness assigned to an individual object/ sequences, equivalent up to a certain level, the most important being the following approaches:

- approach of randomness from a stochastic perspective – *stochasticity* (*unpredictability*)
- approach of randomness from a chaotic perspective – *chaoticity* (*incompressibility*)
- approach of randomness from a typical perspective – *typicality*

Stochastic analysis of the property of randomness [Mises, Wald, Church, Kolmogorov, Loveland] assumes that, in order to be random, the sequence itself, together with its subsequence property must have the property of stability of frequencies, i.e. to meet all the "reasonable"statistical tests – any arbitrary sequence of length k must have the same frequency limit (2^{-k}) or the same degree of nepredictibilitate (for example, the numbers of zero in a sequence to be asymptotically equal to the numbers of one). It appears, therefore, the notion of nepredictibilitate in defining the property of randomness, and that can be treated in terms of the impossibility of building a successful game strategy. The first attempt to define the property of randomness for an individual object from a stochastic perspective was made by von Mises in [MIS19], [MIS57], trying to mathematically formalize the intuitive notion of a string which appears "more" random than another as a result of statistical analysis of the properties of some repetitive events. von Mises was interested in applying the probability theory to the study of real phenomena of nature and he advanced the idea that the study of the probability theory is intrinsically related to the study of random sequences. In an attempt to overcome the criticism of Ville to the stochastic approach of randomness,

Kolmogorov [KOL63] and Loveland [LOV66] independently admit computable selection rules, but they propose a model of nonmonotonic selection. These selection rules are called Kolmogorov-Loveland (*KL*) admissible selection rules and a sequence is Kolmogorov-Loveland (*KL*) stochastic if it is stochastic in relation to the *KL* admissible selection rules.

The idea to analyse the property of randomness from the perspective of incompressibility has been proposed independently by Solomonoff [SOL62], [SOL164], [SOL264], Kolmogorov [KOL63] and Chaitin [CHA66], being the starting point of the development of the concept of algorithmic or descriptive complexity that underpins the AIT. Trying to provide accurate algorithmic definitions randomness, Kolmogorov emphasized the irrelevance of infinite sequences for the justification of probability theory, considering that the development of a measure of the complexity of finite sequences only makes sense from the perspective of frequencies interpretation, namely the perspective of finite sequences. From this point of view, Kolmogorov introduces the concept of complexity of a finit object and provides in [KOL63] an universal definition of this complexities as the length of the shortest binary program which allows the reconstruction (decoding) of the object, or the minimum number of bits that contain all information about a given object and that is enough for the reconstruction (decoding) of the object. Kolmogorov complexity has two big advantages: it classifies sequences as random and nonrandom, and, extremely important, it allows to assign levels to the randomness of sequences – degree of randomness. This last advantage becomes useful in the analysis of infinite sequences.

Being a quantitative approach of the property of randomness, typicality is based on the notion of measure (measure+theoretic): a sequence is regarded random if there is no computable way to specify a set of measure zero containing this sequence. [VS10]. A property or attribute of infinite binary sequences is called special if the probability that the property holds is zero, and is called typical if the probability that the property holds is one. An attribute is special if its complement (negation) is typical, and vice versa [DAS11]. According to Martin-Löf, the data is random to the extent that it can be analyzed by algorithmic methods. Algorithmic formalization of the property of randomness proposed by Martin-Löf is considered the most rigorous and satisfying. If a sequence is random, then it is typical, typicality being a necessary condition for a sequence to be random. Martin-Löf tries to demonstrate that the typicality is a sufficient condition as well for randomness. Thus, according to Martin-Löf, a binary sequence is random if and only if is typical.

Schnorr randomness is a notion of algorithmic randomness for real numbers closely related to Martin-Löf randomness. Schnorr [SC171], [SC271] criticized Martin-Löf randomness as

algorithmically too loose. He proposed two alternatives, both being based on *computable* rather than *computably enumerable* test notions: a sequence is computably random if no computable martingale succeeds on it, and a Schnorr test is a Martin-Löf test in which the measure of every set W_n in the test is a uniformly computable real number – a sequence is Schnorr random if it passes every Schnorr test [DG02].

Chapter 2, Pseudorandom number generators – cryptographic perspective, is a natural continuation of the previous chapter, presenting the theoretical apparatus that underlies the design of pseudorandom number generators (*PRNGs*). It presents, with the purpose of comparing, the concepts of random and pseudorandom number generators, truly random number generators and cryptographically secure pseudorandom number generators. In practice, the cryptographic systems implements the random number generators at software level; however, software generators cannot produce "perfect" random numbers because of the deterministic properties of software algorithms. Therefore, a software generator produces pseudorandom numbers, i.e. sequences of numbers that "seem" statistically random.

In cryptographic terms, the definition of randomness has a (extremely) practical interpretation: the values produced by a source are random if an opponent, even if he/she knows the hardware and software platform running that source, including the previous values generated by the source, cannot predict, based on the known information, the following values produced by that source. The only method available to the attacker remains thus trying all possible values – type of brute-force attack. Cryptography needs such random sources for generating cryptographic keys/passwords and for hiding certain values in communication protocols.

In addition to the problem of integers factorization and of all aspects related to the computational complexity of cryptographic mechanisms, modern cryptography relies heavily on *PRNGs*, plus the concept of indistinguishability. In computational complexity theory, a probability distribution is pseudorandom against a class of adversaries if no adversary from the class can distinguish it from the uniform distribution with significant advantage. The concept of indistinguishability, introduced by Goldwasse Micali [GOM82] and developed by Blum, Micali and Yao [BM84], [YAO82], which mathematically underpins together with the property of randomness the field of cryptography, allows the building of high-quality cryptographic *PRNGs*, using a relatively low level of initial *unpredictability* (*unpredictable* physical processes and phenomena).

The difficulty of defining the concept of randomness and declaring a source as being random has caused the division of random numbers and, implicitly, of *PRNGs* in two classes: truly random

numbers and pseudorandom numbers. The cryptographers unanimously agree that the truly random numbers/bits are produced in a non-deterministic way by hardware random number generators (*HRNGs*). whose operation is based on physical phenomena and processes with or without random quantum properties, and which, at least in theory, are totally unpredictable. A *PRNG* or a deterministic *PRNG* produces results that "seem" statistically random, based on a deterministic causal process – algorithm that generates numbers that approximate the characteristics of true random numbers. The deterministic process uses an algorithm that produces a sequence of bits from an initial value generated from a seed which must contain enough entropy to ensure the randomness of the sequence of bits. But software generators of random numbers/bits cannot achieve the criteria of „perfection" due to the deterministic properties of software algorithms, i.e. the sequence of numbers/bits depends entirely on a relatively small set of initial values (for example, the period of sequence is limited to the range of numbers that can be represented in the system). Because of the deterministic nature of the causal process, the generator produces pseudorandom bits. According to [BK07], a *PRNG* produce unpredictable results if the seed is secret and the algorithm is well built, and the security of entire mechanism based on *PRGN* consists in the entropy source of the input channel.

Chapter 3, Basic elements for building stream cryptographic systems, describes the principles, mechanisms and hardware and software components of the cryptographic stream system architectures.

Linear feedback shift registers (*LFSR*) are used extensively in testing environments, in digital systems design and building methods of compression. In computer science and communications, *LFSRs* are of particular interest in the following types of applications: generating bit/numbers/vectors (pseudo)random, encryption/decryption, wireless transmission, computing checksums for data, data compression. By their capabilities of generating pseudorandom number, *LFSRs* underlies the building of an entire class of stream ciphers. Due to the ease of building electronic and electromechanical circuits, relatively long periods and uniform distribution of output streams, *LFSRs* have found a deserved place in cryptography. But their linear nature involves certain weaknesses demonstrated during cryptanalyses. The *LFSR-based* stream algorithms are vulnerable against *Known-Plaintext* attacks (*KPA*) which exploit statistical vulnerabilities following the selection of certain Boolean functions integrated into the *LFSRs*.

The attack starts from observing the correspondences between the state of *LFSR* outputs and the output of a boolean function which combines the outputs' state of all *LFSR* generators. The attack starts as a brute-force attack, and gradually, once a correlation can be established, it becomes a divide and conquer attack.

Starting from the concept of *One-Time Pad* (*OTP*), derived from the Vernam cipher [VRM19], the stream ciphers are built using *LFSRs*, because they produce words (sequences of bits) with good statistical properties and can be easily implemented in hardware. On the other hand, in the context in which cryptography, and implicitly the stream ciphers are based essentially on the complexity theory, an extremely important element is represented by the *One-Way Function* (*OWF*). The OTP encryption mechanism takes every character or bit of the plaintext and encrypts it using and XOR operation (mod 2) with a randomly generated secret key (keystream or pad), resulting the ciphertext. The security of *OTP* consists of a set of conditionalities imposed to the secret key: it must remain secret, must be perfect-randomly generated, the size must be al least equal to the size of plaintext, and not be reused – at least in theory (mathematics), the fulfillment of these conditions guarantees the impossibility to decrypt the ciphertext without being aware of the encryption key; for this reason, the *OTP* algorithm is called the perfect cipher and is considered unconditionally secure against on a *Ciphertext-Only* attack. The unconditional security means a perfect secrecy and assumes that the observation / analysis of the ciphertext does not provide any useful information.

OTP does not describe how to generate encryption/decryption keys, nor how these keys should be changed between communication partners. It is assumed that these keys, generated and distributed in a secure way only to the communication source and destination, and secretly kept as long as the information submitted to the encryption process is confidential. Protection and detection against unauthorized access to the keys and ensuring the availability of key are mandatory elements for a solid *OTP* cryptosystem, but they are provided through external mechanisms.

A function f is an one-way function (*OWF*) if it is easy to calculate, but difficult to invert; easy means that f is computed in polynomial time (probabilistic), and difficult means that there is no algorithm to compute $f1$ in polynomial time. *OWFs* are fundamental tools in cryptography, primarily for building *PRNGs*. Taking into account the fact that it is quite easy to create an *OWF* from a *PRNG*, studies have shown that a *PRNG* exists if and only if there exists an *OWF* ([BM84], [HIL99]). The paper [BM84] treats for the first time the designing process of a *PRNG*

based on *OWF*, starting from the assumption of the difficulty of discrete logarithm problem. Later, in [YAO82], [LEV87] and [HIL99] the problem is generalized, approaching the building of a pseudorandom generator from any one-way permutation. Besides the discrete logarithms problem, another important principle for buiding pseudorandom generators is that of the difficulty of factorization problem. If f is an *OWF* permutation, then the inverse function f^{-1} consists in finding x. If f is not a permutation, then inversion means the finding any x' such that $f(x') = f(x)$.

Chapter 4, Architecture of the stream cipher algorithms, presents the architectural components and operation modes of stream encryption algorithms.

Stream encryption algorithms bitwise combine/add plaintext with the encryption key (keystream or running-key), whic is which is a sequence of pseudorandom bits. If the algorithm generates for the encryption key a „perfect" random sequence of bits, then the cipher is, at least theoretically, invulnerable. Compared to block encryption algorithms, the stream encryption algorithms runs at higher speed in hardware implementations, and requires less complex hardware circuits. Another great advantage of the stream encryption algorithms is the is extremely low propagation of errors, which is very important the communication medium generates transmission errors with a high probability, as well as lower requirements for temporary storage at buffer level.

Stream encryption algorithms can be with symmetric key or public key (probabilistic encryption mechanism Blum-Goldwasser is an encryption algorithm based on public key). However, the vast majority of stream encryption algorithms are part of the class of encryption mechanisms based on symmetric secret keys. The advantage of these algorithms is that the encryption elements changes for each word or symbol that is being encrypted, and that, in the case of transmission errors, the propagation of errors is removed. Also, stream encryption algorithms become useful useful in a situation where the memory available to encryption process is limited, so that it is necessary to process only one symbol at a time.

Stream encryption algorithms can be divided into two categories:

1. synchronous stream encryption algorithm (synchronous stream cipher): the encryption sequence of pseudorandom bits (keystream) is generated in a way independent of the plaintext and ciphertext; for encryption, the encryption sequence is combined (for binary additive

algorithms, there is XOR operation) with the plaintext, resulting the ciphertext, and for decryption, the encryption sequence is combined with the ciphertext, resulting the plaintext.

2. asynchronous stream encryption algorithm (asynchronous stream cipher): the mechanism for obtaining the encryption key/sequence (keystream) uses a number of *n* bits of ciphertext obtained previously. For encryption, the encryption sequence is combined (for binary additive algorithms, there is XOR operation) with the plaintext, resulting the ciphertext, and for decryption, the encryption sequence is combined with the ciphertext, resulting the plaintext.

The attack methods actually used for the cryptanalysis of stream ciphers/algorithms are: *ciphertext-only attack*, *known ciphertext attack* (*COA*), *known-plaintext attack* (*KPA*), *chosen-plaintext attack* (*CPA*), *chosen-ciphertext attack* (*CCA*), *known/chosen IV attack* (*KIVA*), *distingushing attack* (*DA*).

Rueppel in [RUE86] şi Zenner in [ZEN04] define a basic model of the keystream generator, $G_{base}(S, F, f)$, for synchronous stream ciphers, and Zenner describes in [ZEN04] the integration mechanism of $G_{base}(S, F, f)$ within the structure of stream encryption algorithms. Also, Zenner extends in [ZEN04] the model of $G_{base}(S, F, f)$, introducing an extended keystream generator, $G_{extended}(S, F, f, C)$.

Zenner makes in [ZEN04] a strict separation of keystream generator and key schedule algorithm in stream cipher design, but in an unintegrated way. Therefore, this approach can lead to a neglecting of some security aspects regarding the interconnection and synchronization of cipher components (propagation and sometimes multiplication of security items/vulnerabilities transmitted between components). Therefore, the thesis proposes an unified formal model for sinchronous and asynchronous stream encryption algorithms, called $AlgStream(S_0, S, k, F_0, F, f, crypt, Z, M, C)$, based on the definition of a keystream generator $G(S_0, S, k, F_0, F, f, Z)$, that integrates the components: the component that initializes and modifies an internal state vector, using an initial secret key *k* or a secret seed k_s (*component*_1), the component that produces the secret keystream (*component*_2), and the component that perform the encryption task (*component*_3). The novelty of *AlgStream* model is that it makes a clearer distinction between the key scheduling part and keystream generator part, thus providing a higher degree of modularity, and integrates and unifies all possible flows and modes of operation of stream encryption algorithms, including the optional ones: for example, the choice of using initialization vectors, or the introduction of a new level of the state vector's initialization of algorithm, or the regularly updates of the vector's final state that determine the initialization of keystream generator.

For the *AlgStream*(S_0, S, k, F_0, F, f, *crypt*, Z, M, C) model, it is presented the calculation method for the internal state's size of the stream encryption algorithms.

Based on this size and the approach from [ZEN04], the internal state of stream encryption algorithms are cryptanalyzed, and further it is proposed a general known-plaintext attack model against stream encryption algorithms, called *ModelAtacB*, that takes into account the highest degree of vulnerability of an encryption stream algorithm set by the maximum amount of information that an attacker can gain access to.

Chapter 5, *RC*4 algorithm, cryptanalyses the stream cipher *RC*4: secret states that the algorithm cannot enter, correlations and biases between the secret and public components of the state vector, sets of weak keys and initialization vectors (*IV*), algorithm invariance, correlations and biases of state vector/table, distinguishers of keystream, key recovery attacks, internal state reconstruction attacks, known plaintext attack, ciphertext-only attacks. The chapter focuses mainly on the significant results obtained from cryptanalytic researches on key scheduling algorithm (*KSA*) part of *RC*4, that attempts to reconstruct the secret internal state of *RC*4 based on its combinatorial characteristics.

The first analyses presented are those of Fluhrer, Mantin and Shamir (*FMS attack*). The authors wrote the seminal paper [FMS01] that spelled out how a secret key could be recovered from information leaked by *RC*4, thus summarily defeating the encryption. They advance the concept of invariance weakness, which denotes a vulnerability where particular pattern of a small number of key bits su_ces to completely determine a large number of state bits. Then, they show that with high probability, the patterns of initial states associated with these weak keys also propagate into the first few outputs, and thus a small number of weak key bits determine a large number of bits in the output stream, and describe several cryptanalytic applications of the invariance weakness, including a new type of distinguisher. In the final part of the paper, Fluhrer , Mantin and Shamir describe the second weakness, *IV* weakness, and show that a common method of using *RC*4 is vulnerable to a practical attack due to this weakness, and how both these weaknesses can separately be used in a related key attack.

The next paper analyzed in this chapter is [KNU98]. The aim of the paper is to derive some cryptanalytic algorithms that find the correct initial state of the RC4 stream cipher using only a small segment of output stream, and to give precise estimates for the complexity of the attacks where possible. The cryptanalytic algorithms in this paper exploit the combinatorial nature of *RC*4 and allow to find the initial table, i.e., the state at time $t = 0$. Knowledge of this table

enables to compute the complete output sequence without knowing the secret key. If the first portion of about 2^n output words are known, the proposed algorithm (*Knudsen attack*) allows to find the initial table in a reduced search with complexity much lower than exhaustive search over all possible initial states. A careful analysis, which is confirmed by numerous experiments for different values of the word length n, shows that the complexity of the best attack is lower than the square root of all possible initial states. The proposed algorithms become infeasible for $n > 5$ and thus pose no threat to *RC*4 with $n = 8$ as used in practice. However, the attacks give new insight into the design principles of RC4 and the estimates of the complexity should give some realistic parameters for the security of RC4. The results obtained by authors are intrinsic to the design principles of RC4 and are independent of the key scheduling and the size of the key.

In [OS05] Ohigashi, Shiraishi and Morii (*OSM attack*) demonstrate the weakness of the *FMS* attack-resistant *WEP* implementation by showing that most *IVs* are transformed into weak *IVs* by *OSM* attack. *OSM* attack is a known *IV* attack, that is, the attacker can obtain a part of the session key information from any 24-bit IV. In case of a 128-bit session key, $13/16 \times 2^{24}$ 24-bit *IVs* are transformed into weak *IVs* by *OSM* attack. In order to avoid all the weak *IVs* used in this attack, the authors remove 13/16 (about 81%) of the *IVs*. The rate at which *IVs* are avoided is too large to use practical. *OSM* attack can reduce the computational times for recovering the secret key compared with the exhaustive key search. When a 128-bit session key is used, the efficiency of *OSM* attack fir recovering a 104-bit secret key is $2^{72.1}$in the most effective case. This shows that *OSM* attack can recover a 104-bit secret key within realistically possible computational times. Finally, the *FMS* attack-resistant *WEP* implementation is broken by *OSM* attack.

Shiraishi, Ohigashi and Morii propose in [SOM03] a method (*SOM attack*) for reconstructing an internal state of *RC*4, that is more efficient than *Knudsen* attack. The result of *SOM* attack is that an internal state with the first 73 pre-known entries can be reconstructed within 2^{20} computational iterations. Time complexity of the *SOM* algorithm is reduced by introducing a process of backtracking and deleting one of two recursive searches from the *Knudsen* attack. Consequently, when the number of known entries in initial state is less than in the *Knudsen* attack, *SOM* method still succeeds in reconstructing an internal state. Moreover, the authors found some internal states that can be reconstructed easily when the number of known entries is equal to 73 in $n = 8$. Similarly to the evaluation in the *Knudsen* attack, it is likely that if computational time is about 2^{30}, *SOM* attack can reconstruct an internal state in which only the first 65 entries are known.

Roos discusses in [ROO95] a class of weak keys in *RC*4 stream cipher. He shows that for at least first byte of every 256 possible keys the initial byte of the pseudorandom stream generated by *RC*4 is strongly correlated with only a few bytes of the key, which effectively reduces the work required to exhaustively search *RC*4 key spaces. Roos observes that given a key length of K bytes, and $E < K$, there is a 37 % probability that element E of the state table depends only on elements $0 \ldots E$ (inclusive) of the key. Morover, Roos emphasizes that the most likely value for element E of the state table is $[E] = X(E) + E\,(E + 1)/2$, where $X(E)$ is the sum of bytes $0 \ldots E$ (inclusive) of the key. In conclusion, Roos experimentally observed that the first byte of the keystream is correlated to the first three bytes of the key and the first few bytes of the permutation after the KSA are correlated to some linear combination of the key bytes.

Tomašević, Bojanić and Nieto-Taladriz try in [TBN07] to find the maximum amount of information about the current state available at a given time and to formulating a cryptanalytic attack based on this information (*Tomašević attack*). Therefore, the authors propose the tree representation [YAG06] of the *RC*4 algorithm which contains a set of trees, each for one output symbol. The nodes and branches of these trees encompass all possible information at a given time. In *Tomašević attack* the authors propose an analytical abstraction named the general conditions of the tree information in order to consider a reasonable amount of information. Each general condition practically represents all conditions from a subtree. The general conditions are organized into the tree structure. *Tomašević* algorithm searches this tree applying the hill-climbing strategy to find the internal state. The authors state that the information gained from general conditions can also be used in other attacks on *RC*4 cipher and increase their efficiency. Morover, the authors suggest the modification of the backtracking algorithm that is given in *Knudsen* attack. The estimated complexity of this algorithm is lower than for the exhaustive search. If a sufficient number of output words is known, the deciphering process is successful. Otherwise, the initial table will not be completed. Therefore, in this case, after the last known output word is examined, the set of information valid at this time is obtained. Thus, the general conditions have been incorporated in the existing backtracking algorithm in order to make a better choice for the assignment to unknown entries of the cipher's table. The complexity of backtracking algorithm has been further decreased by the authors, but *Tomašević attack* remains infeasible for a practical attack against *RC*4.

After presentation of these well-known researches on *RC*4 stream cipher, it is proposed a cryptanalytic attack, called *TabuStateTable* (*TST*), based on Tabu search algorithm which tries to reconstruct the internal state of *RC*4. *TST* attack relies on the cryptanalytic algorithm found in

Knudsen attack, the tree representation of the output word Z_t and the tree of general conditions from *Tomašević* attack. Tabu search is a metaheuristic algorithm proposed by Glover [GLO86], [GLO89], [GLO90], [GLOV90] for solving combinatorial optimization problems. The adaptive memory feature of Tabu search has the ability to make use other methods (such as linear programming algorithms) to overcome local optimality. Based on flexible memory functions, the main idea is to record recent moves in a so-called Tabu list, which is updated after each iteration, and forbid search moves to nodes already visited in the search space. Then, the search is carried out towards promising areas of the search space, called aspiration criteria. A given move can override its forbidden/Tabu status and consequently can be considered a new solution when the move improves the threshold of aspiration criteria. Tabu search is in fact a global rather than a local optimization method. In *TST* attack, a metaheuristic Tabu-like search method is applied on the tree of general conditions used in *Tomašević* attack. For the complexity analysis of *TST*, it is employed the same formalism of *Knudsen* attack, and provided the propoer method for *TST* complexity analysis. Followin the analitical calculations, for $n = 3$, $n = 4$ and $n = 5$ the *TST* results are the same as those obtained in *Tomašević* attack. Further, for $n = 6$, $n = 7$ and $n = 8$, the *TST* attack obtains slightly better values (Table – Approximations of the complexities of the *Knudsen*, *Tomašević* and *TST* cryptanalytic attacks on *RC*4). Even the complexity of the *TST* attack is lower than the exhaustive search and the square root of all possible initial states, the attack remains impractical. But combining the *TST* method with other methods of attack, for exemple with distinguisher attacks against *PRNG*, may be of a high interest.

***n* (word size)**	**3**	**4**	**5**	**6**	**7**	**8**
Knudsen attack	2^8	2^{21}	2^{53}	2^{132}	2^{324}	2^{779}
Tomašević attack	2^5	2^{17}	2^{46}	2^{120}	2^{300}	2^{731}
TST attack	2^5	2^{17}	2^{46}	2^{119}	2^{298}	2^{727}

Table – Approximations of the complexities of the *Knudsen*, *Tomašević* and *TST* cryptanalytic attacks on *RC*4

Chapter 6, *KSAm* (*Key Scheduling Algorithm modified*) – Key scheduling algorithm for *RC*4, is the most important part of the thesis in which it is proposed a new key scheduling algorithm for *RC*4, called *Key Scheduling Algorithm modified / KSA modified* (*KSAm*), whose main goals are to eliminate the invariant weakness of the original *KSA*, and to mitigate the weaknesses based on the resolved condition, mainly when initialization vectors *IVs* are used, up to a cryptographically-secure level, especially in the operating mode of *WEP* protocol.

***KSA*(*K*, *S*)**	***KSA*m (*K*, *S*)**	
Initialization:	*Initialization*:	
for $i = 0$ to N – 1	for $i = 0$ to $N - 1$	
$S[i] = i$;	$S[i] = i$;	
$j = 0$;	*Scrambling*_1:	
Scrambling:	for $i = 0$ to $N - 1$	(a)
for $i = 0$ to $N - 1$	$u_i = (S[i] + K[i \bmod \ell]) \bmod N$;	(b)
$j = (j + S[i] + K[i \bmod \ell]) \bmod N$;	for $i = 0$ to $N - 1$	(c)
$swap(S[i], S[j])$;	$swap(S[i], S[u_i])$;	(d)
	$j = 0$;	
	*Scrambling*_2:	
	for $i = 0$ to $N - 1$	
	$j = (j + S[i] + K[i \bmod \ell]) \bmod N$;	
	$swap(S[i], S[j])$;	(e)

Figure – *KSA* vs *KSAm*

The *KSAm* (Figure – *KSA* vs *KSAm*) encompasses an additional scrambling loop (*Scrambling*_1 – lines (a), (b), (c) and (d)): it takes the secret key and initializes a vector of indices $u_0, u_1, \ldots, u_{N-1}$; the values of indices u_i are not necessarily unique within the vector of indices, and they are kept secret. Then, it swaps the two values of S pointed to by i and u_i, so that the *Scrambling*_1 stage of *KSAm* ends with a secret state, which is different from the identity permutation with a very high probability. The rest of operations (*Scrambling 2*) remain the same as in the original *KSA*: it applies the scrambling rounds $N = 2^n$ times, stepping i across S, updating j by adding the previous value of j, $S[i]$ and the next word of the key.

Cryptanalysis of the *KSAm*, based on methods of cryptanalysis of *KSA*, starts with the space and time complexity, and then with the probability of identity permutation after completion of the algorithm.

First of all, the security of *KSAm* comes from its huge internal state. The internal state of the original *KSA* is approximately 1700 bits for 8-bits words. *KSAm* provides a much larger size and, as a result, it is much harder to reconstruct its internal state (the values of indices u_i are not necessarily unique; therefore, the number of all possibilities of distributing 2^n elements into 2^n cells where repetitions are allowed is $(2^n)^{2^n}$) or space complexity is

$$L_{RC4\text{-}KSAm} = \log_2(2^n! \times (2^n)^{2^n} \times (2^n)^2)] = [\log_2(2^n!) + (n \times 2^n) + 2n]$$

$$L_{RC4\text{-}KSAm,\ n=8} \approx 3748 \text{ bits}$$

In comparison with *KSA*, *KSAm* needs only additional 256 bytes of memory for the indices u_i (n = 8). Also, the tests show that the additional computational time of the *KSAm* is negligible – a mod256 operation can be performed with a bitwise AND with 255 (or simple addition of bytes ignoring overflow), while the loop of updating the indices u_i (Figure – *KSA* vs *KSAm*, lines (a) and (b)) can be parallelized on a multi-core machine, considering the independence of these updating operations.

The time complexity of *KSAm* is $O(n)$.

Assessment of the event's probability that the state table *S*, after completing the *KSAm*, is equal to the identity permutation, is included in the general analysis of the probability that a particular value *b* is in the position *a* after running *KSAm* ($S_{2N}[a] = b$).

Assuming that both u_i of *Scrambling*_1 and *j* of *Scrambling*_2 get random values in a uniform manner, the identity permutation is initially analyzed from the perspective of a general *Scrambling* sequence ($Scrambling_{gen}$) that models the behaviour of the two *Scrambling* sequences (*Scrambling*_1 and *Scrambling*_2) of *KSAm*. Then, it is studied the combined effect of two $Scrambling_{gen}$ sequences and its correlation with the combined effect of the *Scrambling*_1 and *Scrambling*_2 sequences from the perspective of identity permutation.

There are defined the concepts of minimum and maximum probability associated with the entries of the state vector *S*, as minimum and maximum threshold values, in order to determine the exact range of values of the event's probability that the value of a vector entry is found, after one or two consecutive $Scrambling_{gen}$ sequences (or after *Scrambling*_1 and *Scrambling*_2 sequences), in the position of initialization phase, i.e. $S_N[i] = i$ or $S_{2N}[i] = i$ (there is interest only for the probability distribution from the perspective of the minimum and maximum values of the values' range. Once established this interval, the values of maximum probability related to the value $1/N$, which is the maximum limit, become extremely important. Another reason for defining the two types of probability, minimum and maximum, is determined by the model approach of cryptographic attacks: in general, an attack againts a cipher takes into account and speculates those vulnerabilities that occur with the highest probability. The above reasoning is correct, only that sometimes an event or a vulnerability with low probability has a significant effect either in increasing an already known vulnerability or, more importantly, in propagation (sequential or fan-like) of some events or vulnerabilities which, combined, speculate the combinatorial characteristics of the actions that manipulate the internal state vector of the encryption algorithm.

Calculating the minimum probabilities assumes tracking the entries' values of the vector *S* at each step of the permutation, and evaluating the probability of the event that the entries' values

of the vector S remain permanently fixed throughout the running *Scrambling* sequences. It is found that for sufficiently large N, the minimum probability associated with an initial entry or the identity permutation low (for $N = 256$, $N = 256$, $P_{\min\_S}(S_N[i] = i) = 0.0014034^{256}$).

The concept of maximum probability is the probability of the event $S[a] = a$ in the worst case, i.e. the maximum threshold value for the event's probability $S[a] = a$, value which is not exceeded for any entry a, where $a \in [0, N-1]$, while taking into account all the possible values for the secret key K.

Tests have shown that none of the possible keys K of length 8, 16, 24 and 32 bits leaves the vector S in a state identical to the identity permutation after running *KSAm* (approximate running times of the tests were: $T_{K=8} \approx 0.003$ sec, $T_{K=16} \approx 0.63$ sec, $T_{K=24} \approx 157.84$ sec, $T_{K=32} \approx 39337$ sec). Weak key $K = 0$ was excluded.

We further analyse the effect of the invariant weakness defined by Fluhrer, Mantin and Shamir (*FMS*) in [FMS01], with appropriate modifications, on the *KSAm* [CRA14]. In this analysis, it is shown that the permutation $S = KSAm_{Scrambling\_1}(K)$ is not *b-conserving*. The only important criptanalitic effect, i.e. the permutation $S = KSAm_{Scrambling\_1}(K)$ to be *b-conserving*, is obtained if $K = 0$ (the only class of weak keys for the *FMS* invariant weakness applied to $KSAm_{Scrambling\_1}$ mechanism). In this case, the *b-exact* key becomes a b_0-*exact* key, which has the definition: : $K[t \bmod l] \equiv (1 - t) \pmod b$ for $t = 1$ and $K(t \bmod l) = 0$ for $t \in \{0, \ldots, N-1\} - \{1\}$. Thus, $u_t = t$, and knowing that $i_t = t$ it follows that the permutation $S = KSAm_{Scrambling\_1}(K)$ is *b-conserving*. Even using the weak key $K = 0$, account should be taken of the fact that the *KSAm* algorithm contains, in addition to *Scrambling*_1, the *Scrambling*_2 sequence, which significantly reduces the "*b-conservingness*" of the permutation S ($S = KSAm(K)$) – even under the conditions for $K = 0$, starting with $i = 2$, *Scrambling*_2 changes the entries of the identity permutation).

It is defined the b_m-*conserving* property for a permutation and it demonstrated the relation:

$$\left(\frac{b-2}{N}\right)^b \times 2/5 \le P[KSAm(K)] \text{ is } \textit{almost } b_m\textit{-conserving}] \le \left(\frac{b-2}{N}\right)^b \times 2/5 + \left(\frac{1}{N}\right)^N$$

where $q \le n$ şi l integers and $b \overset{def}{=} 2^q$, $b \mid l$, K is a special b-exact key of l words. The maximum level of the probability that $KSAm(K)$ is *almost* b_m-*conserving* is established using the term $\left(\frac{1}{N}\right)^N$.

The tests carried out to find any mappings of the secret key bits to identifiable patterns in the initial permutation S led to designing an algorithmic approach model/framework whose

formalization can be used to test any type of *Scrambling* mechanism applied to a permutation permutation which inter-change at every step the values of two entries on the basis of two indices. Based on this model, the number of words in the permutation S which could be determined based on the knowledge of a number m of words from the key K is:

$$NR(m) = [2^n \times (m/l)] \times \alpha = [2^n \times (m/l)] \times (1/2^q)^{l-m}$$

where n is the size of the word in bits, l is the number of the K *b-exact* key's words, m is the number of the K key's words ($0 \leq m \leq l$).

Based on demonstrations made by Paul and Maitra in [PMA07] on the correlation between bytes of the permutation S and bytes of the secret key K at each step of the *KSA* algorithm, we analyze the same correlation probabilities of the entries' values of the permutation S with the values of the secret K after each step of the *KSAm Scrambling*_2 sequence. We determine and demonstrate the general probability of the *b-conservingness* of the permutation S at each step of the *Scrambling*_2 sequence, with the assumption of existence of the *b-conservingness* at the end of the *Scrambling*_1 sequence for any class of keys K (*Scrambling*_2 receives at the end of *Scrambling*_1 a permutation which is *b-conserving*).

Starting from the general probability (b)-*conservingness* of the permutation S at each step of *Scrambling*_2, we determine and propose a model of cryptanalysis approach which speculate the characteristics of Scrambling algorithm combined with the use of weak keys K, in order to discover a proportional correlation between the initial state of the permutation S and the weak keys K, and the final state of the permutation S – the cryptanalysis of the permutation's state, based on the knowledge of the initial internal state of the permutation S, the probability of preserving the initial internal state of the permutation S and the probability of (b)-*conservingness* of the permutation S following a succession of *Scrambling* cycles that swap the elements' values of the permutation S.

The model formalizes a cryptanalysis strategy of permutations used in stream ciphers that provides a minimum benefit which can be improved by speculating the characteristics of *Scrambling* algorithms, weak keys K and initialization state of permutation S.

We tetermine the correlation between the output words Z and a constant sequence, as well as the maximum probability of finding the first four constant words Z. The values obtained for $Z[1]$ and $Z[2]$ cannot be considered significant correlations between the secret key K and output words Z in order to constitute an important criptanalitic advantage.

One of the most important statistical observations was made by Mantin and Shamir in [MS02]: the probability that the second output word Z is 0 is 2/*N*. Under the same conditions, for *KSAm*, it follows the probability for which the correlation of the second output word *Z*[2] = 0 with probabilities 2/*N* and 1 are kept. An important observation is that the analysis is based on the probability that *S*[2] = 0 and *S*[1] ≠ 2 after KSAm, in the context in which it is considered that all the entries' values of the permutation *S* are random after KSAm. We demonstrate that the cumulative probability of the events $S_{0\_S2}[2] = 0$ şi $S_{0\_S2}[1] \neq 2$, for which there is a correlation between the second output word *Z*[2] = 0 and the probability 1 is less than 1/*N*. In conclusion, the correlation described by Mantin and Shamir, although cannot be canceled (*RC*4 and *RC4*m use the same *PRGA*), is reduced in the conditions under which the two *Scrambling* cycles of *KSAm* distribute random values to entries *S*[1] and *S*[2]. In [FMS01] and [MAN201] it is detailed the cryptanalytic effect of combining the secret key *K* and initialization vectors *IV*s. This method is specific to *WEP*, and research studies, in vast majority, emphasize that the insecurity of *WEP* is not due to *RC*4 itself, but due to the way in which the mechanism of combining secret key and initialization vectors is used. *IV* weakness is analyzed on *KSAm.* If the initialization vector *IV* precedes the secret key, in the worst case, i.e. secret keys are made up of only *IV*s, so keys whose values are fully known, the planned number of *IV*s needed to obtain about 100 *IV*s of the appropiate form is approximately 8000000. Excluding the latter (IV-only keys), the *IV* attack becomes practically unfeasible. If the secret key precedes the *IV*, it is shown that the output words cannot be manipulated through *IV*s in order to observe the permutation's state, that further allows to obtain the secret key. When the *IV* is combined XOR with a secret key, the complexity of the attack is equal to the complexity of exhaustive search.

Cryptanalysis of *KSAm* describes two combinatorial properties of *KSAm* in its normal mode of operation, and not from the perspective of an individula implementation. First of oll, it is calculated the sign of permutation *S* after the completion of *KSAm*, whose values allow prediction of one bit with an advantage of 0.91%. . This advantage is still too small to be feasible in an attack. Secondly, it is analyzed the state table entries during the KSAm steps, with special focus on calculating the probability of a linear advance movement of an initial value from a particular state table entry during *KSAm*. The results prove that it is very unlikely to find a location in *S* during such movement where that value may be predicted with a probability significantly greater than 1/*N*. Further, cryptanalysis of *KSAm* and thus of *RC4m*, involves adapting and testing successful methods of attack that have revealed significant vulnerabilities of the original *KSA* or *RC4*. There were chosen and adapted three attack methods that exposed security breaches of *KSA*/*RC*4: *OSM* attack [OS05], *Roos* attack [ROO95] and *Klein*/*PTW* attack

[KLA08], [TW08]. For *OSM*, the results demonstrate infeasibility of the attack against *WEP* with *KSAm*, in circumstances where the minimum efficiency has the value of $2^{103.92}$. Adapting the *Roos* approach to *KSAm* reveals a slight correlation between the first two outputs with the first, respectively the sum of the first two values of the key *K*. Being extremely low, this correlation has no an important cryptanalytic effect, especially since, from the fourth output, the values produced are asymptotic to 0.39. The conclusions drawn from the *Klein/PTW* attack applied to *RC*4*m* are: first, a more superior protection provided by *RC*4*m*; then, the increased size of the initial encryption key has no an influence proportional to the difference in size between 104-bit and 232-bit keys; a so large difference between the size of keys should be significantly noted in the level of traffic protection. Thus, although the number of bits recovered from the initial encryption key does not seem to reach a dangerous threshold, the *IV*s, due to their small size, are the main cause of the vulnerability of *WEP-RC*4*m* mechanism. Another observation is that the presence of the broadcast *ARP* protocol causes the decrease of protection, and a deactivation of it reduces the number of bits recovered fron the encryption key.

It is introduced the *correlation factor* r_c in order to redefine the concepts of *a-state* and *b-predictive* from [MS02], so as to be considered the correlations with initial states, and to model the identification process of distinguishers based on predictive states from the statistic point of view. The correlation factor becomes a very useful cryptanalysis element in the context where the secrete initial state of a *PRGA* algorithm is obtained from a succesion of differnet cycles based on various constraints and a secret key.

The next part of the thesis focuses on aspects of concerning the correlation of the states' entries of a *PRGA* algorithm, based on the concept of distinguisher and on attack mechanisms aginast internal state starting from the values of distinguishers. It introduces and defines the following concepts: *distinguisher*, $distinguisher_{indicator}$, *corellation*, $corellation_{distinguisher}$, *correlation on pattern*, *pattern associated to output sequence*. Based on these concepts, there are proposed attack models against (initial/intermediate) internal state that take into account those entries fo initial state that have the highest probability of being correlated with a *distinguisher*. Each attack is associated with the complexity formula.

Also, the thesis introduces and defines the concept of $distinguisher_{strong}$ whose value is validated according to a threshold value ε determined by some metric associated with the property of randomness, and for which additional confirmations are no longer needed, and the concept of $distinguisher_{weak}$ whose value is considered part of the range of tolerance of the threshold value ε,

but which, under the conditions in which there can be provided additional verifications based on other metrics, it can be considered, with high probability, $distinguisher_{strong}$.

The algorithms for selecting the $distinguisher_{strong}$ and the correlations algorithms, that can be used in attacks against (initial/intermediate) internal state, are presented in details. Based on approaches from [MS02] and [FM01], it is proposed the extension and refinement of the -definition for *a-state* with applicability to both *KSA* and *KSAm*, from the perspective of the initial state and intermediate states that each produce an encryption value part of the output sequence, including the correlation factor r_c between intermediate states (the state of $PRGA_{RC4/RC4m}$ algorithm at each step) and initial state. In this way, the proposed approach allows that the distinguishers to be built either on the basis of the predictive *a-states* as defined in [MS02] or on the basis of some intermediate predictive *a-states* that directly produce the values of the output sequence so that, for these output values among which can be distinguishers, can be more easily correlation relations with the initial state through intermediate predictive *a-states*. From the criptanalitic point of view, the correlation with the initial state from which it starts, combined with specific and known vulnerabilities of individual *PRGA* algorithms allow better predictions of the input of output sequence; on the other hand, the distinguishers are useful in the analysis of the output sequence from the perspective of (pseudo)randomness (general case), and in the possibility of removing the initial states correlated with $distinguishers_{strong}$ and/or $distinguisher_{inficator}$. For *KSAm*, it has been conducted a limited set of tests on romanian language vocabulary. The tests are based on based on statistic analysis of the work of Mihai Eminescu [SEC74]. According to [SEC74], the most commonly used words of Eminescu's work are personal pronouns *el*, *ea* (absolute frequency of 3058, relative frequency of 4.65%), while the highest frequency of nouns category has the word *ochi* (absolute frequency of 299, relative frequency of 0.44%). There were generated with *RC*4*m* 100000 sequences consisting of four words and were used the following Diehard/Dieharder tests [DIE]: *OPSO* (*Overlapping Pairs Sparse Occupance*), *C1s* (*Count the1s, stream*) and *Serial*. The results showed that the third least-significant bit of the sequences produced has an additional correlation of 0.01 on the value of 0 – it means that the value of 0 at the position of the third least significant bit is a distinguisher. The value of 0.01 is added to the 0.02's value of average correlation obtained experimentally, resulting in a correlation value of 0.03. But it can be asserted that the tests had used data sets far too small to be able to validate the results. In any case, the correlation value of 0.03 obtained for a single bit in the sequence produced is a negligible advantage in practice.

The final part of the thesis propese a new concept of weak key, namely X_N-*weak-uncertain*. One of the advantages of *KSAm* lies in the fact that the two *Scrambling* sequences are different, making it difficult to find classes of keys that may be weak for both *Scrambling*_1, and *Scrambling*_2. In this case, the first level of cryptanalysis consists in checking the *KSA* weak keys against *Scrambling*_1 and the combined behavior on KSAm as a whole, and then finding the weak keys related to the *Scrambling*_1 sequence and testing these keys on *Scrambling*_2 sequence. The final conclusion is that a class of keys of the form $K[0] = K[1] = \ldots = K[\square - 1] = c$, where $c > 0$, $c \in Z^+$,, which are still weak due to allocation of equal values to all elements of the vector K, is not a class of X_N-*weak-uncertain* and thus it don't let the permutatio *S* in a X_N-*uncertain* state after two *Scrambling* cycles, different in terms of the implemented algorithm, but that use the same weak key $K = c$. Even if after *Scrambling*_1 the permutation *S* attains the X_N-*uncertain* state, *Scrambling*_2 destroys the model of movement cycle (to the right), and in the final leaves the values of the permutation's elements (pseudo)randomly distributed. This is the reason why the succession of two different *Scrambling* sequences of *N* steps each, chosen properly, are more cryptanalytic resistant than a single *Scrambling* sequence which runs in 2*N* steps.

Bibliography

[AB13] Alfardan, N., Bernstein, D., J., Paterson, K., Poettering, B., Schuldt, J., "On the Security of RC4 in TLS", USENIX Security Symposium, USENIX, 2013.

[AS02] Arbaugh, W., A., Shankar, N., Justin Wan, Y., C., "Your 802.11 Wireless Network has No Clothes", *IEEE Wireless Communications*, Vol. 9, No. 6, 2002, pp. 44-51. http://www.cs.umd.edu/~waa/wireless.pdf.

[BAB95] Babbage, S., "Improved Exhaustive Search Attacks on Stream Ciphers", European Convention on Security and Detection, IEE Conference Publication no. 408, IEE, 1995, pp. 161–166.

[BS06] Barkan, E., Shamir, S., "Rigorous Bounds on Cryptanalytic Time/Memory Tradeoffs", *Advances in Cryptology - CRYPTO 2006*, Lecture Notes in Computer Science, Vol. 4117, ISBN 978-3-540-37432-92006, 2006, pp 1-21.

[BH09] Bienvenu, L., Hölzl, R., Kräling, T., Merkle, W., "Separations of non-monotonic randomness notions", 2009. http://arxiv.org/abs/0907.2324.

[BD89] Beth, T., Dai, Z., D., "On the Complexity of Pseudo-Random Sequences - or: If You Can Describe a Sequence It Can't be Random", Advances in Cryptology — EUROCRYPT '89, Lecture Notes in Computer Science, Vol. 434, Springer Berlin Heidelberg, ISBN 978-3-540-53433-4, 1990, pp. 533-543.

[BSW01] Biryukov, A., Shamir, S., Wagner, D., "Real time cryptanalysis of A5/1 on a PC", Proceedings of PKC 2001, Lecture Notes in Computer Science, Vol. 1978, Springer-Verlag, 2001, pp. 37-44.

[BIT03] Bittau, A., "Additional weak IV classes for the FMS attack", Department of Computer Science, University College London, 2003. http://www.cs.ucl.ac.uk/staff/a.bittau/sorwep.txt.

[BIT06] Bittau, A., Handley, M., Lackey, J., "The Final Nail in WEP's Coffin", in *Proc. 2006 IEEE Symposium on Security and Privacy, S&P'06*, 2006, pp. 386-400. http://tapir.cs.ucl.ac.uk/bittau-wep.pdf.

[BM84] Blum, M., Micali, S., "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits", *SIAM Journal on Computing*, Vol. 13, 1984, pp. 850-864.

[BG01] Borisov, N., Goldberg, I., Wagner, D., "Intercepting mobile communications: The insecurity of 802.11", in. *Proc. 7th Annual International Conference on Mobile Computing and Networking, MobiCom '01*, Rome, pp. 180–189, 2001. http://www.cypherpunks.ca/~iang/pubs/wep-mob01.pdf.

[BK07] Barker, E., Kelsey, J., "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)", *NIST Special Publication 800-90*, Computer Security Division Information Technology Laboratory, 2007.

[DIE] Braun, R., G., Dieharder: A Random Number Test Suite. http://www.phy.duke.edu/~rgb/General/dieharder.php.

[BRO52] Broad, C. D., "Ethics and the History of Philosophy", *New York: Humanities Press*, 1952.

[CAL03] Calhoun P., Loughney J., Guttman E., Zorn G., Arko J., "Diameter Base Protocol", Request for Comments: 3588, Network Working Group, 2003.

[CHA66] Chaitin, G., “On the length of programs for computing finite binary sequences” , *Journal of the ACM*, 13, 1966, pp. 547-569.

[CHA69] Chaitin, G., “On the length of programs for computing finite binary sequences: statistical considerations”, *Journal of the ACM* 16, 1969, pp.145-159.

[CHA74] Chaitin, G., ”Information-theoretic Limitations of Formal Systems", *J. ACM* 21, 1974, pp. 403-424.

[CHA75] Chaitin, G., "A Theory of Program Size Formally Identical to Information Theory." *J. Assoc. Comput. Mach.*, 22, 1975, pp. 329-340.

[CHAG75] Chaitin, G., “Randomness and Mathematical Proof”, *Scientific American 232*, No. 5, 1975, pp. 47-52.

[CHA76] Chaitin, G., J., ”Algorithmic Entropy of Sets", *Comput. & Math. Appls.* 2, 1976, pp.233-245.

[CHAG76] Chaitin, G., ”Information-theoretic Characterizations of Recursive Infinite Strings", *Theoret. Comput. Sci.* 2, 1976, pp.45-48.

[CHA77] Chaitin, G., “Algorithmic information theory”, *IBM Journal of Research and Development*, vol. 21, 1977, pp. 350–359.

[CHAG77] Chaitin, G., ”Program Size, Oracles, and the Jump Operation", *Osaka J. Math.*, Vol. 14, No. 1, 1977, pp. 139-149.

[CHA82] Chaitin, G., “Gödel's theorem and information”, *Int. J. Theor. Phys.*, 21, 1982, pp. 941-954.

[CHA90] Chaitin, G., “A random walk in arithmetic”, *New Scientist 125*, No. 1709, 1990, pp. 44-46.

[CHU40] Church, A., “ On the concept of a random sequence”, *Bulletin of AMS*, vol.46, 1940, pp.130-135.

[COV06] Cover, T., M., Thomas, J., A., “Elements of Information Theory”, 2nd ed., New York, Wiley, 2006.

[CRA05] Crainicu, B., “An Overview of the IPsec Extensions Header – AH (Authentication Header and ESP (Encapsulating Security Payload)”, *Education/Training and Information/Communication Technologies – RoEduNet’05*: *Proceedings of the 4th International Conference RoEduNet Romania*: Târgu Mureş – Sovata, 20-22 May 2005, Editura Universităţii “Petru Maior” din Târgu Mureş, 2005, ISBN 973-7794-29-X, pp. 245-254.

[CRAI05] Crainicu, B., “Web Security: Secure Socket Layer and Transport Layer Security“, *Interdisciplinarity in Engineering: Proceedings of the Scientific Conference Inter-Ing 2005*: Târgu Mureş, “Petru Maior” University, Faculty of Engineering, 10-11 November 2005, Editura Universităţii “Petru Maior” din Târgu Mureş, 2005, ISBN 973-7794-41-9, 2005, pp. 787-800.

[CM06] Crainicu, B., Măruşteri, M., “PGP Cryptographic Keys and Key Rings“, *Proceedings of the 5th RoEduNet IEEE International Conference*: Sibiu, 1-3 June 2006, Romania, Editura Universităţii “Lucian Blaga” din Sibiu, 2006, ISBN (10) 973-739-277-9, (13) 978-973-739-277-0, pp. 138-141.

[CRA08] Crainicu, B., “Wireless LAN Security Mechanisms at the Enterprise and Home Level”, *Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics*, Springer Netherlands, ISBN978-1-4020-8736-3 (Print), 978-1-4020-8737-0 (Online), 2008, pp. 305-310.

[CI08] Crainicu, B., Iantovics, B.L., “Cryptanalysis of KSAm-like Algorithms“, *First International Conference on Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex*

Systems. Biomedical Computing. CANS 2008, Published by IEEE Computer Society, 2008, IEEE Computer Society Order Number P3621, ISBN 978-0-7695-3621-7, Library of Congress Number 2009900732, 2008, pp. 130-148.

[CRI08] Crainicu, B., Iantovics, B., "On A New RC4 Key Scheduling Algorithm", *Proceedings of the International Conference Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing, CANS 2008*, 8-9 November, Târgu Mureş, 2008, Editura Universităţii "Petru Maior" Târgu-Mureş, 2008, ISSN 2065-0426, pp. 16-25.

[CIA08] Crainicu, B., Iantovics, B., "Securing WEP Cryptosystems through A New RC4 Key Scheduling Algorithm", *Complexity in Artificial and Natural Systems*, Editura Universităţii "Petru Maior" Târgu-Mure, ISBN 978-973-7794-76-5, 2008, pp 93-99.

[CRA09] Crainicu, B., "A Local Search Approach for Recovering an Internal State of RC4 Stream Cipher", *11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2009*, Timisoara, Romania, September 26-29, 2009.

[CB10] Crainicu, B., Boian, F., "KSAm – An Improved RC4 Key-Scheduling Algorithm for Securing WEP", *Novel Algorithms and Techniques in Telecommunications and Networking,* Springer Netherlands, ISBN 978-90-481-3661-2 (Print), ISBN 978-90-481-3662-9 (Online)*,* 2010, pp. 391-396.

[CRB10] Crainicu, B., Boian, F., M., "Some Combinatorial Aspects of the KSAm-like Algorithms Suitable for RC4 Stream Cipher", *Studia Universitatis Babes-Bolyai*, Series Informatica, Volume LV, Number 1, 2010, ISSN 1224-869x (paper version), ISSN 2065-9601 (online version), pp. 105-114.

[CE11] Crainicu,B., Enăchescu, C., "A Metaheuristic Tabu Search Approach for Internal State Reconstruction of RC4", Proceedings *of 10th RoEduNet IEEE International Conference*, Iaşi, Romania, 23-25 June 2011, Published by Stef, 2011, ISSN 2247-5443, pp. 164-167.

[CI11] Crainicu,B., Iantovics, B., "An Agent-based Security Approach for Intrusion Detection Systems", *7th International Workshop on Grid Computing for Complex Problems*, *GCCP2011*, Bratislava, Slovakia, October 24 - 26, 2011, Institute of Informatics, Slovak Academy of Sciences, ISBN 978-80-970145-5-1, 2011, pp. 126-133.

[CRA14] Crainicu, B., "On Invariance Weakness in the KSAm Algorithm", *8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014*, 9-10 October 2014, Tirgu-Mures, Romania, Elsevier, ISSN 2212 – 0173, pp. 850-857.

[EAG05] Eagle, A., "Randomness is Unpredictability", *The British Journal for the Philosophy of Science*, Vol. 56, Issue 4, 2005, pp. 749-790.

[EA03] Edney, J., Arbaugh, W., A., "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison Wesley, 2003.

[DAS11] Dasgupta, A., "Mathematical Foundations of Randomness", *Philosophy of Statistics*, North Holland, 2011, pp. 641-710.

[CLP05] De Canniere, C., Lano, J., Preneel, B., "Comments on the rediscovery of time memory data tradeoffs*,"* *eSTREAM, ECRYPT Stream Cipher Project, Report 2005/040*, 2005.

[DH03] Doraswamy, N., Harkins, D., “IPSec: the new security standard for the Internet, intranets, and virtual private networks”, Second Edition, Prentice-Hall, 2003

[DG02] Downey, R., Griffiths, E., “Schnorr randomness”, *Electronic Notes in Theoretical Computer Science*, 66(1), 2002. http://www.elsevier.nl/locate/entcs/volume66.html.

[FER14] Ferriman, B., “Cryptanalysis of the RC4 Stream Cipher using Evolutionary Computation Methods”, School of Computer Science, Master Thesis, University of Guelph, Canada, 2014.

[FIN94] Finney, H., “An RC4 cycle that can’t happen”, Post in sci.crypt, September 1994.

[FIS49] Fisher, R., A., Yates, F., “Statistical tables for biological, agricultural and medical research”, 3rd Edition, London, Oliver and Boyd, 1949.

[FM01] Fluhrer, S., McGrew, D., “Statistical analysis of the alleged RC4 keystream Generator”, in. *Proc. 7th International Workshop, FSE 2000*, New York, Lecture Notes in Computer Science, Vol. 1978, Springer-Verlag, 2001, pp. 66-71.

[FMS01] Fluhrer, S., Mantin, I., Shamir, A., “Weaknesses in the key scheduling algorithm of RC4”, in *Proc. 8th Annual International Workshop, SAC 2001*, Toronto, Lecture Notes in Computer Science, Vol. 2259, Springer-Verlag, 2001, pp. 1-24.

[FMS02] Fluhrer, S., Mantin, I., Shamir, A., “Attacks on RC4 and WEP”, *CryptoBytes (RSA Laboratories)*, Vol. 5, No. 2, 2002, pp. 26–34. http://www.rsa.com/rsalabs/cryptobytes/cryptobytes_v5n2.pdf

[FUN]Funes, P., “Complexity measures for complex systems and complex objects”. http://www.cs.brandeis.edu//~pablo/complex.maker.html

[GAC74] Gács, P., "On the symmetry of algorithmic information”, *Soviet Math. Dokl*., 15, 1974, pp. 1477–1480.

[GAS05] Gast, M., “802.11 Wireless Networks: The Definitive Guide”, Second Edition, O’Reilly, 2005

[GELL95] Gell-Mann, M., “What is Complexity?” *Complexity* 1/1**,** 1995, pp. 16-19.

[GELL96] Gell-Mann, M., Lloyd, S., “Information Measures, Efective Complexity, and Total Information.”, *Complexity* 2/1**,** 1996, pp. 44-52.

[GLO86] Glover, F., “Future Paths for Integer Programming and Links to Artificial Intelligence, *Computer and Operations Research*, Vol. 13, No. 5, 1986, pp. 533-549.

[GLO89] Glover, F., “Tabu Search”, Part I, *ORSA Journal on Computing*, vol. 1, no. 3, 1989, pp. 190-206.

[GLO90] Glover, F., “Tabu Search”, Part II, *ORSA Journal on Computing*, vol. 2, no. 1, 1990, pp. 4-32.

[GLOV90] Glover, F., “Tabu Search: A Tutorial”, *Interfaces*, vol. 20, no. 4, 1990, pp. 74-94.

[GL93] Glover, F., Laguna, M., "Tabu search", C. Reeves (ed.) *Modern Heuristic Techniques for Combinatorial Problems,* London, Blackwell, 1993, pp. 70-150. http://www.dei.unipd.it/~fisch/ricop/tabu_search_glover_laguna.pdf.

[GOD31] Gödel, K., "Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme, I.", *Monatshefte für Math. u. Physik* 38, 1931, pp.173-198.

[GM03] Goldstein D., Moews, D., "The identity is the most likely exchange shuffle for large n", *Aequationes Mathematicae*, Vol. 65, No. 1-2, 2003, pp. 3-30.

[GOM82] Goldwasser, S., Micali, S., "Probabilistic Encryption", *JCSS*, Vol. 28, No. 2, 1982, pp. 270-299.

[GMR89] Goldwasser, S., Micali, S., Rackoff, C., "The Knowledge Complexity of Interactive Proof Systems", *SIAM Journal of Computing*, 18(1), 1989, pp. 186–208.

[GOL97] Golic, J., Dj., "Linear statistical weakness of alleged RC4 keystream generator", in. *Proc. International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT '97*, Konstanz, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, 1997, pp. 226-238.

[GJD97] Golic, J., Dj., Cryptanalysis of Alleged A5 Stream Cipher, Advances in Cryptology — EUROCRYPT '97, Lecture Notes in Computer Science, Vol. 1233, Springer Berlin Heidelberg, ISBN 978-3-540-62975-7, 1997, pp. 239-255.

[GOL82] Golomb, S., W., "Shift Register Sequences", *Holden-Day, Inc., San Francisco, 1967, revised edition*, Aegean Park Press, Laguna Hills, CA, 1982.

[GG05] Gong, G., Gupta, K., C., Hell, M., Nawaz, Y., "Towards a General RC4-like Keystream Generator", in *Proc. First SKLOIS Conference, CISC 2005*, Beijing, Lecture Notes in Computer Science, Vol. 3822, Springer-Verlag, 2005, pp. 162-174.

[GV03] Grünwald, P., and Vitányi, P., "Kolmogorov Complexity and Information Theory With an Interpretation in Terms of Questions and Answers", *Journal of Logic, Language, and Information*, Vol.12, No. 4, 2003.

[GW04] Grünwald, P., Vitányi, P., "Shannon Information and Kolmogorov Complexity", 2004. http://homepages.cwi.nl/~paulv/papers/info.pdf.

[GW08] Grünwald, P., Vitanyi, P., "Algorithmic Information Theory", *In Handbook of the Philosophy of Science*, Volume 8: Philosophy of Information. (edited by P. Adriaans and J. van Benthem), Elsevier Science Publishers, 2008, pp 289-325.

[GMA11] Gupta, S.,S., Maitra, S., Paul, G., Sarkar, S., "Proof of empirical RC4 biases and new key correlations", *Selected Areas in Cryptography*, Lecture Notes in Computer Science, Vol. 7118, ISBN 978-3-642-28495-3, 2011, pp. 151-168.

[GMA14] Gupta, S.,S., Maitra, S., Paul, G., Sarkar, S., " (Non-) Random Sequences from (Non-)Random Permutations – Analysis of RC4 Stream Cipher", *Journal of Cryptology*, Vol. 27, Issue 1, ISSN 0933-2790, 2014, pp. 67-108.

[GW00] Grosul A., Wallach, D., "A related key cryptanalysis of RC4", Technical Report TR-00-358, Department of Computer Science, Rice University, 2000. http://www.weizmann.ac.il/mathusers/itsik/RC4/Papers/GrosulWallach.ps

[HAN86] Hansen, P., "The Steepest Ascent Mildest Descent Heuristic for Combinatorial Programming", *Congress on Numerical Methods in Combinatorial Optimization*, Capri, Italy, 1986.

[HIL99] Hastad, J., Impagliazzo, R., Levin, L., A., Luby, M., "A Pseudorandom Generator form any One-way Function", *SIAM Journal on Computing*, Vol. 28, pp. 1364-1396, 1999.

[HM05] He, C., Mitchell, J., C., "Security Analysis and Improvements for IEEE 802.11i*", The 12th Annual Network and Distributed System Security Symposium (NDSS'05)*, 2005, pp. 90-110.

[HS05] Hong, J., Sakar, P., "New Applications of Time Memory Data Tradeoffs", Advances in Cryptology - ASIACRYPT 2005, Lecture Notes in Computer Science, Vol. 3788, ISBN 978-3-540-30684-9, Springer Berlin Heidelberg, 2005, pp. 353–372.

[HUS05] Huang, J., Seberry, J., Susilo, W., Bunder, M., "Security Analysis of Michael: The IEEE 802.11i Message Integrity Code", *Lectures Notes in Computer Science*, Vol. 3823, Springer Berlin/Heidelberg, November 2005, pp. 423-432.

[HUL01] Hulton, D., "Practical exploitation of RC4 weaknesses in WEP environments", 2001. http://www.datastronghold.com/security-articles/hacking-articles/practical-exploitation-of-rc4-weaknesses-in-wep-environments.html

[HUT07] Hutter, M., "Algorithmic Information Theory: a brief non-technical guide to the field", 2007. http://arxiv.org/abs/cs/0703024.

[HUT09] Hutter, M., "Open Problems in Universal Induction & Intelligence", *Algorithms* 2(3), 2009, pp.879-906.

[IC08] Iantovics, B., L., Crainicu, B., "Complex Mobile Multiagent Systems", *First International Conference on Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing. CANS 2008*, Published by IEEE Computer Society, IEEE Computer Society Order Number P3621, ISBN 978-0-7695-3621-7, Library of Congress Number 2009900732, 2008, pp. 21-30.

[IAC08] Iantovics, B., L., Crainicu, B., "Security in Mobile Multiagent Systems", *Proceedings of the International Conference Complexity and Intelligence of the Artificial and Natural Complex Systems. Medical Applications of the Complex Systems. Biomedical Computing, CANS 2008*, 8-9 November, Târgu Mureş, 2008, Editura Universităţii "Petru Maior" Târgu-Mureş, 2008, ISSN 2065-0426, pp. 183-191.

[ICR08] Iantovics, B., L., Crainicu, B., "Security Measures in Complex Multiagent Systems Compose from Mobile Agents", *Complexity in Artificial and Natural Systems*, Editura Universităţii "Petru Maior" Târgu Mureş, ISBN 978-973-7794-76-5, 2008, pp. 47-55.

[IM10] Iantovics, B., L., Marusteri, M., Kountchev, R., Zamfirescu, C., B., Crainicu, B., "Intelligent CMDS Medical Agents with lerning Capacity", *Proceedings of the International Conference on Virtual learning. ICVL 2010*, October 29-October 31, 2010, Targu Mures, Romania, Bucharest University Press, 2010, ISSN 1844-8933, pp. 325-331.

[IC13] Iantovics, B., L., Crainicu, B, "Sisteme multiagent: o abordare modernă în inteligenţa artificială**",** Editura Universităţii "Petru Maior, ISBN 978-606-581-099-0, 2013.

[IC14] Iantovics, B., L., Crainicu, B., "A Distributed Security Approach for Intelligent Mobile Multiagent Systems", *Advanced Intelligent Computational Technologies and Decision Support Systems, Studies in Computational Intelligence*, Volume 486, Springer International Publishing, ISBN 978-90-481-3661-2 (Print), ISBN 978-90-481-3662-9 (Online), 2014, pp. 175-189.

[IEEE1] *IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control*, IEEE Std 802.1X-2004.

[IEEE2] *IEEE Standard for Information technology- Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Std 802.11i-2004

[ITO2014] Isobe, Takanori, Ohigashi, Toshihiro, "Security of RC4 Stream Cipher", Hiroshima University, 2014.

[JEN98] Jenkins, R., "Isaac and RC4", 1998. http://burtleburtle.net/bob/rand/isaac.html.

[JOH99] Johansson, T., Jonsson, F., "Improved Fast Correlation Attacks on Stream Ciphers via Convolutional Codes", *Advances in Cryptology — EUROCRYPT '99*, Lecture Notes in Computer Science, Vol. 1592, 1999, pp. 347-362.

[KM12] Kamble, B., H., Meshram, B., B., Robustness of RC4 against Differential attack, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, Issue 4, 2012, pp. 661-665.

[KO04] Kang, Y., S., Oh, K., Chung, B., Chung, K., Nyang, D., "Analysis and Countermeasure on Vulnerability of WPA Key Exchange Mechanism", *Lectures Notes in Computer Science*, Vol. 3090, Springer Berlin/Heidelberg, August 2004, pp. 915-924.

[KL10] Kastermans, B., Lempp, S., "Comparing notions of randomness", *Theoretical Computer Science,* 411(3)*,* 2010*,* pp. 602-616.

[KLE43] Kleene, S., C., "Recursive predicates and quantifiers", *Trans. Amer. Math. Soc.,* 53, 1943, pp. 41-73.

[KLA08] Klein, A., "Attacks on the RC4 stream cipher", *Designs, Codes and Cryptography*, Vol. 48, No. 3, Springer-Verlag, 2008, pp. 269-286. http://cage.ugent.be/~klein/RC4/RC4-en.ps.

[KNU98] Knudsen, L., R., Meier, W., Preneel, B., Rijmen, V., Verdoolaege, S., "Analysis Methods for (Alleged) RC4", in *Proc. International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT'98*, Beijing, Lecture Notes in Computer Science, Springer-Verlag, Vol.1514, 1998, pp. 327–341.

[KNT97] Knuth, D., E., "*The Art of Computer Programming: Seminumerical Algorithm***",** Third edition, Volume 2, Addison-Wesley, 1997.

[KI06] Kobara, K., Imai, H., "Key-Dependent Weak IVs and Weak Keys in WEP – How to Trace Conditions Back to Their Patterns –", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E89-A, No. 8, 2006, pp. 2198-2206.

[KI08] Kobara, K., Imai, H., "IVs to Skip for Immunizing WEP against FMS Attack", *IEICE Transactions on Communications*, Vol.E91–B, No.1, 2008, pp. 218-227.

[KOL56] Kolmogorov, A. N. *Foundations of the theory of probability*. Translation, Edited by Nathan Morrison, with an added bibliography by A. T. Bharuch-Reid, Chelsea Publishing Co., New York, 1956.

[KOL63] Kolmogorov, A., N., "On the tables of random numbers", *Sankhya Ser. A 25* 1963, pp. 369-376.

[KOL65] Kolmogorov, A., N., "Three approaches to the definition of the quantity of information", *Problems of Information Transmission (Problemy Peredachi Informatsii)*, No. 1, 1965, pp. 3–11.

[KOL83] Kolmogorov, A., N., “On logical foundation of Probability Theory”, *Proceedings, 4th USSR-Japan Symposium on Probability Theory and Statistics*, Lecture Notes in Math., Vol. 1021, Springer-Verlag, New York/Berlin, 1983, pp. 1-5.

[KOR104] KoreK, *Need security pointers*, 2004.
http://www.netstumbler.org/showthread.php?postid=89036#post89036

[KOR204] KoreK, *Next generation of WEP attacks?*, 2004.
http://www.netstumbler.org/showpost.php?p=93942&postcount=35

[LEG97] Legg, S., “Solomonoff induction”, Technical Report 30, Centre for Discrete Mathematics and Theoretical Computer Science. University of Auckland, 1997.

[LEG06] Legg, S., “Is there an Elegant Universal Theory of Prediction?”, In *Proc. 17th International Conf. on Algorithmic Learning Theory (ALT’06),* Barcelona, 2006, pp. 274-287.

[LEV173] Levin, L., A., “Universal search problems”, *Problems of Information Transmission*, 9(3), 1973, pp. 265–266.

[LEV273] Levin, L., A., “On the notion of a random sequence”, *Soviet Math. Dokl.*, 14(5), 1973, pp.1413–1416.

[LEV74] Levin, L., A., “Laws of information conservation (non-growth) and aspects of the foundation of probability theory”, *Problems Information Transmission*, 10(3), 1974, pp. 206-210.

[LEV76] Levin, L., A., “Measures of complexity for finite objects (axiomatic description)”, *Sov.Math. Dokl.*, 17**,** 1976, pp. 552-526.

[LEV87] Levin, L.A., “One-way Function and Pseudorandom Generators”, *Combinatorica*, Vol. 7, No. 4, pp. 357-363, 1987

[LIV08] Li, M, Vitanyi, P., “An Introduction to Kolmogorov Complexity and Its Applications”, Third Edition, Springer Verlag, 2008.

[LOV66] Loveland, Z., *Math. Logik Grundl. Math.,* 12, 1966, pp.279-294.

[MG08] Maitra, S., Gouta Paul (2008-09-19), "Analysis of RC4 and Proposal of Additional Layers for Better Security Margin", *Progress in Cryptology – INDOCRYPT 2008*, Lecture Notes in Computer Science, Vol. 5365, Springer-Verlag Heidelberg, ISBN 3-540-89753-4, 2008 pp. 27-39.

[MAN101] Mantin, I., “The Security of the Stream Cipher RC4”, Master Thesis, The Weizmann Institute of Science, 2001.

[MAN201] Mantin, I., “Analysis of the Stream Cipher RC4”, Faculty of Mathematics and Computer Science, The Weizmann Institute of Science, 2001.

[MS02] Mantin, I., Shamir, A., “A practical attack on broadcast RC4”, in *Proc. 8th International Workshop, FSE 2001*, Yokohama, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2355, 2002, pp. 87-104.

[MAN105] Mantin, I., “Predicting and Distinguishing Attacks on RC4 Keystream Generator”, in. *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2005*, Aarhus, Lectures Notes in Computer Science, Vol. 3494, Springer-Verlag, 2005, pp. 491-506.

[MAN205] Mantin, I., "A Practical Attack on the Fixed RC4 in the WEP Mode", in *Proc. 11th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2005*, Chennai, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3788, 2005, pp. 395-411.

[MAR98] Marcus, S., "Imprecision, between variety and uniformity: the conjugate pairs", *J.J. Jadacki, W. Strawinski, eds. In the World of Signs, Pozna n Studies in the Philosophy of the Sciences and the Humanities 62*, 1998, pp. 59–72.

[MLO66] Martin-Löf, P., "The definition of random sequences", *Information and Control*, 9 (6), 1966, pp. 602–619.

[MLO68] Martin-Löf, P., "On the notion of randomness", *Intuitionism and Proof Theory*, (Proc. Conf., Bu_alo, N.Y., 1968), pp. 73-78, North-Holland, Amsterdam, 1970 and Proof Theory, New York, 1968. pp. 73-78.

[MLO69] Martin-Löf, "The literature on von Mises' kollectives revisited", *Theoria*, 35, 1969, pp. 12-37.

[MCS061] Măruşteri, M., Crainicu, B., Şchiopu, A., *ROBIOCLUSTER – an open source platform for HPC (high performance computing)/Linux clusters in the biomedical field*, Integrating Biomedical Information: From eCell to ePatient, Proceedings of the European Federation for Medical Informatics, Special Topic Conference, April 6-8, 2006, Timişoara, Romania, Akademische Verlagsgesellschaft Aka GmbH, Berlin, ISBN 3-89838-072-6 (Aka), ISBN-10 1-58603-614-9 (IOS Press), ISBN-13: 978-1586036140 (IOS Press), ISBN 973-625-303-1 (Editura Politehnica), 2006, pp. 174-177.

[MCS062] Măruşteri, M., Ş., Crainicu, B., Şchiopu, A., "New trends in Open Source Educational Platforms – The ROSLIMS Linux Live CD Paradigm", Proceedings of the 5th RoEduNet IEEE International Conference: Sibiu, 1-3 June 2006, Romania, Editura Universităţii "Lucian Blaga" din Sibiu, 2006, ISBN (10) 973-739-277-9, (13) 978-973-739-277-0, pp. 82-86. *Acta Universitatis Cibiniensis*, Vol. LV, Technical Series, Editura Universităţii "Lucian Blaga" din Sibiu, 2007, ISSN 1583-7149, pp. 136-140.

[MCS063] Măruşteri, M., Crainicu, B., Şchiopu, A., *ROSLIMS Linux Live CD – all-in-one cross platform solution for running biomedical software*, Integrating Biomedical Information: From eCell to ePatient, Proceedings of the European Federation for Medical Informatics, Special Topic Conference, April 6-8, 2006, Timişoara, Romania, Akademische Verlagsgesellschaft Aka GmbH, Berlin, ISBN 3-89838-072-6 (Aka), ISBN-10 1-58603-614-9 (IOS Press), ISBN-13: 978-1586036140 (IOS Press), ISBN 973-625-303-1 (Editura Politehnica), 2006, pp. 178-181.

[MEO96] Menezes, A., J., van Oorschot, P., C., "Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)", CRC Press, ISBN 10: 0849385237, 1996.

[MRK08] Merkle, W., " The complexity of stochastic sequences", *Journal of Computer and System Sciences,* 74, 2008, pp. 350-357.

[MIR02] Mironov, I., "(Not So) Random Shuffles of RC4", in *Proc. 22nd Annual International Cryptology Conference, Advances in Cryptology, CRYPTO 2002*, Santa Barbara, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2442, 2002, pp. 304–319.

[MT99] Mister S., Tavares, S., E., "Cryptanalysis of RC4-like Ciphers", in *Proc. 5th Annual International Workshop, SAC 1998*, Kingston, Lecture Notes in Computer Science, Springer-Verlag, Vol.1556, 1999, pp. 131–143.

[MRH04] Moen, V., Raddum, H., Hole, K., J., "Weaknesses in the Temporal Key Hash of WPA", *Mobile Computing and Communications Review*, Vol. 8, No. 2, April 2004, Papers from MC^{2}R Open Call, pp. 76-83.

[MSU98] Muchnik, A., A., Semenov, A., L., Uspensky, V., A., "Mathematical Metaphysics of Randomness", *Theor. Comput. Sci.* 207(2), 1998, pp.263-317.

[OSM05] Ohigashi, T., Shiraishi, Y., Morii, M., "Most IVs of FMS Attack-Resistant WEP Implementation Leak Secret Key Information", in *Proc. 2005 Symposium on Cryptography and Information Security*, Maiko, Vol. 4, 2005, pp. 1957–1962.

[OS05] Ohigashi, T., Shiraishi, Y., Morii, M., "FMS Attack-Resistant WEP Implementation Is Still Broken – Most IVs Leak a Part of Key Information – ", in *Proc. International Conference, CIS 2005*, Xi'an, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3802, 2005, pp. 17-26.

[OSM08] Ohigashi, T., Shiraishi, Y., Morii, M., "New Weakness in the Key-Scheduling Algorithm of RC4", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E91-A, No. 1, 2008, pp. 3-11.

[OWF] **One-Way Function.* http://mathworld.wolfram.com/One-WayFunction.html.

[OP13] Orumiehchiha, M., A., Pieprzyk, J., Shakour, E., Steinfeld, R., "Cryptanalysis of RC4(n,m) Stream Cipher", in *Proc. 6th International Conference on Security of Information and Networks*, *SIN '13*, Aksaray, ACM New York, NY, USA, 2013, pp. 165-172.

[OUG05] Ou, G., "Wireless LAN security guide, Security for any organization large or small", January 2005, http://www.lanarchitect.net/ Articles/ Wireless/SecurityRating/

[PP10] Paar, C., Pelzl, J., "Understanding Cryptography", Springer-Verlag Berlin Heidelberg, ISBN 978-3-642-04101-3, 2010.

[PAP03] Paul S., Preneel, B., "Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator", in *Proc. 4th International Conference on Cryptology in India*, *INDOCRYPT 2003*, New Delhi, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2904, 2002, pp. 52-67.

[PAP04] Paul S., Preneel, B., "A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher", in *Proc. 11th International Workshop, FSE 2004*, Delhi, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3017, 2004, pp. 245–259.

[PMA07] Paul, G., Maitra, S., "RC4 State Information at Any Stage Reveals the Secret Key", *14th Annual Workshop On Selected Areas in Cryptography, SAC 2007*, Ottawa, Canada, 2007, Lecture Notes in Computer Science, Vol. 4876, Springer Berlin Heidelberg, ISBN 978-3-540-77359-7, 2007, pp. 360-377.

[PRM08] Paul, G., Rathi, S., Maitra, S., "On non-negligible bias of the first output bytes of RC4 towards the first three bytes of the secret key", *Designs, Codes and Cryptography*, Vol. 49, No. 1-3, Springer-Verlag, 2008, pp. 123-134.

[PEI10] Peikert, C., "Indistinguishability, Pseudorandomness", *Theoretical Foundations of Cryptography*, Georgia Tech, Spring 2010.

[STC] **Private-key cryptography. Stream Ciphers, Computational Security*, October 5, 2010. http://www.deic.uab.es/material/20375-4-stream-pf.pdf.

[PSG] **Pseudo Random Generators*, School of Computer Science and Communication, CSC, Stockholm University. http://www.nada.kth.se/kurser/kth/2D1441/semteo03/lecturenotes/prg.pdf.

[PRF] **Pseudo Random Functions,* School of Computer Science and Communication, CSC, Stockholm University. http://www.nada.kth.se/kurser/kth/2D1441/semteo03/lecturenotes/prf.pdf.

[RIJ14] Rijmenants, D., "One-time Pad", *Cipher Machines & Cryptology*, 2014. http://users.telenet.be/d.rijmenants/en/onetimepad.htm.

[RIV92] Rivest, R., L., "The RC4 Encryption Algorithm", *RSA Data Security, Inc*., 1992. (Proprietary).

[RIV01] Rivest, R., L., "RSA security response to weaknesses in key scheduling algorithm of RC4", Tech Notes, RSA Laboratories, 2001. http://www.rsasecurity.com/rsalabs/node.asp?id=2009

[RS14] Rivest, R., L., Schuldt, J, C., N., "Spritz – a spongy RC4-like stream cipher and hash function", MIT Talk. 2014. http://people.csail.mit.edu/rivest/pubs/RS14.pdf.

[ROB81] Robbins D., Bolker, E., "The bias of three pseudo-random shuffles", *Aequationes Mathematicae*, Vol. 22, 1981, pp. 268-292.

[ROO95] Roos, A., "Class of weak keys in the RC4 stream cipher", Two posts in sci.crypt, message-id 43u1eh$1j3@hermes.is.co.za and 44ebge$llf@hermes.is.co.za, 1995.

[RUE86] Rueppel, R., A., "Analysis and Design of Stream Ciphers", Communications and Control Engineering Series, , ISBN: 978-3-642-82867-6, Springer Berlin Heidelberg, 1986.

[SS92] Schmidt, F., Simion, R., "Card shuffling and a transformation on S_n", *Aequationes Mathematicae*, Vol. 44, 1992, pp. 11-34.

[SC171] Schnorr, C., P., "Zufalligkeit und Wahrscheinlichkeit. Eine algorithmische Begrundung der Wahrscheinlichkeitstheorie", *Lecture Notes in Mathematics*, Vol. 218, Springer-Verlag, Berlin, 1971.

[SC271] Schnorr, C. P., "A unified approach to the definition of a random sequence", *Mathematical Systems Theory*, Vol. 5, 1971, pp. 246–258.

[SC73] Schnorr, C., P., "Process complexity and effective random tests", *Journal of Computer and System Sciences*, 7(4), 1973, pp. 376–388.

[SEC74] Seche, L., "Lexicul artistic eminescian în lumină statistică", Editura Academiei RSR, Bucureşti, 1974.

[SVV11] Sepehrdad, P., Vaudenay, S., Vuagnoux, M., "Discovery and Exploitation of New Biases in RC4", *Lecture Notes in Computer Science*, Vol. 6544, Springer Heidelberg, 2011, pp. 74–91

[SHA48] Shannon, C.E., "A Mathematical Theory of Communication", *Bell Syst. Tech. J.*, 27, 1948, pp.379-423, pp.623-656.

[SOM03] Shiraishi, Y., Ohigashi, T., Morii, M., "An improved Internal-State Reconstruction Method of a Stream Cipher RC4", in *Proc. IASTED International Conference on Communication, Network, and Information Security, CNIS 2003*, New York, 2003, pp. 132-135.

[SHI10] Shirayev, A., N., “On the evolution of the von Mises’ notion of Randomness”, Mathematical Institute, University of Freiburg, 2010.

http://wochenprogramm.mathematik.uni-freiburg.de/kabstract.en.html?LfdNr=8&Semester=WS2009-2010

[SIE84] Siegenthaler, T., “Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications”, *IEEE Transactions on Information Theory*, Vol. 30 (5), 1984, pp. 776–780.

[SIE85] Siegenthaler, T., “Decrypting a class of stream ciphers using ciphertext only”, *IEEE Transactions on Computers*, Vol. C-34, 1985, pp. 81-85,

[SR11] Singhal, N., Raina, J., P., S., "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", *International Journal of Computer Trends and Technology (IJCTT)*, ,Vol. 1, Issue 3, 2011, pp. 259-263.

[STW03] Shunman W., Tao, R., Wang, Y., Zang, J., "WLAN and it's security problems”, in *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2003, pp 241-244.

[SOL60] Solomonoff, R., J., “A Preliminary Report on a General Theory of Inductive Inference”, (Revision of Report V–131), *Contract AF* 49(639)–376, Report ZTB–138, Zator Co., Cambridge, Mass., Nov. 1960.

[SOL62] Solomonoff, R., "Training Sequences for Mechanized Induction", *Self- Organizing Systems*, M. Yovits, ed., 1962, pp. 425-434.

[SOL164] Solomonoff, R., “A formal theory of inductive inference”, *Information and Control*, Part I, Vol. 7, No. 1, 1964, pp.1-22.

[SOL264] Solomonoff, R., “A formal theory of inductive inference*”, Information and Control*, Part II, Vol. 7, No. 2, 1964, pp.224-254.

[SOL78] Solomonoff, R., J., “Complexity-Based Induction Systems: Comparisons and Convergence Theorems”, *IEEE Trans. on Information Theory*, 24:4, 1978, pp.422–432.

[SOL97] Solomonoff, R., “The discovery of algorithmic probability”, *Journal of Computer and System Sciences*, Vol. 55, No. 1, 1997, pp. 73-88.

[SON08] Song, D., Computer Security, Notes 4, CS 161, Fall 2008. http://inst.eecs.berkeley.edu/~cs161/fa08/Notes/random.pdf.

[STU01] Stubblefield, A., Ioannidis, J., Rubin, A., “Using the Fluhrer, Mantin, and Shamir attack to Break WEP”, Technical Report TD-4ZCPZZ, AT&T Labs, 2001.

[SIR04] Stubblefield, A., Ioannidis, J., Rubin, A., “A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)”, *ACM Transactions on Information and System Security (TISSEC)*, Vol. 7, No. 2, 2004, pp. 319–332.

[TW08] Tews, E., Weinmann, R., P., Pyshkin, A., “Breaking 104 bit WEP in less than 60 seconds”, in *Proc. 8th International Workshop, WISA 2007*, Jeju Island, Lecture Notes in Computer Science, Vol. 4867, Springer-Verlag, 2008, pp. 188-202. http://eprint.iacr.org/2007/120.pdf.

[THO12] Thomsen, M., "Linear Feedback Shift Registers, Galois Fields, and Stream Ciphers", *Cryptography II*, 2012. http://www.cs.rit.edu/~mxt4877/.

[TBN07] Tomašević, V., Bojanić, S., Nieto-Taladriz, O., "Finding an internal state of RC4 stream cipher", *Information Sciences*, Vol. 177, Elsevier, 2007, pp. 1715-1727.

[TUR36] Turing, A., "On computable numbers, with an application to the Entscheidungsproblem", *Proceedings of the London Mathematical Society*, ser. 2. vol. 42 (1936-7), pp.230-265.

[USP06] Uspensky, V. A., "Four algorithmic physiognomies of randomness", *Matematicheskoe prosveshchenie, 10, MCCME,* Moscow, 2006, pp. 71–108.

[LA187] van Lambalgen, M., "Random Sequences", *PhD Thesis*, Department of Mathematics, University of Amsteram, Amsterdam, 1987.

[LA287] van Lambalgen, M., "Von Mises' Definition of Random Sequences Reconsidered", *J. Symb. Log.,* 52(3), 1987, pp.725-755.

[VV07] Vaudenay, S., Vuagnoux, M.,"Passive-only Key Recovery Attacks on RC4", in *Proc. 14th International Workshop, SAC 2007*, Ottawa, Lecture Notes in Computer Science, Vol. 4876, Springer-Verlag, 2007, pp. 344-359. http://infoscience.epfl.ch/record/115086/files/VV07.pdf.

[VER09] Vereshchagin, N., "Kolmogorov Complexity and Model Selection", *Computer Science - Theory and Applications*, Fourth International Computer Science Symposium in Russia, CSR 2009, Novosibirsk, Russia, 2009, LNCS 5675, Springer-Verlag, pp. 19-24.

[VRM19] Vernam, G., S., Secret signaling system, US 1310719 A (US patent), 1919.

[VIL36] Ville, J., "Sur la notion de collectif", *Comptes rendus* 203, 1936, pp.26–27.

[VIL39] Ville, J., "Etude critique de la notion de collectif", *Gauthier-Villars*, Paris, 1939.

[VIT01]Vitányi, P., "Randomness", *CoRR math.*PR/0110086, 2001. http://arxiv.org/abs/math/0110086

[VLE10] Vlek, C., "Definability in the degrees of randomness", *MSc Dissertation*, University of Amsterdam, 2010.

[VOL02] Volchan, S., B., "*What Is a Random Sequence?*", *The American Mathematical Monthly*, Vol. 109, 2002, pp. 46–63.

[MIS19] von Mises, R., "Grundlagen der Wahrscheinlichkeitsrechung", *Math. Z.*, vol. 5, 1919, pp. 52-99.

[MIS57] von Mises, R., "Probability, statistics and truth", 2nd English edition, George Allen and Unwin, London, 1957.

[VS10] Vovk, V., Shen, A., "Prequential randomness and probability", *Theoretical Computer Science*, Vol. 411, No. 29-30, 2010, pp. 2632-2646.

[VYU98] V'yugin, V., V., "Non-stochastic infinite and finite sequences", *Theoretical Computer Science*, 207(2), 1998, pp.363-382.

[WAG95] Wagner, D., "My RC4 weak keys", Post in sci.crypt, message-id 447o1l$cbj@cnn.princeton.edu, 1995.

http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys.

[WAL36] Wald, A., "Sur la notion de collectif dans le calcul des probabilités", *Comptes Rendus des Séances de l'Académie des Sciences*, 202, 1936, pp. 1080-1083.

[WAL37] Wald, A., "Die Widerspruchsfreiheit des Kollektivbegriffes der Wahrscheinlichkeitsrechnung", *Ergebnisse eines Math. Kolloquiums*, Vol. 8, 1937, pp. 38-72.

[WLK00] Walker, J., "Unsafe at any key size: an analysis of the WEP encapsulation," *Tech. Rep. 03628E, IEEE 802.11 committee*, March 2000, http://grouper.ieee.org/groups/802/11/Documents/ DocumentHolder/0-362.zip.

[WIL70] Willis, D., G., "Computational Complexity and Probability Constructions," *Journal of the Assoc. of Comp. Mach.,* 1970, pp. 241-259.

[WOOL] Wool, A., "Lightweight key management for IEEE 802.11Wireless LAN's with key refresh and host revocation", *IEEE 802.11 TGi working group*, http://grouper.ieee.org/groups/802/11/Documents/ DocumentHolder/2-411.zip.

[WO04] Wool, A., "A Note on the Fragility of the "Michael" Message Integrity Code", *IEEE Transactions on Wireless Communications*, Vol. 3, No. 5, September 2004, pp 1459-1462.

[WOO81] Wootters, W., K., "Statistical distance and Hilbert space", *Physical Review D 23*, 1981, pp. 357-362.

[YAO82] Yao, A., C., "Theory and Applications of Trapdoor Functions", *Proc. of the 23rd IEEE, Symp. on Foundation of Computer Science (FOCS)*, 1982, pp. 80-91.

[YAG06] Yager, R., R., "OWA trees and their role in security modeling using attack trees", *Information Science*, Vol. 176, No. 20, 2006, pp. 2933–2959

[ZAW] Zawada, K., "Kolmogorov Complexity", *University of Illinois at Chicago*. http://www.ece.uic.edu/~devroye/courses/ECE534/project/project_Krzysztof_Zawada.pdf.

[ZEN04] Zenner, E., On the Role of the Inner State Size in Stream Ciphers, Reihe Informatik, 01-2004. http://www.erikzenner.name/docs/2004_state_wosis.pdf.

[ZOL04] Zoltak, B., "VMPC One-Way Function and Stream Cipher", in *Proc. 11th International Workshop, FSE 2004*, Delhi, Lectures Notes in Computer Science, Vol. 3017, Springer-Verlag, 2004, pp. 210–225.

[ZVO70] Zvonkin, A., K., Levin, L., A., "The Complexity of Finite Objects and the Development of the Concepts of Information and Randomness by Means of the Theory of Algorithms", *Russian Mathematical Surveys*, Vol. 25, No. 66, 1970, pp. 83-124.