REPUBLIC OF AZERBAIJAN

On the rights of the manuscript

DEVELOPING METHODS OF FORMATION PSEUDO-RANDOM NUMBERS GENERATORS BASED ON M-ARY CODES

Speciality: 3338.01– System analysis, control, and information processing (information security)

Branch of science: Technical sciences

Applicant: **Musa Famil Mammadov**

ABSTRACT

of the dissertation for the degree of Doctor of Philosophy

Baku – 2025

The work was performed at the department of "Computer engineering" of Azerbaijan State Oil and Industry University,

Scientific supervisor: Doctor of Technical Sciences, assoc. prof.

Xazail Nuraddin Rzayev

Official opponents: Doctor of Technical Sciences, professor
Fazil Hazin Alakbarli

Doctor of Technical Sciences, professor
Ramin Rza Rzayev

Doctor of Philosophy in technical sciences
Aziz Mahammad Nuriyev

Disseration council ED 2.48 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at Azerbaijan State Oil and Industry University

Chairman of the Dissertation council: Doctor of Technical Sciences, professor

Rafik Aziz Aliyev

Scientific secretary of the Dissertation council: Doctor of Philosophy in tech.sc assoc. prof

Akif Vali Alizadeh

Chairman of the scientific seminar: Doctor of Technical Sciences, professor

Kamala Rafik Aliyeva

GENERAL DESCRIPTION OF THE WORK

Relevance and degree of development of the topic. The development of high technologies and the expansion of the range of digital services makes it possible to automate almost any area of the world community, in which computing resources have played an integral part in recent years. As part of the expansion of digitization and digitalization during the life cycle, systems and networks are often complexed (synthesized) with each other, which significantly affects the protection of circulating flows. This is how cyber-physical systems are formed by combining mobile Internet technologies, wireless networks with smart technologies, Internet things and classical networks. Under such conditions, in almost all areas of the community, new critical systems are formed, in which the destruction of elements (subsystems) leads to the destruction of the entire system as a whole. In addition, information itself (information flows) becomes a commodity and its value is economically confirmed by the continuity of business processes and the formation of protection systems. A crucial part of such systems, along with symmetric (traditional) cryptosystems, and asymmetric (public key cryptosystems), digital signature and hashing functions, are random number generators, which are practically used in all mechanisms of the security system, to one degree or another[1].

Thus, a special place among the tasks to be solved is occupied by the development of promising methods and algorithms for generating pseudo-random numbers (PRN) for cryptographic means of protecting information while ensuring confidentiality, integrity, authenticity and availability of information technologies, including relational database management systems; to ensure the correct functioning of the components of the information system, including to ensure the absence of undocumented features, ensure the

[1] Yevseiev, S. Development of a method for ensuring confidentiality and authenticity in wireless channels. / S.Yevseiev, Kh.Rzayev, M.Mammadov [et al.] // Eastern-European Journal of Enterprise Technologies, – Kharkov: – 2022. № 9, – p. 15-27.

traceability of information flows in the system, protection of copyrights, rights of information owners, etc., which confirms the relevance of the dissertation.

Goals and objectives of the study. The mathematical basis of modern cryptography was laid by the famous American scientist C. Shannon, who was the first to introduce an abstract definition of a secret system and analytically formalize the process of cryptographic data transformation. Many works are devoted to the issues of studying effective methods for constructing cryptographically secure pseudo-random number generators (PRNG), in which various methods for generating PRN based on the use of recurrent registers with linear and non-linear feedbacks, as well as based on congruent transformations are studied, and the features of their practical use in signal theory and error-correcting coding. Along with high performance indicators, this approach, as a rule, makes it possible to form PRN of the maximum period. Simultaneously, as the results of the research show, the generated PRN are not cryptographically secure, the rule of their formation is easily revealed after the attacker intercepts a fragment of a sequence of small length. A contradiction arises when the existing mathematical apparatus, known methods and algorithms for generating PRN do not allow to fully ensure high performance indicators (cryptographic strength and speed in software and hardware implementation).). To resolve the identified contradiction, it is necessary to develop scientific and practical methods and algorithms for the formation of PRN of provable stability, the specific implementation of which will allow building PRNG with the properties required for practice. A promising direction in this sense is PRNG based on redundant codes.

The purpose of the dissertation – is increasing the performance of provably stable pseudo-random number generators in information and communication systems.

In accordance with the purpose of the work, it is necessary to solve a **scientific problem**, which consists in developing methods for generating PRN based on redundant coding algorithms to increase

the speed of provably stable generators in information systems and technologies.

Object of study. The process of increasing the performance of provably stable pseudo-random number generators in information and communication systems. **Subject of study.** Methods for generating provable stable pseudo-random number generators based on M-ary codes.

Research methods. Methods for generating PRN are developed using the algebraic theory of redundant codes, information theory and Galois fields. The study of the effectiveness of the developed provable stable PRNG, comparison with known analogues was carried out using elements of information security theory, methods of probability theory and statistical hypothesis testing. The development of proposals for the hardware and software implementation of the developed PRNG was carried out using the theory of machines, methods of mathematical and software modeling.

The main provisions submitted for defense. The main goals for the implementation of the dissertation work are the following:

1. To analyze the known methods for the formation of PRN and justify the choice of the direction of research.
2. Develop methods for generating PRN based on redundant block codes.
3. Develop practical algorithms for generating pseudo-random numbers based on redundant block codes.
4. Examine the efficiency of provable stable pseudo-random number generators based on redundant block codes.

Scientific novelty of the research:

1. For the first time, a method for generating PRN based on algorithms of M-ary codes is proposed with the reduction of the problem of calculating a secret key to solving the complexity-theoretic problem of syndromic decoding using a

known code word with errors[2]. The proposed method makes it possible to construct provably stable generators for generating sequences with an increased long period.

2. For the first time, estimates of the cryptographic resistance of the proposed methods for forming the PRN based on M-ary codes to the negative actions of intruders are obtained, which take into account non-algebraic decoding methods, including permutation and syndromic decoding, which allow to substantiate the design parameters of the developed PRNG for their practical use.
3. The method of forming PRN based on M-ary codes has been improved, which differs from the known one by additionally introduced recurrent transformations over sequences of secret key data and syndromic sequences of a redundant block code, which makes it possible to ensure the formation of sequences of the maximum period with the reduction of the problem of calculating a secret key to solving a theoretical complexity syndromic decoding problems[3].
4. The mathematical apparatus for the formation of PRNG based on M-ary codes was further developed, which differs from the known ones by using algebro-geometric codes built on the basis of the mathematical devices of coding theory and parameters of individual curves.

Theoretical and practical significance of the research:

1. Computational algorithms for formation of PRN based on M-ary codes and practical recommendations for their use in information systems and technologies have been developed. Proposals have been developed for software and hardware

[2] Rzayev, X.N., – Psevdo-təsadüfi ədədlər ardıcıllığının formalaşdırılması üsulu, İxtira a2023 0040, Azərbaycan Respublikası / Məmmədov, M.F., Bağırov, E.Y. [və b.]: Azərbaycan Respublikası Əqli Mülkiyyət Agentliyi Patent və Əmtəə Nişanlarının Ekspertiza Mərkəzi, – 2024, – № 5.

[3] Rzayev, X.N., – Psevdo-təsadüfi ədədlər ardıcıllığının yaradılması üsulu, İxtira a2023 0039, Azərbaycan Respublikası / Məmmədov, M.F., Bağırov, E.Y. [və b.]: Azərbaycan Respublikası Əqli Mülkiyyət Agentliyi Patent və Əmtəə Nişanlarının Ekspertiza Mərkəzi, – 2024, – № 4.

implementation of the developed provably stable PRN based on algorithms of M-ary codes.

2. A software implementation of the proposed PRNG has been developed, experimental data have been obtained on their performance in the formation of PRN based on M-ary codes. It has been established that the use of the proposed generators makes it possible to speed up the process of forming a PRN by 3–4 orders of magnitude compared to the known provably stable generators..

3. Experimental results have been obtained on the assessment of the statistical security of the developed PRNG based on redundant coding algorithms. It has been established that, in terms of statistical security, the proposed solutions are comparable to other known provably stable PRNG.

Personal presence of the author. Statement of the problem in the dissertation work, experiments, analysis of the results, generalizations made by the author himself.

Approval and implementation of research: The main results and content of the dissertation were presented at the following conferences:

XI International Scientific and Practical Conference 'Mathematics. Information Technologies. Education.' Lutsk-Svitiaz, Ukraine. June 3–5, 2022.

V International Scientific and Practical Conference 'Issues of Cybersecurity in Information and Telecommunication Systems' (PCSITS)" April 14–15, 2022, Kyiv, Ukraine.

Name of the organization in which the dissertation work was carried out. The research was carried out at the Department of "Computer Engineering" of the Azerbaijan State Oil and Industry University.

The volume of structural units of the dissertation

The structure of the dissertation is as follows: introduction, 4 chapters, conclusion, 2 appendices, and a bibliography. The total work consists of 185 pages, with 12 pages dedicated to images, 14 pages to the bibliography, and 17 pages to the appendices.

Published scientific papers. 13 scientific works have been published on the topic of the dissertation. Among them, 6 are articles. 2 of these articles have been co-authored and published abroad (2 scientific papers are included in the SCOPUS database). 3 abstracts of presentations made at international conferences have been published. Additionally, there are 2 patents confirming the uniqueness of the methods.

THE CONTENT OF THE WORK

The introduction substantiates the relevance of the dissertation, the purpose of the study and the issues to be resolved. The scientific novelty and practical significance of the results obtained are shown..

The first chapter studies the main directions of the theory of information security related to the formation of PRN, analyzes services and security mechanisms. On the basis of research criteria and performance indicators of PRNG, as well as the analysis of known PRNG, the choice of research direction is substantiated and the statement of the scientific problem is mathematically formalized.

The development of information technologies in cyberspace is associated with the development of security services in the components of security: cyber security, information systems security and information security. As a rule, cryptographic algorithms and functions based on symmetric and asymmetric cryptography systems are used to provide security services. A crucial part of such cryptosystems are pseudo-random number generators that allow you to generate a random sequence over a period. One of the evaluation criteria is the duration of the period and its guarantee, i.e. ensuring randomness issued by a random number generator, another criterion is cryptographic strength – ability to resist hacking by the intruders. On the stability of pseudo-random number generators, symmetric flow cryptosystems are formed that ensure the stability of the cryptogram.

Extensive research indicates that, in alignment with the essential guidelines of international standards, the development of an information security system involves multiple interconnected phases. These phases collectively form a lifecycle that ensures the system is not only initially secure but remains resilient over time. Within this framework, two stages are especially pivotal: clearly defining the security services required, and carefully selecting the appropriate mechanisms to support them, tailored to both the organization’s operational environment and its risk profile.

These globally acknowledged standards advocate a structured, risk-oriented methodology to manage information security effectively. A key element of this approach involves identifying which types of security services are essential to counteract potential threats while ensuring compliance with business objectives, legal responsibilities, and regulatory policies. According to the established guidelines, five foundational security services are universally recognized as integral components of a strong cybersecurity posture. These services, visually represented in Figure 1, each serve to mitigate different categories of vulnerabilities. Based on international regulatory documentation[4], these services are defined as follows:

– **Authentication** is the process of verifying the claimed identity of a communication's originator, ensuring the sender or source of information is valid and has not been impersonated or altered.

– **Data privacy** ensures that sensitive or private data is only accessible to authorized parties and remains protected against unauthorized disclosure during both storage and transmission.

– **Access Control** refers to the restriction of entry or usage of specific systems or resources to only those users or entities who have the appropriate permissions.

– **Data Integrity** guarantees that information remains accurate, consistent, and unmodified unless changes are made by authorized individuals under controlled circumstances.

– **Involvement** (sometimes referred to as non-repudiation) provides mechanisms to ensure that participants in digital transactions cannot later deny their involvement or the authenticity of the transmitted data.

[4] ISO/IEC 10181-1:1996. Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview. [Electronic resource] / – 1996

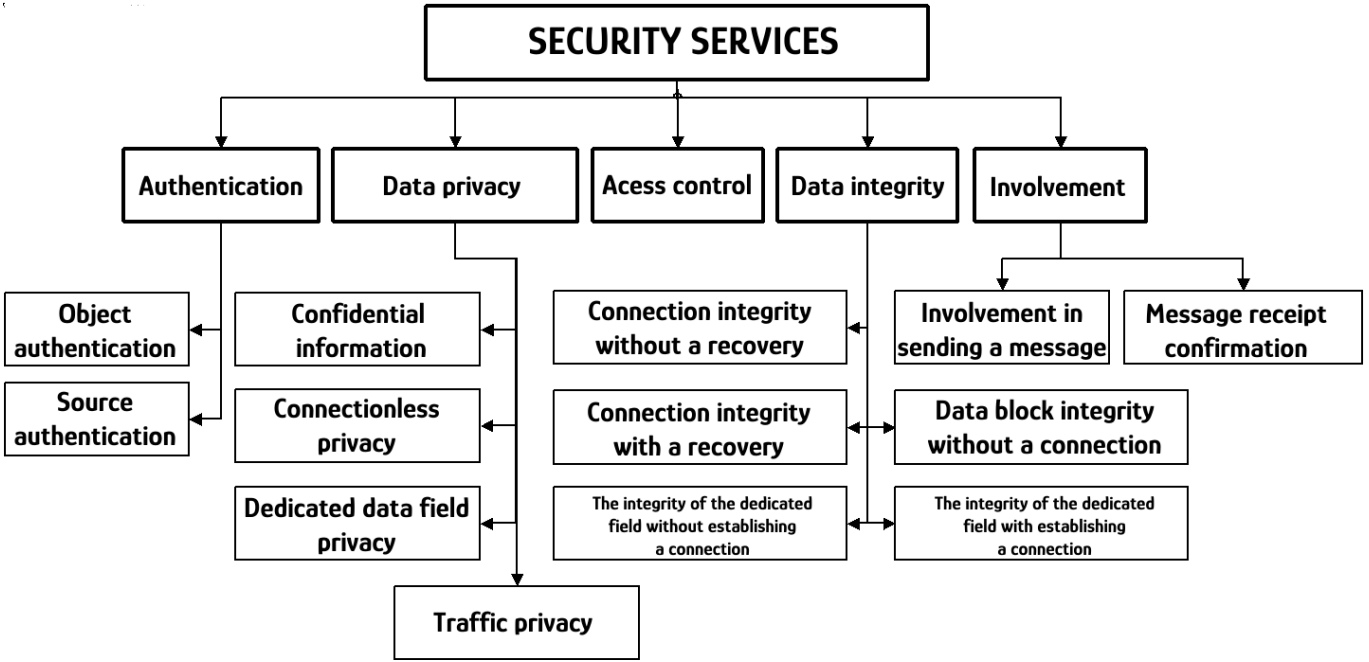

Figure 1. General classification of security services

Together, these five services establish the structural backbone of a secure digital infrastructure. When effectively implemented, they offer a reliable shield against numerous cyber threats, support conformity with international best practices, and enhance the overall trust in digital systems and communications.

The security services shown in figure 1 are provided by appropriate security mechanisms, which are divided into two classes (special and general security mechanisms).

The study of common security mechanisms showed that their use is associated with the development of security policy, the implementation of methods for administering computing resources, logging events and auditing the behavior of the security system as a whole.

Analyzing the process of providing special security services (confidentiality, authentication, integrity, etc.), as well as the tasks of cryptographic information processing related to the provision of these services (information hashing, imitation insertion, digital signature generation, etc.), we can conclude that the need to use special security mechanisms. Since the implementation of most special security mechanisms requires the use of PRNG, the dissertation work has focused on the study of such mechanisms. Special security mechanisms consist of the following elements:

– encryption mechanisms;
– digital signature mechanisms;
– access control mechanisms;
– data integrity mechanisms;
– authentication mechanisms.

Encryption is used to provide confidentiality services, but may also support other security services such as authentication and data integrity protection.

Digital signature mechanisms use "public" keys, which are generated by the sender of data and verified by the recipient. Asymmetric encryption methods can be used to encrypt the checksum of the signed message. The digital signature is used to provide authentication and integrity protection services for which the subject of verification of the signed data is not known in advance. With a certain choice of a controlled parameter, a digital signature can also be used in the implementation of the identity confirmation service.

Access control mechanisms are used to provide access control services and implement policies corresponding to these services. The following types and sources of information can be used in making decisions about granting the type of access requested:

– access control databases, which may contain access control lists or similar structures;

– passwords or other identifying information;

– identification documents or other certificates, the presentation of which indicates the presence of access rights;

– security labels associated with access subjects and objects;

– requested access time;

– requested access route;

– duration of requested access and other information.

Data integrity mechanisms protect the integrity of a single packet or a sequence of data packets by adding to it some control value, which is a function of the data contained in the packet.

The authentication mechanism is usually performed by double or triple handshake. One-way (one-time) exchange provides only one-time authentication and cannot guarantee the timeliness of the exchange. Two-way (double) exchange provides mutual authentication of the source and receiver, but does not ensure the timeliness of the exchange without the use of special synchronization tools. Three-way (triple) exchange allows you to achieve full mutual authentication of systems without additional synchronization. Also, special mechanisms for managing cryptographic keys can be used to

provide authentication. Often, data source authentication is provided by using a data integrity protection mechanism in conjunction with encryption, or a digital signature mechanism. Logical authentication of a user of a computer system is based on a password.

To determine the requirements for PRNG, as well as for the mathematical formalization of the formulation of a scientific problem, we will conduct a study of the criteria and performance indicators of pseudo-random number generators.

The conducted studies have shown that modern PRNG must satisfy the following:

– long period of the generated PRN sequence, $L > 2^{128} - 1$;

– maximum period $L = L_{\max}$, generated PRN sequence $L_{\max} = 2^l - 1$, where l – secret key length, i.e. $l > 128$ bit;

– high structural stealth $S = 1$, which is determined by the ability to resist the definition of an attacker (hacker) PRN sequence elements by known (intercepted) elements (i.e the impossibility of a cryptanalyst solving the problem of determining a pseudo-random sequence from a known fragment (definition - $(i-1)$ -th element γ_{i-1} sequences based on a known fragment of a pseudo-random sequence $\gamma_i \gamma_{i+1} \gamma_{i+2} \cdots \gamma_{i+b-1}$ finite length b, definition $(i+1)$ -th element γ_{i+1} sequences based on a known fragment of a pseudo-random sequence finite length b, determination of key information from a known fragment of a sequence of finite length): $S = \frac{B}{L}$, where B – the minimum number of elements of the PRN sequence required for the unambiguous restoration of the PRN generation rule;

– low probability of opening the PRN generation rule specified by the secret key

$P_{к} = \max\left\{P_{\mathrm{K}_1}, P_{\mathrm{K}_2}, ..., P_{\mathrm{K}_\mathrm{M}}\right\} \le 2^{-l}$, where $P_{\mathrm{K}_\mathrm{i}}$ – the probability of correctly opening the rule for generating a PRN, provided that the attacker uses the i-th cryptanalysis method;

– long safe time $T_{\mathrm{b}} = \min\left\{T_{\mathrm{b}_1}, T_{\mathrm{b}_2}, ..., T_{\mathrm{b}_\mathrm{L}}\right\} \ge \frac{2^l}{\gamma \cdot \psi}$, $T_{\mathrm{b}_\mathrm{i}} = \frac{S_{B_i}}{\gamma \cdot \Psi}$, where S_{Bi} – time complexity of the algorithm that implements the *i*-th cryptanalysis method; γ – const; Ψ – attacker's computing system performance;

– ensuring statistical security (according to the NIST STS method);

– high speed of PRN generation $V_{np.} \approx 10^7 \div 10^9$ bps (in software implementation) and $V_{np.} \approx 10^9 \div 10^{10}$ bps (with hardware implementation).

Ensuring the last requirement is possible with a small number of computational operations performed by the PRN generator to form one bit of the sequence ($V \approx 1 \div 10$ operations per bit).

The statement of the research problem has been formalized and we will formulate it as the problem of increasing the speed of provably stable generators of PRN that satisfy the system of restrictions on individual stability indicators:

$$\min(V): \left\{ \begin{array}{l} L > 2^{128} - 1,\ L = L_{\max} = 2^l - 1,\ S = \frac{B}{L} = 1, \\ P_{к} = \max\left\{P_{\mathrm{K}_1}, P_{\mathrm{K}_2}, ..., P_{\mathrm{K}_\mathrm{M}}\right\} \le 2^{-l}, T = \min\left\{T_1, T_2, ..., T_\mathrm{L}\right\} \ge \frac{2^l}{\gamma \cdot \Psi} \end{array} \right\}$$

In the second chapter, the main provisions of the algebraic theory of redundant coding are considered, and the complexity-theoretic problem of decoding a random code is formulated, which underlies the theoretical justification of the cryptographic strength of the synthesized generators[5].

We work over the finite field *GF(q)* and consider a smooth projective algebraic curve X situated in the projective space P^n over this field. *Let* $g = g(X)$ represent the genus of X. The notation *X(GF(q))* stands for the set of all points of X whose coordinates belong to *GF(q)*, and we write $N = X(GF(q))$ for the total number of such points. Assume C is a divisor class on X with degree α satisfying $\alpha > g - 1$. This divisor produces a mapping $\phi: X \to P^{k-1}$, where k is at least $\alpha - g + 1$. If we take $y_i = \phi(x_i)$, these points define a code. When the image φ(X) meets a hyperplane α in at most $n - d$ points (that is, $n - d \le \alpha$), the obtained code parameters fulfill $k + d \ge n - g + 1$, where n cannot exceed the number of *GF(q)*-rational points on X. In the special case where $2g < \alpha \le n$, one obtains an algebraic–geometric code with parameters $(n, \alpha - g + 1, d)$, $d \ge n - \alpha$.

Let us give the following definition of an algebro-geometric code.

Let X be a smooth projective algebraic curve in the projective space P^n; equivalently, X is the set of points satisfying a homogeneous, irreducible algebraic equation of degree deg with coefficients in *GF(q)*.

Consider the manifold corresponding to the projective hypersurfaces defined in P^n equations $F = 0$, where F – homogeneous monomials of degree *deg*. Let $I(I_0, I_1, \ldots, I_{k-1})$ – information sequence. Algebro-geometric code in GF(q) generated via reflection of the curve X type of $\phi: EC \to P^{k-1}$ – is the linear length code $n \le N$, code words $C=(c_0, c_1, \ldots, c_{n-1})$ which are given by the equation:

---

[5] Rao, T.R.N. Private-key algebraic-coded cryptosystem. / T.R.N.Rao, K.H.Nam // In Advances in Cryptology, – New York: – 1986. CRYPTO 86, – p. 35–48.

$$\sum_{i=0}^{k-1} I_j F_j(P_i) = c_i$$

,

where $P_i(X_i, Y_i, Z_i)$ – projective points of the curve X, that is (X_i, Y_i, Z_i) – solution of a homogeneous irreducible algebraic equation defining a curve X, $i = \overline{1,n}$; $F_j(P_i)$ – values of generator functions at curve points.

This description corresponds to the matrix form of the algebraic–geometric code:

$$G\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1})$$

,

Here G – the generator matrix of size $k \times n$,
where $k = \alpha - g + 1$ and $\alpha = degX \times degF$:

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}$$

.

Let X – smooth projective algebraic curve in P^n, that is, the collection of points that satisfy a homogeneous, irreducible algebraic equation of degree deg with coefficients in GF(q), where F denotes homogeneous monomials.

Algebro-geometric code in GF(q) generated via reflection of the curve X of the type $\phi: EC \to P^{r-1}$ – a code formed from all sequences $(c_0, c_1, ..., c_{n-1})$, having length $n \le N$, that meet the condition $d + g - 1$ equations:

$$\sum_{i=1}^{n-1} c_i F_j(P_i) = 0$$

,

where $c_i \in GF(q)$, $d \ge \alpha - 2g + 2$, $\alpha = deg \times deg$.

The exact values of the upper limit on the number of algebraic curve points over $GF(q)$, $q = 2^m$, $m = \overline{2,10}$ are shown in table 1.

Table 1

An estimate for the upper limit on the number of points of algebraic curves

	$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$	$GF(128)$	$GF(256)$	$GF(512)$	$GF(1024)$
N_{EC}	9	14	25	44	81	151	289	558	108
NH_{ur}	–	21	–	–	105	–	–	197	–
N_{HC}	9	–	65	–	513	–	4 097	–	32769
N_{FC}	–	27	–	–	945	–	–	32 193	–
N_{SC}	17	65	257	1025	4097	16385	65537	262145	1048577

Using the introduced definitions and notation of the theory of redundant coding, methods and computational algorithms for generating PRN are proposed below. They are based on the use of computationally efficient redundant coding algorithms and allow, by reducing the problem of recovering secret key data to solving the complexity-theoretic problem of decoding a random algebro-geometric code, to ensure high cryptographic strength of the synthesized PRNG.

The proposed improved method for forming a PRN without feedback structurally consists of the following stages.

1. Stage. Session key generation.

2. Stage. Pseudo-random formation of *M-ary* sequence with floating weight.

3. Stage. Calculation of the syndrome sequence corresponding to the session key.

4. Stage. Generating a PRN fragment.

The structure of the improved method is formally presented in figure 2. The figure highlights elements that are different from the prototype method.

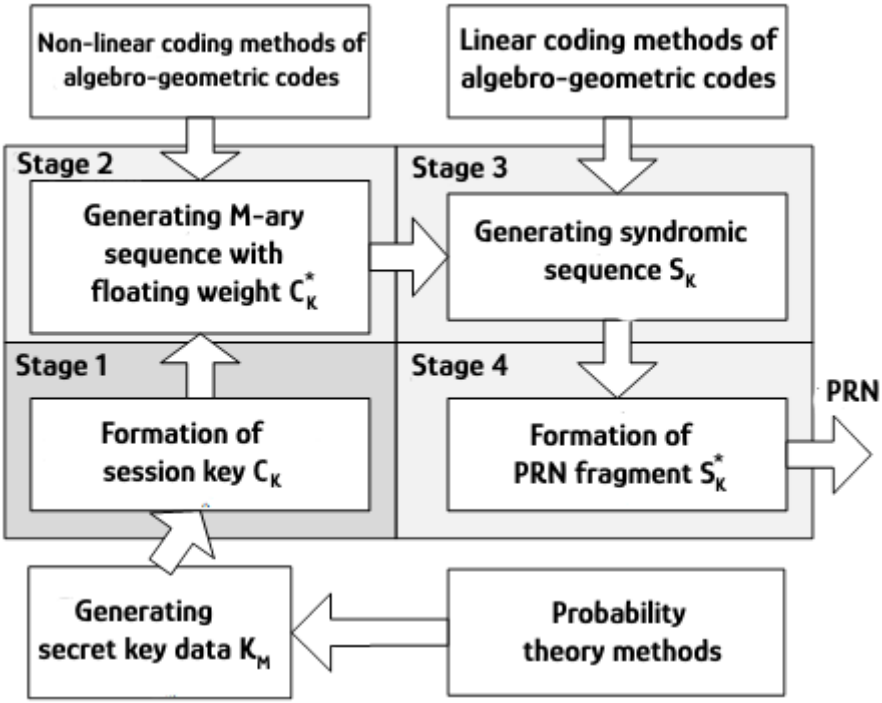

Figure 2. Structural diagram of an improved method for generating PRN without feedback

To form a pseudo-random sequence, an algebro-geometric (*n,k,d*) code is used, over *GF(q)* where:

$$q = 2^m,\ d = 2t+1,\ n = t*log_2(\frac{n}{t})+t*log_2(q)$$

Let's introduce the following notation: $K = \{K_1,\ K_2,\ ...,\ K_M\}$ set of secret keys, where $M = 2^l - 1$, l - key length in bits.

$C_K = \{C_{K_1},\ C_{K_2},\ ...,\ C_{K_M}\}$ – set of session key sequences.

$C_K^* = \{C_{K_1}^*,\ C_{K_2}^*,\ ...,\ C_{K_M}^*\}$ – set of *M-ary* sequences with floating weight, i.e. the set of code words of the code with floating weight at most *w*:

$$C^*_{Ki} \in GF(q) \quad w(C^*_{Ki}) \le w;\ w = t$$

– $S_K = \left\{ S_{K_1},\ S_{K_2},\ ...,\ S_{K_M} \right\}$ – set of syndromic sequences of algebro-geometric *(n, k, d)* code, $r = n - k$: $S_{K_i} = \left\{ S_{K_{i_1}} S_{K_{i_2}} ... S_{K_{i_r}} \right\}$

$$S_{Ki} \in S_K \subseteq GF^r(q)\ \ S_{Ki_j} \in GF(q)$$

In the LFSR scheme in figure 3 values change in all cells of the register involved in the formation of the feedback loop.

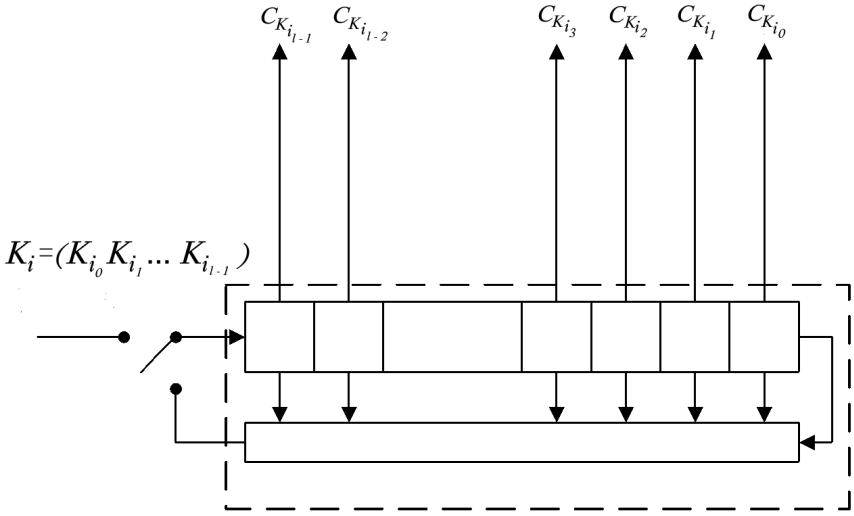

Figure 3. Structural diagram of a device for generating session keys using LFSR

The LFSR scheme in figure 4 is commonly called the Galois configuration.

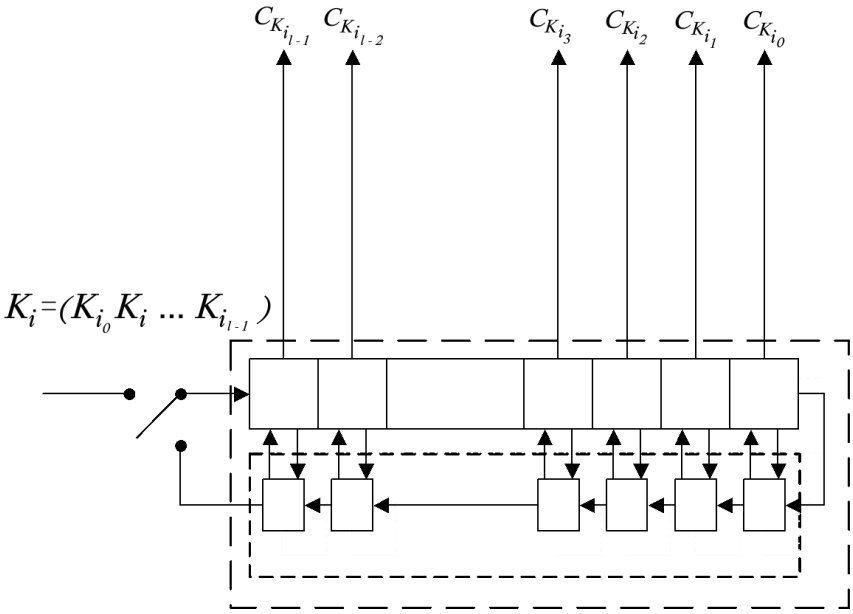

Figure 4. Structural diagram of a device for generating session keys using LFSR

The PRN formed as a result of performing the operations of the method is the result of several functional mappings; in general, let's write as:

$$PRN = \varphi\left(H_X \times \gamma\left(\phi(K)\right)\right)$$

Finding key data K_M according to the known (intercepted) PRN is associated with the search for computationally efficient algorithms for performing the inverse mapping $\varphi^{-1}(PRN)$. This problem is equivalent to the complexity-theoretic problem of decoding a random algebro-geometric code.

The proposed improved method for generating PRN with feedback structurally consists of the following stages.

1. Stage. Session key generation.

2. Stage. Pseudo-random formation of *M-ary* sequence with floating weight.

3. Stage. Calculation of the syndrome sequence corresponding to the session key.

4. Stage. Formation of a PRN fragment and a sequence for feedback.

A distinctive step from option 1 is the introduction to the feedback scheme. The structure of the improved method is formally presented in figure 5.

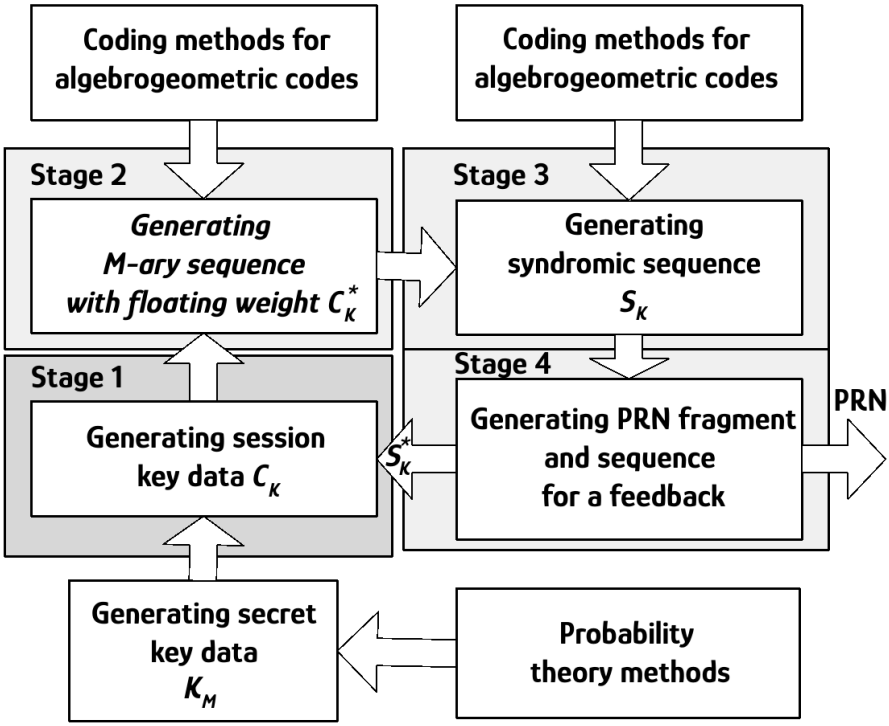

Figure 5. Structural diagram of the improved method for generating PRN with feedback

The PRN formed as a result of performing the operations of the method is the result of several functional mappings; in general, let's write:

$$PRN = \varphi\left(H_X, \gamma\left(\phi\left(\left(K_i\right) \times \left(\phi\left(S_{K_j}\right)\right)\right)\right)\right)$$

Finding key data K_M from a known (intercepted) pseudo-random sequence is associated with the search for computationally efficient algorithms for performing inverse mapping $\varphi^{-1}(PRN)$.

This problem is equivalent to the complexity-theoretic problem of decoding a random algebro-geometric code.

In **the third chapter**, computational algorithms for generating PRN are developed, methods and algorithms for generating a floating weight sequence for generating session keys at the appropriate stages of the proposed methods are studied, and practical proposals are developed for hardware and software implementation of the proposed PRNG.

The process of forming PRN by an improved method without feedback is formalized by a set of the following analytical relations:

- at the first stage according to the entered secret key data $K = \{K_1, K_2, ..., K_M\}$ set of secret keys, where $M = 2^l - 1$, l - key length in bits.

The sequence of the session key is formed $C_K = \{C_{K_1}, C_{K_2}, ..., C_{K_M}\}$ as a display result $\varphi : (K) \rightarrow C_K$

- at the second stage, based on the found sequence of the session key, using the *M-ary* sequence generation algorithm, the session key sequence is converted into an *M-ary* sequence with a floating weight

$$C^*_K = \left\{C^*_{K_1}, C^*_{K_2}, ..., C^*_{K_M}\right\}, C^*_{Ki} \in GF(q), w\left(C^*_{Ki}\right) \le w, w = t,$$

where n – length of *M-ary* sequence, w – number of non-zero elements of the sequence (sequence weight).

– at the third stage according to the formed *M-ary* sequence with floating weight $C^*_K = \left\{ C^*_{K_1},\ C^*_{K_2},\ ...,\ C^*_{K_M} \right\}$ and the checking matrix of the redundant linear block code using the equation

$$S_{K_i} = C^*_K \cdot H^T =$$

$$= (C^*_{K_1}, C^*_{K_2}, ..., C^*_{K_M}) \cdot \begin{pmatrix} h_{0,0} & h_{0,1} & ... & h_{0,n-1} \\ h_{1,0} & h_{1,1} & ... & h_{1,n-1} \\ ... & ... & ... & ... \\ h_{r-1,0} & h_{r-1,1} & ... & h_{r-1,n-1} \end{pmatrix}^T$$

a syndromic sequence of linear block is formed *(n, k, d)* of a code, $r = n - k$:

$$S_{K_i} = \left(S_{Ki_1} \quad S_{Ki_1} \quad ... \quad S_{Ki_r} \right),\ S_{Ki} \in S_K \subseteq GF^r(q),\ S_{Ki_j} \in GF(q).$$

– at the fourth stage, the resulting syndromic sequence is a fragment of the desired PRN:

$$PRN = \varphi\left(H_X \times \gamma(\phi(K)) \right)$$

The operation of generating session key sequences *at the first stage* is implemented using a digital recursive filter with *m* memory cells.

The suggested approach relies on representing the information as a numerical equivalent *A*, followed by further expansion into a linear combination of binomial coefficients[6], each of which is encoded by positional numbering so that a set of coding constraints involving the length of equilibrium sequences *n*, codeword weights *w*, and code power *M* is fulfilled:

---

[6] Евсеев, С. Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования / С.Евсеев, Х.Рзаев, А.Цыганенко // Ukrainian Scientific Journal of Information Security, – Киев: – 2016. Vol. 22. Issue 2, – p. 196–203.

$$\begin{cases} \forall j : w\left(C_j\right) = const = w; \\ 0 \le A < M; \\ 0 \le w \le n; \\ 0 \le C_{j_i} < q. \end{cases}$$

The number A is represented as an equilibrium non-binary sequence $C_A = \left(C_{A_0} \quad C_{A_1} \quad \ldots \quad C_{A_{n-1}}\right)$, moreover

$$A = A_B \times (q-1)^w + A_P$$

where

$$A_B = \sum_{i=0}^{n-1} a_{Bi} b_i, b_i = \binom{n-i-1}{w-l}, A_P = \sum_{l=0}^{w-1} \left(a_l - 1\right) h^l, h = q - 1$$

The process of formation of an equilibrium non-binary sequence can be represented in four stages (figure 6).

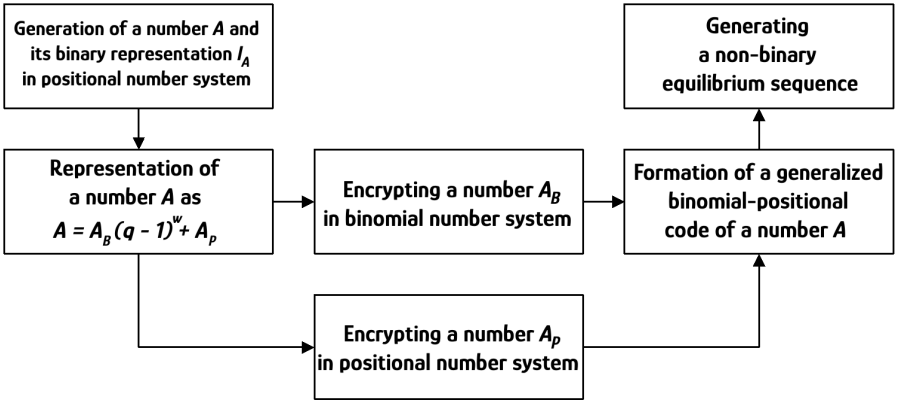

Figure 6. Scheme for generating code words of a non-binary equilibrium code

The paper proposes a scheme for generating sequences with a floating weight, which is based on the use of simple and computationally efficient cryptographic primitives: non-linear catch substitutions (S-box, substitution tables) and multiplexers. At its core, the algorithm for the formation of an equilibrium vector consists in the sequential execution of the following steps:

1. Entering the input sequence $C_K = \left\{ C_{K_1}, C_{K_2}, ..., C_{K_M} \right\}$;
2. Splitting the input sequence $w\left(C^*_{K_i}\right) = w = t$ into sub-blocks of m bits (indicate the error value from the field GF(q), $q = 2^m$) and t subblocks by $log_2(\frac{n}{t})$ bit in each;
3. Non-linear replacement of each sub-block using a substitution table;
4. Multiplexing of received data blocks;
5. Generating the output sequence by concatenating the read values.

The scheme of forming a sequence with a floating weight is shown in figure 7. In figure 8 shows the electrical structural diagram of the floating weight sequencing device.

As a result of performing all the steps of the considered algorithm, a sequence with a floating weight is formed with the number of nonzero elements strictly $w\left(C^*_{K_i}\right) \leq w \leq t$. Values at which t errors equal to 0 are formed simultaneously are removed by software.

The use of the sequence of the maximum period of LFSR as a shaper makes it possible to form sequences of the maximum period, exactly $(2^{21}–1)-2^9=2096639$ sequence elements ($2^{21}–1$- elements form the LFSR, 2^9- zero errors).

Finding key data from a known (intercepted) pseudo-random sequence is associated with the complexity-theoretic problem of decoding a random code.

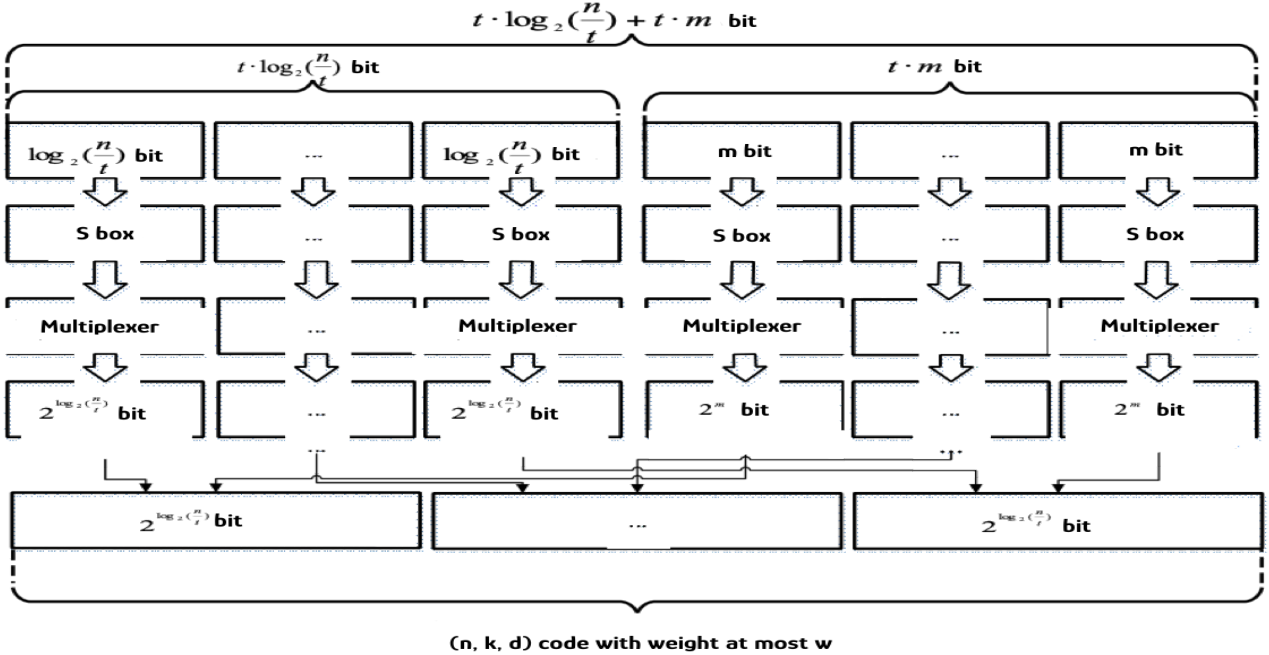

Figure 7. Floating weight sequence generation scheme $w\left(C^*_{K_i}\right) \leq w \leq t$

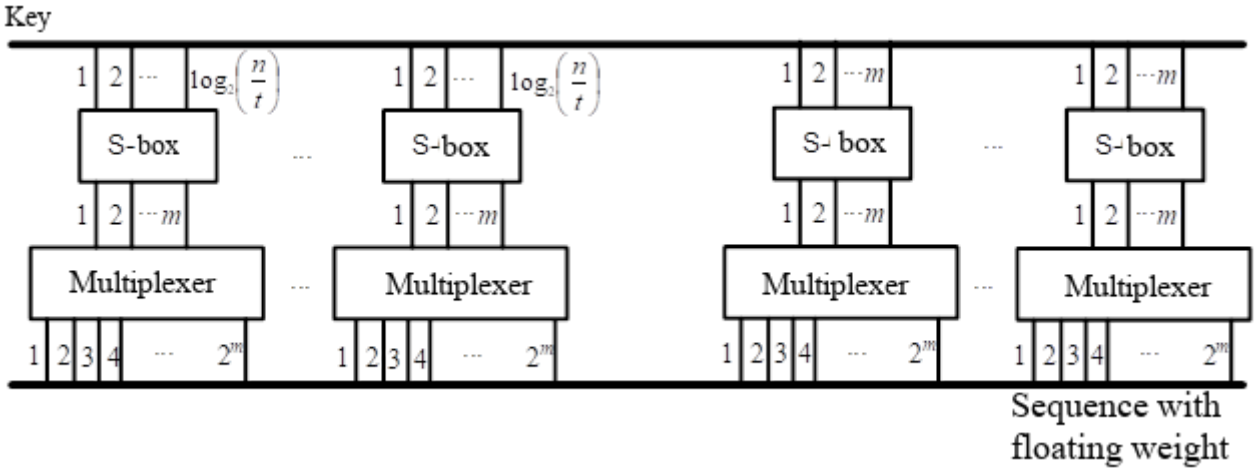

Figure 8. Electrical structural diagram of a floating weight sequence generation device.

Fourth chapter. a study is being made of the resistance of the developed PRNGs to various cryptanalysis attacks, including using non-algebraic coding methods, the statistical security of the generated PRN on M-ary codes is being studied, practical recommendations are developed for the implementation of the results of the dissertation work.

For the developed method of forming PRN with an increased long period, the task of searching for secret key data is reduced to performing an inverse mapping $\xi^{-1}\left(C^{*}_{K_i}\right)$, the secret key in such a generator is two vectors K_i and K^{*}_i, which are the initial states of the corresponding LFSR, i.e. secret keys as a result of back mappings

$$K_i = \phi^{*-1}\left(\gamma^{-1}\left(\psi^{-1}\left(\xi^{-1}\left(\quad *_{K_i}\right)\right)\right)\right), \quad K^{*}_i = \phi^{-1}\left(\xi^{-1}\left(\quad *_{K_i}\right)\right)$$

can only be found by performing an inverse mapping $\xi^{-1}\left(C^{*}_{K_i}\right)$, i.e. solving the decoding problem. Performing inverse mappings ϕ^{*-1}, γ^{-1}, ψ^{-1} makes cryptanalysis more difficult for the attacker, but these transformations are not related to the solution of complexity-theoretic problems. Therefore, in assessing the cryptographic strength of the proposed generators, we will take into account the complexity of implementing inverse mappings ϕ^{*-1}, γ^{-1}, ψ^{-1} and ϕ^{-1}.

Thus, for the proposed methods, the task of finding secret key data by the adversary is equivalent to the task of decoding the applied block code, i.e. performing inverse mappings $\phi^{-1}(PRN)$ (improved method) and $\xi^{-1}(PRN)$ (proposed method with increased period length). In the case when the attacker does not know the fast (algebraic) decoding rule (it may not exist at all if the applied code is

random), then the attacker is forced to use non-algebraic methods for decoding the random code. Forcing the attacker to use a computationally complex non-algebraic decoding algorithm is the main goal of the developer of cryptosystems based on redundant codes.

The simplest and most efficient method for decoding redundant block codes of small length is the correlation method based on comparing the received codeword with errors with all codewords and selecting the nearest codeword (in Hamming metric)[7]. Using *(n, k, d)* block code over *GF(q)* the number of codewords and corresponding comparisons that need to be performed for correlation decoding is given by $N_{k.\partial.} = q^k$, that for small q and k it is easy to implement on modern computer technology. For large values of q and k, the implementation of the correlation decoder is computationally complex and impractical.

The syndromic, or table-based, decoding approach is generally easier to perform than correlation decoding; however, it relies on the assumption that the codeword has a linear structure. In the designed methods for producing pseudo-random numbers, the codes follow a linear design. Consequently, an adversary could exploit syndromic decoding to uncover the secret key. For performing non-algebraic decoding of a linear block code with any given structure, it is adequate to maintain the mapping between all syndromic sequences S_j and their associated error vectors E_j. For decoding by the considered method, the adversary needs to store a table of syndromes and corresponding error vectors, i.e. all needed *2M* table cells, where the parameter *M* is the number of different non-zero error configurations that the linear block code can correct. If block code *(n, k, d)* is used over *GF(q)*, allowing to correct at least

[7] Мамедов, М. Теоретическая оценка криптографической стойкости генераторов на m-ичных кодах // – Баку: Национальная авиационная академия, Научный сборник, – 2023. N 3, – с. 32–43.

$t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors, the number of different configurations of non-zero error vectors is given by the following equation:

$$M = \sum_{i=1}^{\left\lfloor \frac{d-1}{2} \right\rfloor} (q-1)^i \cdot \frac{n!}{i! \cdot (n-i)!}.$$

Thus, the complexity of syndromic decoding is determined by the equation

$$N_{\partial..} = 2 \cdot \sum_{i=1}^{\left\lfloor \frac{d-1}{2} \right\rfloor} (q-1)^i \cdot \frac{n!}{i! \cdot (n-i)!},$$

where $N_{\partial..}$ should be taken as the number of memory cells, required for the implementation of the algorithm, and the number of necessary comparisons performed when searching for the desired vector E_j.

Thus, for small q, n and t syndromic decoding is easy to implement on modern computer technology. For large values q and k implementation of the correlation decoder is computationally complex and impractical. With comparable q and n and small value of t syndromic decoding can be much more efficient than the correlation method. At the same time, for large values q, n and t, the real-world application of the syndromic decoder is computationally complex and impractical.

The permutation decoder allows decoding a linear block code of any configuration through a limited sequence of operations. At its core, it involves a step-by-step modification of the codeword along with a rearrangement of elements that remains unchanged relative to the code. Estimation regarding the computational complexity associated with executing the permutation decoder in the form of an equation:

$$S_{n.\partial.} \geq \left\lceil \frac{n}{n-k} \left\lceil \frac{n-1}{n-k-1} \ldots \left\lceil \frac{n-t-1}{n-k-t-1} \right\rceil \right\rceil \right\rceil, t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

The analysis in this paper demonstrates that when the code length exceeds $n > 100$, both correlation-based and syndrome-based decoding approaches lose computational feasibility, making them unsuitable for practical cryptanalysis. When a permutation decoder is employed — requiring that the adversary possess the generator or the code's parity-check matrix, acting as the public component in the outlined cryptographic framework — the computational complexity of the attack decreases notably. Nonetheless, even with access to the public key and a permutation decoder, once $n > 250$, the effort required for cryptanalysis becomes computationally prohibitive. Figure 9 depicts, on a logarithmic scale, how the complexity of several non-algebraic decoding strategies for redundant block codes changes, considering correlation, syndrome, and permutation decoding.

For high-speed redundant codes, the correlation decoder generally underperforms compared to the syndrome decoder. As the relative code rate decreases, the computational advantage of syndrome decoding also diminishes. When the code rate satisfies $R = k/n < 0.5$, correlation decoding becomes the more favorable option for an adversary seeking to perform cryptanalysis.

Figure 10 provides an overview of the complexity patterns for correlation, syndrome, and permutation decoders in the context of non-algebraic decoding of redundant block codes under the condition $R = k/n < 0.5$.

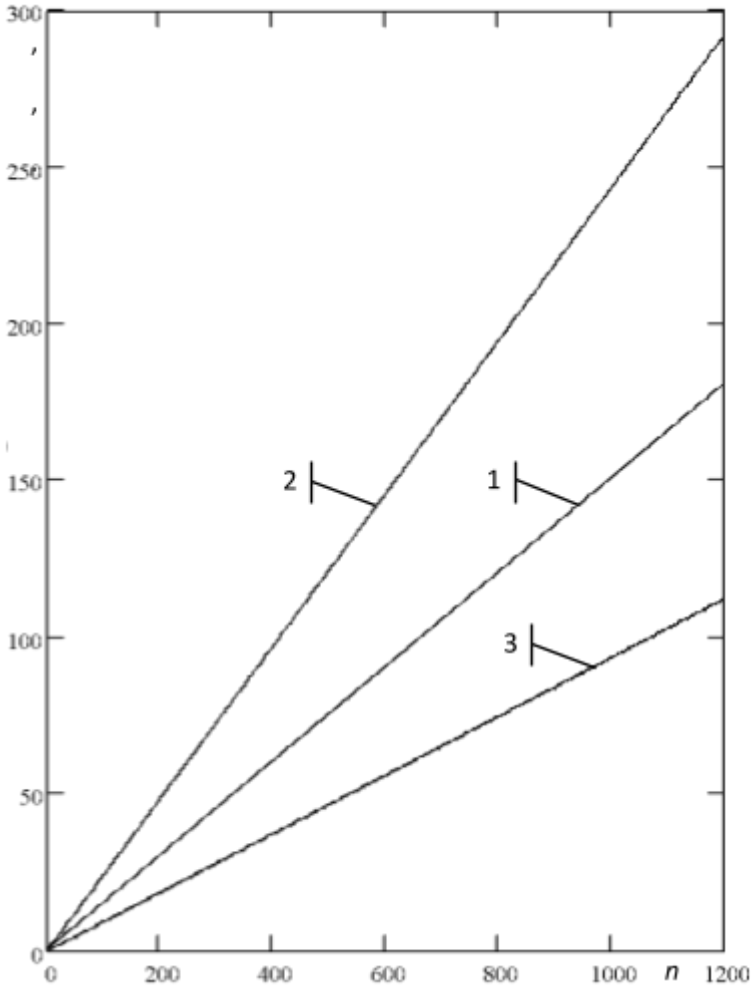

Figure 9. Dependencies: 1) $S_{c.\partial.}(n)$**, 2)** $S_{s.\partial.}(n)$**, 3)** $S_{p.\partial.}(n)$ **for** $q = 2, k = 0.5 \times n$

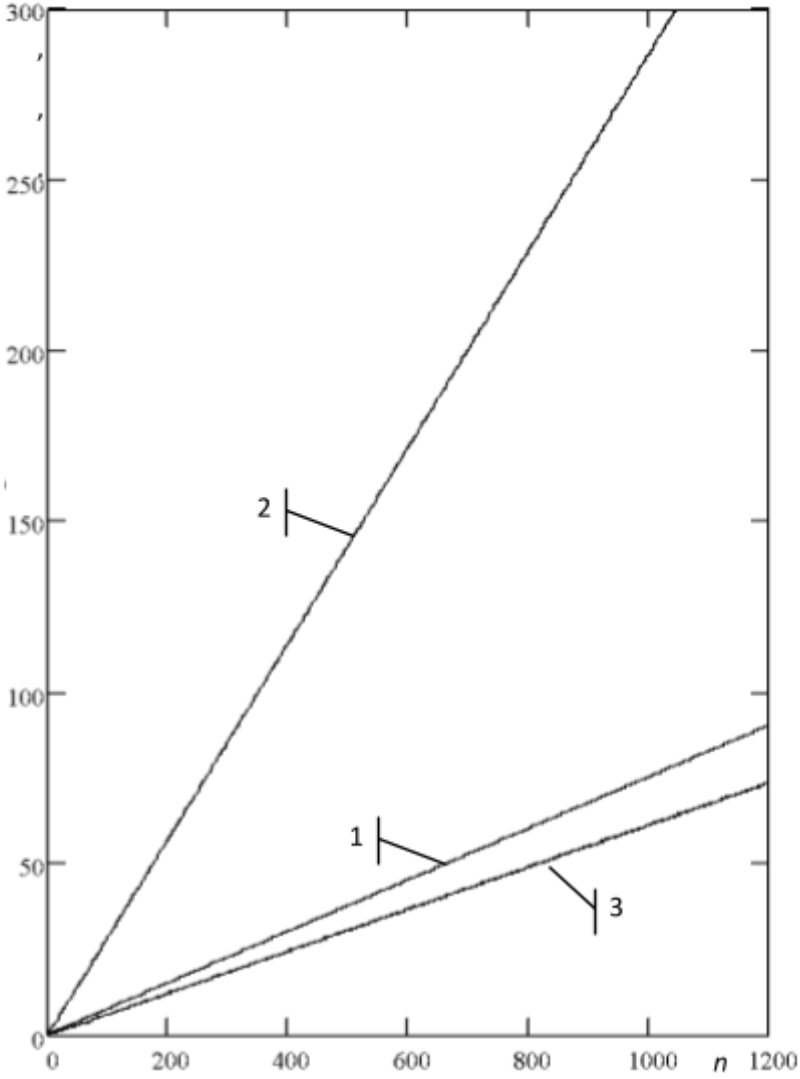

Figure 10. Dependencies: 1) $S_{c.\partial.}(n)$**, 2)** $S_{s.\partial.}(n)$**, 3)** $S_{p.\partial.}(n)$ **for** $q = 2, k = 0.25 \times n$

In figure 11. Dependences $S_{c.\partial.}(R), S_{s.\partial.}(R), S_{p.\partial.}(R)$ and a constant code length of n = 1000 are applied in the study. Syndromic and correlation decoders are equivalent when $R \approx 0,65$ is given.

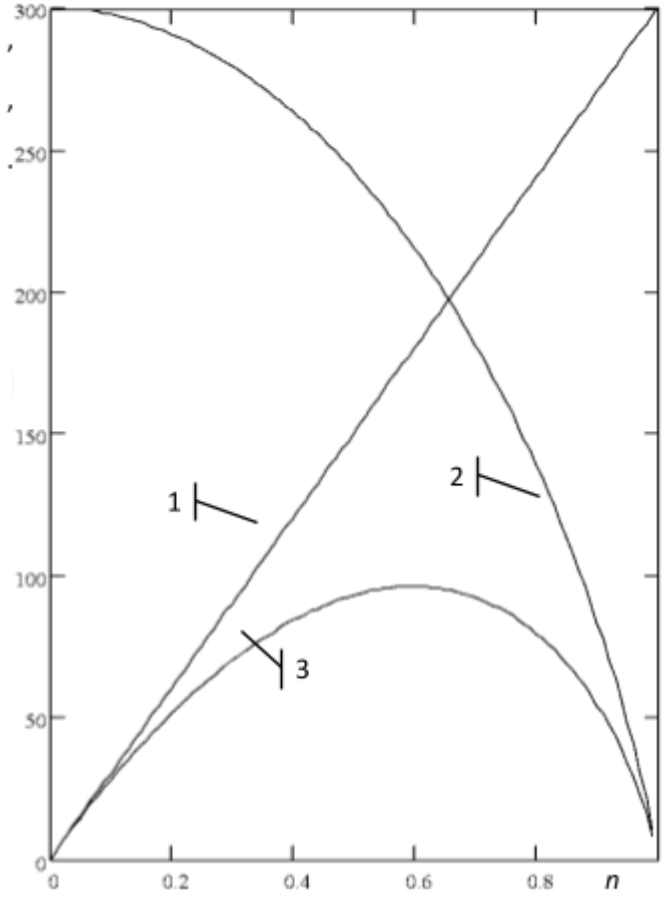

Figure 11. Dependencies: 1) $N_{c.d.}(R)$, 2) $N_{s.d.}(R)$, 3) $N_{p.d.}(R)$ for $q = 2$

Examination of the relationships presented in Figure 11 indicates that employing a permutation decoder while the public key is accessible to an adversary — under the condition $0.1 \leq R = k/n \leq 0.95$ and with the applied code length of $n = 1000$ — renders cryptanalysis computationally unfeasible. In this context, the crypto-code–based security framework provides robust protection for the safe exchange of information within computer systems and network environments.

The development of a software implementation of PRNG using the proposed methods makes it possible to conduct statistical studies of stability, as well as to form libraries for their practical use.

The initial values of the shift register and the feedback values are numbers at most $2^{21}-1$, since the shift register modulo the primitive polynomial is used $g(x)=x^{21}+x^2+1$. The shift register cannot be equal to 0, due to the impossibility of its operation.

Using the developed software implementation of the proposed PRNG generators in the dissertation work, experimental studies of statistical security were carried out using the NIST STS method, and comparative studies were carried out with known generators.

The analysis of the given data shows that the statistical portraits of the proposed generators on redundant block codes are not inferior in their properties to the best known generators.

Thus, there are no statistical tests for the generated PRN that would be passed with a probability lower than 0,96. Most of the tests passed with a very high probability close to 1. The final results of testing according to the NIST STS methodology are summarized in table 2, which shows the number (proportion) of tests in which testing passed with a probability ≥0,99; ≥0,96 and < 0,96[8].

[8] Рзаев Х., Мамедов М., Багиров Е. Оценка безопасности Генератов на М-ичных кодах // Heydər Əliyevin anadan olmasının 100 illiyinə həsr olunmuş tələbə və gənc tədqiqatçıların "Mütərəqqi texnologiyalar və innovasiyalar" mövzusunda VIII Respublika elmi-texniki konfransı, – Bakı: – 2023, – N 8, – s. 7-10.

Table 2

Results of comparative studies of the statistical security of the proposed and some known generators

№	Pseudo-random number generator	The number of tests in which testing passed M sequences (%)		
		M ≥ 99%	M ≥ 96%	M < 96%
1.	G using SHA-1	122(65%)	188 (99,5%)	1 (0,5%)
2.	Linear Congruential	139 (74%)	189 (100%)	–
3.	Micali-Schnorr	130 (69%)	189 (100%)	–
4.	Quadratic Congruential	124 (66%)	181 (96%)	8 (4%)
5.	G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
6.	ANSI X9.17 (3-DES)	121 (64%)	187 (98%)	4 (2%)
7.	BBS	134 (71%)	189 (100%)	–
8.	G using DES	142 (75%)	188 (99,5%)	1 (0,5%)
9.	GPSSD (prototype method)	140 (74%)	189 (100%)	–
10	Improved generator on redundant block codes	140 (74%)	189 (100%)	–
11	Improved generator on redundant block codes with increased period length	142 (75%)	189 (100%)	–

Analysis of the test results summarized in table 2 shows that the proposed generators on redundant block codes have improved indicators of statistical security. They have one of the largest numbers (proportion) of tests that pass the most stringent criteria with a probability ≥0,99 and are not inferior to such well-known generators as the BBS generator and the USA national encryption algorithm in counter mode.

In table 3 are shown the results of an experimental evaluation of the speed of the developed software implementation of PRNG on M-ary codes and comparative studies with software implementations of known generators. The experimental evaluation was carried out with the fixation of the time of formation of the PRN - 1 day, the length of the formed sequence was measured, after which the average time of the formation of the PRN was calculated.

Table 3

The results of comparative studies of the speed of the proposed and some well-known generators

Pseudo-random number generator	Generator performance	
	Absolute value	Relative value
BBS	3,6·102 bit/s	219444
FIPS 197	7,9·107 bit/s	1
Micali-Schnorr	1,1·105 bit/s	718
GPSSD (prototype method)	3,29·107 bit/s	2,4
Improved generator on redundant block codes	2,96·107 bit/s	2,7
Proposed generator based on redundant block codes with increased period length	2,86·107 bit/s	2,8

MAIN RESULTS

In the dissertation work, a theoretical generalization and a new solution to an important scientific and technical problem were obtained, which consists in increasing the speed of provable stable pseudo-random number generators in information and communication systems.

1. The analysis and research carried out that modern telecommunication systems and networks, using the latest achievements in the development of electronic communications and IT technologies, are constantly expanding the range of services provided, including servicing the subjects of automated information interaction, providing access to various multimedia services and technologies, support for remote users, etc. At the same time, the rapid growth in the volume of processed data leads to a tightening of the probabilistic and temporal requirements for the main components of information and communication networks at all stages of information exchange.

2. For the first time, a method for generating a *PRN* based on algorithms of M-ary codes is proposed with the reduction of the problem of calculating a secret key to solving the complexity-theoretic problem of syndromic decoding using a known code word with errors. The proposed method makes it possible to construct provable stable generators for generating sequences with an increased long period.

3. For the first time, estimates of the cryptographic resistance of the proposed methods for forming the PRS on M-ary codes to the negative actions of intruders are obtained, which take into account non-algebraic decoding methods, including permutation and syndromic decoding, which allow to substantiate the design parameters of the developed PRNG for their practical use.

4. The method of forming a *PRN* based on M-ary codes has been improved, which differs from the known one by additionally introduced recurrent transformations over sequences of secret key data and syndromic sequences of a redundant block code, which makes it possible to ensure the formation of sequences of the maximum period with the reduction of the problem of calculating a secret key to solving a theoretical complexity syndromic decoding problem.

5. The mathematical device for the generating *PRN* based on M-ary codes was further developed, which differs from the known ones by using algebro-geometric codes based on the mathematical device of coding theory and parameters of individual curves.

6. Computational algorithms for the formation of PRN based on M-ary codes, and practical recommendations for their use in information systems and technologies have been developed. Proposals have been developed for software and hardware implementation of the developed provable stable PRNG based on algorithms of M-ary codes.

7. The results of the dissertation work are recommended to be used when conducting research and development work to create new information security tools for comprehensive security and reliability of data transmission in computer systems and networks. The results of the research will become a handful for teaching specialists in higher educational institutions and in the study of academic disciplines in information security theory, cryptography, information theory and coding.

Published works based on the materials of the dissertation

1. Mammadov, M. Development of an improved method for forming pseudorandom numbers based on redunte m-ary codes / M.Mammadov, E.Baghirov, R.Korolov [et al.] // Системи обробки інформації, – 2022. № 1 (168), P.11–13.
2. Mammadov, M. Development of a method for ensuring confidentiality and authenticity in wireless channels. / M.Mammadov, Kh.Rzayev, S.Yevseiev [et al.] // Eastern-European Journal of Enterprise Technologies, – Kharkov: – 2022. № 9, – p. 15-27.
3. Мамедов, М., Рзаєв, Х.Н., Корольов, Р.В. Розробка генератора псевдовипадкових чисел гарантованого періоду // Інформатика, управління та штучний інтелект: тези 9-ї міжнар. наук.-техн. конф.,–Харків – Краматорськ: – наук. ред. В.Д. Дмитрієнко ; Нац. техн. ун-т "Харків. політехн. ін-т", – 11-13 травня, – 2022 р., – с. 111.
4. Mammadov, M., Korolov, R., Milevskyi, S. [et al.] Research of Periodic Properties of the Generator Based on m-ary Codes // IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), – Kharkiv, Ukraine: – 2022.
5. Мамедов, М., Багіров, Е., Корольов, Р. Розробка вдосконаленого методу формування псевдовипадкових чисел на основі надлишкових m-ічних кодів // V Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”, – Київ: – 14–15 квітня, – 2022, С. 11–13.
6. Мамедов, М. Теоретическая оценка криптографической стойкости генераторов на m-ичных кодах // – Баку: Национальная авиационная академия, Научный сборник, – 2023. N 3, – с. 32–43.
7. Мамедов, М. Разработка Легковесного Блочного Симметричного Шифра Lea. / М.Мамедов, Х.Н.Рзаев, Е.Багиров // – Баку: Сумгаитский государственный университет Журнал научных новостей Раздел естественных и технических наук, – 2023. N 4, – С. 81-89.

8. Мамедов, М. Результаты Оценки Статистической Безопасности Генераторов На М-Ичных Кодах На Основе Пакета NIST 802STS. / М.Мамедов, Х.Н.Рзаев, Е.Багиров // – Баку: Новости Азербайджанской Инженерной Академии Международный научно-технический журнал, – 2023. N 4, – С. 97-107.
9. Мамедов М., Рзаев Х, Багиров Е. Алгоритм Блочно-Симметричного Шифрования На Основе Расширенных Полей Галуа // Ümummilli lider Heydər Əliyevin anadan olmasının 100 illiyinə və qələbənin üçüncü ildönümünə həsr olunmuş Milli Təhlükəsizlik və Müasir Hərb Sənəti mövzusunda elmi-praktiki konfrans, – Bakı: 2023, – N 9, – s. 479-484.
10. Мамедов М., Рзаев Х., Багиров Е. Оценка безопасности Генератов на М-ичных кодах // Heydər Əliyevin anadan olmasının 100 illiyinə həsr olunmuş tələbə və gənc tədqiqatçıların "Mütərəqqi texnologiyalar və innovasiyalar" mövzusunda VIII Respublika elmi-texniki konfransı, – Bakı: – 2023, – N 8, – s. 7-10.
11. Мамедов, М. Верификация легковесного блочного симметричного шифра LEA / М.Мамедов, Х.Н.Рзаев, Е.Багиров // Новости высших технических учебных заведений Азербайджана, – Баку: – 2024. N 5, – с. 361–375.
12. Rzayev, X.N., – Psevdo-təsadüfi ədədlər ardıcıllığının yaradılması üsulu, İxtira a2023 0039, Azərbaycan Respublikası / Məmmədov, M.F., Bağırov, E.Y. [və b.]: Azərbaycan Respublikası Əqli Mülkiyyət Agentliyi Patent və Əmtəə Nişanlarının Ekspertiza Mərkəzi, – 2024, – № 4.
13. Rzayev, X.N., – Psevdo-təsadüfi ədədlər ardıcıllığının formalaşdırılması üsulu, İxtira a2023 0040, Azərbaycan Respublikası / Məmmədov, M.F., Bağırov, E.Y. [və b.]: Azərbaycan Respublikası Əqli Mülkiyyət Agentliyi Patent və Əmtəə Nişanlarının Ekspertiza Mərkəzi, – 2024, – № 5.

The defense will be held on 23 September 2025 at 16:00 at the meeting of the Dissertation council ED 2.48 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at Azerbaijan State Oil and Industry University.

Address: Baku, Azadlig Avenue 20, Az1010.

Dissertation is accessible at the Azerbaijan State Oil and Industry University Library.

Electronic versions of dissertation and its abstract are available on the official website of Azerbaijan State Oil and Industry University.

Abstract was sent to the required addresses on 22 August 2025

Signed for print: 17.06.2025

Paper format: A5

Volume: 37933

Number of hard copies: 70