О. В. Малсугенов [O. V. Malsugenov][1]
Г. С. Алиев [G. S. Aliev][2]

УДК: 681.327.67

РАЗРАБОТКА МЕТОДА НЕЯВНОГО ХРАНЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ФНФ НА ОСНОВЕ СОЗУ В СМАРТ КАРТАХ

DEVELOPMENT OF THE METHOD OF IMPLICIT STORAGE OF KEY INFORMATION USING SRAM PUF IN SMART CARDS

[1]Управление инфраструктуры и информационных технологий ФГАОУ ВО «Северо-Кавказский федеральный университет» / North-Caucasus Federal University,
e-mail: omalsugenov@ncfu.ru

[2]Институт информационных технологий и телекоммуникаций, ФГАОУ ВО «Северо-Кавказский федеральный университет» / North-Caucasus Federal University,
e-mail: georgyaliev@gmail.com

Аннотация. *В статье приведены результаты исследования и декомпозиция системы смарт-карт, рассмотрена организация подсистем и их взаимосвязи, определены недостатки и угрозы ключевой информации.*

Материалы и методы. *Проведен анализ технологии ФНФ на основе СОЗУ, описана разработанная экспериментальная установка, с помощью которой были получены значения неинициализированной памяти в ячейках, проанализированы и определены закономерности распределения значений, определено количество измерений для определения стабильности значения ячеек памяти. Анализ результатов указывает на необходимость тестирования микросхем СОЗУ при их использовании в качестве ФНФ. Рассмотрена возможность дальнейшего изучения авто-корреляционной функции для исключения коллизии в системах взаимной аутентификации. Дополнительно для всестороннего изучения определенный интерес представляет изучение изменения зависимости количества стабильных и нестабильных ячеек в кристалле СОЗУ в течение жизненного цикла микросхемы, изучение температурных зависимостей значений в ячейках памяти.*

Результаты, обсуждение и вывод. *Разработан метод неявного хранения ключевой информации в смарт картах с использованием ФНФ на основе СОЗУ. Разработан алгоритм взаимной аутентификации с использованием ФНФ на основе СОЗУ для повышения имитостойкости системы. Данная работа заложила основу для определения оптимальной длины вектора инициализации при использовании микросхем СОЗУ в качестве ФНФ в системах со взаимной аутентификацией.*

Ключевые слова: смарт карта, физически неклонируемая функция, статические оперативно запоминающие устройства, микросхема, стабильные и нестабильные ячейки. системный анализ, ключевая информация, алгоритм взаимной аутентификации.

Abstracts. *The article present results of research and decomposition smart cards systems. Subsystems organization and they relationships were reviewed. Weakness and threats of key information were identified. SRAM PUF technology was analyzed. Paper describes experimental setup for getting values of initialization memory, analyzed and detected system properties, determined numbers of measurements to detect stable memory cells. An analysis of the results indicates the need for testing the circuits of the RAM when using them as PUF. The possibility of further study of the auto-correlation function to eliminate collisions in mutual authentication systems is considered. Additionally, for a comprehensive study, it is of certain interest to study the change in the dependence of the number of stable and unstable cells in the RAM chip during the life cycle of the microcircuit, and study the temperature dependences of the values in the memory cells.*

A method has been developed for implicit storage of key information in smart cards using SRAM PUF. An algorithm for mutual authentication using PUF based on the SRAM is developed to increase the system imitability. This work laid the foundation for determining the optimal length of the initialization vector when using the RAM chip as an PUF in systems with mutual authentication.

Key words: system analysis, smart card, physical unclonable function, static random access memory, microcircuit, stable and unstable cells, key information, mutual authentication algorithm.

Introduction. Smart cards were chosen as the object of research, since they are currently widely used in various fields, such as: cellular communications, industry, transport and warehouse logistics, access control systems, medicine, libraries, transport payments, remote control, agriculture, human implants, baggage and cargo management systems in transport companies, real-time object localization systems, car immobilizers, bank cards. They became widespread due to the low cost, simplicity of the technical production process, and the development of the "Internet banking" technology.

Smart cards are plastic cards with a built-in microcircuit. In most cases, smart cards contain a microprocessor and an operating system that controls the device and controls access to objects in its memory. There are smart cards with the ability to perform cryptographic calculations.

According to the principle of data exchange, smart cards are divided into 3 types:

1. Contact
2. Contactless
3. Hybrid

By the presence of a battery, smart cards are divided into active and passive. Active batteries have a built-in battery, and passive ones, respectively, lack it.

According to the method of exchange with a reader, contact smart cards are divided into 2 categories: cards of the ISO / IEC 7816 standard (cellular sim cards, bank cards) and cards with a USB interface (tokens). Such cards do not contain a battery; the energy is supplied to them by the reader. Cards with a USB interface are more convenient for computer authentication, since they do not require additional devices, they are often used to carry out cryptographic calculations.

Contactless smart cards use RFID (radio channel) technology to transfer data between the card and the reader without physically contacting the transponder and the reader. An oscillatory circuit is used to transmit data and supply power to the card, which consists of a capacitor and an inductor. Proximity cards are subdivided according to their operating frequency characteristics into low frequency (LF - 125-134 kHz), high frequency (HF - 13.56 MHz) and ultra-high frequency (UHF - 860-960 MHz). The reader emits an alternating electromagnetic field of a given frequency, which excites an alternating electric current in the inductance coil and in the oscillatory circuit of the card, the current is converted into direct current and charges a sufficiently capacious capacitor that feeds the microcontroller of the card. The exchange of information between the card and the reader is carried out through the same coil by modulating the oscillations of the transponder's electromagnetic field. In the simplest systems, the card transmits only its unique number (identifier). In more complex systems, a two-way exchange of information takes place on the basis of a request-response principle; in such systems, cards have memory and can memorize a certain amount of information, for example, the state of the counter, store an arbitrary number, a unique identifier, and key information.

System decomposition. Based on the methods of systems theory and system analysis, decomposition was performed, evaluation criteria, analysis of smart cards and evaluation of the storage subsystem were determined for its subsequent improvement.

Decomposition is a scientific method that uses the structure of a problem and allows you to replace the solution of one large problem with the solution of a series of smaller problems, albeit interrelated, but simpler. Decomposition, as a process of dismemberment, allows to consider any investigated system as complex, consisting of separate interconnected subsystems, which, in turn, can also be dismembered into parts. Not only material objects, but also processes, phenomena and concepts can act as systems.

The main goal of this study is to improve the efficiency and reliability of information exchange between smart cards and the reader in the process of performing the function of mutual authentication using FNF. Achieving the goal of the research involves solving the following tasks and subtasks:

1. decomposition of the hardware and software part of modern smart cards and authentication systems;
2. analysis of existing methods of mutual authentication;
3. analysis of hardware components that implement a physically non-clonable function;
4. increasing the efficiency and reliability of smart cards functioning as a means of mutual authentication in various systems;
5. synthesis of hardware and software solutions for the implementation of the proposed method.

As a sign of decomposition in this study we used:

1. The functional purpose of the parts,
2. Constructive device.

Modeling of the structure of the object was carried out for visualization, study of properties, identification of significant connections, verification of the compatibility of components, study of the stability of the object in various modes.

Under the behavior of an object in this study, we will take the changes that occur with it over time. In other words, the reaction of the object to the impact, the information response to the impact. Modeling of behavior is necessary for: predicting the behavior of an object under various influences, establishing connections with other objects, developing control functions, designing technical devices, etc.

In this study, the decomposition of the smart card system by functional purpose and structural elements was carried out. Regardless of the type of power source, the system will look like:

1. the control subsystem consists of a microcontroller;
2. the data storage subsystem consists of microcircuits or individual crystals that implement random access memory (RAM) and read-only memory (PROM);
3. The communication subsystem consists of a transmit-receive interface and batteries.

The subsystem connection diagram is shown in Figure 1:

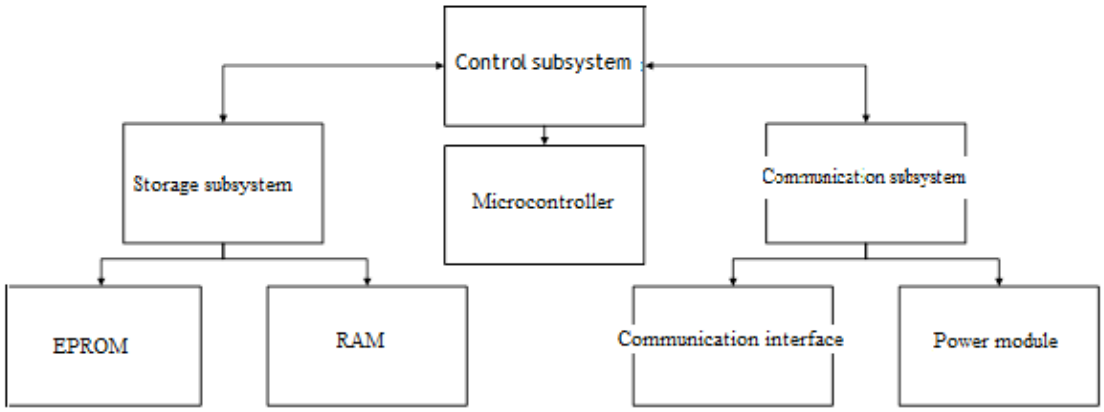

Fig. 1. Decomposition of the smart card system

Figure 1 shows that the control subsystem has feedback from the storage and communication subsystems. Depending on the type of card, the communication interface can be contact or wireless. The overwhelming majority of modern smart cards do not contain autonomous energy sources; for this reason, the power module is part of the communication subsystem. The power supply of the electronic components of the smart card is carried out through data lines with a contact method of transmitting information, or inductively using antennas or communication coils.

Smart card storage subsystem organization. The decomposition diagram shown in Figure 1 shows that the smart card memory consists of RAM and EPROM modules. RAM is the non-volatile and most expensive memory in a smart card. It is used by the processor to store fragments of executable code and intermediate data during operations, since it is the fastest type of memory. The access time to RAM is several tens of nanoseconds. A feature of the RAM is the loss of all data stored in it in case of loss (disconnection) of power supply. This is quite an important feature in the case when the device does not have its own power source.

EPROM is designed for long-term storage without power supply of identifier, key information and program code, which consists of non-volatile Flash cells, erasable programmable read-only memory (EPROM) or electrically erasable programmable read-only memory (EEPROM). The stored data can be any information required for the operation of certain applications, for example: card issuer, card serial number, or other user information. Key information and identifier can be stored explicitly or encrypted. EPROM data can only be written once and is used with prepaid cards such as telephone or disposable transit cards. Electrically Erasable Programmable EEPROM has up to 500,000 rewrite cycles and built-in logic to update the rewrite counter, as well as another limitation on operation - this is speed, it usually takes from 2 to 10 ms to erase and rewrite data into EEPROM memory. Memory card security can be ensured by symmetric cryptographic algorithms with a key length of up to 128 bits, which are used to encrypt data transferred from the card.

Figure 2 shows the relative sizes of a multiply enlarged memory cell of various types.

Fig. 2. Comparative sizes of memory boards of different types with a size of 1 bit per chip

Figure 2 shows that the largest size is in the RAM memory cells, which are used for RAM, and the smallest - in the memory cells used to store the identifier and key information. The analysis should also note the economic component of the production of smart cards with different memory sizes. Thus, a unit of EPROM memory is 4 times more expensive than a unit of ROM and 4 times cheaper than a unit of RAM.

Smart card network subsystem organization. According to the performed decomposition of the smart card system (Fig. 1), the communication subsystem consists of a communication interface and a power supply module. To provide power to the electronic components located in the smart card frame, the reader constantly maintains the required potential on the wired contacts or emits the carrier frequency in the case of using a wireless interface. The inter-

action of the reader and the smart card occurs after the formation of the required electrical potential on the electronic components and the loading of the controller microcode. Interaction protocols implement both one-way and two-way data exchange; both the reader and the smart card can act as initiators of the connection, depending on the used communication protocol.

The structure of the communication interface depends on the type of card, contact cards are of the ISO / IEC 7816 or USB standard, and contactless ones use RFID technology based on the ISO 14443, ISO 15693 standards, etc. In contact cards, the I / O channel of the chip for a smart card is a unidirectional serial interface, so at each moment only 1 bit of information can be transmitted over it and transmitted only in one direction (half duplex). To organize data transfer between the reader and the card in a contact way, two lines of the card interface are used. The I / O line (I / O line) carries data bits. The second line is the clock (CLK line) indicates when to sample in the I / O line to receive a data bit, so each exchange participant monitors whether it is in a transmit or receive state. The USB interface uses two additional lines to form a second I / O channel or full duplex connection, which can increase the speed up to 1.5 Mbps.

In contactless cards, communication with the reader takes place via radio signals. To carry out the procedure of reading information, it is necessary to place the card in the area of action of the electromagnetic field of the reader coil. For different frequency ranges and types of readers, the maximum distance varies from 12 to 50 cm. The contactless method of information transmission is often used in those areas where it is necessary to perform the operation of information transfer quickly, for example, in public transport, in access control and management systems.

The wireless data transfer protocol between the reader and the smart card generally contains the following operations:

1. The reader is waiting for the connection or appearance of the card in the access zone when using the contactless system

2. The card, connecting or appearing in the zone of a sufficient level of the reader's radio signal, receives power supply by contact or induction.

3. The reader receives the card's identifier and can optionally send a request to read the memory storing information for verification (key information, initialization vector).

4. The card generates a data packet containing key information and card identifier, and transmits to the reader

5. The reader compares the received data with the reference one, if the card identifier matches the password, identification is successful. If the key information does not match, the access control subsystem reader denies service.

The research carried out on the principles of construction and algorithms for the operation of smart cards made it possible to classify it as a complex system. Like any complex system, a smart card has a number of disadvantages, such as:

1. Key information is stored explicitly,

2. Access to key information can be obtained by any reader,

3. Low imitation resistance of the system,

4. In contactless cards, communication takes place via an open communication channel.

Implementation of these vulnerabilities will allow an attacker to:

1. Having obtained physical access to the smart card, extract key information and use it for subsequent verification and access,

2. After intercepting the key information of the wireless card for the reader, reuse it,

3. After gaining access to the smart card, change the secret information so that a trusted user will not gain access to the system.

These vulnerabilities can lead to threats of loss, theft or modification of key information and personal data, disruption of the correct and efficient operation of the system. Studies have shown that the information storage subsystem has the largest number of vulnerabilities. This is due to the peculiarities of operation and the hardware architecture of the cards. To increase the imitation resistance of the system, it is proposed to use the technology of physically non-cloning functions as a method of implicit storage of key information and an algorithm for mutual authentication of the reader and smart card.

Development of a method for implicit storage of key information using PUF based on SRAM

A physically unclonable function (PUF) is a function applied using a physical system that has the following properties:

1. on a request to a function (impact on a physical system), it is easy to get an answer - the result of a function's work (a reaction of a physical system);

2. the given function is practically difficult to reproduce, it is computationally difficult to mathematically simulate or copy in some other way (non-cloning property);

3. for a unique request, the function must return a unique response.

A mathematically physically non-clonable function can be described by the values of pairs of input and output values, which are respectively the values of the CH (Challenge) request signals and the values of the R (Response) output signals [1]. Thus, any FNF can be represented by a set of possible request-response values and can be described by the following function:

$$R_i = PUF(CH_i) \quad (1)$$

In other words, it is a function embodied in a physical structure that is easy to assess but difficult to characterize, simulate, or reproduce. The physical structure containing the PUF consists of many random components that are formed during the manufacturing process of the PUF carrier and are uncontrollable. The output crypto-material is exactly the "request-response" pair. The mathematical analogue of a physically non-clonable function is a hash function. In this case, the physical system itself acts as the key of the hash function. Physically non-cloning functions are unidirectional - it is almost impossible to recover the request from the response. PUF has two important properties:

1. the practical impossibility of creating a physical copy of the PUF;
2. the impossibility of creating an accurate mathematical model of the PUF,

The response cannot be computed if the exact request parameters and other request-response pairs are known. These properties together and define the concept of "non-cloning".

The variability of the PUF implementation on a chip of integrated circuits allows us to determine the main directions of PUF application [2]: digital watermarks and fingerprints [3], generation of random number sequences [4], identification and authentication [5], implementation of hardware hash functions [6], detection of hardware bugs [7], generation of encryption keys [8], radio frequency identifiers [9], etc.

Since the smart card contains a RAM microcircuit, it is of the greatest interest to study the possibility of using SRAM-based PUF as a method of implicit storage of key information to improve imitation resistance.

Static random access memory (SRAM) is a semiconductor random access memory in which each binary or ternary bit is stored in a positive feedback circuit that maintains state without the regeneration required in heap memory. This type of memory has features that will allow you to use it as FNF:

1. Stores data only while there is power,
2. Has unpredictable (random) memory contents after power-on.

The memory cell of the RAM consists of four transistors that implement two inverters with cross-feedback, which are always in one of two states, which allows it to be used to store one bit of information. When the supply voltage is applied, all SRAM cells are set to one of two possible states; moreover, due to the circuitry symmetry of the RS-flip-flop, it is not known beforehand which final state the cell will take - "0" or "1". This state is random and is determined by many factors, such as: features of the technology of manufacturing microcircuits and many asymmetric elements in each cell of the RAM (length of connecting conductors, their geometric dimensions, inhomogeneity of the physical and chemical properties of silicon, deviation of signal delays, etc.). These features allow obtaining a unique PUF each time power is applied to the memory card.

In [10], during memory initialization, two types of values in memory cells were identified: stable and unstable. In stable cells, the same values appeared every time during initialization. they can be used as a method for storing key information of smart cards, physical key based authentication. In unstable cells, random values appeared every time. They can be used as a built-in hash function for a mutual authentication algorithm, a random sequence generator for encryption, or as additional blocks of pseudo-random data when transmitting useful information.

Identifying static properties of the values in SRAM cells. To conduct research on uninitialized memory, an experimental setup was assembled, shown in Figure 3, which is based on a universal Arduino Mega board based on an Atmel 2560 processor, static RAM chips, a quick-detachable panel for memory chips, and a transistor switch for controlling the device's power supply. The microcontroller in this setup is used to read uninitialized memory, control interruption and power supply between readings, primary processing and transfer of data to a personal computer. Ten HM62256 static random access memory chips from different manufacturers (Hynix, Toshiba, Hundai) were used as the samples under study. The main goal of this stage is to determine the statistical properties of values in the cells of static RAM microcircuits when they are used as physically non-clonable functions. The main tasks of this stage are: determining the number of stable and unstable memory cells, the number of stable and unstable bits, identifying periodic patterns in the formation of initialization values of static RAM microcircuits.

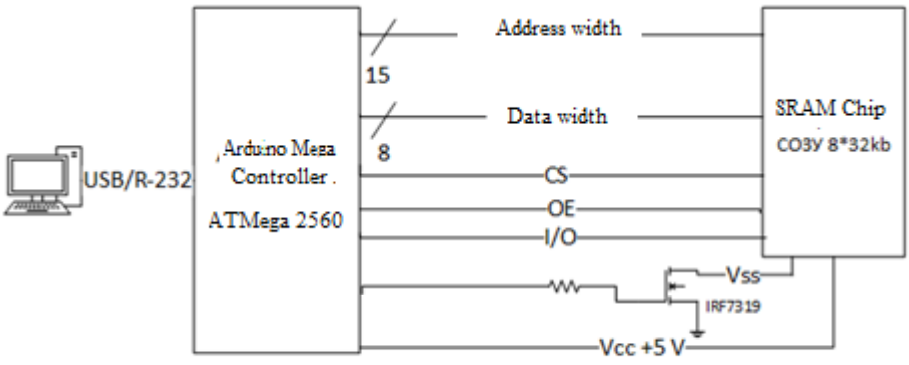

Fig. 3. Scheme of the experimental setup

To solve the set tasks, it is necessary to use data from the technical documentation of RAM memory cards to determine the delays between readings of cell values. The timeline for the selected memory cards is shown in Figure 4.

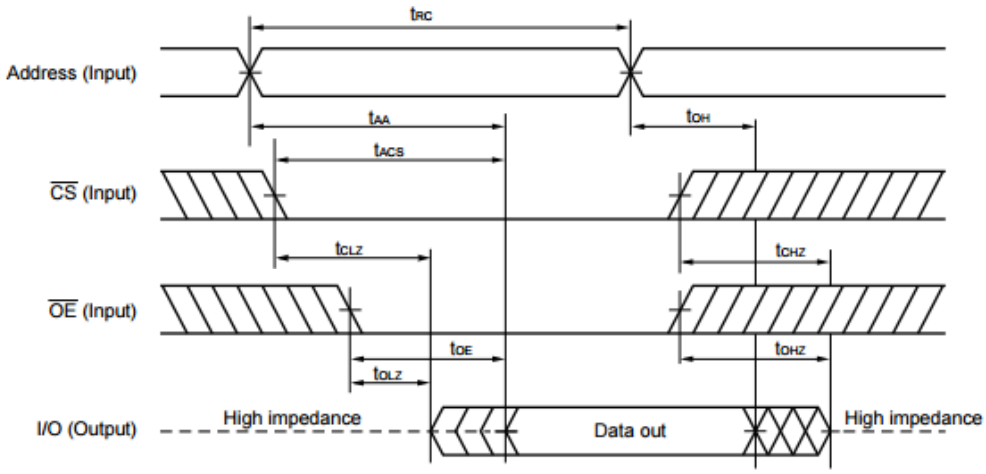

Fig. 4. Timeline of access to the static RAM cell

The timeline determines the sequence of signals for each stage of interaction with the RAM microcircuit and the delay times of the control signals for the memory microcircuit.

The algorithm for reading data reading in general is shown in Figure 5. It uses the following variables: i is the counter of the experiment number, N is the specified number of measurements for the experiment, Adr is the address of the memory cell for reading, S is the memory length, V Is the value of the initialized memory cell, t is the delay for changing the address, T is the delay with turning off the power for a repeat experiment.

At the initial stage, to solve the problem in order to improve the accuracy of the study, 100 measurements were used for each investigated sample of RAM.

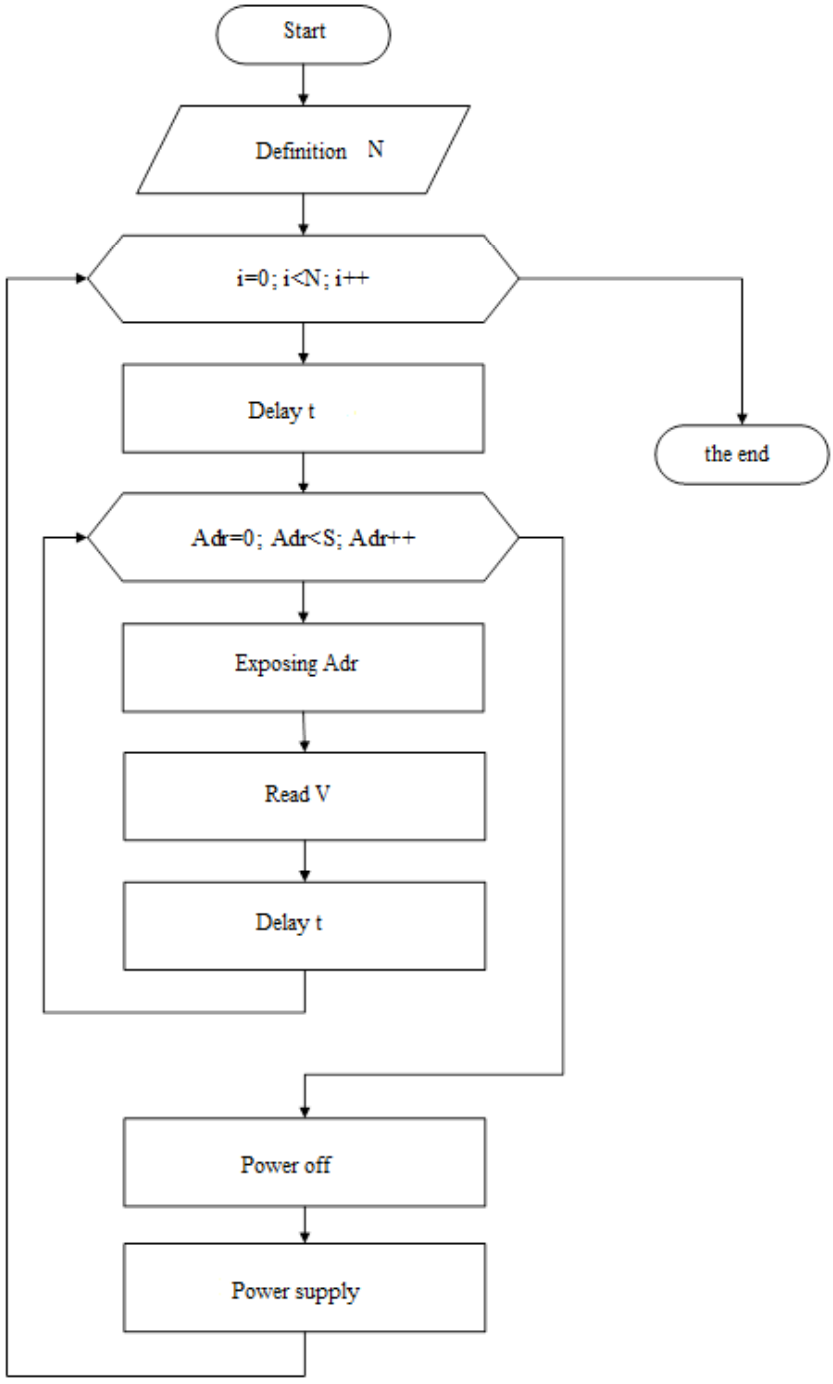

Fig. 5. Algorithm for reading the values of the initialized memory

To determine stable and unstable cells and their addresses, the results obtained in the algorithm (Fig. 5), it is necessary to compare the values of the corresponding cells in all measurements.

Additionally, the data analysis showed that for all the samples under study the condition

$$N_{стаб} * 8 < n_{стаб} \quad (2)$$

where $N_{стаб}$ – number of stable bytes, $n_{стаб}$ – number of stable bits.

This confirms the original assumption that in unstable bytes, some of the bits remain stable. This fact limits the range of random values generated in memory cells during initialization. Thus, the studies carried out make it clear that when used as an identifier or an initialization vector, a sequence of 8 bytes (64 bits) length, subject to a uniform distribution of the probability of occurrence of values "0" and "1" in each position of each byte, gives under the condition of "brute force "264 = 18446744073709551616 values, while if each byte changes not 8, but 4 bits, and the rest remain

stable, then under the condition of" brute force "the number of unique combinations is reduced to 232 = 4294967296 values.

Thus, an optimization problem arises on the one hand, to reduce the predictability of the initialization vector, and on the other hand, to increase the reliability of detecting the displacement of the initialization vector in the memory "snapshot" with the general task of reducing the length of the transmitted data sequence.

Figures 6-8 show the distribution maps of values for memory cards.

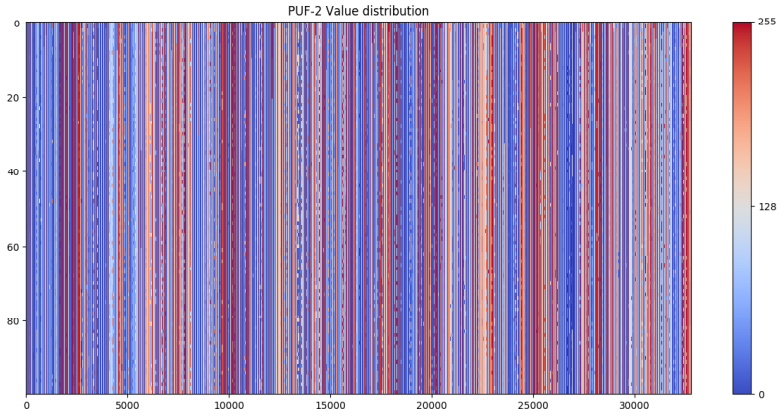

Fig. 6. Map of the distribution of values in the memory cells of the sample SRAM No. 2 for 100 measurements

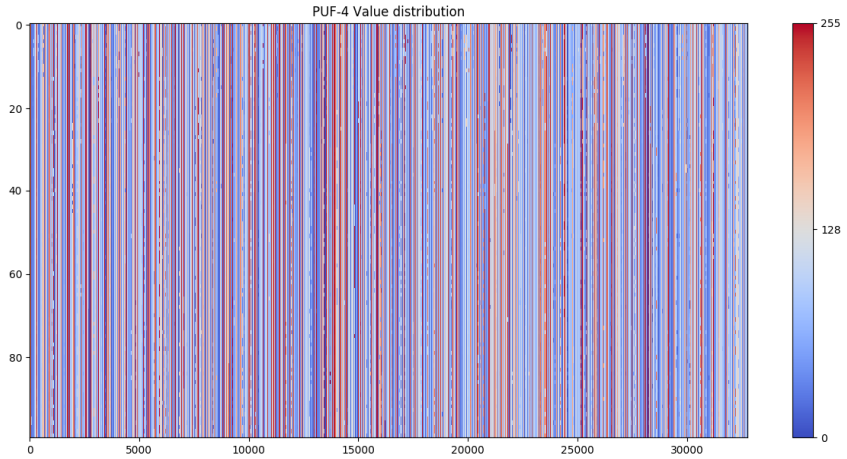

Fig. 7. Map of the distribution of values in the memory cells of the sample SRAM No. 4 for 100 measurements

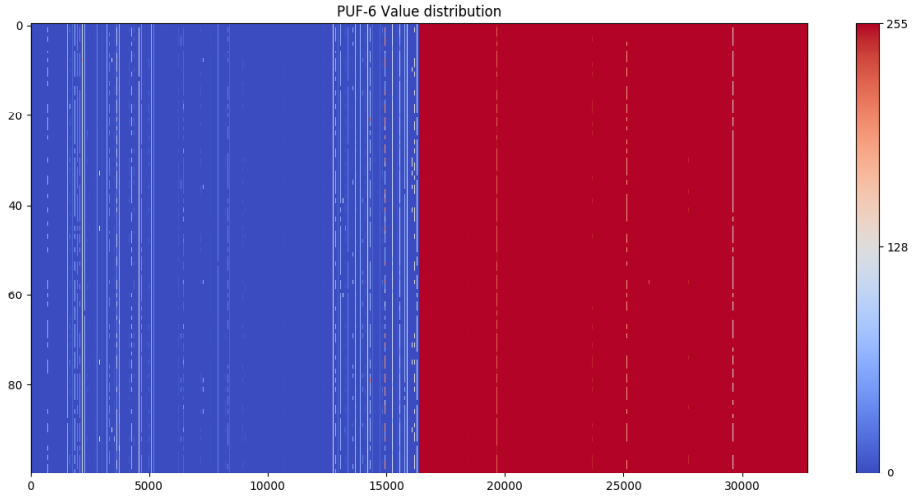

Fig. 8. Map of distribution of values in memory cells of sample SRAM No. 6 for 100 measurements

The results of the studies carried out for the most characteristic samples No. 2, No. 4 and No. 6 for 100 measurements are presented in Figures 6-8. The addresses of the cells are plotted along the horizontal axis, along the vertical

axis of the measurement numbers. The color on each card shows the value in the memory cell in the range from 0 to 255.

The measurements performed and the initial analysis of the data show that a significant number of cells are unstable, while in sample No. 2 there are periodically repeating regions with a predominance of zero and one values in all bit positions (numbers 0 and 255). Sample No. 6 (and in the general case, samples 6 to 10) have two pronounced areas of prevalence of values "0" and "1", which means that there are 2 "banks" of memory in the board. Solid vertical lines on maps indicate stable values, color indicates the value in a given cell. Broken vertical lines represent unstable cells. The alternation of solid and dashed lines, as well as different colors of solid lines is an important characteristic of an ideal physically non-cloning function proposed for use in a smart card for storing key information in an implicit form.

Studies have shown that FNFs in the cells of the RAM have a chaotic distribution, using stable values, you can modify the smart card storage subsystem in such a way that it will not permanently store key information, and the initialization vector will appear in memory only at the moment of authentication, and its random distribution only a trusted system will know, in which a snapshot of values in stable cells and their addresses will be stored, so the purpose of the study in increasing imitation resistance and imposing an intercepted signal (key information) is implemented by modifying the storage subsystem. To increase the speed of the initial calculation of the FNF in the cells of the RAM and register the impression in the system, it is necessary to reduce the initial number of measurements, so, using the theorem of the product of probabilities for independent events carried out under normal conditions, we obtain formula 3:

$$P_{ош} = 2^{-N} \tag{3}$$

where $P_{ош}$ – the probability of an error, N – is the number of studies performed.

Thus, increasing the number of experiments reduces the likelihood of errors, but complicates the process of initial registration of the card. Using 25 measurements, we will reduce the initial registration time by 4 times compared to 100 measurements, and we get expression 3:

$$P_{ош} = 2^{-25} = 0.00000003 \tag{4}$$

Thus, the analysis of 25 measurements will reduce the error probability to 1 error in 33 million.

To increase the accuracy of the study and to compensate for possible errors, it is of interest to analyze the possibility of using an auto-correlation function, which will allow a signal that has an error to be accepted as reliable with a certain probability of less than one.

The studies carried out make it possible to increase imitation resistance and reduce the likelihood of selection by enumerating key information.

Thus, the analysis and decomposition of the system, the study of the properties of PUF based on SRAM, makes it possible to develop a model of a smart card, replacing the traditional storage scheme for key information on PUF based on stable values in the cells of the SRAM, imitation resistance of the system. To improve the communication subsystem, it is necessary to develop a mutual authentication algorithm. To exclude the possibility of using the intercepted message.

Algorithm of mutual authentication using SRAM PUF as method of implicit storage of key information

The main disadvantage of the communication subsystem is the use of an open communication channel for the transmission of password-key information. So, by gaining access to a contact card or by intercepting a contactless radio signal, you can get unauthorized access to key information. The analysis of the existing vulnerabilities of smart cards and existing solutions excludes the possibility of protecting the communication channel, therefore we have proposed a new approach and the use of a mutual authentication system.

For the initial registration of the card, a modified algorithm will be used (Fig. 5), in which there will be 25 consecutive reads of uninitialized memory and further comparison of the values of each cell of all measurements, after which an array of stable values and their addresses is formed, which will be further used as a key ...

To increase the imitation resistance, namely the imposition of the intercepted signal, we propose to use the mutual authentication algorithm, which is shown in Figure 9:

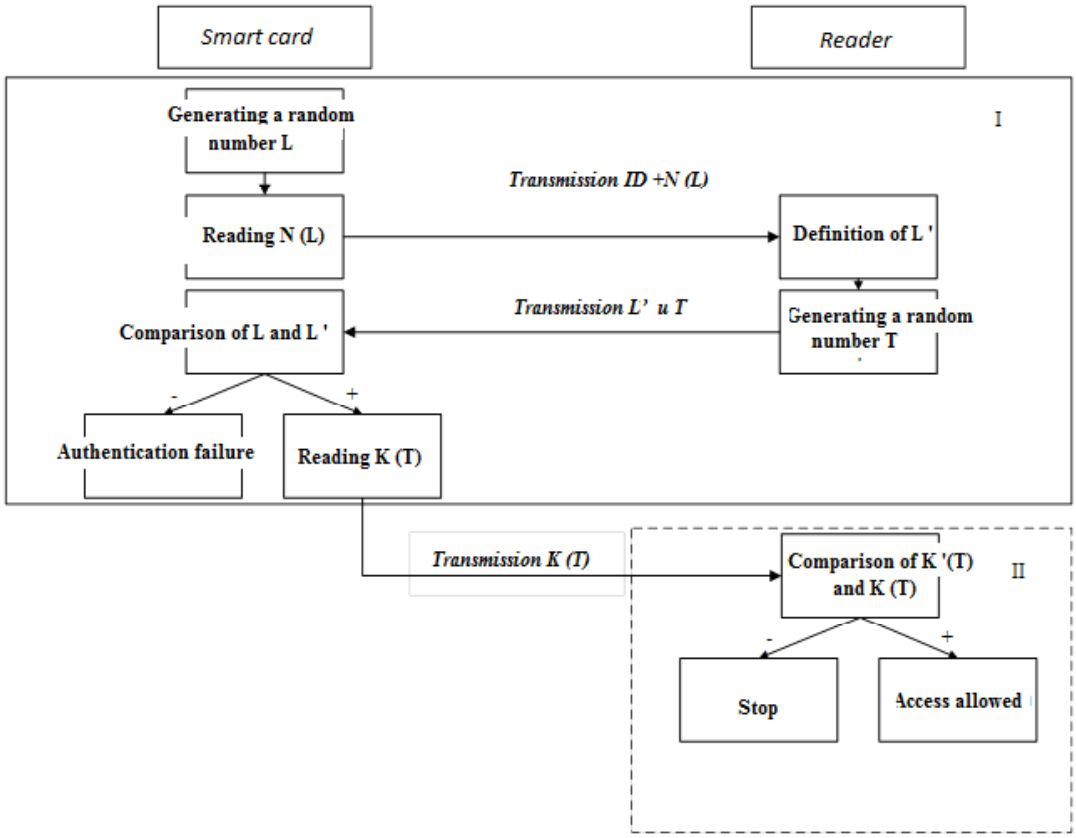

Fig. 9. Mutual authentication algorithm

The algorithm consists of two main stages. The task of the first stage is to check the reliability of the reader. The smart card microcontroller generates a random number L, reads N bytes from the uninitialized RAM starting at offset L, and then sends N (L) and a unique card ID (CardID). The reader calculates an offset L' based on a pre-existing snapshot of a specific RAM. If the offset is calculated correctly, then the map goes to stage 2. The task of the second stage is to check if the card is trying to gain access, so the reader calculates a random offset T and sends it to the card, the smart card receives T and reads successive K bytes with offset T, after which the card sends K (T) if K '(T) match the system snapshot, the card and reader are mutually authenticated. So each time using random values K and N, you can endlessly use the same RAM board, an attacker cannot get a full snapshot of the system by intercepting a secret message and even receiving it - it will be a random set of bytes with a random offset. Thus, with each authentication procedure, the initialization vector N (L) and the key K (T) are changed.

For the impossibility of creating a snapshot of the system in further studies, it is necessary to consider the possibility of using encryption to protect the stages of information exchange, for which unstable PUF values can be used as an analogue of the hash function.

Conclusions. The analysis of the results of our research shows an increase in the imitation resistance of smart cards by using PUF based on SRAM as a method for storing key information in an implicit form. Using a mutual authentication algorithm eliminates the possibility of imposing an intercepted signal. For a comprehensive study, it is of interest to use the autocorrelation function to eliminate errors and interference in the signal, and to use the encryption of some stages in the authentication algorithm using unstable PUF values as an analog of the hash function.

ЛИТЕРАТУРА / REFERENCES

1. Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kevenaar. – Springer, 2007. – 344 P.

2. Заливако, С. С. Физически неклонируемые функции / Заливако С. С., Иванюк А. А. // Информационные технологии и системы 2019 (ИТС 2019) = Information Technologies and Systems 2019 (ITS 2019) : материалы международной научной конференции, Минск, 30 октября 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2019. – С. 8 – 21.

3. Zheng, J. X. A digital PUF-based IP protection architecture for network embedded systems / J. X. Zheng M. Potkonjak // Proc. ACM/IEEE Symp on Archit. for Netw and Comm. Syst. (ANCS'14). – Marina Del Rey, USA, 2014. – P. 255–256.

4. Efficient Implementation of True Random Number Generator Based on SRAM PUFs / V. Leest [et al.] // Cryptography and Security: From Theory to Applications / ed. by D. Naccache. – Springer, 2012. – P. 300–318.

5. Zalivaka, S.S. Arbiter PUF based FPGA chip identification and authentication methods with enhanced reliability and modeling attack resistance: PhD Thesis. – Singapore: NTU, 2018. – 162 P.

6. Bolotnyy, L. Physically unclonable function-based security and privacy in RFID systems / L. Bolotnyy, G. Robins // Proc. IEEE Int. Conf. on Perv. Comp. and Comm. (PerCom'07). – White Plains, USA, 2007. – P. 211–218.

7. Zhang, X. On-chip structures and techniques to improve the security, trustworthiness and reliability of integrated circuits / X. Zhang [Electronic resource]. _ Mode of access: http://digitalcommons.uconn.edu/cgi/viewcontent.cgi?article=6219&context =dissertations. – PhD Thesis, 2013. – Date of access: 14.10.2019.

8. Maes, R. PUFKY: A Fully Functional PUFBased Cryptographic Key Generator / R. Maes, A. V. Herrewege, I. Verbauwhede // Proc. Crypt. Hardw. and Emb. Syst. (CHES'12). – White Leuven, Belgium, 2012. – P. 302–319.

9. Verayo. Security and authentication solutions based on silicon physical unclonable functions (PUF) technology [Electronic resource]. – Mode of access: http://www.verayo.com/. – 2013, Verayo, Inc. – Date of access: 14.10.2019.

10. George Aliev, Oleg Malsugenov and Oksana Mezentseva Examination of Distribution Regularities in Static RAM Microcircuit Cells in Case of Using Them as a Physically Unclonable Function in a Mutual Authentication Module [Electronic resource]. – Mode of access: http://ceur-ws.org/Vol-2500/– 2019.

ОБ АВТОРАХ | ABOUT AUTHORS

Малсугенов Олег Владимирович, кандидат физико-математических наук, доцент, начальник управления инфраструктуры информационных технологий ФГАОУ ВО СКФУ,
e-mail: omalsugenov@ncfu.ru, тел.: +79624509250
Malsugenov Oleg Vladimirovich, Candidate of Physics and Mathematics Sciences, Associated Professor, Chief of the IT and infrastructure department, NCFU, e-mail: omalsugenov@ncfu.ru, tel.: +79624509250

Алиев Георгий Самедович, студент 4 курса аспирантуры ФГАОУ ВО СКФУ,
e-mail: georgyaliev@gmail.com, тел. +79054654826
Aliev Georgy Samedovich, Phd student of 4th course, NCFU,
e-mail: georgyaliev@gmail.com, tel.:+79054654826

Дата поступления в редакцию: 07.02.2020
После рецензирования: 08.05.2020
Дата принятия к публикации: 11.06.2020