cogent engineering

COMPUTER SCIENCE | RESEARCH ARTICLE

# Development of an automated system model of information protection in the cross-border exchange

Begimbayeva Yenlik[1]*, Ussatova Olga[2], Biyashev Rustem[1] and Nyssanbayeva Saule[1]

Received: 28 October 2019
Accepted: 18 January 2020

*Corresponding author: Begimbayeva Yenlik, The Institute of Information and Computational Technologies of MES RK, 125 Pushkin Street, Almaty, 050010, Republic of Kazakhstan
Email enlik_89@mail.ru

Reviewing editor:
Duc Pham, School of Mechanical Engineering, University of Birmingham, Birmingham, UK

Additional information is available at the end of the article

**Abstract:** A model of an automated system for secure cross-border information exchange is considered. This automated system presents as a complex of the following modules which ensure the information security: data encryption, an electronic digital signature (EDS), access control to the stored information based on two-factor authentication, resolution of possible conflict situations. In this paper, models of two modules for an automated system are described: the electronic digital signature and access control to information based on two-factor authentication. The mathematical model of the formation and verification of the digital signature is described in detail. The phased software implementation of this model with the analysis of the results is described. The two-factor authentication algorithm based on the authenticator program and a mobile phone is considered. A secret string generator based on the method of exhaustive search was carried out. A generator of trigonometric functions is described, which is used to calculate

## ABOUT THE AUTHORS

The goals and objectives of the research are development and analysis of methods, algorithms and means of cryptographic protection of information based on modular arithmetic during its transmission and storage in info communication systems and networks.
Begimbayeva Yenlik - Scientific Researcher in the Information Security Laboratory of the Institute of Information and Computational Technologies (ISL of IICT). PhD in information security systems from Al-Farabi Kazakh National University (KazNU) and IICT.

Ussatova Olga - PhD student from KazNU, IICT in specialty: «Information Security Systems». Research interests theme - database protection using 2FA.

Biyashev Rustem - Head of ISL of IICT. He has over 170 papers published, including 2 monographs, 6 copyright certificates of the USSR, over 10 certificates for Intellectual Property of the Kazakhstan.

Nyssanbayeva Saule - Chief Researcher in the ISL of IICT. She has over 130 papers published, including, over 10 certificates for Intellectual Property of theKazakhstan.

## PUBLIC INTEREST STATEMENT

A secure automated exchange has become an important part of interaction states. Because of the complicated condition of the information exchange between states, different technologies are applied for the security of the transmitted information and its access control leads to problems of recognition of state standards of information protection in different countries. The most popular method of ensuring information protection is thecryptographic method. In this study to ensure the information security of this automated system, the module of electronic digital signature, in which an algorithm based on nonpositional polynomial notations and module of access control to information based on two-factor authentication are proposed.

a one-time password. The phased software implementation of this model is given. The analyzed results of the algorithm are presented.

**Subjects: Applied Mathematics; Cryptography; Mathematical Modeling**

**Keywords: cross-border information exchange; information security; digital signature; nonpositional polynomial notations; two-factor authentication; data security; identification**

## 1. Introduction

In modern conditions, a large amount of information in electronic exchange has led to an increase in the relevance of the tasks of creating an automated system of secure electronic information exchange. Protection of information in automated systems (AS) is an extremely necessary task that ensures its reliability, safety and confidentiality (Ivanov, Yurchenko, & Yarmonov, 2016).

State Standard of the Republic of Kazakhstan (2019) defines the automated system as a system consisting of personnel and a set of automation tools for its activities, implementing information technology for performing the established functions. Information in the AS is safe if all components of the automated system protected from possible threats at the required level. The automated systems that provide security information are called secure (Zegzhda, 1996).

When sending information from a company (resident) to another (non-resident), as a rule, adhere to corporate, industry and national requirements for such exchange. However, the situation between departments of different states in cross-border interaction becomes more complicated. The solution to this issue was successfully achieved in the European Union member countries. In order to realize a legally meaningful interaction, they took into account the laws and requirements for cooperation of the 28 countries of the European Union. The creation of such an exchange took more than 10 years. The exchange of documents between the “Department-Department” and “Department-European Commission” units was initially carried out based on the EDS. Along with this, the opportunity of exchange was realized based on the third trusted party—exchange operators. In August 2014, after the appearance of a new legal act on electronic identification and trust services for electronic transactions in the domestic market, and the repeal of Directive 1999/93/EC appeared in the possibility of implementing exchange (Anikin et al., 2017).

The Law of the Eurasian Economic Union (EEU) has rules that define the concept of cross-border space of trust, which is necessary to create a legally significant cross-border electronic exchange of documents. In this case, national law regulates the implementation of cross-border electronic exchange of each member of the EEU. This Union does not have a single cryptographic algorithm that could be used for cross-border interaction and this is the problem of secure cross-border information interaction in the EEU (Gaydamakin, 2003; Hosmer, 1993; Sandhu & Samarati, 1994; The Secret of Cross-Border Correspondence, 2017).

In a cross-border exchange, each automated workstation is the property of one of the interacting parties and protected by means of protection adopted in the corresponding party. Each of the parties determines the protection of their workplace: cryptographic and hardware-software means of protecting information, including from unauthorized access, as well as other necessary hardware and software (Biyashev, Nyssanbayeva, & Begimbayeva, 2016). Consequently, there is a need to develop an automated system (AS) of secure cross-border information exchange (SCBIE).

The developed automated system of SCBIE consists of a set of information protection modules: data encryption, electronic digital signature (EDS), access control to the stored information in the databases based on two-factor authentication and module of resolution of a possible conflict situation. Models of two modules for an automated system are further described in Sections 1 and

2: the electronic digital signature and access control to information based on two-factor authentication.

Important in ensuring information security in the automated management system is ensuring the availability and integrity of configuration management information and personal data information. Increased attention has been paid to the prevention of unauthorized access to the system to maintain its stable functioning. However, due to the constantly increasing number of different services and various attacks on user accounts, there is a need to use two-factor authentication methods to ensure information security. In the past decade, these methods have been widely used in various areas of information and communication technologies. They are related to issues of identification and access of a subject to confidential information. They are trusted by a large number of companies, including high-tech organizations, financial and insurance sectors of the market, large banking institutions and public sector enterprises, independent expert organizations, as well as research firms. Consider the algorithm of two-factor authentication based on the authentication program and a mobile application for secure user identification.

## 2. Development of the electronic digital signature module for the automated system

### *2.1. Development of the digital signature algorithm based on modular arithmetic*

The electronic digital signature (EDS) module for the automated system of the information security in the process of cross-border exchange is developed. The extension (modified) algorithm for formation and verification EDS based on nonpositional polynomial notations (modular arithmetic or number systems in residual classes with polynomial bases) and the digital signature DSS. Nonpositional polynomial notations (NPNs) allow creating effective cryptographic systems of high reliability, which enable the confidentiality, authentication and integrity of stored and transmitted information (Biyashev, 1985; Biyashev & Nyssanbayeva, 2012).

To create the signature of an electronic message *M* (hereinafter—the message) of a given length of *N* bits based on the extension (modified) algorithm, the following steps are necessary:

Stage 1. Formation of the nonpositional polynomial notations (NPNs). In NPNs, the bases are irreducible polynomials over a field GF (2). For the process of NPNs formation for the message *M* of a given length *N* bits by choosing a system of polynomial bases is formed:

$$p_1(x), p_2(x), \ldots, p_s(x) \tag{1.1}$$

where $p_i(x)$—irreducible polynomials with binary coefficients of degree $m_i$ respectively, $i = \overline{1, s}$. These bases are called working bases. The main working range in NPNs is represented by a polynomial $P(x) = p_1(x) \cdot p_2(x) \cdots p_s(x)$ of the degree $m = m_1 + m_2 + \ldots + m_s$. According to the Chinese remainder theorem, the entire selected working base should be different from each other, even if they are irreducible polynomials of one degree.

In the NPNs, any polynomial $F(x)$, whose degree is less than *m*, has a non-positional representation as a sequence of residues from its division into working bases $p_1(x), p_2(x), \ldots, p_s(x)$, which is unique:

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_s(x)), \tag{1.2}$$

where $F(x) = \alpha_i(x)(mod(p_i(x)))$, $i = \overline{1, s}$. The positional representation of $F(x)$ is reconstructed from its form (1.3) (Biyashev, 1985; Biyashev & Nyssanbayeva, 2012).

$$F(x) = \sum_{i=1}^{s} \alpha_i(x) B_i(x), B_i(x) = \frac{P_s(x)}{p_i(x)} M_i(x), i = \overline{1, s} \tag{1.3}$$

Polynomials $M_i(x)$ are been chosen to satisfy the congruence in (1.3).

Stage 2. Formation of EDS keys. For each of the working base numbers, the corresponding generating elements (polynomials) $g_1(x), g_2(x), \ldots, g_s(x)$ are selected. Generating polynomials are analogous to primitive elements in finite field modulo prime number, of degree $g_i(x)$ is less than $m_i$, where $i=\overline{1,s}$. Then, the primitive element of the extended EDS algorithm is interpreted as a sequence of residues from the division of a certain polynomial $g(x)$ by the working base numbers $p_1(x), p_2(x), \ldots, p_s(x)$ respectively (Kalimoldayev, Biyashev, Nyssanbayeva, & Begimbayeva, 2016):

$$g(x) = (g_1(x), g_2(x), \ldots, g_s(x)) \tag{1.4}$$

where $g(x) = g_i(x)(mod(p_i(x)))$, $i = \overline{1,s}$.

The sender's private key $b$ in the range of $[1, 2^m]$ and $q_i(x),$ which is a divider $p_i(x) - 1$is selected.

The value of the public key $y(x)$ is calculated:

$$y(x) = (y_1(x), y_2(x), \ldots, y_s(x)) \tag{1.5}$$

where $y(x) \equiv g_i^b(x)(mod(p_i(x))), i = \overline{1,s}$.

Stage 3. Hashing the message. The developed extended EDS algorithm uses the procedure for calculating the hash value $h(x)$ in NPNs.

$$h(F(x)) = (\alpha_{s+1}(x), \alpha_{s+2}(x), \ldots, \alpha_{s+U}(x)), \tag{1.6}$$

where $\alpha_{s+1}(x), \alpha_{s+2}(x), \ldots, \alpha_{s+U}(x) -$ redundant residues (remainders) from dividing the reconstructed polynomial $F(x)$ by redundant bases $p_{s+1}(x), p_{s+2}(x), \ldots, p_{s+U}(x)$.

Stage 4. Formation of EDS. A random integer $k$ is selected from the range $[1, 2^m]$.

The polynomial $r(x) = (r_1(x), r_2(x), \ldots, r_s(x))$ is represented in a nonpositional form as a sequence of residues from their division into bases of the NPNs and is calculated as

$$r_i(x) \equiv g_i^k(x)(mod(p_i(x))), i = \overline{1,s} \tag{1.7}$$

then, $w(x) = (w_1(x), w_2(x), \ldots, w_s(x))$ calculated as

$$w_i(x) \equiv k^{-1}(h(x) + b + k)mod(q_i(x)), i = \overline{1,s} \tag{1.8}$$

Digital signature for the message $M$ is a pair of polynomials $(r(x), w(x))$.

For the developed extension algorithm for the formation of EDS, an algorithm for verification of the EDS is created.

Stage 5. Verification of a digital signature is carried out as follows:

The versions $(r(x), w(x))$ received by the addressee are denoted by $(r'(x), w'(x))$.

Calculates the hash value$h_1(x)$ from the received message $M'$.

The polynomial $v(x) = (v_1(x), v_2(x), \ldots, v_s(x))$ is calculated as a sequence of residues from their division into bases of the NPNs and is determined as

$$v(x) \equiv g_i^{u_1}(x)u_2^{w_i(x)^{-1}}(x)(mod(p_i(x))) \tag{1.9}$$

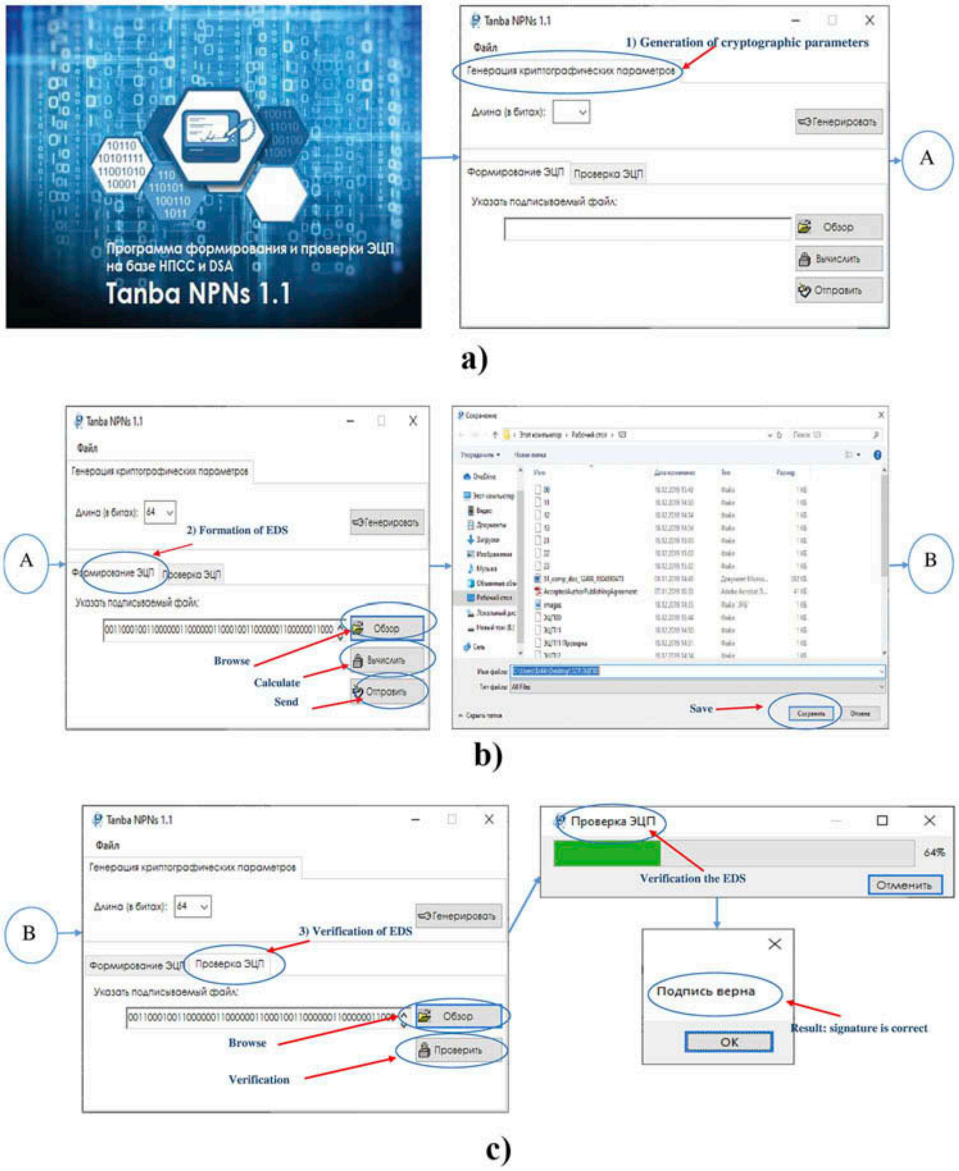
where polynomial values are calculated as $u_1(x) = (h_1(x)w^{-1}(x))mod(q(x))$ and $u_2(x) = (r'(x)y(x))mod(p_i(x))$.

If the equality $r'(x) = v(x)$ is satisfied, then the EDS is accepted, i.e. during the transmission, the integrity of the message is not compromised. If the equality is not fulfilled, the EDS is considered invalid.

### *2.2. Software implementation of the digital signature module*

The algorithm that was described in Section 1.1 is software implemented: the computer program "Tanba NPNs 1.1" has been created (Figure 1). The program consists of three tabs on which interface elements are grouped (text fields, buttons, etc.). These tabs are used to enter parameter values and run to perform the specified functions. Switching between sections is done by selecting the appropriate tab: (1) Generation of cryptographic parameters (Figure 1(a)). The first tab generates cryptographic parameters by selecting the length in bits. Next, you need to save the generated private key. (2) Formation of EDS (Figure 1(b)). In the second section, the EDS of the signed message formed. To do this, open the private key and select the message to be signed by clicking the "Browse" button and select the file. Next, you need to generate a digital signature of this message, by clicking "Calculate". In the beginning, for each message block the EDS is calculated, according to the algorithm which is performed above, and

**Figure 1. Software implementation of the formation and verification of EDS.**



the EDS of the entire message is the bitwise sum of the EDS of all the blocks. Then, the formed EDS is saved and "Send" for verification. (3) Verification of EDS (Figure 1(c)). The third section verifies the received EDS messages and the authenticity of the message. To do this, open the signed message by clicking the "Browse" button and select the file and then click the "Verification" button. During the process of verification, the EDS, a window opens to show the process of verification of EDS and its result.

Table 1 shows the results of the formation and verification of EDS for different lengths of the message block and key.

As seen from Table 1, with increasing key sizes, signature formation for the same file based on the above algorithm is slower. On the other hand, the formation of a signature using this algorithm is faster than verification signatures.

## 3. Development of the algorithm of two-factor authentication based on the authentication program

### *3.1. The algorithm for generating a temporary password*

Consider an example of the proposed information protection system using a combination of two factors: permanent and temporary passwords (Nyssanbayeva, Wojcik, & Ussatova, 2019). The user chooses a permanent password (the first factor) himself and uses it when registering an account (account). Before this, authorization must be registered in the application. After that, the application starts to enter user data (login and password), which must correspond to the registered data. Then, you need to enter the application on your smartphone and enter the initial data to generate a temporary password. A one-time or temporary password (the second factor) is generated on the server according to the proposed algorithm (Two-factor authentication, 2019) and is valid for a specific length of time for one authentication session. The advantage of a one-time password is that the password is not reused. Thus, an attacker who intercepted data from a successful authentication session cannot use the copied password to gain access to the protected system. The generation of a temporary password is possible online. To obtain a temporary password, additional software is used (Figure 2).

The software sends a request to the authorization server to generate a temporary password. This temporary password is generated on the server and displayed to the user in additional software on the smartphone. This temporary password has a short duration of 20 seconds. The temporary password is generated based on the result of the selected trigonometric function, which has a number of variable parameters. The trigonometric function is combined into a table, the dimension of 256 × 256 is a multiple of degree 2. The choice of this function and its initial parameters is based on the result of the hash function of the SHA256 standards (FIPS 140-2 Standard and self-Encryption Technology, 2018; National Institute of Standards and Technology (NIST), 2018; Two-factor authentication, 2019). This is a cryptographic hash function developed by the US National Security Agency (National Security Agency, 2018). The purpose of the hash function is the transformation (or hashing) of an arbitrary set of elements in the data into a fixed-length value. This value will characterize the set of source data without the possibility of extraction.

The input string for the hash function is a combination of user credentials, the current Greenwich Mean Time, and an additional secret string. The result of the hash function is divided into individual numbers, which will be the indices for selecting the function and its initial data. The secret string is a required field that will be randomly selected from the array. The secret line at each input is named, which makes it much more difficult to open the initial input line, which allows you to further strengthen the protection.

**Table 1. Formation and verification of EDS**

| File name | The length of the message block and key | Formed signature | Signature formation time (ms) | Signature verification time (ms) |
|---|---|---|---|---|
| Images.jpg | 64 bits | 100,100,111,000,100,111 11,010,111,111,110 1,010,010,011,101,001 1,100,000,011 | 71.52 | 71.97 |
| Images.jpg | 128 bits | 111,101,100,010,000,111 11,010,001,101,010,100 111,101,011,011,111,110 10,111,111,100,011,011 101,001,110,000,101,100 101,000,011,010 1,010,010,001,000 | 74.34 | 73.49 |
| Certificate.pdf | 64 bits | 11,100,110,101,010,001 10,100,000,110,010,101 1,100,111,110,010,100,101 101,000,111 | 54.95 | 67.42 |
| Certificate.pdf | 128 bits | 1,101,010,000,110,010,101 1,110,010,101,101,110 1,100,100,010,110,110,100 1,100,000,100,011,001,110 111,011,111,111,101,011 10,001,010,101,000,011 101,011,100,110,000 | 82.51 | 111.56 |
| Word.doc | 64 bits | 101,101,000,100 1,111,100,011,000,100,010 1,010,001,001 111,101 | 128,25 | 132.41 |
| Word.docx | 128 bits | 1,111,011,110,001,101,100 1,100,000,001,100,001,100 1,000,001,001,110,010,010 1,001,001,111,011,010,010 1,111,101,111,000,010,100 1,000,000,111,001,011,101 10,011,010,100,100 | 137.63 | 146.45 |
| Picture.JPG | 64 bits | 101,111,010,101 111,000,000,110,001 1,111,010,111,100,010 1,111,000,001 | 87,16 | 89.1 |
| Picture.JPG | 128 bits | 11,111,011,101,111,010 1,011,110,010,010,010 1,101,101,000,010,010 1,110,110,100,111,111 1,110,110,000,100,000 101,111,110,110,100,001 100,110,110,001,001,001 1001 | 99.82 | 107.55 |

The initial data for the input string will be the following values:

- Login: user16
- assword: pass17word
- Current moment: 2019 11 21 15:19:31
- Secret line: saLte

The input line will look like:
user16pass17word20191121151931saLte

The result of the SHA256 hash function is as follows:
90CC9939B3C05AA8D36A16B95EE5416B19632332CFCF46B30C4D37DFDE3F7DB7

The first symbols of the result are used to select a trigonometric function. Then, the index of the function in the table with the size of 256 × 256 will be (42, 168)—the decimal representation of the hexadecimal numbers 2A, A8. Using this index, the function will be selected and its parameters will be determined. Two hexadecimal numbers from the end of the hash function are used as initial parameters, and a hexadecimal number from position 10 is used as the "x" value. Based on the results of the calculation, the numbers after the comma are taken from the fifth position and the length in six digits.

For the formation of a secret string, a generator has been developed that allows one to randomly form words. Word dictionaries were not used, as words are easier to crack. The generator is based on the use of the Latin alphabet of capital and uppercase characters in a total of 52. The length of the generated word is 5 characters (Ussatova & Nyssanbayeva, 2019).

For the analysis of the generator used the method of complete enumeration. According to this method, the length of the string is taken into account (the length of the string is 5 characters in the appendix) and, for example, the search speed of 100,000 words per second is used. The number of options is calculated by the formula (2.1) and the search time is calculated by the formula (2.2):

$$S = A^n \tag{2.1}$$

where $S$ is the number of options, $A$ is the number of characters, and $n$ is the length of the string.

$$ST = \mathrm{S/P} \tag{2.2}$$

where $ST$ is the search time, $S$ is the number of options, and $P$ is the search speed.

For example, we calculate the time of crossing:

S = $52^5$ = 380,204,032
ST = 380,204,032/100,000 = 3802, 04032 seconds/60 = 63 minutes.

An example of the analysis of the generator is presented in Table 2.

It can be seen from the table that five characters are sufficient to generate a secret word since the secret word is one of the parameters for hash generation.

Due to the fact that, according to the developed two-factor authentication algorithm, the generation of a one-time password occurs every 20 seconds, the probability of hacking the generated secret word is almost impossible. This confirms the efficiency of the proposed generator.

**Table 2. Analysis of the generator**

| Number of characters | Number of options | Persistence | Search time |
|---|---|---|---|
| 1 | 52 | 5 bit | Less than a second |
| 2 | 2704 | 10 bit | Less than a second |
| 3 | 140,608 | 15 bit | 1 second |
| 4 | 7,311,616 | 21 bit | 1 minutes 22 seconds |
| 5 | 380,204,032 | 26 bit | 63 minutes |
| 6 | 19,770,609,664 | 31 bit | 55 hours |

The obtained data of the secret string are used to select the trigonometric function. For implementation, a generator of trigonometric functions has been developed, the use of which will greatly facilitate their formation.

To generate a trigonometric function, the number of variables is taken as the basis. There are seven of them in this generator: a, b, c, x, y, p1, p2. Initially, a list of variables is formed, resulting in a random number of variables Count from 1 to the number of variables minus 1. Then, the array is searched through the array with certain variables *N* times based on a random number from 0 to the length of the array minus 1. Read variable from the array, which is added in the new array and removed from the old. After the cycle is completed, a list of variables for the function is formed. Based on this list, the constituent parts (Math.sin (a), 1/Math.tan (p2)) of the format—"[‘Math.sin ()’, ‘Math.cos ()’, ‘Math.tan () ‘,’ (1/Math.tan ()) ‘,’ () ‘]". The ComponentsCount function (the number of elements minus 1) starts the loop through the array with the generated variables. In the loop at each step, a random number componentIndex from 0 to componentsCount is formed. The element with the corresponding value of the componentIndex is converted by replacing the symbol "with a variable from the list and added to the new array. As a result, a list of component parts with variables is formed. Next, rows are formed based on a random number from 1 to 3. In the cycle, the components, separated by signs of mathematical expressions, merge randomly. As a result, we obtain a generated string function, which we use to calculate a one-time two-factor authentication password.

### *3.2. The software implementation of the algorithm*

The software implementation of the considered algorithm is presented in Figure 2.

Then, the temporary password will be the number that must be entered into the application (Figure 2).

Consider the effect of generating a temporary password on the software implementation of information security tools based on two-factor authentication. For assessment of the sgenirovanny temporary password, different input data that show efficiency of realization of an algorithm were taken. Table 3 shows the results of the study of the generation of a temporary password according to the algorithm described above.

Table 3 shows the generation of a one-time password, which consists of five columns:

(1) Column "Nº s/n"—sequence number of locks;
(2) Column "Input data"—credentials for user authorization (Login, Password, Current moment, Secret line);
(3) Column "Hash value"—the obtained hash value, which is used for operation of the algorithm described above;
(4) Column "Trigonometric function" is a trigonometric function and a series of variables that is generated from the 256 × 256 array by random;

**Figure 2. Software implementation.**

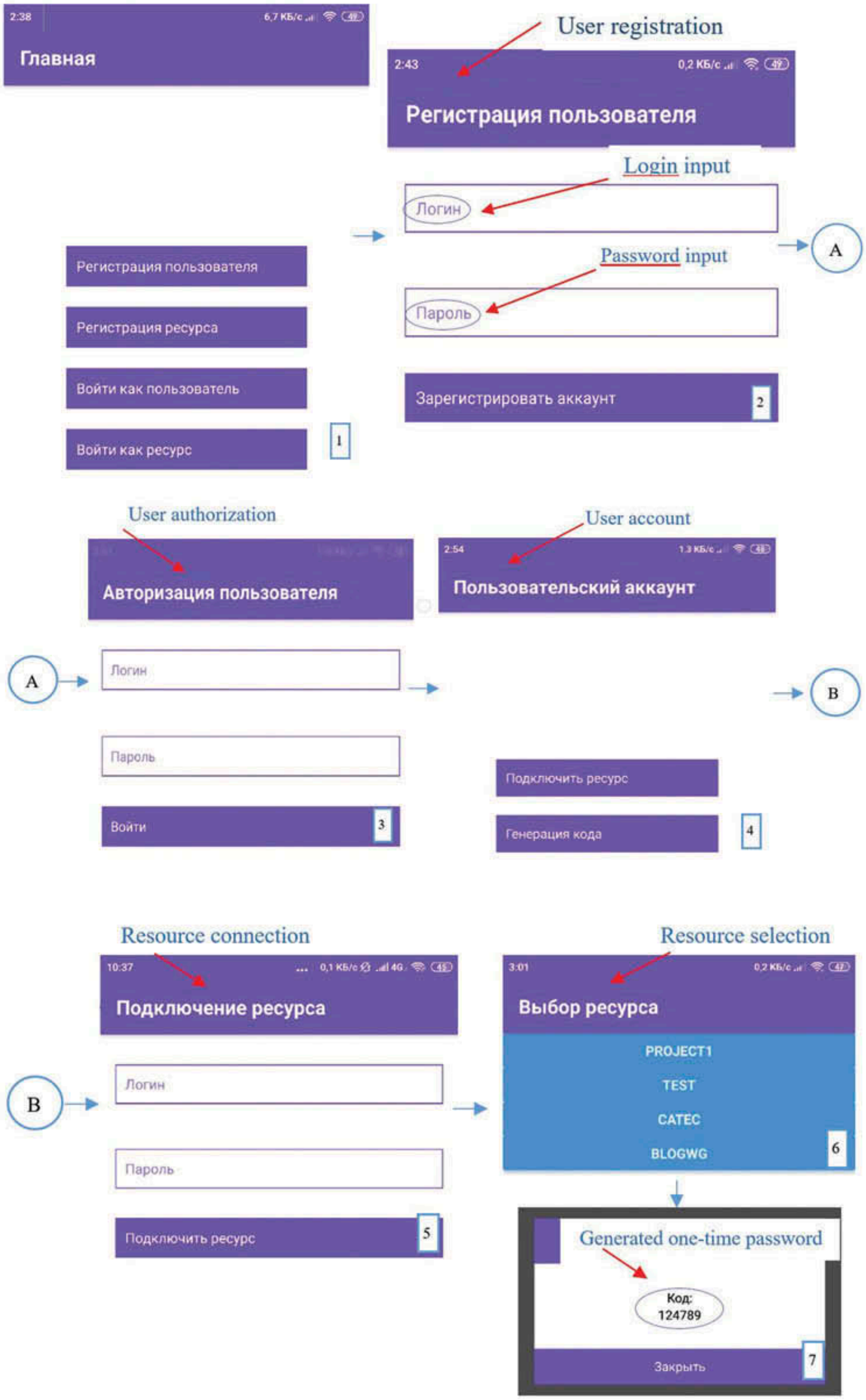


**Table 3. Generating a temporary password using this algorithm**

| Nº s/n | Input data | Hash value | Trigonometric function | Password generated |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| | User16<br>pass17word<br>20191121151931<br>saLte | 90CC9939B3C05AA8D36A16B95EE5416B19632332CFCF46B30C4D37DFDE3F7DB7 | (p1,p2,x) ≤ {return((Math.pow(Math.sin(x),3) + Math. sin (Math.pow(x),2))/(p1/p2)} “ p1,p2,x “ | 511,132 |
| | Login1<br>pas123<br>2,019,121,716,362<br>seret | 73BD8C18ED83B1171DC437C71A762210DE52080EF9DF64C1178967BCEEDC6CAD | (y,p1,x,c) ≤ {return((y * Math.pow(Math.sin(p1),2) + 4 * Math.pow(Math.tan(x),4)) * c)} “y,p1,x,c” | 711,633 |
| | Login1<br>pas123<br>20,191,217,163,947<br>seret | 3CF82991E4FB8B0D2C748013662A0C20FCCAE7D871A60A6E06F634F67900C81A | (y,c,b,x) ≤ {return ((Math.cos(y) * (x * Math.sin(c)))/Math.tan (Math.sqrt(b)))} “y,c,b,x” | 101,010 |
| | User123<br>password456<br>20,191,217,164,158<br>Werol | 2F37FB8B50E6D2E5611F8CA6B56CEF60D2F78B399C0E3DBD720CC447C3D45018 | (p1,y,c,p2) ≤ {return(p1 * Math.pow(Math.cos(y),2)—Math.sin (2 * c)—Math.pow(Math.cos(p2),3))} “p1,y,c,p2” | 005996 |
| | Pinokio<br>qwert<br>2,019,121,716,449<br>asdfA | BBA39EFC927C6BBA86AD45FE524DDAC6BCEE9F0A0830BE62F67A5474B0B8BBD9 | (a,b,y) ≤ {return(Math.sqrt(a) * Math.sin(b + Math.PI/y))} “a,b,y” | 296,145 |
| | Olga<br>pass20line<br>20,191,217,165,354<br>saKlt | 985465A101B8CFD070FE44CB16CA7D4F5CB5B9FAA0741051B286FBA6B910A6AD | (p1,y,c,p2) ≤ {return(p1 * Math.pow(Math.cos(y), 2)—Math.sin (2 * c)—Math.pow(Math.cos (p2),3))} “p1,y,c,p2” | 124,789 |

(5) Column “Password generated“—received a one-time password from the result of the calculation of trigonometric function.

The analysis of the work showed that the software implementation corresponds to the described algorithm. The developed client–server application works correctly, the generated one-time password is not repeated and changes even when entering duplicate data. The proposed two-factor authentication method can, is an additional means of protecting information stored in the system.

## 4. Conclusion

Cryptographic strength of the developed extension algorithm of EDS based on NPNs is characterized by the full secret key. This key is dependent on key length (pseudorandom sequence), on the chosen system of polynomial bases of NPNs, and on the number of all possible permutations of bases in the system. In NPNs, the cryptographic strength of the algorithm for generating an electronic digital signature (EDS) is also significantly increased, with a significant reduction in the length of the hash value and signature. The extension algorithm of EDS based on NPNs is used in the creating of this system.

The use of two-factor authentication allows you to enhance the protection of information. The proposed algorithm will eliminate the existing disadvantage of using two-factor authentication based on SMS—messages, since the proposed method uses two types of two-factor authentication: the authenticator application and input verification using a smartphone based on the client–server application. The use of generators to work in the formation of a one-time password allows you to enhance the level of protection of the described system. The software implementation of the proposed method shows that the considered algorithm works correctly and corresponds to described above.

In the Republic of Kazakhstan, the results of the research will be used in the automated system of information protection in cross-border exchange.

**Acknowledgements**
Research work was carried out within the framework of the project AP05132584 “Development of Kazakhstan segment of the protected cross-border information interaction”, which is being implemented at the Institute of Information and Computer Technologies.

**Funding**
This work was supported by the Ministry of Education and Science of the Republic of Kazakhstan, AP05132584.

**Author details**
Begimbayeva Yenlik[1]
E-mail: enlik_89@mail.ru
ORCID ID: http://orcid.org/0000-0002-4907-3345
Ussatova Olga[2]
E-mail: uoa_olga@mail.ru
Biyashev Rustem[1]
E-mail: brg@ipic.kz
Nyssanbayeva Saule[1]
E-mail: sultasha1@mail.ru
[1] Information Security Laboratory, The Institute of Information and Computational Technologies of MES RK, Almaty, 050010, Republic of Kazakhstan.
[2] DepartmentofInformation Systems, Al-Farabi Kazakh National University, Almaty, 050040, Republic of Kazakhstan.

**Citation information**
Cite this article as: Development of an automated system model of information protection in the cross-border exchange, Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem & Nyssanbayeva Saule, *Cogent Engineering* (2020), 7: 1724597.

**References**

Anikin, S. N., Domrachev, A. A., Dralo, M. P., Dupan, A. S., Kiryushkin, S. A., & Furgel, A. (2017). Methodology of forming a cross-border trust space. Information Security. INSIDE. 3. -pp. 6–12 (In Russian).

Biyashev, R. G. (1985). *Development and investigation of methods of the overall increase in reliability in data exchange systems of distributed ACSs* (Doctoral Dissertation in Technical Sciences), Moscow.

Biyashev, R. G., & Nyssanbayeva, S. E. (2012). Algorithm for creation a digital signature with error detection and correction. *Cybernetics and Systems Analysis*, 4, 489–497. doi:10.1007/s10559-012-9428-5

Biyashev, R. G., Nyssanbayeva, S. E., & Begimbayeva, Y. Y. (2016). Development of the model of protected cross-border information interaction. *Open Engineering*, *6*, 199–20. doi:10.1515/eng-2016-0025

FIPS 140-2 Standard and Self-Encryption Technology. (2018). [Electronic resource]. Retrieved from https://www.seagate.com/files/www-content/solutions-content/security-and-encryption/id/docs/faq-fips-sed-lr- mb-605-2-1302-ru.pdf/

Gaydamakin, N. A. (2003). *Differentiation of access to information in computer systems* (pp. 328). Ekaterinburg: Publishing house Ural. University.

Hosmer, H. 1993. The multipolicy paradigm for trusted systems. In J. B. Michael, V. Ashby, & C. Meadows (Eds.), *Proceedings on the 1992-1993 workshop on New security paradigms (NSPW ‘92-93)* (pp. 19–32). New York, NY, USA: ACM. doi:10.1145/283751.283768

Ivanov, K.K., Yurchenko, R. N., & Yarmonov, A. S. (2016). *Information security in automated systems* (Vol. 29, pp. 22–24). Young Scientist (In Russian).

Kalimoldayev, M. N., Biyashev, R. G., Nyssanbayeva, S. E., & Begimbayeva, Y. Y. (2016). Modification of the digital signature, developed on the nonpositional polynomial notations. *Eurasian Journal of Mathematical and Computer Applications*, 4(2), 33–38.

National Institute of Standards and Technology (NIST). (2018). [Electronic resource]. Retrieved from https://www.nist.gov/

National Security Agency. (2018). [Electronic resource]. Retrieved from https://www.cryptomuseum.com/intel/nsa/index.htm/

Nyssanbayeva, S., Wojcik, W., & Ussatova, O. (2019). Algorithm for generating temporary password based on the two- factor authentication model. *Przegląd Elektrotechniczny*, *5*, 101–106. Poland, ISSN 0033-2097, R. 95, P.

Sandhu, R. S., & Samarati, P. (1994). Access control: Principle and practice. *IEEE Communications Magazine*, *32*(9), 40–48. doi:10.1109/35.312842

The Secret of Cross-Border Correspondence. (2017). Retrieved from http://www.synerdocs.ru/5926669.aspx

State Standard of the Republic of Kazakhstan. (2019). Information technology. Set of standards for automated systems. Automated systems. Terms and Definitions. ST RK 34.014-2002. Retrieved from https://online.zakon.kz/Document/?doc_id=31056334

Two-factor authentication. (2019). [Electronic resource]. Retrieved from https://www.infobip.com/ru/glossariy/dvukhfaktornaya - autentifikatsiya

Ussatova, O., & Nyssanbayeva, S. (2019). Generators of one-time two-factor authentication passwords. Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska, Poland, 2, ISSN 2083-0157, R. 72, P. 60–64. doi:10.5604/01.3001.0013.2550

Zegzhda, D. P. (1996). *Theory and practice of information security*. M.: Yachtsman, 302 p. (In russian).