UDC 004.056.55

# TWO-FACTOR AUTHENTICATION PROTOCOL IN ACCESS CONTROL SYSTEMS

Irina V. Strelkovskaya, Oleksiy V. Onatskiy, Larysa G. Yona

International Humanitarian University, Odesa, Ukraine

**Background.** To ensure the protection of the biometric access control system used in unsecured communication channels, it is necessary to exclude the storage and transfer, transfer of biometric data as well as sequences generated on their basis. The paper proposes a cryptographic protocol of two-factor authentication with the zero-knowledge over the extended field $GF(2^m)$ on elliptic curves using biometric data and the private key of the user.

**Objective.** The aim of the article is to develop a cryptographic protocol for zero-knowledge two-factor authentication based on elliptic curves using biometric data and the user's private key, which allows increasing cryptographic strength and reducing the duration of the authentication process.

**Methods.** The process of implementing zero-knowledge proof protocols is as follows: one user (proofer) can convince another user (verifier) that he has some secret without disclosing the secret itself.

**Results.** A cryptographic protocol for two-factor authentication with zero-knowledge over the extended field $GF(2^m)$ of elliptic curves using user biometric data is proposed, which significantly reduces the size of the protocol parameters and increases cryptographic strength (computational complexity of the breaking). There is no leakage of private key information and biometric data of the user during the execution of the zero-knowledge proof protocol.

**Conclusions.** The implementation of a cryptographic protocol with zero-knowledge proof two-factor authentication based on elliptic curves allows significantly reducing the size of protocol parameters and increasing the cryptographic strength (computational complexity of the breaking).

***Keywords:*** *authentication; zero-knowledge proof; cryptographic protocol; biometric cryptosystems; elliptic curve; supersingular elliptic curve; non-supersingular elliptic curve; elliptic curve discrete logarithm problem.*

## 1. Introduction

The use of open transmission channels creates potential opportunities for attackers. Therefore, one of the important tasks of ensuring information security in the interaction of users is the use of methods and means that allow one (verifying) party to verify the authenticity of the other (proving) party. In challenge-response protocols, an attacker, controlling the communication channel, can impose specially selected requests and, by analyzing the responses, obtain confidential user information. To avoid this, zero-knowledge proof protocols are used to verify the accuracy of a statement without disclosing additional information about the statement itself. The zero-knowledge concept was first introduced in 1985 by researchers S. Goldwasser, S. Micali, and C. Rackoff [1], [2] and since then has been developed and applied in various projects, standards [3] in the field of cryptography and blockchain technology.

The standard [3] defines mechanisms for authenticating objects using zero-knowledge methods based on: factorization of integers, discrete logarithms, asymmetric encryption systems, discrete logarithms on elliptic curves. These mechanisms are built using zero-knowledge principles and methods. For example, the in the standard [3] regulates the response formation as a pair of values $(C, H)$, where $C$ is ciphertext, that is obtained by encrypting plaintext $M$ by using a hash function $h(M) = H$. Having received the answer $(C, H)$, the verifier can make sure that the decrypted message $M$ is known to the proofer. This in itself is enough to calculate the value of the hash function of the recovered message and compare it with the value of another element of the response.

Paper [4] proposes a zero-knowledge cryptographic proof protocol based on elliptic curves using public keys and random messages. To verify the protocol [4], the tools of the security protocol Animator package for Automated Validation of Internet Security Protocols and Applications were used.

Also, one of the main factors indicating the security status of a particular key information infrastructure system is the efficiency of the access control subsystem of its information security system. Efficient operation is ensured by maximum reliability and speed of the authentication process and confidentiality of data processing. Therefore, an important aspect of the practical implementation of the access control

subsystem is methods of protection against current threats, including unauthorized access to user authentication data. In particular biometric cryptography is used for biometric access control systems. Depending on the purpose of applying biometrics in cryptography, several types of biometric cryptosystems have appeared [5], [6]:

– Key Release Cryptosystems (KRC);
– Key Binding Cryptosystems (KBC);
– Key Generation Cryptosystems (KGC).

According to [5], [6], the biometric KRC key and the biometric standard are stored separately. Biometric authentication is independent of the release mechanism. The key is released after successful biometric authentication (for example, biometric-based authentication). Biometric KBC [5] – a biometric sample (e.g. fingerprint) and a key are cryptographically linked. The key is locked with the user's biometric sample and stored in this form in the database. If the biometric data comparison is successful, the key is extracted from the biometric sample. The security of this method depends on the secrecy of the key closure and recovery algorithms (for example, fuzzy vault, fuzzy commitment scheme, biometric encryption). Biometric KGC [5] – the key does not require storage, since it is created from biometric data. The main advantage of this system over others is that it does not store the key obtained from biometric data (for example, fuzzy extractor).

## 2. Problem statement

The aim of the article is to develop a cryptographic protocol for zero-knowledge two-factor authentication based on elliptic curves using biometric data and the user's private key, which allows increasing cryptographic strength (computational complexity of the breaking), reduce the duration of the authentication process.

The process of implementing Zero-Knowledge Proof (ZKP) protocols is as follows: one user (the prover, for example, user *A*) can convince another user (the verifier, for example, user *B*) that he has some secret without disclosing the secret itself. There is no leakage of private key information during the execution of the ZKP protocol. This is relevant because protocols of this type are built using a public key that contains complete information about the owner's private secret key.

Protocols ZKP should have three properties [7], [8]:

1. Completeness refers to the ability of the evidence to guarantee that the statement being tested is true.

2. Soundness refers to the ability of a proof to ensure that the claim being tested is accurate and not falsified.

3. Zero-knowledge refers to the ability of a proof to reveal no additional information about the statement being tested.

ZKP protocols are executed as a sequence of independent cycles (rounds), each of which consists of three steps of a certain type (Fig. 1):

1. $A \rightarrow B$: $\alpha$ witness;
2. $A \leftarrow B$: $\beta$ challenge;
3. $A \rightarrow B$: $\gamma$ response,

where $\alpha, \beta, \gamma \in \{1, 2, \ldots, N\}$.

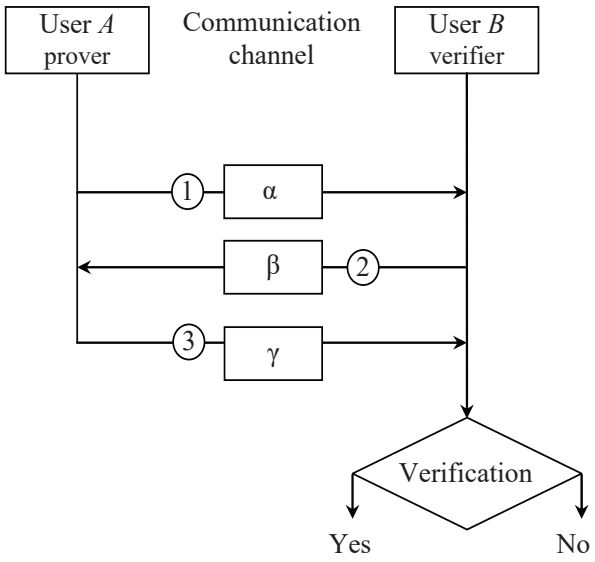


**Fig. 1. Structure ZKP protocol**

After each cycle, the verifier (user *B*) decides on the truth of the proof. ZKP cryptographic protocols based on asymmetric encryption are widely used. The most well-known protocols are Fiat-Shamir, Schnorr, Okamoto, Guillou-Quisquater, Brickell-McCurley, Feige-Fiat-Shamir (Table 1) [5], [6], [7], [8], [9], [10]. The stability of these protocols is determined by the Discrete Logarithm Problem (DLP) in the finite field $Z_n$ or $Z_p$, as well as by increasing the number of accreditation cycles at different values of $\alpha$ and $\beta$.

## 3. Materials and methods

In cryptosystems based on Elliptic Curves (EC), it is proposed to use crypto-transformations based on transformations and multiplication of points of elliptic curves over Galois fields $GF(p)$, $GF(2^m)$, $GF(p^m)$, where $p$ and $m$ are primes [11], [12]. The main advantages of elliptic cryptography are: a much shorter key length compared to "classical" asymmetric

cryptography (example RSA) and fast software and hardware implementation (Table 2).

**Table 1 – Cryptographic protocols ZKP**

| Protocol | Calculation | Verification |
|---|---|---|
| Fiat–Shamir | 1. $A \to B$: $Y_A$, $\alpha \equiv r^2 \pmod n$;<br>2. $A \leftarrow B$: $\beta$;<br>3. $A \to B$: $\gamma \equiv (r k^{\beta}) \bmod n$. | $\alpha \equiv (\gamma^2 Y_A^{\beta}) \bmod n$ |
| Schnorr | 1. $A \to B$: $Y_A$, $\alpha \equiv t^r \pmod p$;<br>2. $A \leftarrow B$: $\beta$;<br>3. $A \to B$: $\gamma \equiv (r + k\beta) \bmod q$. | $\alpha \equiv (t^{\gamma} Y_A^{\beta}) \bmod p$ |
| Okamoto | 1. $A \to B$: $Y_A$, $\alpha \equiv (t_1^{r_1} t_2^{r_2}) \bmod p$;<br>2. $A \leftarrow B$: $\beta$;<br>3. $A \to B$: $\gamma_1 \equiv (r_1 + k_1\beta) \bmod q$;<br>$\gamma_2 \equiv (r_2 + k_2\beta) \bmod q$. | $\alpha \equiv (t_1^{\gamma_1} t_2^{\gamma_2} Y_A^{\beta}) \bmod p$ |
| Guillou–Quisquater | 1. $A \to B$: $Y_A$, $\alpha \equiv r^e \pmod n$;<br>2. $A \leftarrow B$: $\beta$;<br>3. $A \to B$: $\gamma \equiv (r k^{\beta}) \bmod n$. | $\alpha \equiv (\gamma^e Y_A^{\beta}) \bmod n$ |
| Brickell–McCurley | 1. $A \to B$: $Y_A$, $\alpha \equiv t^r \pmod p$;<br>2. $A \leftarrow B$: $\beta$;<br>3. $A \to B$: $\gamma \equiv (r + k\beta) \bmod (p-1)$. | $\alpha \equiv (t^{\gamma} Y_A^{\beta}) \bmod p$ |
| Feige–Fiat–Shamir | 1. $A \to B$: $Y_{A_1},\ldots,Y_{A_k}$, $\alpha \equiv r^2 \pmod n$;<br>2. $A \leftarrow B$: $\beta_1,\ldots,\beta_k$;<br>3. $A \to B$: $\gamma \equiv [r(k_1^{\beta_1} \cdot \ldots \cdot k_k^{\beta_k})] \bmod n$. | $\alpha \equiv [\gamma^2 (Y_{A_1}^{\beta_1} \cdot \ldots \cdot Y_{A_k}^{\beta_k})] \bmod n$ |

**Table 2 – Key size for EC cryptography and RSA**

| EC cryptography key, bits | RSA key, bits | Key ratio |
|---|---|---|
| 163 | 1024 | 1 : 6 |
| 256 | 3072 | 1 : 12 |
| 384 | 7680 | 1 : 20 |
| 512 | 15360 | 1 : 30 |

In cryptosystems over the extended field $GF(2^m)$, the equation EC has the form [11, 12]:

$$y^2 + xy \equiv (x^3 + ax^2 + b) \pmod{f(x), 2}$$

for non-supersingular curves, denote $E(a, b), f(x)$;

$$y^2 + cy \equiv (x^3 + ax + b) \pmod{f(x), 2}$$

for supersingular curves, denote $E(a, b, c), f(x)$,
where $x, y$ – points of EC, $a, b, c$ – parameters of EC; $c, b \neq 0 \pmod{f(x), 2}$; $f(x)$ – primitive polynomial of degree $m$ over the field $GF(2)$ of the form

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \ldots + h_{m-1} x^1 + h_m$$

moreover $h_i \in GF(2)$, where $i \in \{1, 2, \ldots, m\}$.

Let us define an addition operation for points from the elements of the field $GF(2^m)$. Let the coordinates of the two point's $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, be known, then the sum of $P + Q = (x_3, y_3)$ is determined as follows [11, 12]:

1) if the points $P$ and $Q$ belong to a non-supersingular curve, then

$$\begin{cases} x_3 \equiv (\lambda^2 + \lambda + x_1 + x_2 + a) \bmod (f(x), 2); \\ y_3 \equiv [\lambda(x_1 + x_3) + x_3 + y_1] \bmod (f(x), 2), \end{cases} \quad (1)$$

where $\lambda \equiv \left(\frac{y_1 + y_2}{x_1 + x_2}\right) \bmod (f(x), 2)$;

2) if the points $P$ and $Q$ belong to a supersingular curve, then

$$\begin{cases} x_3 \equiv (\lambda^2 + x_1 + x_2) \bmod (f(x), 2); \\ y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2), \end{cases} \quad (2)$$

where $\lambda \equiv \left(\frac{y_1 + y_2}{x_1 + x_2}\right) \bmod (f(x), 2)$;

Similarly, the operation of doubling the point $2P = P + P = (x_3, y_3)$ can be represented, then we use (1) and (2) we have:

1) for a $2P$ point that belongs to a non-supersingular curve,

$$\begin{cases} x_3 \equiv (\lambda^2 + \lambda + a) \bmod (f(x), 2); \\ y_3 \equiv [x_1^2 + (\lambda + 1)\, x_3] \bmod (f(x), 2), \end{cases} \quad (3)$$

where $\lambda \equiv \left( x_1 + \frac{y_1}{x_1} \right) \bmod (f(x), 2)$;

2) for a $2P$ point that belongs to a supersingular curve,

$$\begin{cases} x_3 \equiv \lambda^2 \bmod (f(x), 2); \\ y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2), \end{cases} \quad (4)$$

where $\lambda \equiv \left( \frac{x_1^2 + a}{c} \right) \bmod (f(x), 2)$.

Consider the cryptographic protocol of two-factor authentication on EC, which is shown in Fig. 2.

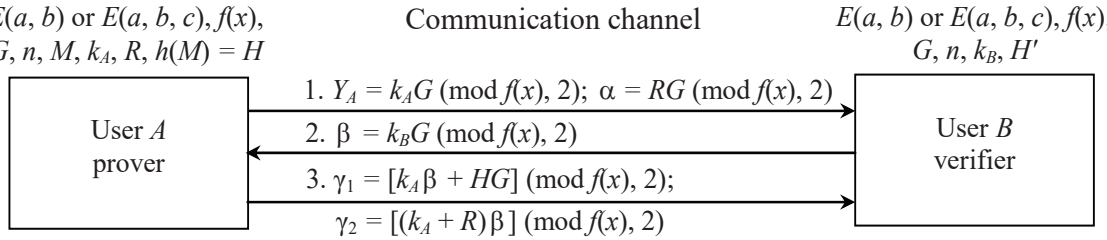


**Fig. 2. Two-factor authentication protocol with zero-knowledge on elliptic curves**

Let $E(a, b)$ or $E(a, b, c)$ be an elliptic curve of the field $GF(2^m)$; $G$ – a point of this curve; $n$ – the group order of the curve; $M$ – a set of biometric data and $k_A$ – the personal key of user $A$; $k_B$ – the session key of user $B$; $h(M) = H$ – the message digest of the hash function $h$. User $A$ calculates the value of the public key $Y_A = k_A G \pmod{f(x), 2}$, which it sends to user $B$ along with the witness $\alpha = RG \pmod{f(x), 2}$, where $R$ is a random value. User $B$ selects the session key $k_B$ and calculates the value of the challenge $\beta = k_B G \pmod{f(x), 2}$, which it transmits to user $A$. User $A$ calculates the response in the form of two values:

$$\gamma_1 = [k_A \beta + HG] \pmod{f(x), 2};$$
$$\gamma_2 = [(k_A + R)\beta] \pmod{f(x), 2},$$

which it transmits to user $B$. User $B$ performs the following verification:

1) User $B$ verification the equality of the values $H'G = HG$, where $H'$ and $H$ are digests of the message of the hash-function $h(M)$ under the condition

$$H'G = [\gamma_1 - k_B Y_A] \pmod{f(x), 2};$$

2) User $B$ verification the equality of the values $k_B \alpha = k_B \alpha'$ from the condition

$$k_B \alpha' = [\gamma_2 - k_B Y_A] \pmod{f(x), 2}.$$

For proving user $A$, the values of $M$ and $k_A$ are known, so it can respond to any challenge $\beta$ of user $B$. In this case, verifying user $B$ is convinced of the fairness of the rations:

$$\begin{aligned} 1)\ H'G &= [\gamma_1 - k_B Y_A] \pmod{f(x), 2} = \\ &= [k_A \beta + HG - k_B Y_A] \pmod{f(x), 2} = \\ &= [k_A k_B G + HG - k_B k_A G] \pmod{f(x), 2} = HG; \\ 2)\ k_B \alpha' &= [\gamma_2 - k_B Y_A] \pmod{f(x), 2} = \\ &= [(k_A + R)\beta - k_B Y_A] \pmod{f(x), 2} = \\ &= [k_A \beta + R\beta - k_B Y_A] \pmod{f(x), 2} = \\ &= [k_A k_B G + k_B RG - k_B k_A G] \pmod{f(x), 2} = \\ &= k_B RG \pmod{f(x), 2} = k_B \alpha. \end{aligned}$$

If all the equations are satisfied, the verifying user $B$ accepts the proof; if at least one of the equations is not satisfied, the proof is rejected, i.e., the authentication of user $A$ fails.

We will give an example of the calculation of the proposed protocol. Let a supersingular elliptic curve $E(11, 100, 1)$ over the extended field $GF(2^{11})$ and a primitive polynomial $f(x) = x^{11} + x^2 + 1$ over the field $GF(2)$ be given, which has the form

$$y^2 + y \equiv (x^3 + 11x + 100) \bmod (100000000101, 2);$$

the group order of the curve $n = 2113$; generating point $G = (1001000, 10)$; private key $k_A = 978$ user $A$; random number $R = 1207$; session key $k_B = 2093$ user $B$; biometric data $M = 2000$; message digest $h(2000) = H = 568$.

According to the protocol (Fig. 2), we will calculate the value of the public key $Y_A$ and the witness $\alpha$ of user $A$:

$$Y_A = 978(1001000, 10) \bmod (100000000101, 2) = (10111100, 11100110010);$$
$$\alpha = 1207(1001000, 10) \bmod (100000000101, 2) = (100001010, 1111001100).$$

Next, we calculate the value of challenge $\beta$ of user *B*:

$$\beta = 2093(1001000, 10) \bmod (100000000101, 2) = (1000000000, 1101011).$$

Let's calculate the value of user *A* response in the form of $\gamma_1$ and $\gamma_2$ values:

$$\gamma_1 = [978(1000000000, 1101011) + 568(1001000, 10)] \bmod (100000000101, 2) =$$
$$= [(10000000110, 110001000) + (1100110111, 10011010010)] \bmod (100000000101, 2) =$$
$$= (1011001001, 11100001011);$$
$$\gamma_2 = [(978 + 1207)(1000000000, 1101011)] \bmod (100000000101, 2) =$$
$$= 2185(1000000000, 1101011) \bmod (100000000101, 2) = (1110110111, 11011001000).$$

User *B* performs the following verification:
1) Equality of hash function message digests $H'G = HG$:

$$H'G = 568(1001000, 10) \bmod (100000000101, 2) = (1100110111, 10011010010) = (823, 1234);$$
$$HG = [(1011001001, 11100001011) - 2093(10111100, 11100110010)] \bmod (100000000101, 2) =$$
$$= [(1011001001, 11100001011) - (10000000110, 110001000)] \bmod (100000000101, 2) =$$
$$= (1100110111, 10011010010) = (823, 1234).$$

This, equalities are fulfilled $H'G = HG = (1100110111, 10011010010) = (823, 1234)$.
2) Comparing values $k_B\alpha = k_B\alpha'$

$$k_B\alpha = 2093(100001010, 1111001100) \bmod (100000000101, 2) = (11001001, 10111100110) = (201, 1510);$$
$$k_B\alpha' = [(1110110111, 11011001000) - 2093(10111100, 11100110010)] \bmod (100000000101, 2) =$$
$$= [(1110110111, 11011001000) - (10000000110, 110001000)] \bmod (100000000101, 2) =$$
$$= (11001001, 10111100110) = (201, 1510).$$

This, the equality are fulfilled $k_B\alpha = k_B\alpha' = (11001001, 10111100110) = (201, 1510)$.

Since two verification have been completed, verifying user *B* accepts proof that user *A* two-factor authentication has been successful.

## 4. Experiments

To analyze and validation the proposed cryptographic protocol for resistance to adversary attacks, we used the Automated Validation of Internet Security Protocols and Applications (AVISPA) software product [13].

AVISPA is a push-button tool for the automated validation of Internet security-sensitive protocols and applications. AVISPA is a used for automated falsification of security protocols. AVISPA uses a language High Level Protocol Specification Language (HLPSL) to write specifications for security protocols and then specifications HLPSL are translated to low level Intermediate Format (IF) using automatic translator HLPSL2IF. This language is based on roles: basic roles for representing each participant role, and composition roles for representing scenarios of basic roles. Each role is independent from the others, getting some initial information by parameters, communicating with the other roles by channels [13]. The architecture of AVISPA tool is shown in Fig. 3.

AVISPA supports four (Fig. 3) different verification tools (back-ends) that can analyze IF specifications [13]:

– On-the-Fly Model Checker (OFMC);
– Constraint-Logic-based Attack Searcher (CL-AtSe);
– SAT-based Model Checker (SATMC);
– Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP).

In this work, the model of the proposed protocol was tested using the protocol simulation of the Security Protocol Animator (SPAN) tool for AVISPA [14] (Fig. 4). The result of modeling the attacker's attack on the protocol is shown in Fig. 5, and the modeling of the attacker's attack on the protocol is shown in Fig. 6 (the notation used in AVISPA: $\alpha$ = Y, $\beta$ = Yb, $\gamma_1$ = Y1, $\gamma_2$ = Y2).

Software verification of the protocol and stability of the protocol against attacker attacks was performed using the OFMC and CL-AtSe AVISPA software back-ends (Fig. 5, 6). As a result of checking the proposed protocol, no known attacks were found.

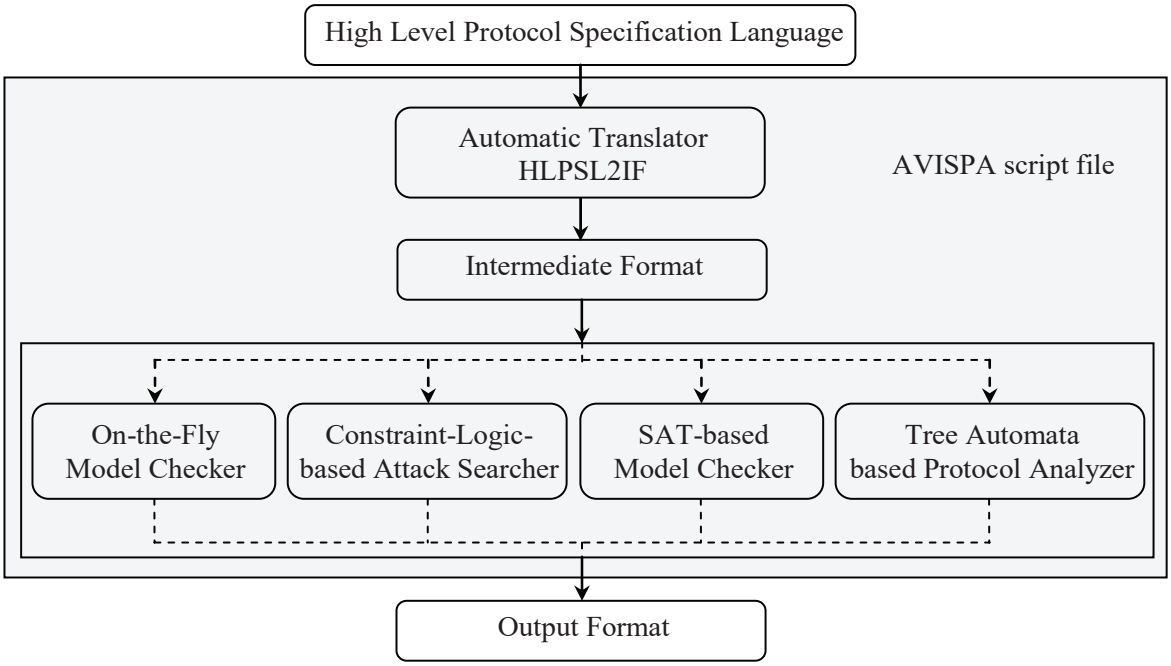


**Fig. 3. Architecture of the AVISPA**

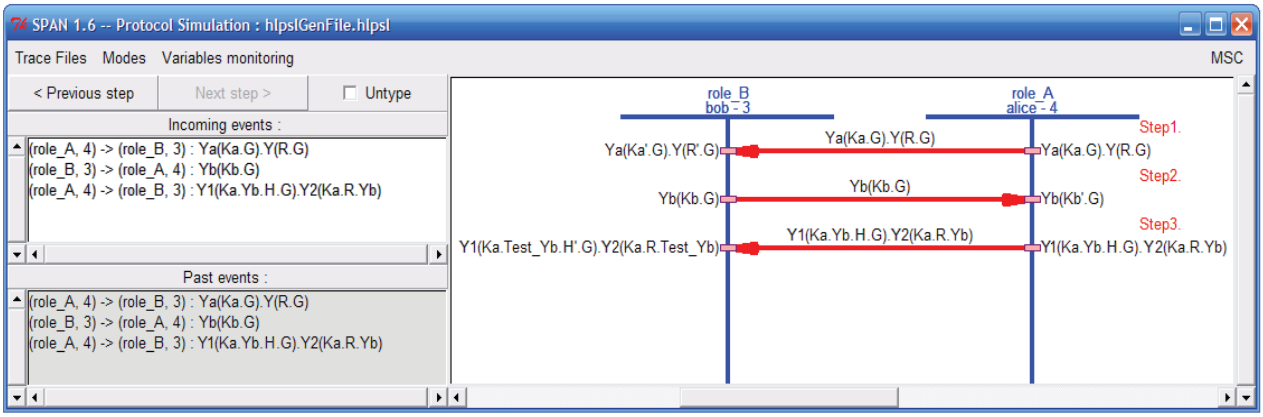


**Fig. 4. Verification of the cryptographic protocol model**

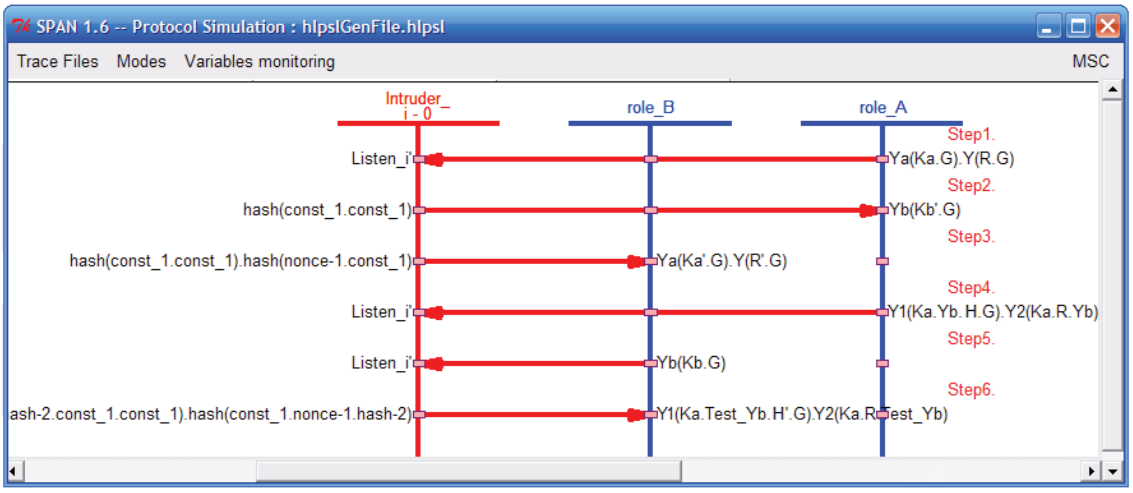


**Fig. 5. The result of modeling the attacker's action on the protocol**

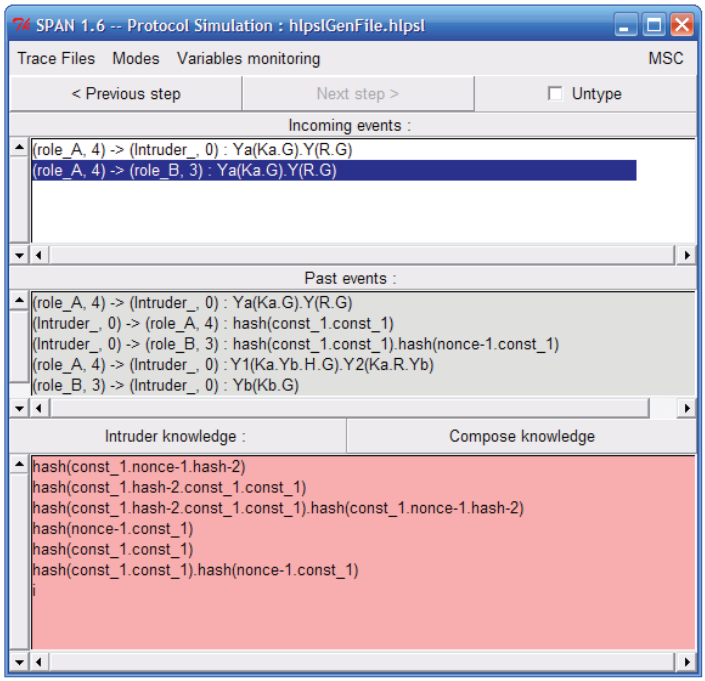


**Fig. 6. The process of modeling the action of an attacker on the protocol**

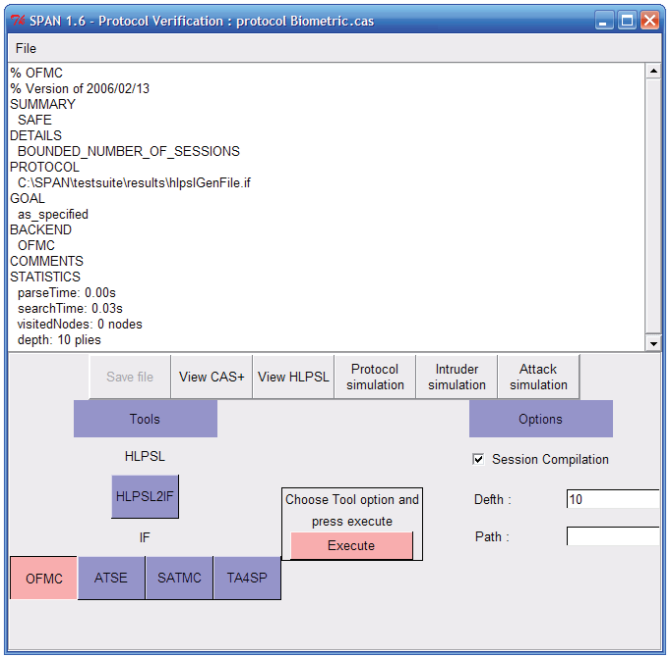


**Fig. 5. Protocol verification using the OFMC**

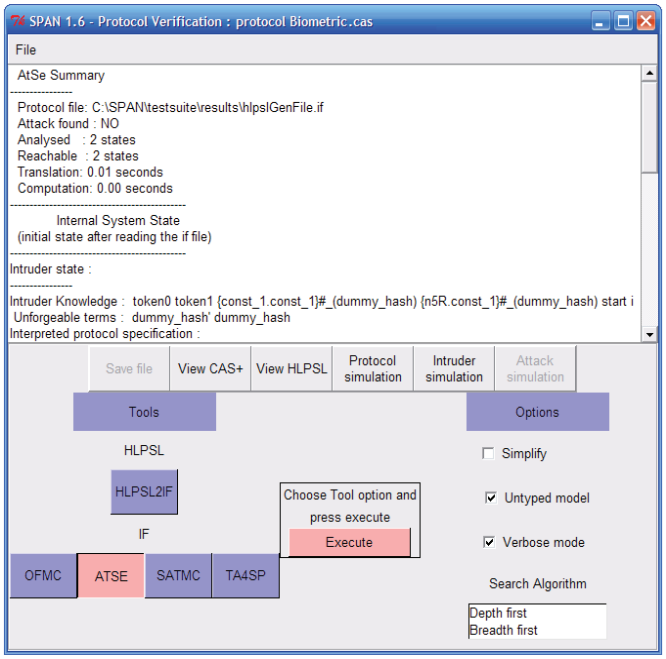


**Fig. 6. Constraint Logic based Attack Searcher**

## 5. Conclusions

1. A cryptographic protocol for two-factor authentication with zero-knowledge over the extended field $GF(2^m)$ of elliptic curves using user biometric data is proposed, which significantly reduces the size of the protocol parameters and increases cryptographic strength (computational complexity of the breaking). The advantages of the protocol are the ability to maintain data confidentiality, which allows you to verify the integrity and accuracy of information without disclosing additional information about the approval itself; speed, the proof within the ZKP method can be made very short and simple, which means that it takes a minimum of time to verify it; compatibility with smart contracts, which allows you to use ZKP to create smart contracts with increased privacy.

2. Model validation and protocol verification were performed. As a result of the verification of the two-factor authentication protocol, no known attacks on the protocol were found. To implement the proposed protocol, we can use the recommended elliptic curves according to FIPS 186-4 (Appendix D: NIST Recommended Elliptic Curves) [15], SEC 2: Recommended Elliptic Curve Domain Parameters [16] and DSTU 4145-2002 [17].

## References


1. Goldwasser S., Micali S., Rackoff C. Knowledge Complexity of Interactive Proofs. STOC '85: *Proceedings of the seventeenth annual ACM symposium on theory of computing*. December 1985, pp. 291–304, https: //doi.org/10.1145/22145.22178
2. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // *SIAM Journal on Computing* / M. Sudan – SIAM, 1989. Vol. 18, Iss. 1. pp. 186–208, https: //doi.org/ 10.1137/0218012
3. ISO/IEC 9798-5:2009. Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique. // Retrieved from: https://www.iso.org/standard/ 50456.html
4. Onatskiy A.V., Garova O.V. Cryptographic authentication protocol zero-knowledge secret on elliptic curves using public keys and random messages. Digital technologies. Odesa: ONAZ named after O.S. Popova, 2019. Issue 26. pp. 16–23.
5. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996. – 816 p.
6. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. – 863 p.
7. Feige U., Fiat A., Shamir A. Zero knowledge proofs of identity. *Journal of Cryptology*, 1988. Vol. 1, pp. 77–94.
8. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems. Proc. Crypto '86, A.M. Odlyzko, Ed., *Lecture Notes in Computer Science*, 1987. Vol. 263. Advances in Cryptology, Berlin, Springer-Verlag, pp. 186–194.
9. Guillou L.C., Quisquater J.-J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. Proc. Eurocrypt '88, C.G. Günther, Ed., *Lecture Notes in Computer Science*, 1988. Vol. 330. Advances in Cryptology, Berlin, Springer-Verlag, pp. 123–128.
10. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. – 784 p.
11. Hankerson D., Menezes A., Vanstone S., Hankerson D. Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004. – 358 p.
12. Horbenko I. D., Horbenko Yu. I. Applied cryptology. Theory. Practice: a monograph, Kharkiv: "Fort" Publishing House, 2012. - 880 p.
13. AVISPA. // Retrieved from: https://www.avispa-project.org/
14. Security Protocol Animator. // Retrieved from: https://www.irisa.fr/celtique/genet/ span/
15. FIPS 186-4. // Retrieved from: https://nvlpubs.nist. gov/nistpubs/FIPS/NIST.FIPS. 186-4.pdf
16. SEC 2: Recommended Elliptic Curve Domain Parameters. // Retrieved from: https://www.secg.org/ SEC2-Ver-1.0.pdf
17. DSTU 4145-2002. // Retrieved from: https://uk. wikipedia.org/wiki/ДСТУ_4145-2002


/

***Стрелковська І.В., Онацький О.В., Йона Л.Г.***

**Протокол двофакторної автентифікації у системах контролю доступу**

**Проблематика.** Для забезпечення захисту біометричної системи управління доступом, які використовуються у незахищених каналах зв'язку, необхідно виключити зберігання, передачу біометричних даних та послідовність, згенерованих на їх основі. В роботі запропоновано криптографічний протокол двофакторної автентифікації з нульовим розголошенням над розширеним полем $GF(2^m)$ еліптичних кривих з використанням біометричних даних та особистого ключа користувача.

**Мета дослідження.** Метою статті є розробка криптографічного протоколу двофакторної автентифікації з нульовим розголошенням на основі еліптичних кривих з використанням біометричних даних та особистого ключа користувача для збільшення криптографічної стійкості та прискорення процесу автентифікації.

**Методика реалізації.** Процес реалізації протоколів доказу з нульовим розголошенням полягає в наступному: один користувач (доказуючий) може переконати іншого користувача (перевіряючого) у тому, що він має деякий секрет, без розкриття самого секрету. Виконана розробка протоколу на основі еліптичних кривих.

**Результати дослідження.** Запропонований криптографічний протокол дозволяє значно зменшити розмір параметрів протоколу й збільшити криптографічну стійкість (обчислювальну складність завдання злому). У процесі виконання протоколу з нульовим розголошенням немає будь-якого витоку інформації про особистий ключ та

біометричних даних користувача.

**Висновки.** Реалізація криптографічного протоколу двофакторної автентифікації з нульовим розголошенням на основі еліптичних кривих дозволяє значно зменшити розмір параметрів протоколу й збільшити криптографічну стійкість (обчислювальну складність завдання злому).

***Ключові слова:*** *автентифікація; доказ із нульовим розголошенням; криптографічний протокол; біометричні криптографічні системи; еліптична крива; суперсингулярна еліптична крива; несуперсингулярна еліптична крива; проблема дискретного логарифмування в групах точок еліптичної кривої.*