UDC: 004.056.55: 003.26

CRYPTOGRAPHIC AUTHENTICATION PROTOCOL ZERO-KNOWLEDGE SECRET ON ELLIPTIC CURVES USING PUBLIC KEYS AND RANDOM MESSAGES

ONATSKIY A.V. [1], ZHAROVA O.V. [2]

[1] *O.S. Popov Odessa national academy of telecommunications,*
1 Kuznechna St., Odessa, 65029, Ukraine.
onatsky@meta.ua

[2] *Odessa national polytechnic university,*
1 Shevchenko ave., Odessa, 65044, Ukraine
Ksenia.gds@gmail.com

КРИПТОГРАФІЧНИЙ ПРОТОКОЛ АВТЕНТИФІКАЦІЇ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ СЕКРЕТУ НА ЕЛІПТИЧНИХ КРИВИХ ІЗ ЗАСТОСУВАННЯМ ВІДКРИТИХ КЛЮЧІВ І ВИПАДКОВИХ ПОВІДОМЛЕНЬ

ОНАЦЬКИЙ О.В. [1], ЖАРОВА О.В. [2]

[1] *Одеська національна академія зв'язку ім. О.С. Попова,*
65029, Україна, м. Одеса, вул. Кузнечна 1,
onatsky@meta.ua

[2] *Одеський національний політехнічний університет*
65044, Україна, м. Одеса, просп. Шевченка 1,
Ksenia.gds@gmail.com

Abstract. *We propose a cryptographic protocol with zero-knowledge proof (ZKP) on elliptic curves (EC) using public keys and random messages, allowing to establish the truth of a statement not conveying any additional information about the statement itself. The cryptographic protocols based on zero-knowledge proof allow identification, key exchange and other cryptographic operations to be performed without leakage of sensitive information during the information exchange. The implementation of the cryptographic protocol of the zero-knowledge proof on the basis of the mathematical apparatus of elliptic curves allows to significantly reduce the size of the protocol parameters and increase its cryptographic strength (computational complexity of the breaking). The security of cryptosystems involving elliptic curves is based on the difficulty of solving the elliptic curve discrete logarithm problem. We determine the completeness and correctness of the protocol and give an example of the calculation is given. The cryptographic protocol was modeled in the High-Level Protocol Specification Language, the model validation and verification of the protocol were also performed. The software verification of the cryptographic protocol was performed using the software modules On the Fly Model Checker and Constraint Logic based Attack Searcher. In order to validate the cryptographic protocol resistance to intruder attacks, we used the Security Protocol Animator package for Automated Validation of Internet Security Protocols and Applications. The security of the proposed cryptographic protocol ZKP EC is based on the difficulty of solving the elliptic curve discrete logarithm problem). The recommended elliptical curves according to DSTU 4145-2002 may be used to implement such cryptographic protocol.*

Key words: *cryptographic protocol, elliptic curves, identification, authentication, zero-knowledge proof, elliptic curve discrete logarithm problem.*

Анотація. *Запропоновано криптографічний протокол доказу із нульовим розголошенням (Zero-Knowledge Proof – ZKP) на основі математичного апарату еліптичних кривих (Elliptic Curves – EC) з використанням відкритих ключів і випадкових повідомлень, що дозволяє встановити істинність твердження й при цьому не передавати будь-якої додаткової інформації про саме твердження. Криптографічні протоколи, засновані на доказі з нульовим розголошенням, дозволяють зробити процедури ідентифікації, обміну ключами та інші криптографічні операції без витоку секретної інформації протягом інформаційного обміну. Реалізація криптографічного протоколу доказу з нульовим розголошенням на основі математичного апарата еліптичних кривих дозволяє значно зменшити розмір параметрів протоколу й збільшити криптографічну стійкість (обчислювальну складність завдання злому). Безпека криптосистем на еліптичних кривих заснована на труднощах розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP). У роботі визначено повноту і коректність протоколу, надано приклад розрахунку, виконано моделювання криптографічного протоколу мовою High-Level Protocol Specification Language, виконано перевірку моделі і верифікацію протоколу. Програмна верифікація криптографічного*

протоколу ZKP EC була виконана за допомогою програмних модулів On the Fly Model Checker і Constraint Logic based Attack Searcher. Для перевірки криптографічного протоколу на стійкість до атак зловмисника були застосовані засоби пакету Security Protocol Animator для Automated Validation of Internet Security Protocols and Applications. Для реалізації криптографічного протоколу ZKP EC можна використовувати рекомендовані еліптичні криві згідно ДСТУ 4145-2002.

Ключові слова: *криптографічний протокол, еліптичні криві, ідентифікація, автентифікація, доказ із нульовим розголошенням, дискретне логарифмування в групах точок еліптичної кривої.*

The use of insecure communication channels opens the way for eavesdropping and other intruder activities. Therefore one of the basic tasks for the information security during the user communications is the use of the tools and techniques which let one party (the verifier) to check the authenticity of another (the prover), e.g. by checking whether the prover possesses some secret without disclosing the secret itself. This way there will be no leakage of sensitive information in the course of communication.

The purpose of the article is to develop a cryptographic authentication protocol with zero-knowledge secret based on the mathematics of elliptic curves the use of the public keys and random messages.

The zero-knowledge proof (ZKP) protocols [1–3] are executed in the form of a series of independent rounds, each consisting of the following steps:

1. $A \rightarrow B$: γ witness;
2. $A \leftarrow B$: y challenge;
3. $A \rightarrow B$: x response.

At the end of each round the verifier makes a decision on the proof validity. Some widely used cryptographic ZKP protocols are based on the asymmetric encryption, the most well known are Fiat-Shamir, Schnorr, Okamoto, Guillou-Quisquater, Brickell-McCurley, Feige-Fiat-Shamir [1–6]. The correctness and strength of these protocols is determined by the discrete logarithm problem over the finite prime field Z_n / Z_p and the number of verification rounds with different random values r and x.

Here we propose a cryptographic protocol with zero-knowledge secret based on elliptic curves (EC). The security of elliptic curves cryptography (ECC) [7–9] is mostly ensured by the infeasibility of the elliptic curve discrete logarithm problem (ECDLP) over the group of elliptic curve points [7, 10, 11]. Solving the ECDLP is even more complex than the DLP.

Cryptographic authentication protocol zero-knowledge secret on elliptic curves using public keys and random messages is show in Fig. 1.

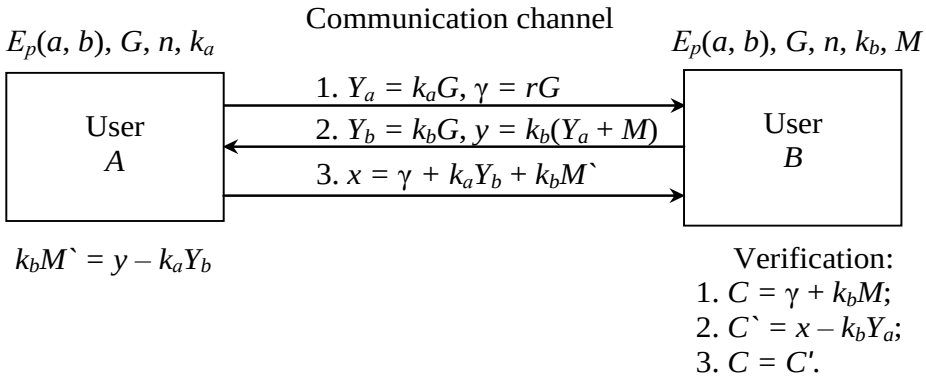

Figure 1 – Cryptographic authentication protocol zero-knowledge secret on elliptic curves using public keys and random messages

et $E_p(a,b)$ be the elliptic curve known to all users of information exchange; G – the pre-agreed base point on this curve (the generator); $\neq E_p(a,b) = n$ – the order of group $E_p(a,b)$. The user A chooses the private key k_a $(1 < k_a < n)$ and computes the corresponding public key $Y_a = k_aG$,

and transfers it to the user B together with the request $\gamma = rG$, where r is the random value $(1 < r < n)$. The user B chooses the private key k_b $(1 < k_b < n)$ and computes the corresponding public key $Y_b = k_b G$, and then forms a challenge $y = k_b(Y_a + M)$, where M is the random message. Y_b and y are transferred from user B to the user A. Next the user A computes the value $k_b M' = y - k_a Y_b$ and returns the response $x = \gamma + k_b M' + k_a Y_b$ to the user B. Finally, user B checks the equality $\gamma + k_b M = x - k_b Y_a$ or $C = \gamma + k_b M$, $C' = x - k_b Y_a$, $C = C'$.

Protocol completeness. The proving user A knows the value k_a, so they are able to answer any requests of the user B. The verifying user B is convinced in the relation validity:

$$\gamma + k_b M = x - k_b Y_a = \gamma + k_b M' + k_a Y_b - k_b Y_a = \gamma + k_b M' + k_a k_b G - k_b k_a G = \gamma + k_b M'.$$

Example. Let $E_{10007}(-3, 75)$; $G = (451, 3780)$; $n = 10099$; $p = 10007$, which corresponds to the curve $y^2 = x^3 - 3x + 75$. Suppose the user A chooses the private key $k_a = 9278$ and computes the public key $Y_a = 9278(451, 3780) = (5250, 8885)$.

User B chooses the private key $k_b = 7325$ and computes its public key $Y_b = 7325(451, 3780) = (8847, 8811)$.

Let us consider two rounds of the protocol.

First round.

1. User A sends its public key Y_a and the request γ to user B (the random $r = 10037$).

$$A \to B: Y_a = (5250, 8885),\ \gamma = 10037(451, 3780) = (4673, 254).$$

2. User B sends its public key Y_b and the challenge y back to the user A. To form the challenge y the user B generates a random point $M = (9888, 8538)$ on the elliptic curve $E_{10007}(-3, 75)$.

$$A \leftarrow B: Y_b = (8847, 8811),$$
$$y = 7325[(5250, 8885) + (9888, 8538)] = 7325(4149, 9409) = (3334, 3507).$$

3. User A computes the value $k_b M'$ and sends a response x to the user B.

$$k_b M' = (3334, 3507) - 9278(8847, 8811) = (3334, 3507) - (9601, 3320) = (9869, 6063).$$
$$A \to B: x = (4673, 254) + (9869, 6063) + 9278(8847, 8811) =$$
$$= (6556, 7696) + (9601, 3320) = (9646, 1970).$$

4. User B performs the verification:

$$C = (4673, 254) + 7325(9888, 8538) = (4673, 254) + (9868, 6063) = (6556, 7696).$$
$$C' = (9646, 1970) - 7325(5250, 8885) = (9646, 1970) - (9601, 3320) = (6556, 7696).$$
$$C = C' = (6556, 7696) \text{ – verification completed.}$$

Second round.

1. User A sends its public key Y_a and the request γ to user B (the random $r = 3112$).

$$A \to B: Y_a = (5250, 8885),\ \gamma = 3112(451, 3780) = (1866, 6503).$$

2. User B sends its public key Y_b and the challenge y back to the user A. To form the challenge y the user B generates a random point $M = (1480, 949)$ on the elliptic curve $E_{10007}(-3, 75)$.

$$A \leftarrow B: Y_b = (8847, 8811),$$
$$y = 7325\left[(5250, 8885) + (1480, 949)\right].$$
$$= 7325(6271, 5975) = (3819, 6973)$$

3. User A computes the value $k_b M'$ and sends a response x to the user B.

$$k_b M' = (3819, 6973) - 9278(8847, 8811) = (3819, 6973) - (9601, 3320) = (3483, 2872).$$
$$A \rightarrow B: x = (1866, 6503) + (3483, 2872) + 9278(8847, 8811) =$$
$$= (5387, 8505) + (9601, 3320) = (247, 932).$$

4. User B performs the verification:

$$C = (1866, 6503) + 7325(1480, 949) = (1866, 6503) + (3483, 2872) = (5387, 8508).$$
$$C' = (247, 932) - 7325(5250, 8885) = (247, 932) - (9601, 3320) = (5387, 8508).$$
$$C = C' = (5387, 8508) \text{ – verification completed.}$$

In order to test the resistance of the proposed ZKP EC cryptographic protocol to the intruder attacks, we used the software package AVISPA (Automated Validation of Internet Security Protocols and Applications) [14]. The major advantage of AVISPA is the ability not only to check the protocol for defects, but also to find the possible attacks for this protocol. AVISPA uses the high-level protocol specification language (HLPSL) which broadens the class of studied protocols substantially, and lets one integrate multiple distinct methods into a single platform [5, 14] (Fig. 2).

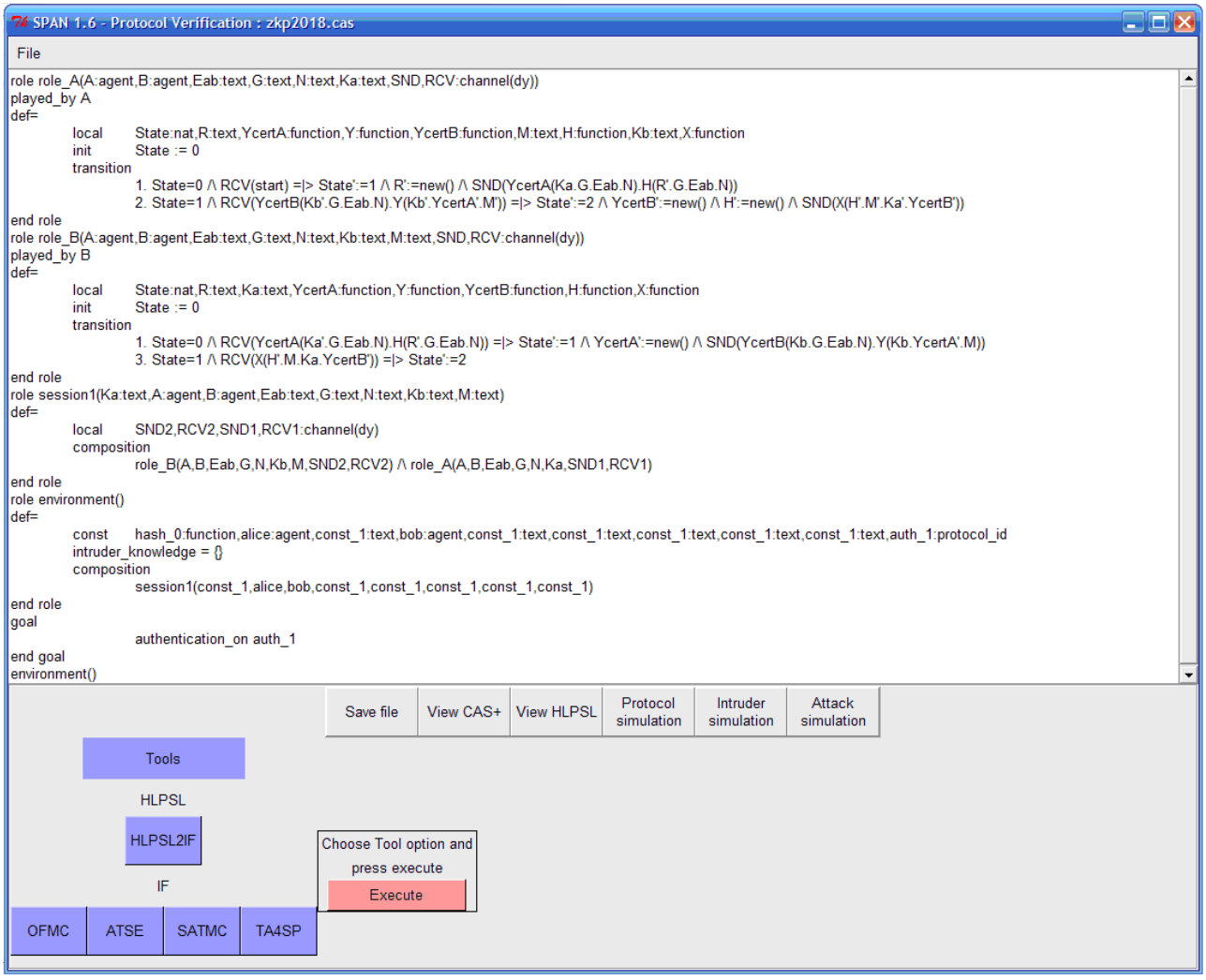

Figure 2 – A model of the ZKP EC protocol in HLPSL

We performed a verification of the proposed cryptographic ZKP EC protocol using the protocol simulation package SPAN (Security Protocol Animator) [15] (Figs. 3, 4).

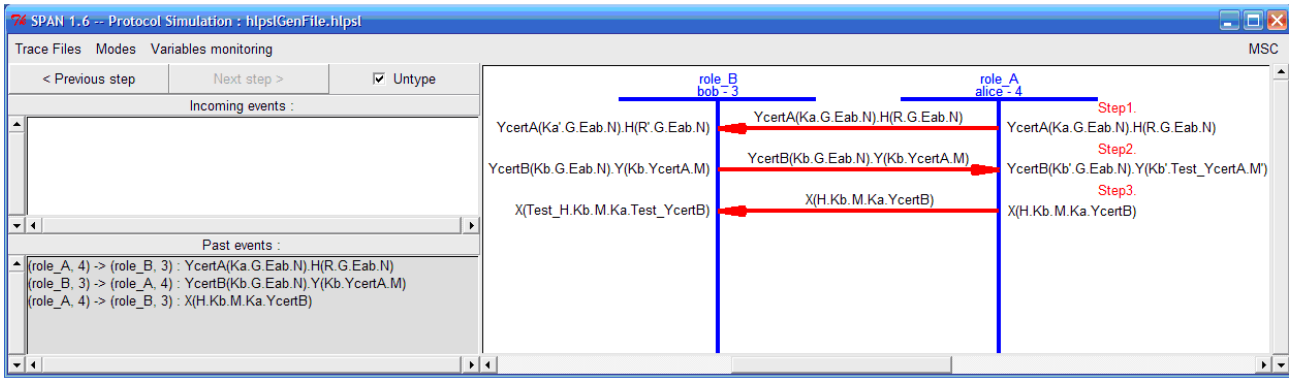

Figure 3 – Simulation of the ZKP EC protocol

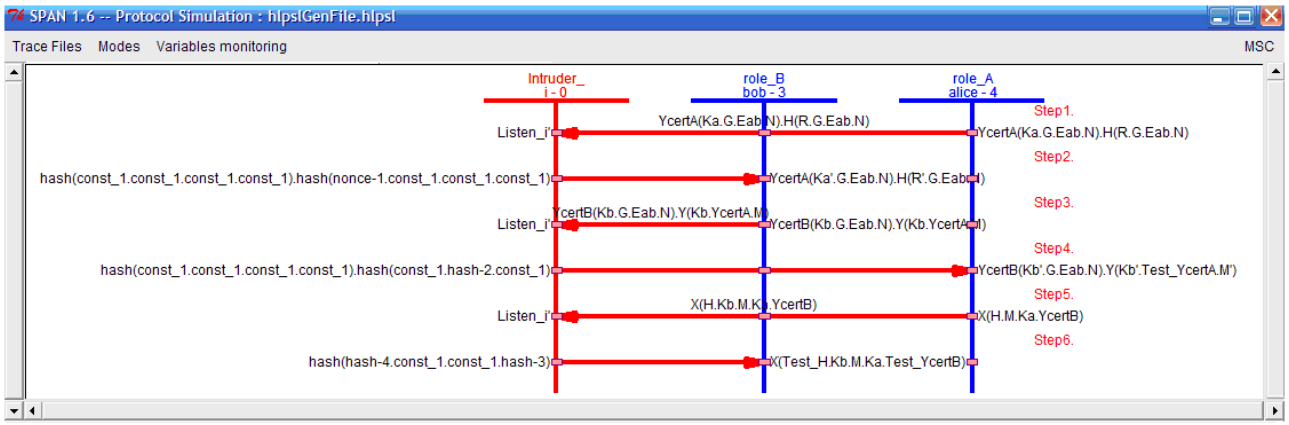

Figure 4 – Simulation of the intruder attack on the ZKP EC protocol

The software verification of the cryptographic ZKP EC protocol and its resistance to attacks was performed using the software modules OFMC (On the Fly Model Checker) and CLAtSe (Constraint Logic based Attack Searcher) [16] (Fig. 5).

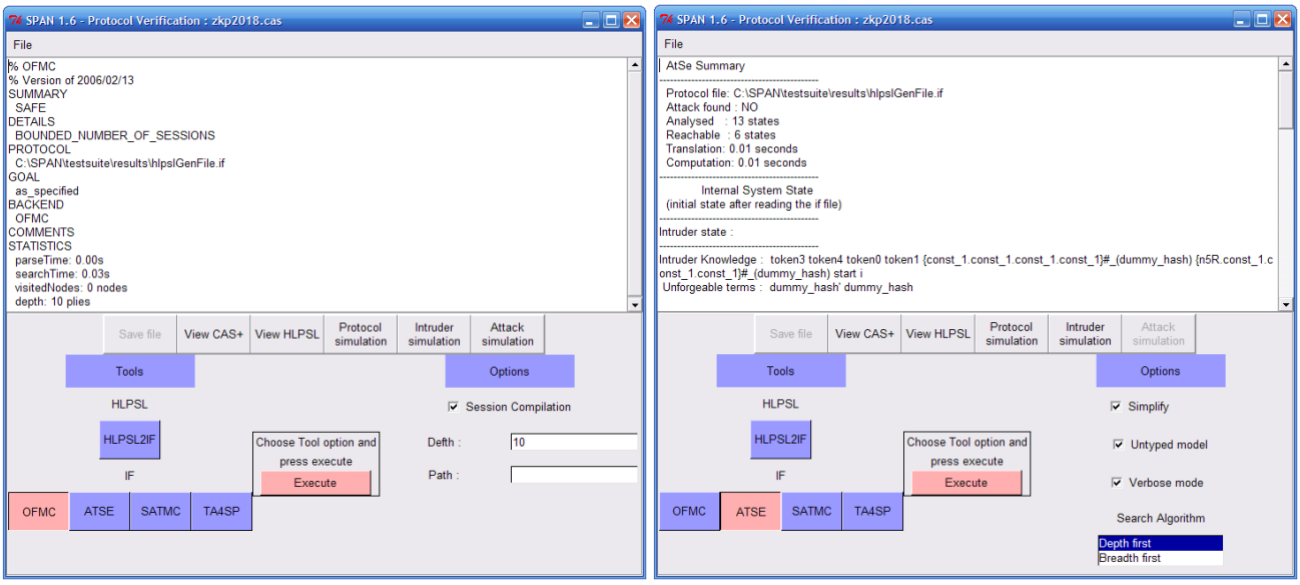

Figure 5 – Verification of the ZKP EC protocol and its resistance to attacks

The verification of the proposed cryptographic ZKP EC protocol did not reveal any existing attacks for this protocol.

The cryptographic protocols based on zero-knowledge proof allow to perform the

authentication, key exchange and other cryptographic operations without the leakage of sensitive information during the information exchange. In the present paper we proposed a cryptographic authentication protocol with zero-knowledge secret based on the mathematics of the elliptic curves together with the use of public keys and random messages. The recommended elliptical curves according to DSTU 4145-2002 may be used to implement the ZKP EC cryptographic protocol [17].

We determined the completeness and the correctness of the protocol, gave an example of the computation and performed the protocol simulation and verification. To test the resistance of the ZKP EC protocol to the intruder attacks we used the SPAN package for AVISPA. The test did not reveal any known attacks to the ZKP EC protocol. So the intruder is only able to access the information by solving the ECDLP. In addition, the complexity of the transformation in the Abelian group is estimated as $O\left(\log^2 p\right)$, while in the multiplicative group of the field it is $O\left(\log^3 p\right)$, so the advantage of EC is obvious. Thus, the use of the cryptographic ZKP EC protocol enables to reduce the size of the protocol parameters, increases the cryptographic strength and reduces the authentication time.

REFERENCES

1 Молдовян А.А. и А.Б. Левина. Протоколы аутентификации с нулевым разглашением секрета / А.А. Молдовян, А.Б. Левина // –СПб: Университет ИТМО. –2016.

2 Menezes, A., P. van Oorschot, and S.Vanstone *Handbook of Applied Cryptography.* CRC Press, 1996.

3 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты языке СИ – М.: Триумф, –2002. – 816 с.

4 Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин// – М.: ДМК Прес, –2002. – 656 с.

5 Черемушкиін А. В. Криптографические протоколы. Основные свойства и уязвимости / А. В. Черемушкін – М.: Академія, – 2009. – 272 с.

6 Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности / Запечников С. В. – М.: Горячая лінія-Телеком, – 2007. – 320 с.

7 Hankerson D. Guide to Elliptic Curve Cryptography / Hankerson D., Menezes A., Vanstone S. – Springer-Verlag, 2004. – 358 p.

8 Болотов А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А. А. Болотов, С. Б. Гашков, А. Б. Фролов// – М.: КомКніга. –2006. – 328 с.

9 Болотов А. А. Элементарное введение в эллиптическую криптографиію: Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКниіга. –2006. – 280 с.

10 Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / Василенко О. Н. –М.: МЦНМО, – 2003. – 328 с.

11 Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – М.: Професіонал. –2005. – 490 с.

12 Молдовян Н. А. Криптография: от примеров к синтезу алгоритмов / Н. А. Молдовян, А.А. Молдовян, М.А. Еремеев. – SPb.: BHV-Петербург, –2004. – 448 с.

13 An Elliptic Curve Cryptography (ECC). Primer why ECC is the next generation of public key cryptography. The Certicom ‘Catch the Curve’ White Paper Series, June 2004. – 24 с.

14 AVISPA [Електронний ресурс]. – Режим доступу: http://www.avispa-project.org/.

15 *SPAN* –Security Protocol Animator [Електронний ресурс]. - Режим доступа: http://people.irisa.fr/Thomas.Genet/ span /.

16 An On-The-Fly Model-Checker for Security Protocol Analysis [Електронний ресурс]. – Режим доступу: http://www.avispa-project.org/papers/ofmc-esorics03.pdf.

17 ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка [Електронний ресурс]. - Режим доступа: http://itender-online.ru/help/dstu-4145-2002.pdf.

REFERENCES

1 Moldovyan A.A., D.N. Moldovyan, and A.B. Levina. *Protokoly autentifikaczii s nulevym razglasheniem sekreta (Zero-Secret Authentication Protocols).* SPb: Universitet ITMO, 2016.

2 Menezes, A., P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

3 Shnajer, B. *Prikladnaja kriptografija. Protokoly, algoritmy, ishodnye teksty na jazyke Si (*Applied cryptography.

Protocols, algorithms, source codes C language*).* M.: Triumf, 2002.

4 Sokolov, A. V., and V. F. Shan'gin. *Zashhita informacii v raspredelennyh korporativnyh setjah i sistemah (*Information security in distributed corporate networks and systems*).* M.: DMK Press, 2002.

5 Cheremushkin, A. V. *Kriptograficheskie protokoly. Osnovnye svojstva i ujazvimosti (*Cryptographic protocols. Key features and vulnerabilities*).* M.: Akademija, 2009.

6 Zapechnikov, S. V. *Kriptograficheskie protokoly i ih primenenie v finansovoj i kommercheskoj dejatel'nosti (*Cryptographic protocols and their application in financial and commercial activities*).* M.: Gorjachaja linija-Telekom, 2007.

7 Hankerson, D., A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography* Springer-Verlag, 2004.

8 Bolotov, A. A., S. B. Gashkov, and A. B. Frolov *Elementarnoe vvedenie v ellipticheskuju kriptografiju: Algebraicheskie i algoritmicheskie osnovy (An Elementary Introduction to Elliptic Cryptography: Algebraic and Algorithmic Foundations).* M.: KomKniga, 2006.

9 Bolotov, A. A., Gashkov S. B., and Frolov A. B. *Elementarnoe vvedenie v ellipticheskuju kriptografiju: Protokoly kriptografii na jellipticheskih krivyh (An Elementary Introduction to Elliptic Cryptography: Elliptic Curve Cryptography Protocols).* M.: KomKniga, 2006.

10 Vasilenko, O. N., *Teoretiko-chislovye algoritmy v kriptografii (*Numerical Algorithms in Cryptography*).* M.: MCNMO, 2003.

11 Rostovcev A. G., E. B. Mahovenko. *Teoreticheskaja kriptografija* (Theoretical cryptography). M.: Professional, 2005.

12 Moldovjan, N. A., Moldovjan A. A., and Eremeev M. A. *Kriptografija: ot primitivov k sintezu algoritmov (*Cryptography: from examples to the synthesis of algorithms*).* SPb.: BHV-Peterburg, 2004.

13 *An Elliptic Curve Cryptography (ECC). Primer why ECC is the next generation of public key cryptography*. The Certicom 'Catch the Curve' White Paper Series, June 2004.

14 *AVISPA. avispa-project,* http://www.avispa-project.org/.

15 *SPAN (Security Protocol Animator).* http://people.irisa.fr/Thomas.Genet/span/.

16 Basin, David, Sebastian Modersheim, and Luca Vigano. "An On-The-Fly Model-Checker for Security Protocol Analysis." *avispa-project*, http://www.avispa-project.org/papers/ofmc-esorics03.pdf.

17 DSTU 4145-2002. Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Tsyfrovyy pidpys, shcho gruntuyet′sya na eliptychnykh kryvykh. Formuvannya ta perevirka (Information Technology. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification) http://itender-online.ru/help/dstu-4145-2002.pdf.