УДК: 004.056.55: 003.26

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С ИСПОЛЬЗОВАНИЕМ ОДНОСТОРОННЕЙ ХЭШ-ФУНКЦИИ

ОНАЦКИЙ А.В.[1], ЖАРОВА О.В.[2]

[1] Одесская национальная академия связи им. А.С. Попова,
ул. Кузнечная, 1, Одесса, 65029, Украина
onatsky@mail.ru
[2] Одесский национальный политехнический университет,
просп. Шевченко, 1, г. Одесса, 65044, Украина,
kseniazharova@mail.ru

КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ДОКАЗУ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ НА ЕЛІПТИЧНИХ КРИВИХ З ВИКОРИСТАННЯМ ОДНОСТОРОННЬОЇ ГЕШ-ФУНКЦІЇ

ОНАЦЬКИЙ О.В.[1], ЖАРОВА О.В.[2]

[1] Одеська національна академія зв'язку ім. О.С. Попова,
вул. Кузнечна, 1, Одеса, 65029, Україна
onatsky@mail.ru
[2] Одеський національний політехнічний університет
просп. Шевченка, 1, м. Одеса, 65044, Україна
kseniazharova@mail.ru

CRYPTOGRAPHIC PROTOCOL ZERO-KNOWLEDGE PROOF ON ELLIPTIC CURVES USING ONE-WAY HASH FUNCTION

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

[1] O.S. Popov Odessa national academy of telecommunications,
Kuznechna st.,1 , Odessa 65029, Ukraine.
onatsky@mail.ru
[2] Odessa national polytechnic university,
Shevchenko Ave., 1, Odessa, 65044, Ukraine.
kseniazharova@mail.ru

Аннотация. *Предложен криптографический протокол доказательства с нулевым разглашением на эллиптических кривых с использованием односторонней хэш-функции, позволяющий установить истинность утверждения и при этом не передавать какой-либо дополнительной информации о самом утверждении.*

Ключевые слова: *криптографический протокол, эллиптические кривые, идентификация, аутентификация, доказательство с нулевым разглашением, односторонняя хэш-функция.*

Анотація. *Запропоновано криптографічний протокол доказу із нульовим розголошенням на еліптичних кривих з використанням односторонньої геш-функції, що дозволяє установити істинність твердження й при цьому не передавати будь-якої додаткової інформації про саме твердження.*

Ключові слова: *криптографічний протокол, еліптичні криві, ідентифікація, автентифікація, доказ із нульовим розголошенням, одностороння геш-функція.*

Abstract. *Proposed cryptographic protocol with zero-knowledge proof on elliptic curves using one-way hash function, allowing to establish the truth of allegation and does not convey any additional information about the approval.*

Key words: *cryptographic protocol, elliptic curves, identification, authentication, zero-knowledge proof, one-way hash function.*

Применение открытых каналов передачи данных создаёт потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспече-

ния информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. В протоколах типа «запрос–ответ» (challenge–response) нарушитель, контролируя канал связи, может навязывать специально подобранные запросы и, анализируя ответы, получать информацию о секрете. Чтобы избежать этого, применяют протоколы доказательства знания, которые реализованы на основе модульных преобразований в полях Галуа, и обладают дополнительным свойством нулевого разглашения секрета [1, 2]. С развитием методов и средств криптоанализа, а также быстрого развития технологий и мощности вычислительных компьютерных систем, возникает необходимость увеличивать размеры общесистемных параметров протокола, вследствие чего увеличивается ресурсоёмкость и сложность выполнения базовых операций в полях. Однако решение данного вопроса может быть достигнуто за счёт реализации криптографических протоколов доказательства с нулевым разглашением на основе математического аппарата эллиптических кривых и с использованием односторонней хэш-функции, что позволяет значительно уменьшить размер параметров протокола и увеличить криптографическую стойкость (вычислительную сложность задачи взлома).

Целью статьи является разработка криптографических протоколов доказательства с нулевым разглашением на основе математического аппарата эллиптических кривых.

Прежде чем получить доступ к ресурсам системы, пользователь должен пройти процесс первичного взаимодействия с системой, который включает идентификацию и аутентификацию [3]. Протоколы идентификации и аутентификации можно рассматривать как вид интерактивного доказательства знания. Интерактивное доказательство (interactive proof) – понятие теории сложности вычислений, составляющее основу понятия доказательства с нулевым разглашением (zero-knowledge proof – ZKP) [4, 5]. Интерактивное доказательство проводится путем выполнения протокола с двумя участниками, доказывающим и проверяющим. Участники обмениваются сообщениями (запросами и ответами), обычно зависящими от случайных чисел, которые могут содержаться в секрете. Цель доказывающего – убедить проверяющего в истинности некоторого утверждения. Проверяющий либо принимает, либо отвергает доказательство. В криптографических протоколах с нулевым разглашением доказательство имеет вероятностный характер. Если доказываемое утверждение, верно, то доказательство должно быть справедливым с вероятностью, стремящейся к единице при увеличении числа циклов протокола. Если же доказываемое утверждение ложно, то при увеличении числа циклов протокола вероятность правильности доказательства должна стремиться к нулю [5, 6].

Протокол интерактивного доказательства должен учитывать возможность обмана со стороны обоих участников. Если участник A (доказывающий) на самом деле не знает доказываемого утверждения (либо от имени участника A выступает кто-либо другой), то участник B (проверяющий) должен обнаружить факт обмана. Поэтому доказательство знания характеризуется тремя свойствами: полнотой, корректностью и нулевым разглашением [4, 5].

Протоколы доказательства выполняют в виде последовательности независимых циклов (раундов), каждый из которых состоит из трёх шагов определённого вида.

1. $A \rightarrow B$: γ свидетельство (заявка) – witness.
2. $A \leftarrow B$: y запрос – challenge.
3. $A \rightarrow B$: x ответ – response.

Эти шаги образуют один цикл протокола, называемый аккредитацией. После выполнения каждого цикла проверяющий принимает решение об истинности доказательства.

Широкое распространение при идентификации получили криптографические протоколы ZKP на базе ассиметричного шифрования, наиболее известными являются: Fiat–Shamir, Schnorr, Okamoto, Guillou–Quisquater, Brickell–McCurley, Feige–Fiat–Shamir [1 … 3, 5, 6].

Корректность и стойкость данных протоколов определяется дискретным логарифмированием (Discrete Logarithm Problem – DLP) в простом конечном поле Z_n/Z_p, а также увеличе-

нием количества циклов аккредитации при разных случайных значениях *r* и *x*.

В работе предложен криптографический протокол доказательства знания с нулевым разглашением на основе эллиптических кривых (Elliptic Curves – EC).

Криптосистемы на эллиптических кривых (Elliptic Curves Cryptography – ECC) [7 … 9] относятся к классу криптосистем с открытым ключом. Безопасность ECC, как правило, основана на трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой (Elliptic Curve Discrete Logarithm Problem – ECDLP) [7, 10, 11]. Решение проблемы ECDLP является более сложным, чем решение проблемы DLP. В этом заключается основная причина преимущества использования ECC, которые обеспечивают такой же уровень стойкости при использовании чисел меньшего размера по сравнению с более традиционными криптосистемами, надёжность которых заключается в сложности задачи факторизации или DLP в конечном поле. Соответственно, при использовании чисел одинаковой размерности, уровень стойкости криптосистем на эллиптических кривых значительно выше. Многочисленные исследования показали [10 … 12], что криптосистемы на основе эллиптических кривых превосходят другие системы с открытым ключом по двум важным параметрам: степени защищённости в расчёте на каждый бит ключа и быстродействию при программной и аппаратной реализации.

В ECC используется уравнение вида $y^2\left(x^3+ax+b\right)\bmod p$, где $a,b\in GF\left(p\right)$, $(4a^3+27b^2)\bmod p\neq 0, p>3$ – простое. Множество $E_p\left(a,b\right)$ состоит изо всех точек $\left(x,y\right)$, $x\geq 0, p>y$, удовлетворяющих уравнению $y^2\equiv\left(x^3+ax+b\right)\bmod p$, и бесконечно удалённой точки *O*. Для точек на эллиптической кривой вводится операция сложения, которая может быть описана следующим образом.

1. $P+O=O+P=P$.

2. Если $P=\left(x,y\right)$, то $P+\left(x,-y\right)=O$. Точка $\left(x,-y\right)$ является отрицательным значением точки *P* и обозначается *–P*.

3. Если $P=\left(x_1,y_1\right)$ и $Q=\left(x_2,y_2\right)$, то $Q=\left(x_2,y_2\right)$ определяется в соответствии с правилами

$$x_3=(\lambda^2-x_1-x_2)\bmod p; \tag{1}$$

$$y_3=[\lambda\left(x_1-x_3\right)-y_1]\bmod p, \tag{2}$$

где

$$\lambda\equiv\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}\left(\bmod\ p\right), & \text{если}\quad P\neq Q;\\ \dfrac{3x_1^2+a}{2y_1}\left(\bmod\ p\right), & \text{если}\quad P=Q.\end{cases}$$

Число λ – угловой коэффициент секущей, проведённой через точки $P=\left(x_1,y_1\right)$ и $Q=\left(x_2,y_2\right)$. При $P=Q$ секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ.

Количество точек, принадлежащих эллиптической кривой, называется рангом кривой. Рангом точки $P\in E$ называется такое минимальное целое положительное число *n*, что $nP=O$. Ранг точки определяет порядок группы точек эллиптической кривой, с которыми осуществляются криптографические преобразования [7 … 9].

С помощью описанных выше правил сложения можно вычислить точку *kP* для любого целого числа *k* и любой точки *P* эллиптической кривой. Однако решение обратной задачи –

нахождение числа k по известным точкам P и kP – является трудноразрешимой проблемой – ECDLP. Сложность решения проблемы ECDLP обусловлена ресурсоёмкостью операций сложения и дублирования точек, с помощью которых вычисляется kP, как видно из приведённых выше формул. Отсюда следует возможность применения более коротких ключей (табл. 1) [13].

Таблица 1 – Размер ключей для ECC и RSA согласно NIST

ECC key, Bits	RSA key, Bits	Key ratio
163	1024	1 : 6
256	3072	1 : 12
384	7680	1 : 20
512	15360	1 : 30

Криптографический протокол доказательства с нулевым разглашением на основе эллиптических кривых с использованием односторонней хэш-функции (рис. 1). Пусть $E_p(a,b)$ – эллиптическая кривая, известная участникам информационного процесса; G – предварительно согласованная и опубликованная точка этой кривой; MD5 – односторонняя хэш-функция. Абонент A выбирает секретный ключ $k_a\,(1<k_a<n)$ и вычисляет значения открытого ключа $Y_a=k_aG$, который передаёт абоненту B вместе с заявкой γ. Абонент B выбирает сессионный ключ $k_b\,(1<k_b<n)$ и вычисляет два значения $y_1=k_bG, y_2=k_bY_a+M$, где M – случайное сообщение. Абоненту B передаются абоненту A – y_1, y_2. Абонент A вычисляет $M`=y_2-k_ay_1$ и передаёт хэш-функцию $h(M`)$ абоненту B. Абонент B проверяет равенство $h(M)=h(M`)$.

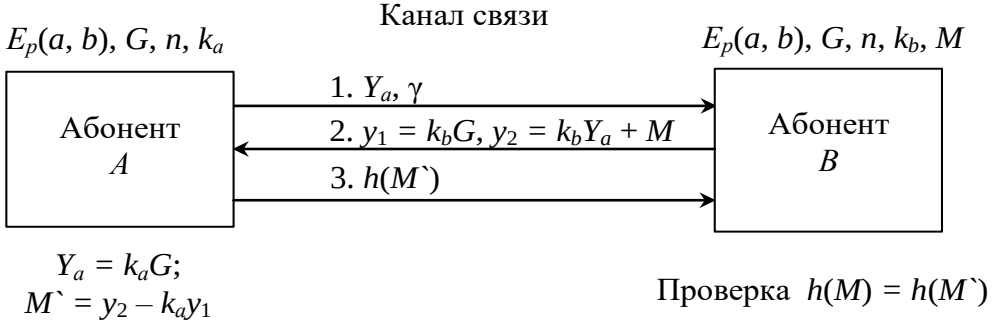

Рисунок 1 – Криптографический протокол доказательства с нулевым разглашением на основе эллиптических кривых с использованием односторонней хэш-функции

Полнота протокола. Доказывающий A знает значения k_a, поэтому он в состоянии ответить на любые запросы абонента B. При этом проверяющий B убеждается в справедливости соотношения

$$M`=y_2-k_ay_1=k_bY_a+M-k_ak_bG=k_bk_aG+M-k_ak_bG=M\,.$$

Пример. Пусть $E_{31991}(-3,130); G=(1,12510); n=31859; p=31991$, что соответствует кривой $y^2=x^3-3x+130$. Предположим, что абонент A выбирает секретное число $k_a=2347$ и вычисляет значения открытого ключа $Y_a=2347(1,12510)=(25097,2812)$.

Рассмотрим два цикла протокола.

Первый цикл протокола.

1. Абонент A отправляет открытый ключ Y_a и заявку γ абоненту B

$A \to B: Y_a = (25097, 2812),\ \gamma = 1.$

2. Абонент *B* выбирает случайное сообщение $M = (20094, 20680)$ и сессионный ключ $k_b = 31105$. Вычисляет значения y_1 и y_2, которые отправляет абоненту *A*

$A \leftarrow B: y_1 = 31105(1, 12510) = (31138, 17196),$

$y_2 = 31105(25097, 2812) + (20094, 20680) = 15796, 11509) + (20094, 20680) = (26922, 13593)$.

3. Абонент *A* вычисляет *M`* и передаёт хэш-функцию *h*(*M`*) абоненту *B*

$A \to B: M` = (26922, 13593) - 2347(31138, 17196) = (26922, 13593) - (15796, 11509) = (20094, 20680),$

$h(100111001111110.10100001100100) = 9480ce799a0456675771d4c1d9a2c34c.$

Абонент *B* выполняет проверку

$h(M) = h(M`) = h(100111001111110.10100001100100) = 9480ce799a0456675771d4c1d9a2c34c$ –

– проверка выполнена.

Второй цикл протокола.

1. Абонент *A* отправляет открытый ключ Y_a и заявку γ абоненту *B*

$A \to B: Y_a = (25097, 2812),\ \gamma = 1.$

2. Абонент *B* выбирает случайное сообщение $M = (14000, 30002)$ и сессионный ключ $k_b = 9148$. Вычисляет значения y_1 и y_2, которые отправляет абоненту *A*

$A \leftarrow B: y_1 = 9148(1, 12510) = (14774, 7451)$,

$y_2 = 9148(25097, 2812) + (14000, 30002) = (28106, 27452) + (14000, 30002) = (21025, 14036).$

3. Абонент *A* вычисляет *M`* и передаёт хэш-функцию $h(M`)$ абоненту *B*

$A \to B: M` = (21025, 14036) - 2347(14774, 7451) = (21025, 14036) - (28106, 27452) = (14000, 30002),$

$h(11011010110000.111010100110010) = 4da9dfba9dd356a69ea45fc95734b0bd$.

Абонент *B* выполняет проверку

$h(M) = h(M`) = h(11011010110000.111010100110010) = 4da9dfba9dd356a69ea45fc95734b0bd$ –

проверка выполнена.

Для анализа предложенного криптографического протокола ZKP EC на устойчивость к атакам противника был применён программный продукт AVISPA (Automated Validation of Internet Security Protocols and Applications) [14]. Главное преимущество AVISPA, состоит в том, что её применение позволяет не только определить, есть ли недостатки у конкретного протокола, но и найти атаки на данный протокол, если это возможно. AVISPA использует язык HLPSL (High-Level Protocol Specification Language), что позволяет существенно расширить класс изучаемых протоколов, а также интегрировать в единую платформу сразу несколько различных методов [5, 14] (рис. 2).

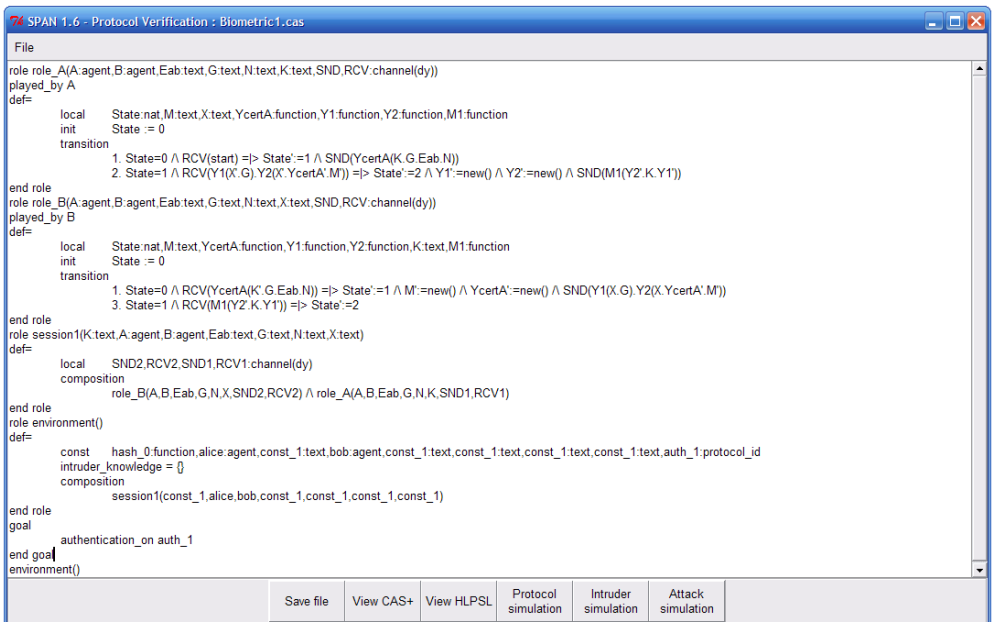

Рисунок 2 – Моделирование протокола ZKP EC на языке HLPSL

Выполнена проверка модели предложенного криптографического протокола ZKP EC с помощью Protocol Simulation пакета SPAN (Security Protocol Animator) [15] (рис. 3).

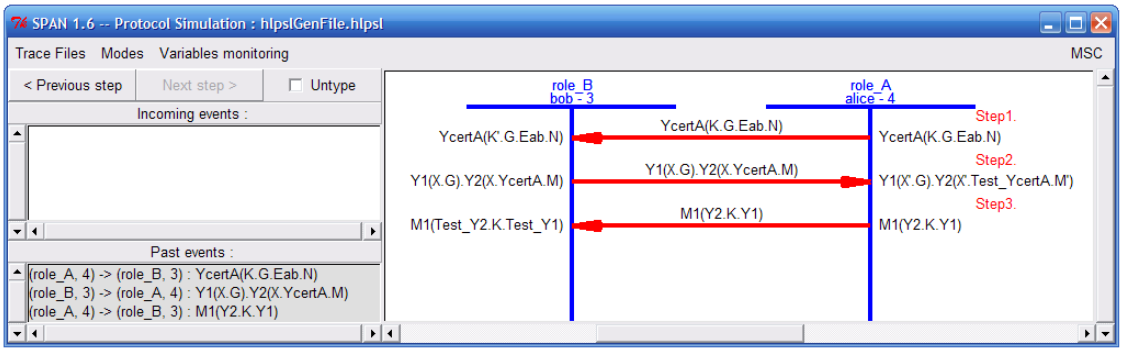

Рисунок 3 – Моделирование протокола ZKP EC

Программная верификация криптографических протоколов и устойчивость протоколов к атакам противника была выполнена с помощью программных модулей OFMC (On-the-Fly Model-Checker) и CLAtSe (CL-based Attack Searcher) AVISPA [16] (рис. 4). В результате проверки предложенного криптографического протокола ZKP EC известных атак на протокол не найдено.

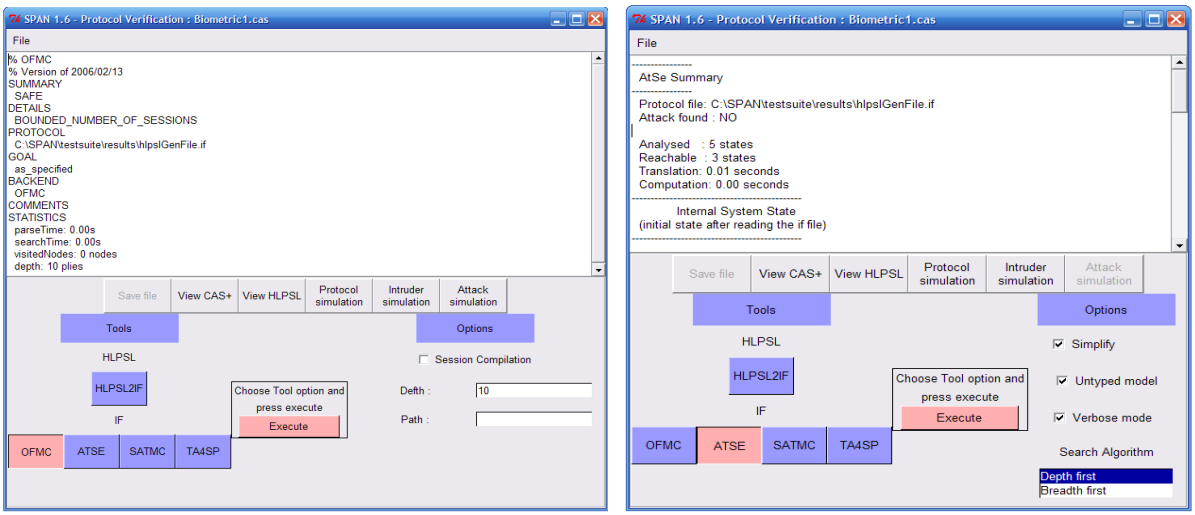

Рисунок 4 – Верификация и устойчивость протокола ZKP EC к атакам

Криптографические протоколы, основанные на доказательстве с нулевым разглашением, позволяют произвести процедуры идентификации, обмена ключами и другие криптографические операции без утечки секретной информации в течение информационного обмена. В работе предложен криптографический протокол доказательства с нулевым разглашением на основе математического аппарата эллиптических кривых. Для реализации протокола ZKP EC можно использовать рекомендованные эллиптические кривые согласно ДСТУ 4145-2000 [17] и хэш-функцию ГОСТ 34.311-95 [18].

В работе определена полнота и корректность протокола, приведён пример расчёта, выполнена проверка модели и верификация протокола. Для проверки криптографического протокола ZKP EC на устойчивость к атакам противника были применены средства пакета SPAN для AVISPA. В результате проверки протокола ZKP EC известных атак на протокол не найдено. Злоумышленник может получить доступ к информации, только решив задачу ECDLP. Кроме того, сложность выполнения преобразования в абелевой группе на EC оценивается величиной $O(\log^2 p)$, а в мультипликативной группе поля – $O(\log^3 p)$, преимущество использования EC очевидно. Следовательно, при использовании криптографического протокола ZKP EC позволит уменьшить размеры параметров протокола, увеличить криптографическую стойкость, уменьшить длительность процесса идентификации.

ЛИТЕРАТУРА

1 Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.

2 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Шнайер Б. – М.: Триумф, 2002. – 816 с.

3 Соколов А. В. Защита информации в распределённых корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

4 Погорелов Б. А. Словарь криптографических терминов / Б. А. Погорелов, В. Н. Сачков. – М.: МЦНМО, 2006. – 91 с.

5 Черемушкин А. В. Криптографические протоколы. Основные свойства и уязвимости / Черемушкин А. В. – М.: /Академия/, 2009. – 272 с.

6 Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности / Запечников С. В. – М.: Горячая линия-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 / Болотов А. А., Гашков С. Б. , Фролов. А. Б. – М.: КомКнига, 2006. – 328 с.

9 Болотов А. А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / Болотов А. А. ,. Гашков С. Б, Фролов А. Б. – М.: КомКнига, 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.: Профессионал, 2005. – 490 с.

12 Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов/ Молдовян Н. А. ,Молдовян А. А., Еремеев М. А. . – СПб.: БХВ-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. [Электронный ресурс]. – Режим доступа: http://www.avispa-project.org/.

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

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

17 ДСТУ 4145-2002. [Электронный ресурс]. – Режим доступа: http://itender-online.ru/help/dstu-4145-2002.pdf.

18 ГОСТ 34.311-95. [Электронный ресурс]. – Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=132760.

REFERENCES

1 Menezes A., P. van Oorschot and S. Vanstone. Handbook of applied cryptography. CRC Press, 1996. Print.

2 Schneider B. Applied cryptography: Protocols, algorithms, and source code in C. Moscow: Triumph, 2002. Print.

3 Sokolov A.V. and V.F. Shan'gin. Information protection in distributed corporate networks and systems. Moscow: DMK Press, 2002. Print.

4 Pogorelov B. A. Glossary of cryptographic terms. Moscow: MCCME, 2006. Print.

5 Cheremushkin A.V. Cryptographic protocols. Basic properties and vulnerabilities. Moscow: «Academy», 2009. Print.

6 Zapechnikov S.V. Cryptographic protocols and their application in the financial and commercial activities. Moscow: Hot line-Telecom, 2007. Print.

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

8 Bolotov A.A., S.B. Gashkov and A.B. Frolov. An elementary introduction to elliptic curve cryptography: Algebraic and algorithmic foundations. Moscow: ComBook, 2006. Print.

9 Bolotov A.A., S.B. Gashkov and A.B. Frolov. An elementary introduction to elliptic curve cryptography: Cryptographic protocols on elliptic curves. Moscow: ComBook, 2006. Print.

10 Vasilenko O.N. Number-theoretic algorithms in cryptography. Moscow: MCCME, 2003. Print.

11 Rostovtsev A.G. and E.B. Makhovenko. Theoretical cryptography. Moscow: Professional, 2005. Print.

12 Moldovyan N.A., N.A. Moldovyan and M.A. Eremeev. Cryptography: from primitive to the synthesis algorithms. Saint Petersburg: BHV-Petersburg, 2004. Print.

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. 1–24. Print.

14 "AVISPA". Web. <http://www.avispa-project.org/>.

15 "Security Protocol Animator". Web. <http://people.irisa.fr/Thomas.Genet/span/>.

16 "An On-The-Fly Model-Checker for Security Protocol Analysis". Web. <http://www.avispa-project.org/papers/ofmc-esorics03.pdf>.

17 GOST 4145-2002. Web. <http://itender-online.ru/help/dstu-4145-2002.pdf>.

18 GOST 34.311-95. Web. <http://protect.gost.ru/document.aspx? control=7&id=132760>.