УДК: 004.056.55: 003.26

ПАРАЛЛЕЛЬНАЯ СХЕМА ИДЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Онацкий А.В.
Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
onatsky@mail.ru

ПАРАЛЕЛЬНА СХЕМА ІДЕНТИФІКАЦІЇ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ НА ЕЛІПТИЧНИХ КРИВИХ

Онацький О.В.
Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Ковальська, 1.
onatsky@mail.ru

PARALLEL CIRCUIT IDENTIFICATION WITH ZERO-KNOWLEDGE ON ELLIPTIC CURVES

Onatskiy A.V.
O.S. Popov Odessa national academy of telecommunications,
1 Kovalska St., Odessa, 65029, Ukraine.
onatsky@mail.ru

Аннотация. Предложен протокол идентификации с нулевым разглашением на эллиптических кривых, 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.

Анотація. Запропоновано протокол ідентифікації із нульовим розголошенням на еліптичних кривих, 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.

Abstract. Proposed identification protocol with zero-knowledge on elliptic curves allows 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.

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечения 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 ресурсоемкость и сложность выполнения базовых операций в полях. Однако решение данного вопроса может быть достигнуто за счет реализации криптографических протоколов доказательства с нулевым разглашением на основе математического аппарата

эллиптических кривых, что позволяет значительно уменьшить размер параметров протокола и увеличить криптографическую стойкость (вычислительную сложность задачи взлома).

Целью статьи является разработка параллельной схемы идентификации доказательства знания с нулевым разглашением на основе 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 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 [4, 5].

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 нулевое разглашение [4, 5].

Протоколы доказательства выполняют в виде последовательности независимых циклов (раундов), каждый из которых состоит из трех шагов определенного вида:

1. $A \rightarrow B$: γ свидетельство (заявка) – witness.
2. $A \leftarrow B$: x запрос – challenge.
3. $A \rightarrow B$: y 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 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 увеличением количества циклов аккредитации при разных случайных значениях r и x.

В статье предложена параллельная схема идентификации 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, надежность 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, 11], что криптосистемы на основе эллиптических кривых превосходят другие системы с открытым ключом по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при программной и аппаратной реализации.

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

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

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

3. Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ определяется в соответствии с правилами

$$x_3 \equiv (\lambda^2 - x_1 - x_2) \bmod p; \quad (1)$$

$$y_3 \equiv [\lambda (x_1 - x_3) - y_1] \bmod p, \quad (2)$$

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

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

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 ресурсоемкостью операций сложения и дублирования точек, с помощью которых вычисляется kP, как видно из приведенных выше формул.

Параллельная схема идентификации доказательства с нулевым разглашением на основе эллиптических кривых (рис. 1). Пусть $E_p(a, b)$ – эллиптическая кривая, известная участникам информационного процесса, G – предварительно согласованная и опубликованная точка этой кривой. Абонент A выбирает секретные числа k_i $(1 < k_i < n)$ и вычисляет значения открытого ключа $Y_{ai} = k_i G$, который передает абоненту B вместе с заявкой γ. Абонент B отправляет абоненту A некоторую случайную двоичную строку из t бит: $x_1, ..., x_t$, где $x_i \in \{0, 1\}$.

1. Абонент A выбирает случайное число r, $1 < r < n$ и отправляет абоненту B заявку γ

$A \rightarrow B$: $Y_{ai}, \gamma = rG$.

2. Абонент B отвечает случайным запросом x – двоичная строка из t бит

$A \leftarrow B$: $x_1, \ldots, x_i, \ldots, x_t$.

3. Абонент A вычисляет и отправляет абоненту B ответ y

$$A \rightarrow B: y = \left(r + \sum_{i=1}^{t} x_i k_i\right) G.$$

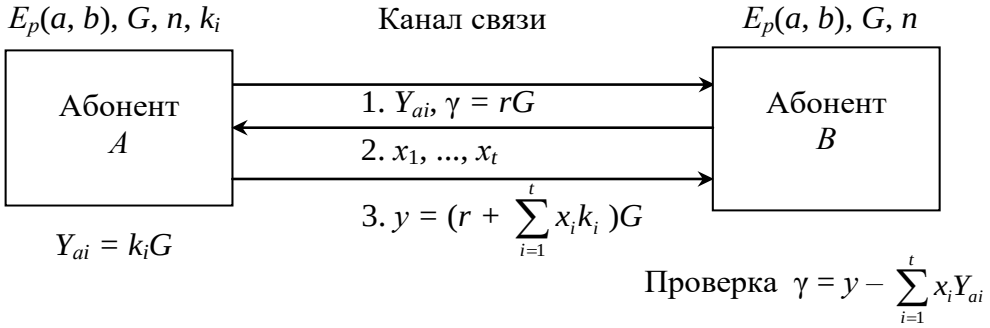

Рисунок 1 – Параллельная схема идентификации доказательства с нулевым разглашением на основе эллиптических кривых

Абонент *B* проверяет равенство $y - \sum_{i=1}^{t} x_i Y_{ai} = \gamma$.

Полнота протокола. Доказывающий *A* знает значения k_i, поэтому он в состоянии ответить на любой запрос *x* абонента *B*. При этом проверяющий *B* убеждается в справедливости соотношения

$$y - \sum_{i=1}^{t} x_i Y_{ai} = (r + \sum_{i=1}^{t} x_i k_i)G - \sum_{i=1}^{t} x_i Y_{ai} = rG + \sum_{i=1}^{t} x_i k_i G - \sum_{i=1}^{t} x_i k_i G = rG = \gamma. \qquad (3)$$

Пример 1. Пусть $E_{31991}(-3, 130)$; $G = (1, 12510)$; $n = 31859$; $p = 31991$; $t = 5$, что соответствует кривой $y^2 = x^3 - 3x + 130$. Предположим, что абонент *A* выбирает секретные числа $K = (153, 2347, 659, 12958, 30607)$ и вычисляет значения открытого ключа Y_a:

$Y_a = \{(18302, 16002); (25097, 2812); (10177, 28747); (6899, 17464); (11252, 30920)\}$.

Рассмотрим два цикла протокола.

Первый цикл протокола.

1. Абонент *A* выбирает случайное число $r = 100$ и вычисляет заявку γ

$A \rightarrow B$: Y_a, $\gamma = 100(1, 12510) = (7751, 5268)$.

2. $A \leftarrow B$: $x = \{1, 1, 0, 1, 1\}$.

3. $A \rightarrow B$: $y = (100 + 153 + 2347 + 12958 + 30607)(1, 12510) = 14306(1, 12510) = (24314, 1755)$.

Абонент *B* выполняет проверку

$(24314, 1755) - [(18302, 16002) + (25097, 2812) + (6899, 17464) + (11252, 30920)] =$

$= (24314, 1755) + (30803, 19514) = (7751, 5268) = \gamma$ – проверка выполнена.

Второй цикл протокола.

1. Абонент *A* выбирает случайное число $r = 23456$ и вычисляет заявку γ

$A \rightarrow B$: $\gamma = 23456(1, 12510) = (20353, 31190)$.

2. $A \leftarrow B$: $x = \{1, 0, 1, 1, 0\}$.

3. $A \rightarrow B$: $y = (23456 + 153 + 659 + 12958)(1, 12510) = 5367(1, 12510) = (4197, 26901)$.

Абонент *B* выполняет проверку

$(4197, 26901) - [(18302, 16002) + (10177, 28747) + (6899, 17464)] =$

$= (4197, 26901) + (8578, 13495) = (20353, 31190) = \gamma$ – проверка выполнена.

Предложенную параллельную схему идентификации можно модифицировать с использованием открытого ключа абонента *B*.

Параллельная схема идентификации доказательства с нулевым разглашением на основе эллиптических кривых с использованием открытого ключа абонента B (рис. 2). Пусть $E_p(a, b)$ – эллиптическая кривая, известная участникам информационного процесса; G – предварительно согласованная и опубликованная точка этой кривой. Абонент A выбирает секретные числа k_i $(1 < k_i < n)$ и вычисляет значения открытого ключа $Y_{ai} = k_i G$, который передает абоненту B вместе с заявкой γ. Абонент B выбирает секретное число k_b $(1 < k_b < n)$ и вычисляет открытый ключ $Y_b = k_b G$, который передает абоненту A вместе с запросом x.

Рисунок 2 – Параллельная схема идентификации доказательства с нулевым разглашением на основе эллиптических кривых с использованием открытого ключа абонента B

1. Абонент A выбирает случайное число r, $1 < r < n$ и отправляет абоненту B заявку γ

$A \rightarrow B$: $Y_{ai}, \gamma = rG$.

2. Абонент B отвечает случайным запросом x и отправляет свой открытый ключ Y_b

$A \leftarrow B$: $Y_b, x_1, \ldots, x_i, \ldots, x_t$.

3. Абонент A вычисляет и отправляет абоненту B ответ y

$$A \rightarrow B: y = (r + \sum_{i=1}^{t} x_i k_i) Y_b.$$

Абонент B проверяет равенство $y k_b^{-1} - \sum_{i=1}^{t} x_i Y_{ai} = \gamma$.

Полнота протокола. Доказывающий A знает значения k_i, поэтому он в состоянии ответить на любой запрос x_i абонента B. При этом проверяющий B убеждается в справедливости соотношения

$$y k_b^{-1} - \sum_{i=1}^{t} x_i Y_{ai} = (r + \sum_{i=1}^{t} x_i k_i) k_b^{-1} Y_b - \sum_{i=1}^{t} x_i k_i G = (r + \sum_{i=1}^{t} x_i k_i) k_b^{-1} k_b G - \sum_{i=1}^{t} x_i k_i G =$$

$$= rG + \sum_{i=1}^{t} x_i k_i G - \sum_{i=1}^{t} x_i k_i G = rG = \gamma. \qquad (4)$$

Пример 2. Пусть $E_{10007}(-3, 75)$; $G = (1, 4594)$; $n = 10099$; $p = 10007$; $t = 6$, что соответствует кривой $y^2 = x^3 - 3x + 75$. Предположим, что абонент A выбирает секретные числа, $K = (5623, 899, 9079, 83, 3060, 10024)$ и вычисляет значения открытого ключа Y_a:

$Y_a = \{(1773, 3148); (3710, 2292); (9552, 9047); (9716, 2177); (6526, 9413); (7497, 8558)\}$.

Абонент B выбирает секретное число $k_b = 4960$ и вычисляет открытый ключ Y_b:

$$Y_b = 4960(1, 4594) = (2283, 4005).$$

Первый цикл протокола.

1. Абонент A выбирает случайное число $r = 1127$ и вычисляет заявку γ

$A \rightarrow B$: Y_a, γ = 1127(1, 4594) = (5016, 5129).

2. $A \leftarrow B$: (2283, 4005), x = {1, 1, 1, 1, 0, 1}.

3. $A \rightarrow B$: y = (1127 + 5623 + 899 + 9079 + 83 + 10024)(2283, 4005) = (2850, 59).

Абонент B выполняет проверку

8350(2850, 59) – [(1773, 3148) + (3710, 2292) + (9552, 9047) + (9716, 2177) + (7497, 8558)] =

= (3451, 6626) + (8640, 5984) = (5016, 5129) = γ – проверка выполнена.

Второй цикл протокола.

1. Абонент A выбирает случайное число r = 10023 и вычисляет заявку γ

$A \rightarrow B$: γ = 10023(1, 4594) = (8032, 3223).

2. $A \leftarrow B$: x = {1, 0, 1, 0, 1, 0}.

3. $A \rightarrow B$: y = (10023 + 5623 + 9079 + 3060)(2283, 4005) = 7587(2283, 4005) = (3349, 9616).

Абонент B выполняет проверку

8350(3349, 9616) – [(1773, 3148) + (9552, 9047) + (6526, 9413)] = (3656, 6367) + (9589, 8572) =

= (8032, 3223) = γ – проверка выполнена.

Для анализа предложенных протоколов идентификации ZKP EC на устойчивость к атакам противника был применен программный продукт AVISPA (Automated Validation of Internet Security Protocols and Applications) [12]. Выбор данного продукта обусловлен тем, что AVISPA интегрирует все современные подходы к анализу протоколов, такие как проверка на модели, древовидные автоматы, временная логика. Главное преимущество AVISPA, в отличие от других средств (REVERE, Athena, NRL Protocol Analyzer, FDR, HERMES, ProVerif) состоит в том, что ее 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, 12].

Выполнена проверка модели предложенных протоколов идентификации ZKP EC с помощью Protocol Simulation пакета SPAN (Security Protocol Animator) [13] (рис. 3 и 4).

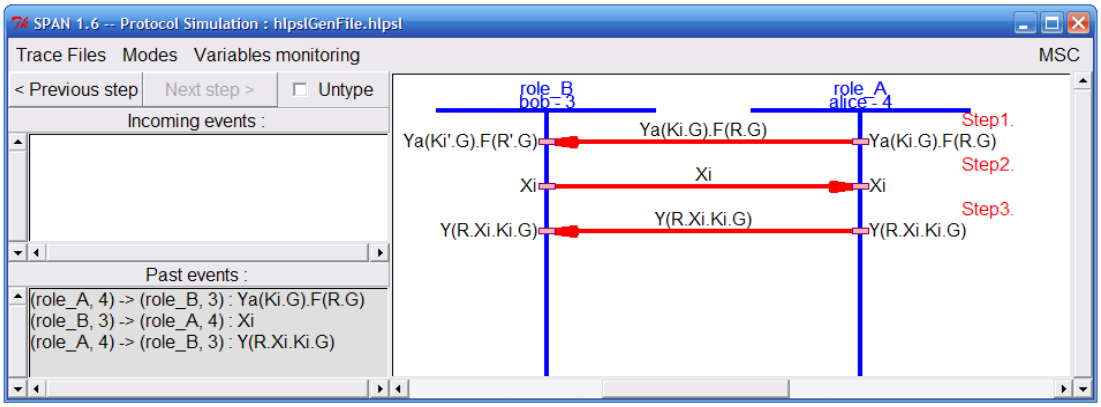

Рисунок 3 – Моделирование параллельной схемы идентификации ZKP EC

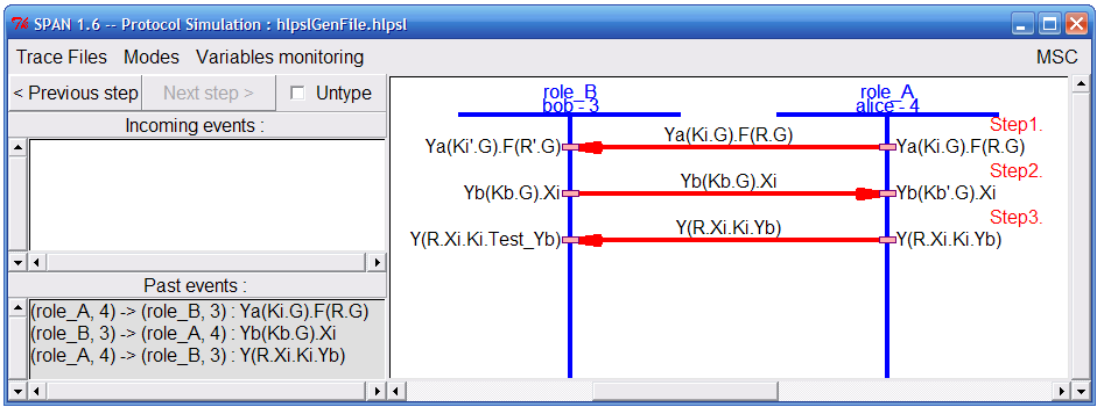

Рисунок 4 – Моделирование параллельной схемы идентификации ZKP EC с использованием открытого ключа абонента *B*

Программная верификация протокола и устойчивость протокола к атакам противника была выполнена с помощью программных модулей OFMC (On-the-Fly Model-Checker) и CLAtSe (CL-based Attack Searcher) AVISPA (рис. 5). В результате проверки протокола ZKP EC известных атак на протокол не найдено.

Рисунок 5 – Верификация и устойчивость протокола идентификации 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 статье предложены параллельные схемы идентификации доказательства с нулевым разглашением на основе эллиптических кривых, которые позволяют увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации. Определена полнота и корректность протоколов, приведены примеры расчета, выполнена проверка модели и верификация протоколов идентификации. Для проверки протоколов идентификации ZKP EC на устойчивость к атакам противника были применены средства пакета SPAN для AVISPA. В результате проверки протоколов известных атак на протоколы не найдено. Злоумышленник может получить доступ к информации, только решив задачу ECDLP. Следовательно, при использовании параллельной схемы идентификации ZKP EC позволяет значительно уменьшить размеры параметров протокола, увеличить криптографическую стойкость и уменьшить длительность процесса идентификации. К основным направлениям дальнейших исследований нужно отнести оценку вычислительной сложности и криптографической стойкости протоколов идентификации ZKP EC.

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 распределенных 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. AVISPA. [Электронный ресурс]. – Режим доступа: http://www.avispa-project.org/.
13. Security Protocol Animator. [Электронный ресурс]. – Режим доступа: http://www.irisa.fr/celtique/genet/span/.

REFERENCES:

1. Menezes A., van Oorschot P., Vanstone S. (1996). Handbook of applied cryptography. CRC Press, 816.
2. Schneier B. (2002). Applied cryptography: Protocols, algorithms, and source code in C. Moscow, Triumph, 816.
3. Sokolov A.V., Shan'gin V.F. (2002). Information protection in distributed corporate networks and systems. – Moscow: DMK Press, 656.
4. Pogorelov B. (2006). Glossary of cryptographic terms. – Moscow, MCCME, 91.
5. Cheremushkin A.V. (2009). Cryptographic protocols. Basic properties and vulnerabilities. Moscow, Academy, 272.
6. Zapechnikov S.V. (2007). Cryptographic protocols and their application in the financial and commercial activities. Moscow, Hot line-Telecom, 320.
7. Hankerson D., Menezes A., Vanstone S. (2004). Guide to Elliptic Curve Cryptography. Springer-Verlag, 358.
8. Bolotov A.A., Gashkov S.B., Frolov A.B. (2006). An elementary introduction to elliptic curve cryptography: Algebraic and algorithmic foundations, 328.
9. Bolotov A.A., Gashkov S.B., Frolov A.B. (2006). An elementary introduction to elliptic curve cryptography: Cryptographic protocols on elliptic curves, 280.
10. Vasilenko O.N. (2003). Number-theoretic algorithms in cryptography. – M.:MCCME, 328.
11. Rostovtsev A.G., Makhovenko E.B. (2005). Theoretical cryptography. Professional, 490.
12. AVISPA. http://www.avispa-project.org/.
13. Security Protocol Animator. http://www.irisa.fr/celtique/genet/span/.