УДК: 004.056.55: 003.26

Онацкий А.В., Горохов С.М., Жарова О.В.
Онацький О.В., Горохов С.М., Жарова О.В.
Onatskiy A.V., Gorokhov S.M., Garova O.V.

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ДОКАЗУ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ НА ЕЛІПТИЧНИХ КРИВИХ

CRYPTOGRAPHIC PROTOCOL ZERO-KNOWLEDGE PROOF ON ELLIPTIC CURVES

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

Анотація. Запропоновано криптографічний протокол доказу із нульовим розголошенням знання на еліптичних кривих, що дозволяє встановити істинність твердження й при цьому не передавати будь-якої додаткової інформації про саме твердження.

Summary. Proposed cryptographic protocol zero-knowledge proof on elliptic curves allows to establish the truth of allegation and does not convey any additional information about the approval.

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных проблем 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 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 криптографического протокола доказательства 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 нулевым разглашением.

Полнота (completeness property) – свойство криптографического протокола, означающее, что при выполнении честными участниками протокол решает ту задачу, для которой он создан [4, 5].

Корректность (soundness property) – способность криптографического протокола противостоять угрозам со стороны нарушителя (противника), не располагающего необходимой секретной информацией, но пытающегося выполнить протокол за участника [4, 5].

Нулевое разглашение (zero-knowledge property) – свойство протокола доказательства знания, обеспечивающее такое его выполнение, что никакая информация о доказываемом утверждении, кроме факта его истинности, не может быть получена нечестным путем [5].

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

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

После выполнения каждого такого цикла проверяющий принимает решение об истинности доказательства.

Широкое распространение при идентификации и аутентификации получили криптографические протоколы ZKP на базе ассиметричного шифрования, наиболее известными являются: Фиата–Шамира, Шнорра, Окамото, Гиллоу–Кискатр, Брикелла–Мак-Карли, Фейга–Фиата–Шамира (табл. 1) [1 … 3, 5, 6].

Таблица 1 – Криптографические протоколы с нулевым разглашением

Название протокола	Вычисление	Проверка
Фиата–Шамира (Fiat–Shamir)	1. $A \rightarrow B$: Y_a, $\gamma \equiv r^2 \pmod n$. 2. $A \leftarrow B$: x. 3. $A \rightarrow B$: $y \equiv r\,k^x \pmod n$	$\gamma = (y^2\, Y_a^{\,x}) \bmod n$
Шнорра (Schnorr)	1. $A \rightarrow B$: Y_a, $\gamma \equiv \alpha^r \pmod p$. 2. $A \leftarrow B$: x. 3. $A \rightarrow B$: $y \equiv (r + kx) \bmod q$	$\gamma = (\alpha^y\, Y_a^{\,x}) \bmod p$
Окамото (Okamoto)	1. $A \rightarrow B$: Y_a, $\gamma \equiv \alpha_1^{\,r_1}\, \alpha_2^{\,r_2} \pmod p$. 2. $A \leftarrow B$: x. 3. $A \rightarrow B$: $y_1 \equiv (r_1 + k_1 x) \bmod q$; $y_2 \equiv (r_2 + k_2 x) \bmod q$	$\gamma = (\alpha_1^{\,y_1}\, \alpha_2^{\,y_2}\, Y_a^{\,x}) \bmod p$
Гиллоу–Кискатр (Guillou–Quisquater)	1. $A \rightarrow B$: Y_a, $\gamma \equiv r^e \pmod n$. 2. $A \leftarrow B$: x. 3. $A \rightarrow B$: $y \equiv r\,k^x \pmod n$	$\gamma = (Y_a^{\,x}\, y^e) \bmod n$
Брикелла–Мак-Карли (Brickell–McCurley)	1. $A \rightarrow B$: Y_a, $\gamma \equiv \alpha^r \pmod p$. 2. $A \leftarrow B$: x. 3. $A \rightarrow B$: $y \equiv (r + kx) \bmod (p-1)$	$\gamma = (\alpha^y\, Y_a^{\,x}) \bmod p$
Фейга–Фиата–Шамира (Feige–Fiat–Shamir)	1. $A \rightarrow B$: Y_a, $\gamma \equiv r^2 \pmod n$. 2. $A \leftarrow B$: $x_1, \ldots, x_k$. 3. $A \rightarrow B$: $y \equiv r(k_1^{x_1} \cdot k_2^{x_2} \cdot \ldots \cdot k_k^{x_k}) \bmod n$	$\gamma = y^2(Y_{a_1}^{x_1} \cdot Y_{a_2}^{x_2} \cdot \ldots \cdot Y_{a_k}^{x_k}) \bmod n$

Корректность и стойкость представленных протоколов в табл. 1 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 работе предложен новый криптографический протокол доказательства с нулевым разглашением на основе эллиптических кривых (Elliptic Curves – EC) над конечными полями.

Криптосистемы на эллиптических кривых (Elliptic Curves Cryptography – ECC) [7 … 9] относятся к классу криптосистем с открытым ключом. Их безопасность, 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 (нахождение числа x по заданному числу $y \equiv g^x \bmod p$ при известных основании g и модуле p), на которой базируются криптографические протоколы, представленные в табл. 1. 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 должна 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 $$\lambda \equiv \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \pmod p, & \text{если } P \neq Q; \\ \dfrac{3x_1^2 + a}{2y_1} \pmod p, & \text{если } P = Q. \end{cases}$$

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.

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 ресурсоемкостью операций сложения и дублирования точек, с помощью которых вычисляется kP, как видно из приведенных выше формул. Отсюда следует возможность применения более коротких ключей (табл. 2) [12].

Таблица 2 – 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

Протокол 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 секретное

число k_a ($1 < k_a < n$) и вычисляет открытый ключ $Y_a = k_a G$, который передает абоненту B вместе с заявкой. Абонент B выбирает секретное число k_b ($1 < k_b < n$) и вычисляет открытый ключ $Y_b = k_b^{-1} G$, который передает абоненту A вместе с запросом.

Рисунок 1 – Криптографический протокол ZKP на основе эллиптических кривых

1. Абонент A выбирает случайное число r, $1 < r < n - 1$ и отправляет абоненту B число γ: $A \rightarrow B$: $Y_a, \gamma = rG$.

2. Абонент B отвечает случайным запросом x: $A \leftarrow B$: Y_b, x.

3. Абонент A отправляет абоненту B ответ, число y: $A \rightarrow B$: $y = (r + xk_a)Y_b$.

Абонент B проверяет равенство $\gamma = yk_b - xY_a$.

Полнота. Доказывающий A знает значение k_a, поэтому он в состоянии ответить на любой запрос x абонента B. При этом проверяющий B убеждается в справедливости соотношения

$$yk_b - xY_a = (r + xk_a)Y_b k_b - xk_a G = rk_b Y_b + xk_a k_b Y_b - xk_a G =$$
$$= rk_b k_b^{-1} G + xk_a k_b k_b^{-1} G - xk_a G = rG + xk_a G - xk_a G = rG = \gamma. \qquad (3)$$

Пример. Пусть $E_{751}(-1, 188)$; $G = (1, 375)$; $n = 727$; $p = 751$, что соответствует кривой $y^2 = x^3 - x + 188$. Предположим, что абонент A выбирает числа $k_a = 327$, $r_1 = 619$, $r_2 = 157$ (рассмотрим два цикла протокола) и вычисляет $Y_a = 327(1, 375) = (354, 153)$. Абонент B выбирает числа $k_b = 513$, $x_1 = 191$, $x_2 = 573$ и вычисляет $Y_b = 513^{-1}(1, 375) = (693, 70)$.

Первый цикл протокола:

1. $A \rightarrow B$: $(354, 153)$, $\gamma = 619(1, 375) = (391, 564)$.
2. $A \leftarrow B$: $(693, 70)$, $x_1 = 191$.
3. $A \rightarrow B$: $y = (619 + 191 \cdot 327)\,(693, 70) = 63076(693, 70) = (256, 342)$.

Абонент B выполняет проверку

$513(256, 342) - 191(354, 153) = (274, 422) + 191(354, 598) = (391, 564) = \gamma$.

Второй цикл протокола:

1. $A \rightarrow B$: $\gamma = 157(1, 375) = (361, 8)$.
2. $A \leftarrow B$: $x_2 = 573$.
3. $A \rightarrow B$: $y = (157 + 573 \cdot 327)\,(693, 70) = 187528(693, 70) = (205, 161)$.

Абонент B выполняет проверку

$513(205, 161) - 573(354, 153) = (484, 161) + (733, 265) = (361, 8) = \gamma$.

Для анализа предложенного криптографического протокола ZKP EC на устойчивость к атакам противника был применен программный продукт AVISPA (Automated Validation of Internet Security Protocols and Applications) [13]. 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, 13]. На рис. 2 представлена спецификация протокола ZKP EC на языке HLPSL средствами пакета SPAN (Security

Protocol Animator) [14] для AVISPA.

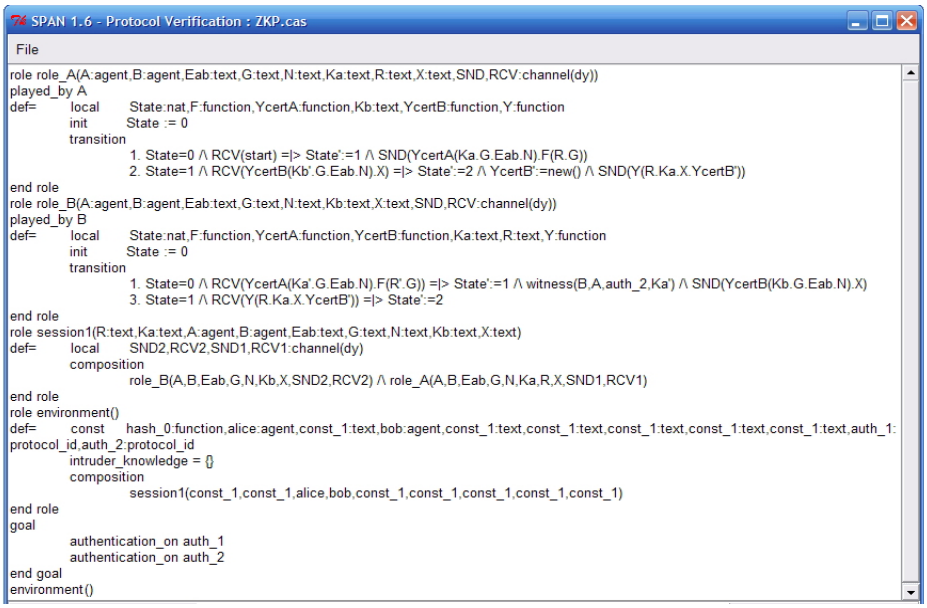

Рисунок 2 – Протокол ZKP EC на языке HLPSL

Выполнена проверка модели предложенного протокола с помощью Protocol Simulation пакета SPAN (рис. 3).

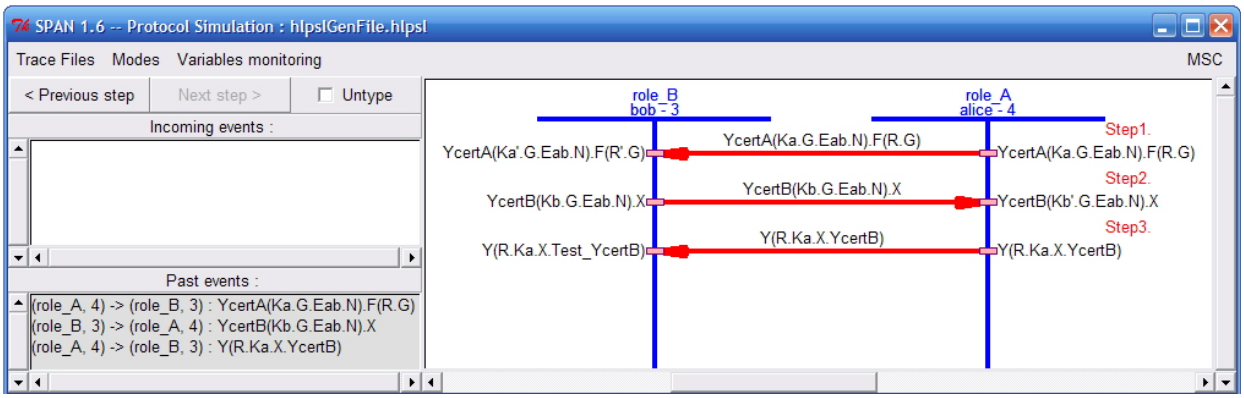

Рисунок 3 – Моделирование протокола ZKP EC

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. В результате проверки протокола ZKP EC известных атак на протокол не найдено (рис. 4).

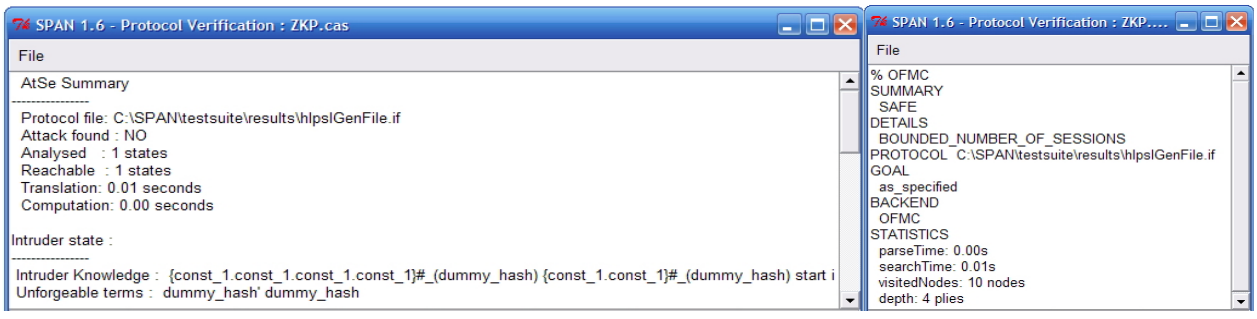

Рисунок 4 – Верификация и устойчивость протокола ZKP EC к атакам

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. Для проверки протокола ZKP EC на устойчивость к атакам противника были применены средства пакета SPAN для AVISPA. В результате проверки протокола известных атак на протоколы не найдено. Противник может получить доступ к информации, только решив задачу ECDLP. Соответственно, при использовании криптографических протоколов ZKP EC позволяет значительно уменьшить размеры параметров протокола и увеличить криптографическую стойкость.

Таким образом, в статье предложен новый криптографический протокол ZKP EC. Определена полнота и корректность протокола, приведен пример расчета, выполнена проверка модели и верификация протокола, а также устойчивость протокола к атакам противника. К основным направлениям дальнейших исследований нужно отнести оценку вычислительной сложности и криптографической стойкости предложенного протокола 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. *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.
13. *AVISPA* [Электронный ресурс]. – Режим доступа: http://www.avispa-project.org/
14. *Security Protocol Animator*. [Электронный ресурс]. – Режим доступа: http://www.irisa.fr/celtique/genet/span/.