**УДК: 004.056.55: 003.26**

# ПРОТОКОЛ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

ОНАЦКИЙ А.В.

Одесская национальная академия связи им. А.С. Попова

# ZERO-KNOWLEDGE PROOF PROTOCOL ON ELLIPTIC CURVES

ONATSKIY A.V.

Odessa national academy of telecommunications n.a. O.S. Popov

***Аннотация.*** *Предложен 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.*

***Abstract.*** *Proposed zero-knowledge proof protocol 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 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 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 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 нулевое разглашение [4, 5].

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

1. $A \rightarrow B$: $\gamma$ (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 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 работе предложен новый 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. 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 уравнения 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 $y^2 \in (x^3 + ax + b) \bmod p$, и бесконечно удаленной точки *O*. Для точек на эллиптической кривой вводится операция сложения, которая 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

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

$$y_3 \equiv [l(x_1 - x_3) - y_1] \bmod p, \tag{2}$$

где

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

Число λ – угловой коэффициент секущей, проведённой 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.

*Протокол доказательства с нулевым разглашением на основе эллиптических кривых* (рис. 1). Пусть $E_p(a, b)$ – эллиптическая кривая, известная участникам информационного процесса; *G* и *Q* – предварительно согласованные и опубликованные точки этой кривой. Абонент *A* выбирает секретные числа $k_1,k_2\,(1<k_1,k_2<n)$ и вычисляет открытый ключ $Y_a=k_1G+k_2Q$, который передаёт абоненту *B* вместе с заявкой. Абонент *B* выбирает секретное число $k_b\,(1<k_b<n)$ и вычисляет открытый ключ $Y_b=k_b(G+Q)$, который передаёт абоненту *A* вместе с запросом.


Рисунок 1 – Протокол ZKP на основе эллиптических кривых

1. Абонент *A* выбирает случайные числа $r_1$ и $r_2$, $1<r_1,r_2<n-1$ и отправляет абоненту *B* заявку γ:
   $A\to B: Y_a,\ \gamma=r_1G+r_2Q$.
2. Абонент *B* отвечает случайным запросом *x*:
   $A\leftarrow B: Y_b, x$.
3. Абонент *A* вычисляет и отправляет абоненту *B* значения $y_1,y_2,y_3$:
   $A\to B: y_1=(r_1+xk_1)Y_b, y_2=(r_2+xk_2)Y_b, y_3=(r_1+xk_1)Q+(r_2+xk_2)G$.

Абонент *B* проверяет равенство $(y_1+y_2)-y_3-xY_a=\gamma$.

*Полнота.* Доказывающий *A* знает значения $k_1$ и $k_2$, поэтому он в состоянии ответить на любой запрос *x* абонента *B*. При этом проверяющий *B* убеждается в справедливости соотношения

$$(y_1+y_2)-y_3-xY_a=(r_1+xk_1)Y_b+(r_2+xk_2)Y_b-(r_1+xk_1)Q-(r_2+xk_2)G-$$
$$-x(k_1G+k_2Q)=(r_1+xk_1)k_b(G+Q)+(r_2+xk_2)k_b(G+Q)-r_1Q-xk_1Q-$$
$$-r_2G-xk_2G-xk_1G-xk_2Q=r_1k_bG+xk_1k_bG+r_1k_bQ+xk_1k_bQ+$$
$$+r_2k_bG+xk_2k_bG+r_2k_bQ+xk_2k_bQ-r_1Q-xk_1Q-r_2G-xk_2G-xk_1G-$$
$$-xk_2Q=r_1G+xk_1G+r_1Q+xk_1Q+r_2Gxk_2G+r_2Q+xk_2Q-r_1Q-xk_1Q-r_2G-$$
$$-xk_2G-xk_1G-xk_2Q=r_1G+r_2Q=\gamma.$$

*Пример.* Пусть $E_{751}(-1,188);\ G=(1,375);\ Q=(2,373);\ p=751$, что соответствует кривой $y^2=x^3-x+188$. Предположим, что абонент *A* выбирает секретные числа $k_1=327, k_2=715$ и вычисляет открытый ключ $Y_a$:

$$Y_a=327(1,375)+715(2,373)=(354,153)+(513,610)=(139,413).$$

Абонент $B$ выбирает секретное число $k_b = 496$ и вычисляет открытый ключ $Y_b$:

$$Y_b = 496[(1,375) + (2,373)] = 496(1,376) = (352,686).$$

Рассмотрим два цикла протокола.

Первый цикл протокола.

1. Абонент $A$ выбирает случайные числа $r_1 = 619, r_2 = 157$ и вычисляет γ:

$$A \to B: \ (139,413), \ \gamma = 619(1,375) + 157(2,373) = (391,564) + (710,731) = (605,454);$$

2. $A \leftarrow B: \ (352,686), x = 191.$

3. $A \to B: y_1 = (619 + 191 \cdot 327)(352,686) = 554(352,686) = (637,301);$

$$y_2 = (157 + 191 \cdot 715)(352,686) = 46(352,686) = (653,422);$$

$$y_3 = (619 + 191 \cdot 327)\ (2,373) + (157 + 191 \cdot 715)(1,375) =$$

$$= 554(2,373) + 46(1,375) = (389,146) + (597,423) = (43,322).$$

Абонент $B$ выполняет проверку

$$107\left[(637,301) + (653,422)\right] - (43,322) - 191(139,413)) = 107(366,575) + (43,429) +$$

$$+ (361,743) = (268,229) + (585,108) = (605,454) = \gamma$$ – проверка выполнена.

Второй цикл протокола.

1. Абонент $A$ выбирает случайные числа $r_1 = 39, r_2 = 599$ и вычисляет γ:

$$A \to B: \ (139,413), \ \gamma = 39(1,375) + 599(2,373) = (270,589) + (740,389) = (5,225).$$

2. $2. A \leftarrow B: \ (352,686), x = 303.$

3. $3. A \to B: y_1 = (39 + 303 \cdot 327)(352,686) = 248(352,686) = (246,698);$

$$y_2 = (599 + 303 \cdot 715)(352,686) = 598(352,686) = (197,644);$$

$$y_3 = (39 + 303 \cdot 327)\ (2,373) + (599 + 303 \cdot 715)(1,375) =$$

$$= 248(2,373) + 598(1,375) = (352,686) + (224,248) = (646,162).$$

Абонент $B$ выполняет проверку

$$107[(246,698) + (197,644)] - (646,162) - 303(139,413) = 107(348,523) + (646,589) +$$

$$+ (666,666) = (231,176) + (432,310) = (5,225) = \gamma$$ – проверка выполнена.

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) [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]. На рис. 2 представлена спецификация протокола ZKP EC на языке HLPSL средствами пакета SPAN (Security Protocol Animator) [13] для AVISPA.

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

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

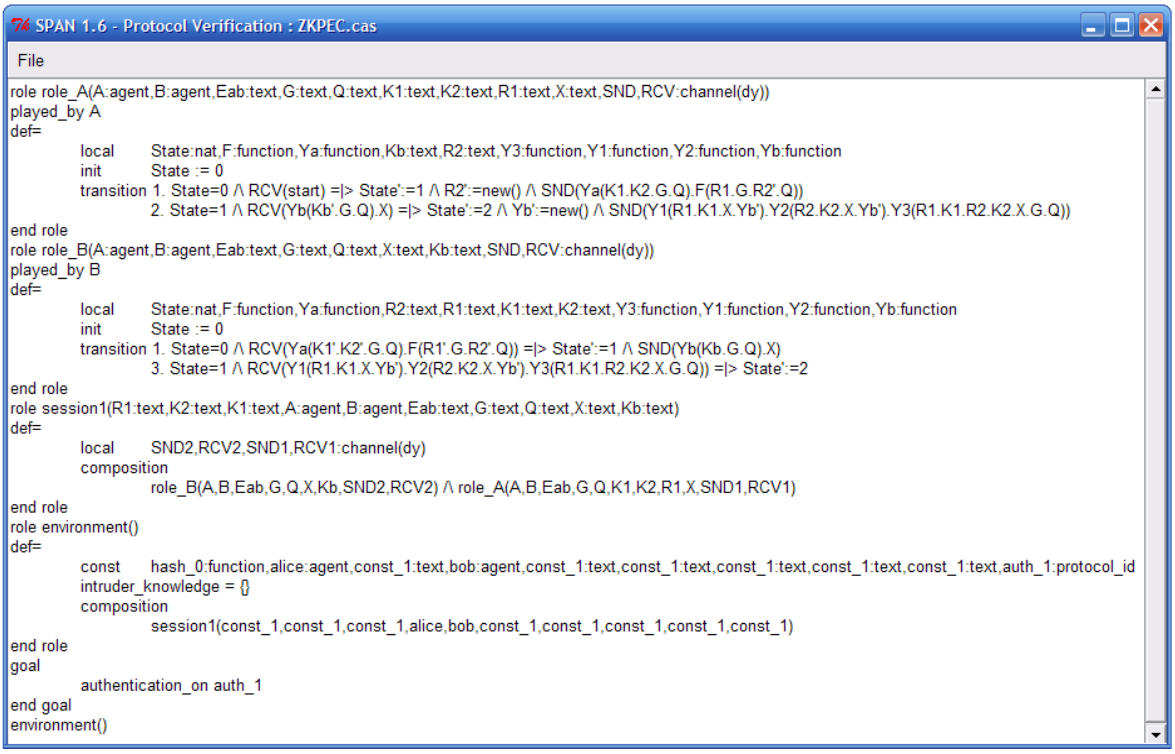


Рисунок 2 – Протокол ZKP EC на языке HLPSL

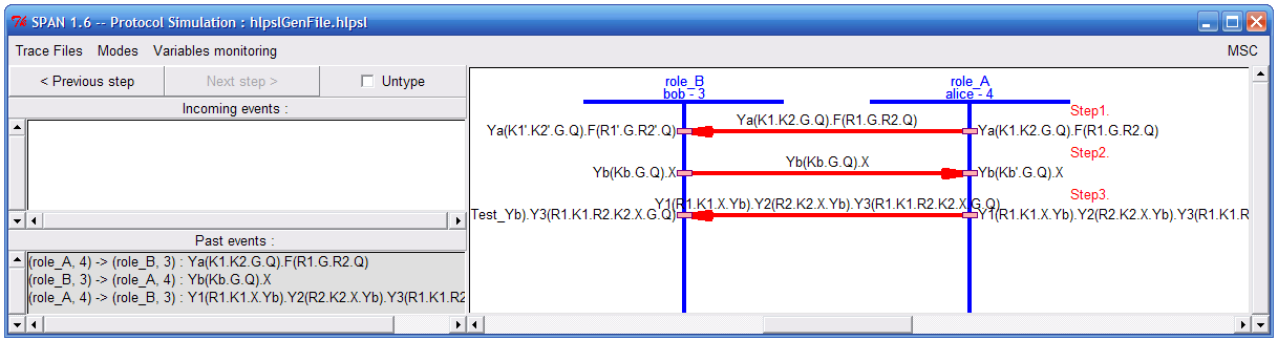


Рисунок 3 – Моделирование протокола ZKP EC

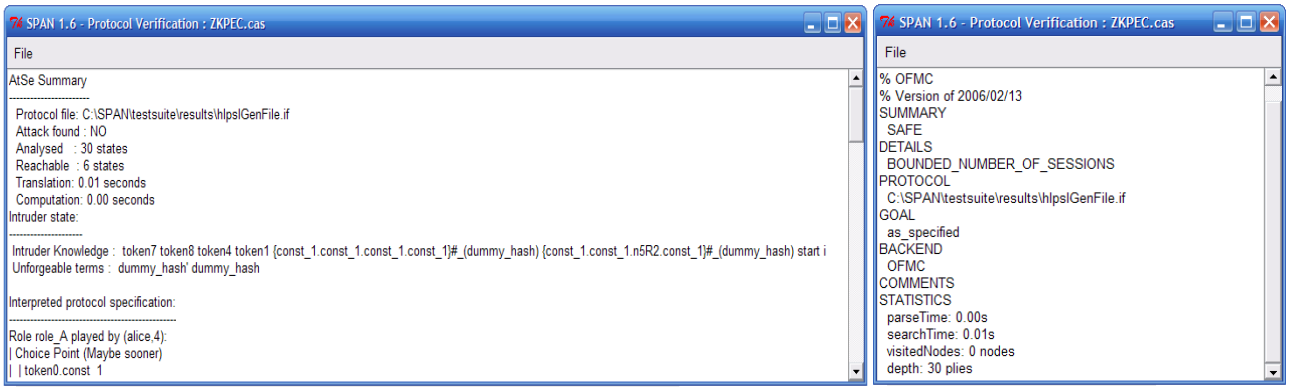


Рисунок 4 – Верификация и устойчивость протокола ZKP EC к атакам

## ВЫВОДЫ

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 новый криптографический протокол ZKP EC. Определена полнота и корректность протокола, приведены примеры расчета, выполнена проверка модели и верификация протокола. 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. Следовательно, при использовании протокола ZKP EC, позволяет значительно уменьшить размеры параметров протокола и увеличить криптографическую стойкость. 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 / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – 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/.