УДК 004.056.55: 003.26

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С ИСПОЛЬЗОВАНИЕМ СЛУЧАЙНЫХ СЕАНСОВЫХ КЛЮЧЕЙ И СООБЩЕНИЙ

Онацкий А.В.[1], Жарова О.В.[2]

[1] Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
onatsky@meta.ua
[2] Одесский национальный политехнический университет
65044, Украина, г. Одесса, просп. Шевченко, 1.
Ksenia.gds@gmail.com

КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ДОКАЗУ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ НА ЕЛІПТИЧНИХ КРИВИХ З ВИКОРИСТАННЯМ ВИПАДКОВИХ СЕАНСОВИХ КЛЮЧІВ І 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

CRYPTOGRAPHIC PROTOCOL ZERO-KNOWLEDGE PROOF ON ELLIPTIC CURVES USING RANDOM SESSION KEYS AND MESSAGES

Onatskiy A.V.[1], Garova 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

Аннотация. Предложен криптографический протокол доказательства с нулевым разглашением на основе математического аппарата эллиптических кривых с использованием случайных сеансовых ключей и сообщений, позволяющий установить истинность утверждения и при этом не передавать какой-либо дополнительной информации о самом утверждении. Определена полнота и корректность протокола, дан пример расчета, выполнена проверка модели и верификация протокола. Программная верификация криптографического протокола была выполнена с помощью программных модулей On the Fly Model Checker и Constraint Logic based Attack Searcher. Для проверки криптографического протокола на устойчивость к атакам злоумышленника были применены средства пакета Security Protocol Animator для AVISPA. Стойкость предложенного криптографического протокола основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

Ключевые слова: криптографический протокол, эллиптические кривые, идентификация, аутентификация, доказательство с нулевым разглашением, сеансовый ключ.

Анотація. Запропоновано криптографічний протокол доказу із нульовим розголошенням на основі математичного апарату еліптичних кривих з використанням випадкових сеансових ключів і повідомлень, що дозволяє встановити істинність твердження й при цьому не передавати будь-якої додаткової інформації про саме твердження. Визначено повноту і коректність протоколу, надано приклад розрахунку, виконано перевірку моделі і верифікацію протоколу. Програмна верифікація криптографічного протоколу 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 пакета Security Protocol Animator для AVISPA. Стійкість запропонованого криптографічного протоколу ґрунтується на складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої.

Ключові слова: криптографічний протокол, еліптичні криві, ідентифікація, автентифікація, доказ із нульовим розголошенням, сеансовий ключ.

Abstract. Proposed cryptographic protocol with zero-knowledge proof on the basis of the mathematical apparatus of elliptic curves using random session keys and messages, allowing to establish the truth of allegation and does not convey any additional information about the approval. The completeness and correctness of the protocol, an example of calculation is given, model validation and verification of the protocol are performed. Software verification of the cryptographic protocol was performed using the software modules On the Fly Model Checker and Constraint Logic based Attack Searcher. To validation the cryptographic protocol for resistance to intruder attacks was used the Security Protocol Animator package for AVISPA. The security of the proposed cryptographic protocol is based on the difficulty of solving the elliptic curve discrete logarithm problem.

Key words: cryptographic protocol, elliptic curves, identification, authentication, zero-knowledge proof, session key.

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 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 трех шагов определенного 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 увеличением 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 сложности 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 … 12], 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.

Криптографический протокол доказательства с нулевым разглашением на основе эллиптических кривых с использованием случайных сеансовых ключей и сообщений (рис. 1). Пусть $E_p(a, b)$ – эллиптическая кривая, известная участникам информационного процесса; G – предварительно согласованная и опубликованная точка кривой. Абонент A выбирает секретный ключ k_a $(1 < k_a < n)$ и вычисляет значения открытого ключа $Y_a = k_aG$, который передает абоненту B вместе с заявкой $\gamma = rG$, где r – случайное число. Абонент B выбирает сеансовый 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. Абонент B передает абоненту A запрос – y_1, y_2. Абонент A вычисляет $M = y_2 - k_ay_1$ и передает абоненту B ответ $x = (r + k_a)G + M$. Абонент B проверяет равенство $\gamma = x - (M + Y_a)$.

Рисунок 1 – Криптографический протокол доказательства с нулевым разглашением на основе эллиптических кривых с использованием случайных сеансовых ключей и сообщений

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

$$\gamma = x - (M + Y_a) = (r + k_a)G + M - M - k_aG = rG + k_aG + M - M - k_aG = rG = \gamma.$$

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

$A \rightarrow B$: $Y_a = (25097, 2812)$; $\gamma = 17653(1, 12510) = (30803, 19514)$.

2. Абонент B выбирает случайное сообщение $M = (20094, 20680)$ и сеансовый 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 передает ответ x абоненту B

$M = (26922, 13593) - 2347(31138, 17196) = (26922, 13593) - (15796, 11509) = (20094, 20680)$.

$A \rightarrow B$: $x = [(17653 + 2347)(1, 12510)] + (20094, 20680) = (26671, 23585) + (20094, 20680) = (3872, 18802)$.

Абонент B выполняет проверку

$\gamma = (3872, 18802) - [(20094, 20680) + (25097, 2812)] = (3872, 18802) - (31308, 10885) = (30803, 19514)$ – проверка выполнена.

Второй цикл протокола.

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

$A \rightarrow B$: $Y_a = (25097, 2812)$; $\gamma = 23983(1, 12510) = (6817, 29794)$.

2. Абонент B выбирает случайное сообщение $M = (14000, 30002)$ и сеансовый 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 передает ответ x абоненту B

$M = (21025, 14036) - 2347(14774, 7451) = (21025, 14036) - (28106, 27452) = (14000, 30002)$.

$A \rightarrow B$: $x = [(23983 + 2347)(1, 12510)] + (14000, 30002) = (14063, 691) + (14000, 30002) = (1103, 29627)$.

Абонент B выполняет проверку

$\gamma = (1103, 29627) - [(14000, 30002) + (25097, 2812)] = (1103, 29627) - (26666, 6308) = (6817, 29794)$ – проверка выполнена.

Для анализа предложенного криптографического протокола на устойчивость к атакам противника был применен программный продукт AVISPA (Automated Validation of Internet Security Protocols and Applications) [13]. Главное преимущество AVISPA 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) и IF (Intermediate Format), что позволяет существенно расширить класс изучаемых протоколов, а также интегрировать в единую платформу сразу несколько различных методов [5, 13] (рис. 2).

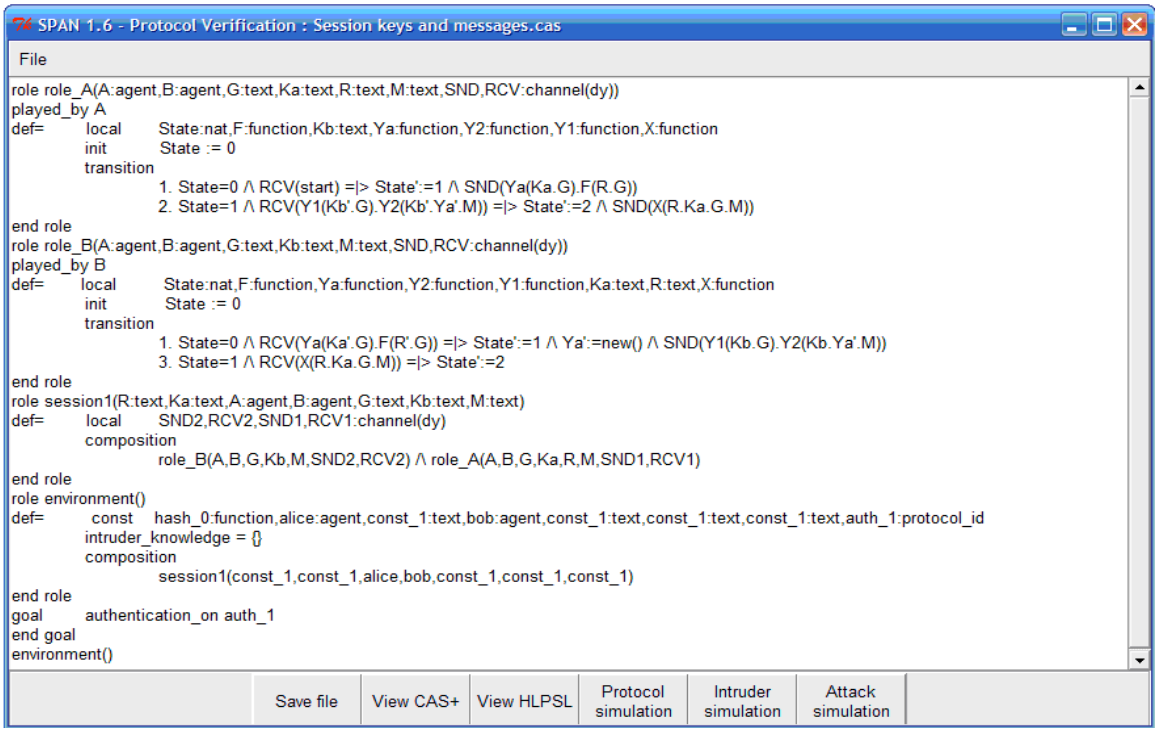

Рисунок 2 – Модель криптографического протокола на языке HLPSL

Выполнена проверка модели предложенного криптографического протокола с помощью Protocol Simulation пакета SPAN (Security Protocol Animator) [14] (рис. 3, 4).

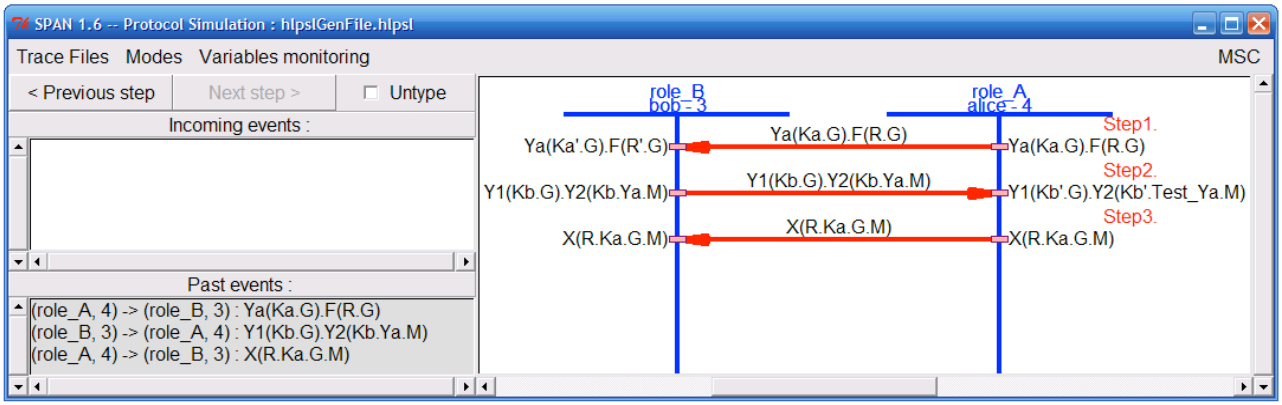

Рисунок 3 – Моделирование криптографического протокола

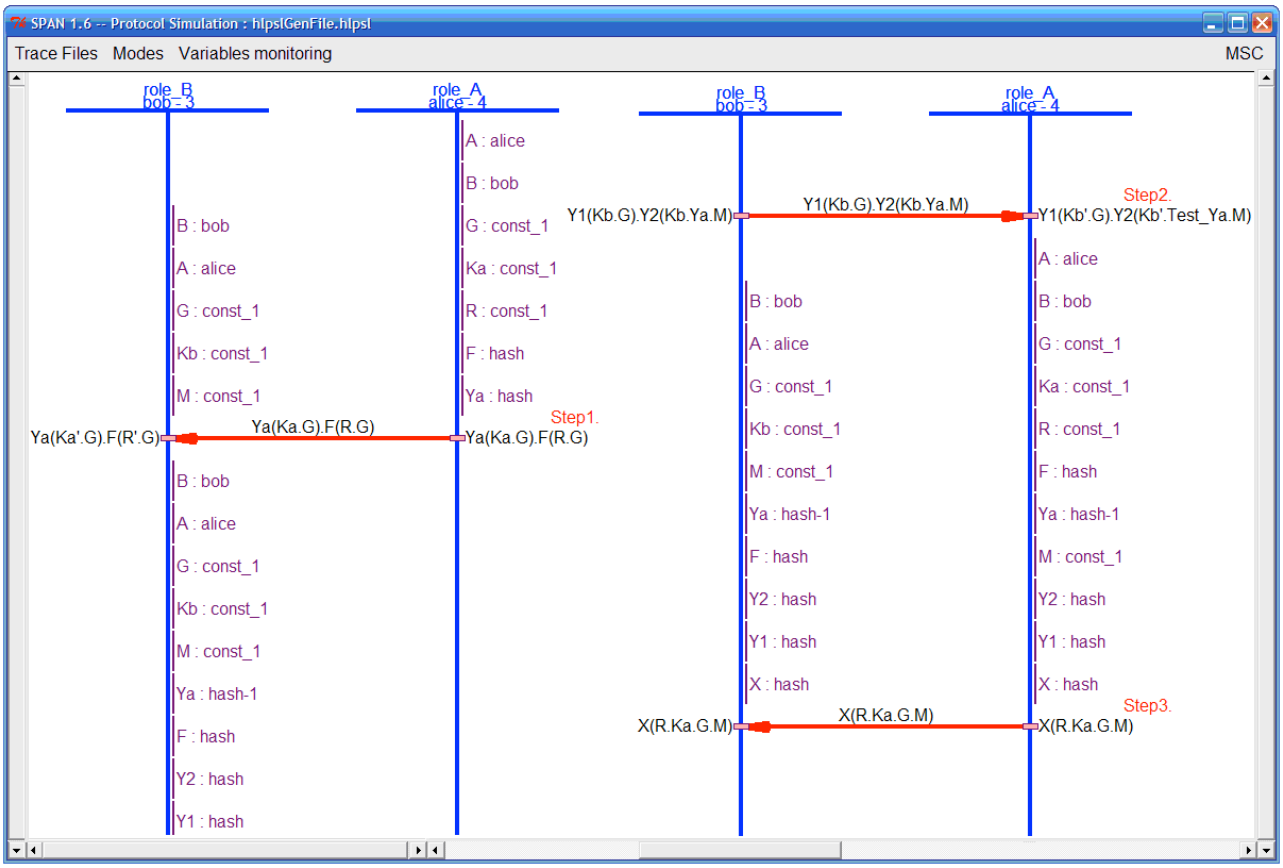

Рисунок 4 – Проверка модели криптографического протокола

Программная верификация криптографического протокола и устойчивость протокола к атакам противника была выполнена с помощью программных модулей OFMC (On the Fly Model Checker) и CLAtSe (Constraint Logic based Attack Searcher) AVISPA [15]. Модуль OFMC выполняют верификацию методом проверки на модели. В результате проверки криптографического протокола известных атак на протокол не найдено (рис. 5).

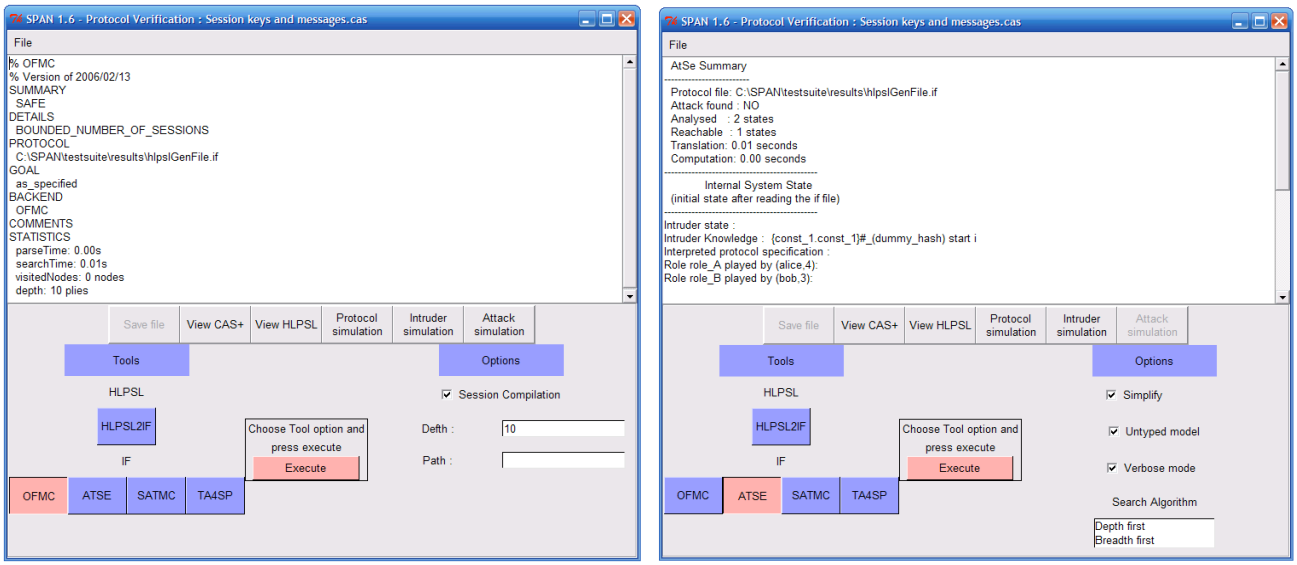

Рисунок 5 – Верификация и устойчивость протокола к атакам

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. Важным условием работы протока является использование случайных сеансовых ключей k_{bi} и сообщений M_i для каждого цикла аккредитации.

В работе определена полнота и корректность протокола, дан пример расчета, выполнена проверка модели и верификация протокола. Для проверки криптографического протокола на устойчивость к атакам противника были применены средства пакета SPAN для AVISPA. В результате проверки протокола 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 ЕС оценивается величиной $O(\log^2 p)$, а в мультипликативной группе поля – $O(\log^3 p)$, преимущество использования ЕС очевидно. Следовательно, при использовании криптографического протокола ZKP ЕС позволит уменьшить размеры параметров протокола, увеличить криптографическую стойкость, уменьшить длительность процесса идентификации.

ЛИТЕРАТУРА:

1. Menezes A. Handbook of Applied Cryptography / Menezes A., Oorschot P. van, Vanstone S. – 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. 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. AVISPA [Электронный ресурс]. – Режим доступа: http://www.avispa-project.org/.
14. Security Protocol Animator [Электронный ресурс]. – Режим доступа: http:// people.irisa.fr/ Thomas.Genet/span/.
15. An On-The-Fly Model-Checker for Security Protocol Analysis [Электронный ресурс]. – Режим доступа: http://www.avispa-project.org/papers/ofmc-esorics03.pdf.

REFERENCES:

1. Menezes A., P. van Oorschot and S. Vanstone. *Handbook of applied cryptography*. CRC Press, 1996: Print.
2. Shnajer B. Prikladnaja kriptografija. Protokoly, algoritmy, ishodnye teksty na jazyke Si / Shnajer B. – M.: Triumf, 2002. – 816 p.

3. Sokolov A. V. Zashhita informacii v raspredelennyh korporativnyh setjah i sistemah / A. V. Sokolov, V. F. Shan'gin. – M.: DMK Press, 2002. – 656 p.
4. Pogorelov B. A. Slovar kriptograficheskih terminov / B. A. Pogorelov, V. N. Sachkov. – M.: MCNMO, 2006. – 91 p.
5. Cheremushkin A. V. Kriptograficheskie protokoly. Osnovnye svojstva i ujazvimosti / Cheremushkin A. V. – M.: Akademija, 2009. – 272 p.
6. Zapechnikov S. V. Kriptograficheskie protokoly i ih primenenie v finansovoj i kommercheskoj dejatel'nosti / Zapechnikov S. V. – M.: Gorjachaja linija-Telekom, 2007. – 320 p.
7. Hankerson D., A. Menezes and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004. Print.
8. Bolotov A. A. Jelementarnoe vvedenie v jellipticheskuju kriptografiju: Algebraicheskie i algoritmicheskie osnovy / Bolotov A. A., Gashkov S. B., Frolov A. B. – M.: KomKniga, 2006. – 328 p.
9. Bolotov A. A. Jelementarnoe vvedenie v jellipticheskuju kriptografiju: Protokoly kriptografii na jellipticheskih krivyh / Bolotov A. A., Gashkov S. B., Frolov A. B. – M.: KomKniga, 2006. – 280 p.
10. Vasilenko O. N. Teoretiko-chislovye algoritmy v kriptografii / Vasilenko O. N. – M.: MCNMO, 2003. – 328 p.
11. Rostovcev A. G. Teoreticheskaja kriptografija / A. G. Rostovcev, E. B. Mahovenko. – M.: Professional, 2005. – 490 p.
12. Moldovjan N. A. Kriptografija: ot primitivov k sintezu algoritmov / Moldovjan N. A., Moldovjan A. A., Eremeev M. A. – SPb.: BHV-Peterburg, 2004. – 448 p.
13. AVISPA [Jelektronnyj resurs]. – Rezhim dostupa: http://www.avispa-project.org/.
14. Security Protocol Animator [Jelektronnyj resurs]. – Rezhim dostupa: http://people.irisa.fr/ Thomas.Genet/ span/.
15. An On-The-Fly Model-Checker for Security Protocol Analysis [Jelektronnyj resurs]. – Rezhim dostupa: http://www.avispa-project.org/papers/ofmc-esorics03.pdf.