С. М. Рацеев, М. А. Ростов, О протоколах аутентификации с нулевым разглашением знания, *Изв. Сарат. ун-та. Нов. сер. Сер.: Математика. Механика. Информатика*, 2019, том 19, выпуск 1, 114–121

DOI: 10.18500/1816-9791-2019-19-1-114-121

УДК 519.7

О протоколах аутентификации с нулевым разглашением знания

С. М. Рацеев, М. А. Ростов

Рацеев Сергей Михайлович, доктор физико-математических наук, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, Россия, 432017, Ульяновск, ул. Л. Толстого, д. 42, ratseevsm@mail.ru

Ростов Михаил Александрович, студент кафедры информационной безопасности и теории управления, Ульяновский государственный университет, Россия, 432017, Ульяновск, ул. Л. Толстого, д. 42

В работе приводится сравнительный анализ производительности протокола аутентификации Шнорра и протокола аутентификации на основе задачи о нахождении гамильтонова цикла в графе. Показано, что с применением технологии CUDA производительность протоколов на графах не уступает производительности протокола Шнорра. Важность такого исследования заключается в том, что протоколы на графах (протокол аутентификации на основе доказательства изоморфизма графов, протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе и т. д.) обладают свойством нулевого разглашения знания. Данные протоколы основаны на NP-полных задачах, поэтому являются независимыми от квантовых вычислений, а именно устойчивы к квантовым атакам. Также в работе приводятся модифицированные алгоритмы двухшаговых протоколов аутентификации на основе асимметричных шифров с использованием эллиптических кривых.

Ключевые слова: протокол аутентификации, нулевое разглашение, эллиптическая кривая, технология CUDA.

Поступила в редакцию: 24.05.2018 / Принята: 18.12.2018 / Опубликована онлайн: 28.02.2019

DOI: https://doi.org/10.18500/1816-9791-2019-19-1-114-121

ВВЕДЕНИЕ

Протоколы аутентификации разделяют на следующие классы: протоколы, основанные на паролях (слабая аутентификация); протоколы, использующие технику «запрос-ответ» (сильная аутентификация); протоколы, основанные на технике доказательства знания; протоколы аутентификации, основанные на протоколах доказательства знания с нулевым разглашением.

В парольных схемах нарушитель может запомнить передаваемые сообщения и в следующий раз использовать эту информацию. В протоколах типа «запрос-ответ» нарушитель, контролируя канал связи, может навязывать специально подобранные запросы и, анализируя ответы, получить информацию о секрете. Чтобы избежать этого, применяют протоколы доказательства знания (некоторой секретной информации), которые обладают дополнительным свойством нулевого разглашения секрета. Более подробную информацию о данных протоколах можно найти, например, в работах [1, 2].

Хорошо известный протокол аутентификации Шнорра [3] основан на трудной задаче дискретного логарифмирования. В ходе выполнения данного протокола не происходит никакой (дополнительной) утечки информации о секретном ключе. Существуют также протоколы аутентификации на основе техники доказательств знания, построенных на основе NP-полных задач. Такими протоколами, в частности,

являются протокол аутентификации на основе доказательства изоморфизма графов, протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе и т.д. Эти протоколы основаны на NP-полных задачах и поэтому являются независимыми от квантовых вычислений.

Целью данной работы является попытка ускорения протоколов аутентификации с использованием графов на основе применения технологии CUDA (Compute Unified Device Architecture), в результате чего будет показано, что данные протоколы не уступают в скорости некоторым протоколам аутентификации на примере протокола Шнорра. В качестве испытуемых берутся протокол аутентификации Шнорра и протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе.

Также в данной работе исследуются протоколы аутентификации на основе асимметричных шифров. Преимущество таких протоколов в том, что они являются двухшаговыми. В данной работе приводятся некоторые протоколы аутентификации на основе асимметричных шифров с использованием эллиптических кривых. Сам принцип функционирования криптосистем на эллиптических кривых подробно изложен в [4]. Безопасность криптосистем на эллиптических кривых ECC (Elliptic Curve Cryptography), как правило, основана на трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой [4]. Исследования показывают, что в классе криптосистем с открытым ключом криптосистемы на эллиптических кривых превосходят классические криптосистемы на основе модулярной арифметики как минимум по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при аппаратной и программной реализации. Наглядно это демонстрируется в работе [5].

1. ПРОТОКОЛ АУТЕНТИФИКАЦИИ ШНОРРА

Протокол аутентификации Шнорра [3] основан на трудной задаче дискретного логарифмирования. Пусть p — простое число, q — простой делитель числа $p-1$, $g \in \mathbb{Z}_p$, имеющий порядок q. Абонент A выбирает случайное число x, для которого выполнено $1 \leqslant x \leqslant q-1$, и вычисляет значение открытого ключа $y = g^{-x} \pmod p$.

Число x — секретный ключ, элементы p, q, g, y — открытые параметры протокола. Протокол аутентификации Шнорра имеет следующий вид:

1) доказывающий A генерирует случайное целое число k, где $1 \leqslant k \leqslant q-1$, вычисляет $r = g^k \pmod p$ и отправляет проверяющему B значение r;
2) проверяющий B генерирует случайный число a из диапазона от 0 до $2^t - 1$, которое передает абоненту A;
3) абонент A вычисляет и передает проверяющему B значение $s = k + ax \pmod q$;
4) проверяющий B проверяет выполнение сравнения $r \equiv g^s y^a \pmod p$. Если оно выполнено, то доказательство принимается, в противном случае — отвергается.

2. ИТЕРАТИВНЫЙ И ТРЕХШАГОВЫЙ ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ЗАДАЧИ О НАХОЖДЕНИИ ГАМИЛЬТОНОВА ЦИКЛА В ГРАФЕ

Гамильтоновым циклом в графе называется непрерывный путь, проходящий через все вершины графа ровно по одному разу. Понятно, что если в графе n вершин (занумерованных числами $1, 2, \ldots, n$) и в нем имеется гамильтонов цикл, то путем перебора всех перестановок симметрической группы S_n мы найдем гамильтонов цикл $(\tau(1), \tau(2), \ldots, \tau(n))$ для некоторой перестановки $\tau \in S_n$. Так как $|S_n| = n!$, то

уже при сравнительно небольших значениях n такой подход становится практически нереализуемым. Доказано, что задача нахождения гамильтонова цикла в графе является NP-полной (для ее решения неизвестны алгоритмы, существенно более быстрые, чем метод перебора).

Рассмотрим протокол, в котором абонент A будет доказывать абоненту B, что он знает гамильтонов цикл в некотором графе G так, чтобы абонент B не получил никаких знаний об этом цикле (доказательство с нулевым разглашением). Пусть абонент A знает гамильтонов цикл в графе G из n вершин, который передал ему доверенный центр. Он может это доказывать абоненту B (и всем, кто имеет этот граф) с помощью описываемого ниже протокола.

Протокол доказательства состоит из следующих шагов:

1) абонент A случайно выбирает перестановку $\sigma \in S_n$ и применяет ее к номерам вершин графа G, получив при этом граф $H = \sigma(G)$. Понятно, что графы G и H изоморфны. Зная гамильтонов цикл в графе G, абонент A знает гамильтонов цикл и в графе H. Граф H передается проверяющему B;
2) абонент B, получив граф H, случайным образом выбирает $a \in \{0, 1\}$ и передает a абоненту A;
3) если $a = 0$, то абонент A предоставляет абоненту B перестановку σ (тем самым показывая, что он знает изоморфизм графов G и H). Если $a = 1$, то абонент A предоставляет проверяющему B гамильтонов цикл графа H;
4) проверяющий B проверяет, что в случае $a = 0$ предъявленная перестановка σ действительно переводит граф G в граф H, а в случае $a = 1$ проверяет гамильтонов цикл графа H.

Эти четыре шага повторяются независимо t раз. Трехшаговый протокол для предыдущего случая примет следующий вид:

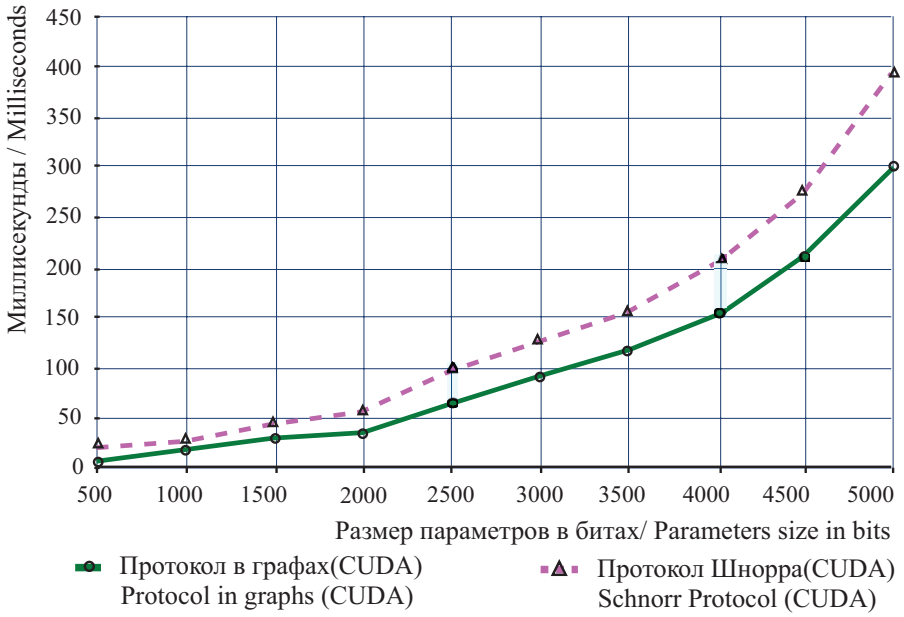
1) абонент A случайно выбирает перестановки $\sigma_i \in S_n$ и применяет их к номерам вершин графа G, получив при этом графы $H_i = \sigma_i(G)$, $i = 1, \ldots, m$, которые передаются абоненту B;
2) проверяющий B генерирует случайную битовую строку $(a_1, \ldots, a_m) \in \{0, 1\}^m$ и передает ее абоненту A;
3) при $a_i = 0$ абонент A фиксирует перестановку σ_i, при $a_i = 1$ — перестановку, являющуюся гамильтоновом циклом графа H_i, $i = 1, \ldots, m$. Данные перестановки передаются абоненту B;
4) абонент B проверяет, что в случае $a_i = 0$ предъявленная перестановка σ_i действительно переводит граф G в граф H_i, а в случае $a_i = 1$ проверяет гамильтонов цикл графа H_i, $i = 1, \ldots, m$.

Приведенный выше протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе был реализован вторым автором на следующих широко используемых языках программирования: Java, C, C#, PHP. В работе [6] показано, что асимптотически хорошие скорости выполнения протокола показывают языки C и Java. Также для данного протокола в рамках исследования применялась технология CUDA. В работе [6] показано, что технология CUDA имеет очень высокую скорость выполнения по сравнению с самой быстрой реализацией на языке C.

3. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛА ШНОРРА И ТРЕХШАГОВОГО ПРОТОКОЛА НА ОСНОВЕ ЗАДАЧИ О НАХОЖДЕНИИ ГАМИЛЬТОНОВА ЦИКЛА В ГРАФЕ

Хорошо известно, что на современном этапе развития информационных технологий одним из основных факторов увеличения вычислительной мощности является использование графических процессоров. Одними из наиболее эффективно используемых графических процессоров (GPU — graphics processing unit) для выполнения общих вычислений являются видеоускорители компании nVidia с архитектурой CUDA (Compute Unified Device Architecture). Вычислительные задачи, реализованные на CUDA, получают значительное ускорение в таких областях, как молекулярная динамика [7, 8], астрофизика [9], медицинская диагностика [10] и т. д.

На рисунке приведены графики зависимости времени выполнения трехшаговых протоколов (протокола Шнорра и протокола на основе задачи о нахождении гамильтонова цикла в графе при $m = 12$) от размера параметров в битах. Оба протокола реализованы с использованием технологии CUDA. При этом для первого протокола учитывается количество значащих бит двоичного представления простого числа p, для второго протокола — количество значащих бит двоичного представления числа $n!$, где n — число вершин графа G.



Графики зависимости времени выполнения (в миллисекундах) трехшаговых протоколов от размера параметров в битах
Graphs of execution time (in milliseconds) of three-step protocols on the size of the parameters in bits

На данном рисунке видно, что применение технологии CUDA значительно улучшает производительность протоколов аутентификации на основе графов (для протокола аутентификации на основе доказательства изоморфизма графов ситуация аналогична). Более того, протоколы на основе графов с применением технологии CUDA имеют более высокую производительность нежели протокол Шнорра. И эта разница в производительности становится все более заметна с ростом числа вершин графа. Высокая производительность вычислений протоколов на графах достигается за счет более удобного взаимодействия с блоками памяти в графическом процессоре, так как матричные вычисления наиболее оптимизированы для такого рода расчетов.

Тесты проводились на ПК со следующими характеристиками: ОС Windows 10, GPU GeForce GTX 1050 2 Gb, ОЗУ DDR3 8 Gb, CPU Intel Core i5 3,2 GHz.

4. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ АСИММЕТРИЧНЫХ ШИФРОВ

Построение протоколов с нулевым разглашением можно реализовать, используя известные алгоритмы открытого шифрования. В качестве секретной информации, которой владеет доказывающая сторона A, будет использоваться секретный ключ x асимметричного шифра. Пусть D_x — алгоритм расшифрования на секретном ключе x, E_y — алгоритм шифрования на открытом ключе y. Проверяющая сторона шифрует некоторое сообщение M на открытом ключе y и передает криптограмму $C = E_y(M)$ абоненту A. Абонент A демонстрирует владение секретной информацией x тем, что расшифровывает сообщение своим секретным ключом: $M = D_x(C)$ и передает сообщение M проверяющей стороне B. Для проверяющей стороны B это не несет никакой дополнительной информации о секретном ключе x, так как у B до этого было то же самое сообщение M. При этом при построении протоколов с нулевым разглашением знания нужен некоторый механизм, который позволит владельцу секретного ключа (доказывающему A) до передачи восстановленного сообщения M проверяющему B убедиться в том, что последнее уже известно проверяющему B.

В качестве такого механизма могут использоваться алгоритмы хеширования (хеш-функции). Данный механизм используется в протоколах с нулевым разглашением, описанных в стандарте [11].

В стандарте [11] регламентируется формирование запроса в виде пары значений (C, H), где C — шифртекст, полученный путем шифрования некоторого сообщения M по открытому ключу доказывающего A и H — значение хеш-функции, вычисленное от сообщения M с использованием некоторой специфицированной хеш-функции h: $H = h(M)$. Получая запрос (C, H), доказывающий имеет возможность убедиться в том, что восстановленное им из шифртекста C сообщение M известно проверяющему. Для этого достаточно вычислить значение хеш-функции от восстановленного сообщения и сравнить его со значением второго элемента запроса.

В соответствии с [11] двухшаговый протокол с нулевым разглашением знания включает следующие шаги:

1) проверяющий B выбирает произвольное сообщение M и, используя специфицированный алгоритм открытого шифрования E_y и открытый ключ y доказывающего, зашифровывает сообщение : $C = E_y(M)$. Затем, используя специфицированную хеш-функцию h, вычисляет значение хеш-функции от M: $H = h(M)$. После этого он отправляет доказывающему A пару значений (C, H) в качестве своего запроса;
2) доказывающий A расшифровывает криптограмму C, используя свой личный секретный ключ x, в результате чего получает сообщение $\widetilde{M} = D_x(C)$. Затем он вычисляет значение хеш-функции от $\widetilde{M}$: $\widetilde{H} = h(\widetilde{M})$, сравнивает значения $\widetilde{H}$ и H и если $\widetilde{H} = H$, то отправляет проверяющему значение $\widetilde{M}$ в качестве своего ответа;
3) если выполнено равенство $\widetilde{M} = M$, то проверяющий B принимает доказательство; если равенство не выполнено, то отвергает.

Протокол аутентификации на основе шифра Эль-Гамаля с использованием эллиптических кривых. Пусть q — некоторый (достаточно большой) простой делитель числа $|E|$, где E — эллиптическая кривая, и некоторая точка $G \in E$ имеет порядок q.

Общедоступные параметры системы: q, G, E. Абонент A выбирает секретный ключ x, $0 < x < q$, и вычисляет открытый ключ $Y = [x]G$. Протокол аутентификации имеет следующий вид:

1) проверяющий B генерирует случайную точку $M = [r]G \in E$ для некоторого случайного r, $0 < r < q$, генерирует случайным образом некоторое число k, $0 < k < q$, вычисляет точки эллиптической кривой

$$C_1 = [k]G, \quad C_2 = M + [k]Y,$$

вычисляет $H = h(M)$ и отправляет доказывающему A тройку значений (C_1, C_2, H);
2) доказывающий A вычисляет $\widetilde{M} = C_2 + [q - x]C_1$, $\widetilde{H} = h(\widetilde{M})$. Если $\widetilde{H} = H$, то отправляет проверяющему значение $\widetilde{M}$ в качестве своего ответа.
3) после этого проверяющий B проверяет равенство $\widetilde{M} = M$.

Протокол аутентификации на основе схемы Диффи – Хеллмана с использованием эллиптических кривых. Пусть q — некоторый (достаточно большой) простой делитель числа $|E|$, где E — эллиптическая кривая. Пусть некоторая точка $G \in E$ имеет порядок q. Абонент A выбирает случайное число (секретный ключ) x, $1 \leqslant x \leqslant q - 1$, и вычисляет значение открытого ключа $Y = [x]G$. Протокол аутентификации имеет следующий вид:

1) проверяющий B генерирует случайное число k, $1 < k < q - 1$, вычисляет точки эллиптической кривой E и соответствующее значение хеш-функции:

$$C = [k]G, \quad Z = [k]Y, \quad H = h(Z)$$

и отправляет доказывающему A пару значений (C, H);
2) доказывающий A вычисляет $\widetilde{Z} = [x]C$, $\widetilde{H} = h(\widetilde{Z})$. Если $\widetilde{H} = H$, то отправляет проверяющему точку эллиптической кривой $\widetilde{Z}$ в качестве своего ответа;
3) после этого проверяющий B проверяет равенство $\widetilde{Z} = Z$.

В работе [2] предложен подход к синтезу двухшаговых протоколов с нулевым разглашением секрета, основанных на асимметричных шифрах, отличающийся использованием меток, встраиваемых в шифруемое сообщение. Для данных алгоритмов также можно применить эллиптические кривые, как и в протоколах, рассмотренных выше.

Библиографический список

1. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости. М. : ИЦ «Академия», 2009. 272 с.
2. *Молдовян А. А., Молдовян Д. Н., Левина А. Б.* Протоколы аутентификации с нулевым разглашением секрета. СПб. : Университет ИТМО, 2016. 55 с.
3. *Schnorr C. P.* Efficient Identification and Signatures for Smart Cards // Advances in Cryptology – CRYPTO'89. Proceedings. CRYPTO 1989. Lecture Notes in Computer Science. Vol. 435. N. Y. : Springer, 1990. P. 239–252. DOI: https://doi.org/10.1007/0-387-34805-0_22
4. *Hankerson D., Menezes A., Vanstone S.* Guide to Elliptic Curve Cryptography. N. Y. : Springer-Verlag, 2004. 358 p. DOI: https://doi.org/10.1007/b97644

5. An Elliptic Curve Cryptography (ECC) Primer: why ECC is the next generation of public key cryptography. The Certicom Corp. 'Catch the Curve' White Paper Series, June 2004. 24 p. URL: https://www.certicom.com/content/dam/certicom/images/pdfs/WP-ECCprimer.pdf (дата обращения: 05.09.2018).
6. *Рацеев С. М., Ростов М. А.* Методы ускорения и усовершенствования протокола аутентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе // Научные ведомости БелГУ. Экономика. Информатика. 2017. № 16(265), вып. 43. С. 131–137.
7. *Stone J. E., Phillips J. C., Freddolino P. L., Hardy D. J., Trabuco L. G., Schulten K.* Accelerating molecular modeling applications with graphics processors // J. Comput. Chem. 2007. Vol. 28, № 16. P. 2618–2640. DOI: https://doi.org/10.1002/jcc.20829
8. *Van Meel J. A., Arnold A., Frenkel D., Zwart S. P., Belleman R.* Harvesting graphics power for MD simulations // Molecular Simulation. 2008. Vol. 34, № 3. P. 259–266. DOI: https://doi.org10.1080/08927020701744295
9. *Harris C., Haines K., Staveley-Smith L.* GPU accelerated radio astronomy signal convolution // Exp. Astron. 2008. Vol. 22, iss. 1–2. P. 129–141. DOI: https://doi.org/10.1007/s10686-008-9114-9
10. *Muyan-Ozcelik P., Owens J. D., Xia J., Samant S. S.* Fast deformable registration on the GPU: A CUDA implementation of demons // Proc. Int. Conf. Computational Science and its Applications. Perugia, Italy, 2008. P. 223–233. DOI: https://doi.org/10.1109/ICCSA.2008.22
11. ISO/IEC 9798-5:2009(E) «Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique». URL: https://www.iso.org/standard/50456.html (дата обращения: 05.09.2018).

Образец для цитирования:
Рацеев С. М., Ростов М. А. О протоколах аутентификации с нулевым разглашением знания // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2019. Т. 19, вып. 1. С. 114–121. DOI: https://doi.org/10.18500/1816-9791-2019-19-1-114-121

Zero-Knowledge Proof Authentication Protocols

S. M. Ratseev, M. A. Rostov

Sergey M. Ratseev, http://orcid.org/0000-0003-4995-9418, Ulyanovsk State University, 42 L. Tolstoy St., 432017 Ulyanovsk, Russia, ratseevsm@mail.ru

Mihail A. Rostov, Ulyanovsk State University, 42 L. Tolstoy St., 432017 Ulyanovsk, Russia

The paper presented the comparative analysis of the authentication Shnorr's protocol and the authentication protocol based on the task of finding a Hamilton cycle in the graph. It is shown that with the use of CUDA technology the productivity of protocols on graphs is as high as Shnorr's protocol productivity. The importance of such research is that protocols on graphs (the authentication protocol on the basis of the proof of graph isomorphism, the authentication protocol based on the task of finding a Hamilton cycle in the graph, etc.) have the property of zero-knowledge proof. These protocols are based on NP complete tasks therefore they are independent of quantum computings, namely, are resistant to the quantum attacks. Also the modified algorithms of two-step authentication protocols with zero-knowledge proof based on asymmetric ciphers with the use of elliptic curves are also given.

Keywords: authentication protocol, zero-knowledge proof, elliptic curve, CUDA technology.

Received: 24.05.2018 / Accepted: 18.12.2018 / Published online: 28.02.2019

References

1. Cheremushkin A. V. *Kriptograficheskie protokoly. Osnovnye svoistva i uyazvimosti* [Cryptographic Protocols. Basic Properties and Vulnerability]. Moscow, IC "Akademiya", 2009. 272 p. (in Russian).
2. Moldovyan A. A., Moldovyan D. N., Levina A. B. *Protokoly autentifikacii s nulevym razglasheniem sekreta* [Authentication protocols with zero-knowledge proof]. St. Petersburg, ITMO Univ., 2016. 55 p. (in Russian).
3. Schnorr C. P. Efficient Identification and Signatures for Smart Cards. *Advances in Cryptology – CRYPTO'89. Proceedings. CRYPTO 1989. Lecture Notes in Computer Science*, vol. 435. New York, Springer, 1990, pp. 239–252. DOI: https://doi.org/10.1007/0-387-34805-0_22
4. Hankerson D., Menezes A., Vanstone S. *Guide to Elliptic Curve Cryptography*. New York, Springer-Verlag, 2004. 358 p. DOI: https://doi.org/10.1007/b97644
5. *An Elliptic Curve Cryptography (ECC) Primer: why ECC is the next generation of public key cryptography*, The Certicom Corp. 'Catch the Curve' White Paper Series, June 2004. 24 p. Available at: https://www.certicom.com/content/dam/certicom/images/pdfs/WP-ECCprimer.pdf (accessed 05 September 2017).
6. Ratseev S. M., Rostov M. A. Methods of an acceleration and enhancement of the cryptography authentication protocol with zero disclosure of knowledge on the basis of the task about finding of a hamilton cycle in the graph. *Belgorod State University Scientific Bulletin. Economics. Computer Science*, 2017, no. 16(265), iss. 43, pp. 131–137 (in Russian).
7. Stone J. E., Phillips J. C., Freddolino P. L., Hardy D. J., Trabuco L. G., Schulten K. Accelerating molecular modeling applications with graphics processors. *J. Comput. Chem.*, 2007, vol. 28, no. 16, pp. 2618–2640. DOI: https://doi.org/10.1002/jcc.20829
8. Van Meel J. A., Arnold A., Frenkel D., Zwart S. P., Belleman R. Harvesting graphics power for MD simulations. *Molecular Simulation*, 2008, vol. 34, no. 3, pp. 259–266. DOI: 10.1080/08927020701744295
9. Harris C., Haines K., Staveley-Smith L. GPU accelerated radio astronomy signal convolution. *Exp. Astron.*, 2008, vol. 22, iss. 1–2, pp. 129–141. DOI: https://doi.org/10.1007/s10686-008-9114-9
10. Muyan-Ozcelik P., Owens J. D., Xia J., Samant S. S. Fast deformable registration on the GPU: A CUDA implementation of demons. In: *Proc. Int. Conf. Computational Science and its Applications*, Perugia, Italy, 2008, pp. 223–233. DOI: https://doi.org/10.1109/ICCSA.2008.22
11. ISO/IEC 9798-5:2009(E): *Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique*. Available at: https://www.iso.org/standard/50456.html (accessed 05 September 2018).

Cite this article as:
Ratseev S. M., Rostov M. A. Zero-Knowledge Proof Authentication Protocols. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2019, vol. 19, iss. 1, pp. 114–121 (in Russian). DOI: https://doi.org/10.18500/1816-9791-2019-19-1-114-121