Ссылка на статью:
// Ученые записки УлГУ. Серия Математика и информационные технологии. 2024, № 1, с. 44-50.

Поступила: 25.02.2024
Окончательный вариант: 25.02.2024

УДК 519.7

О высокоскоростной реализации протоколов аутентификации с нулевым разглашением знания

Рацеев С.М. [*]***, Тарасов Д.А.***

[*]ratseevsm@mail.ru
Ульяновский государственный университет, Россия

В работе приводится сравнительный анализ производительности протокола аутентификации Шнорра и протокола аутентификации на графах. Показано, что с применением технологии CUDA производительность протоколов на графах не уступает производительности хорошо известного протокола Шнорра.

Ключевые слова*: протокол аутентификации, нулевое разглашение, технология CUDA*

Введение

В работе рассматриваются протоколы, которые основаны на технике доказательства с нулевым разглашением знания [1]. Хорошо известным протоколом из данного класса протоколов является протокол Шнорра [1, 5]. Он основан на трудной задаче дискретного логарифмирования. Заметим, что некоторая утечка информации в этом протоколе о секретном ключе происходит только на этапе публикации открытого ключа. Но уже во время выполнения этого протокола никакой утечки не происходит. Другим хорошо известным протоколом с нулевым разглашением знания является протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе. Этот протокол основан на NP-полной задаче, поэтому является независимым от квантовых вычислений, чего нельзя сказать о протоколе Шнорра. В работе показано, как можно увеличить производительность протоколов аутентификации на основе графов, чтобы эти протоколы по производительности не уступали протоколу Шнорра.

1. Протокол аутентификации Шнорра и протокол на графах

Протокол аутентификации Шнорра. Пусть p – достаточно большое простое число, q – достаточно большой простой делитель числа $p-1$, g – элемент из кольца вычетов по модулю p, имеющий порядок q. Абонент A генерирует случайным равновероятным образом элемент x, для которого выполнено $0 \le x < q$, после чего вычисляет значение открытого ключа $y = g^{-x} (\mathrm{mod}\, p)$. Число x является секретным ключом, набор параметров p, q, g, y не держится в секрете. Протокол аутентификации Шнорра имеет следующий вид.

- Доказывающий A генерирует случайное целое k, где $0 \le k < q$, вычисляет значение $r = g^x \pmod{\mathrm{p}}$ и отправляет r проверяющему B.
- Проверяющий B генерирует случайным равновероятным образом целое число a (с условием $0 \le a \le 2^t - 1$, где t – некоторый параметр), которое передает абоненту A.
- Абонент A вычисляет и передает проверяющему B значение $s = k + ax \pmod{q}$.

Теперь если выполнено равенство $r = g^s y^a \pmod{p}$, то проверяющий B принимает доказательство; если равенство не выполнено, то отвергает.

Протокол 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 $1, \dots, n$) и в нем имеется гамильтонов цикл, то путем перебора всех перестановок симметрической группы S_n мы найдем гамильтонов цикл $(\tau(1), \dots, \tau(n))$ для некоторой перестановки $\tau \in S_n$. Так как $|S_n| = n!$, то уже при сравнительно небольших значений n (например, $n = 100$) такой подход становится практически нереализуемым.

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 никакой информации об этом цикле (в теоретико-информационном плане).

Пусть абонент A знает гамильтонов цикл в графе G из n вершин, который передал ему доверенный центр. Он может это доказывать абоненту B с помощью следующего протокола.

- Абонент A случайно равновероятно выбирает перестановку $\sigma \in S_n$ и применяет ее к номерам вершин графа G, получив при этом граф $H = \sigma(G)$. Граф H передается проверяющему B.
- Абонент B, получив граф H, случайным образом выбирает $a \in \{0,1\}$ и передает a абоненту A.
- Если $a = 0$, то абонент A передает абоненту B перестановку σ. Если $a = 1$, то абонент A передает проверяющему B гамильтонов цикл графа H.

Проверяющий B проверяет, что в случае $a = 0$ перестановка σ действительно переводит граф G в граф H, а в случае $a = 1$ проверяет гамильтонов цикл графа H.

Весть протокол повторяется t раз. Вероятность обмана при t реализациях протокола не превосходит 2^{-t}.

2. Тестирование производительности протоколов

Характеристики испытательной системы: операционная система Microsoft Windows 10 (64-bit); процессор Intel Core i5 7500 3.5ГГц; видеокарта NVIDIA GeForce GTX960 2GB; оперативная память: 8Gb DDR3.

Протоколы аутентификации реализованы на следующих языках программирования: C, C#, PHP и технология CUDA. Язык PHP является самым распространённым языком для написания логики серверов. Язык C# использован как пример современного высокоуровневого объектно-ориентированного языка программирования. Язык C является довольно низкоуровневым языком и должен показывать хорошие результаты по производительности. Технология CUDA основана на языке C и предназначена для ускорения параллельных вычислений с использованием GPU.

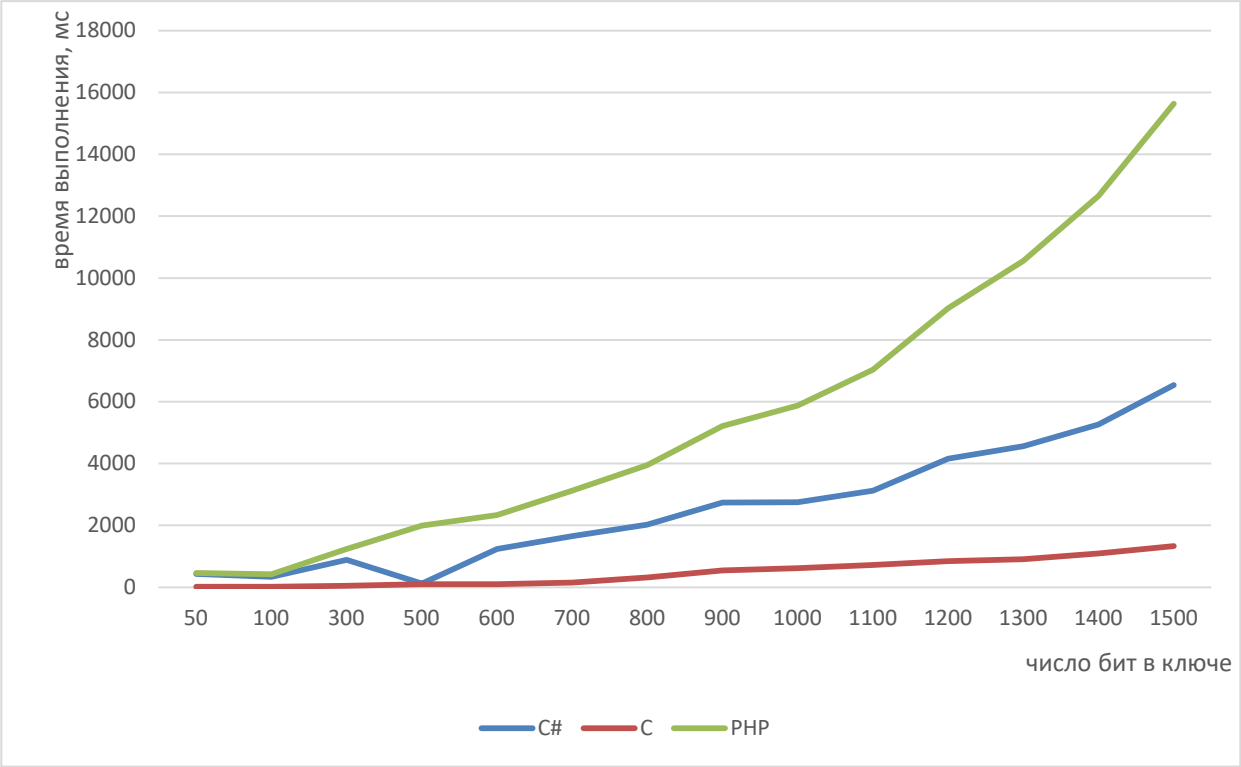

Рис. 1. Графики скоростей выполнения протокола Шнорра на языках C, C#, PHP

Как видно из рис. 1, хорошие скорости выполнения программной реализации протокола показывает язык C [3].

Протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе также был реализован на этих же языках программирования. На рис. 2 приведены графики зависимости времени выполнения протокола от длины ключа.

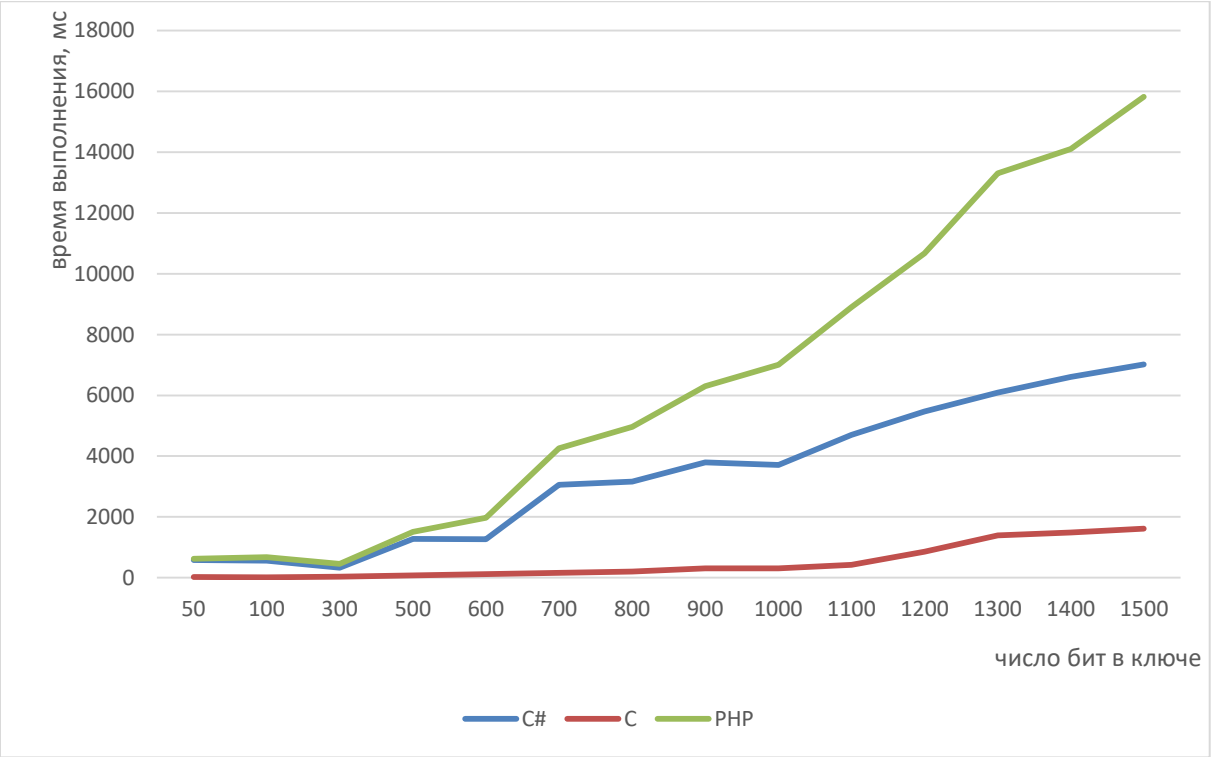

Рис. 2. Графики скоростей выполнения протокола на графах на языках C, C#, PHP

Как видно из рис. 2, как и ранее, асимптотически хорошие скорости выполнения протокола показывает язык C.

3. Применение технологии CUDA

Целью данной работы было ускорение протоколов аутентификации на графах с помощью применения технологии CUDA (Compute Unified Device Architecture), в результате чего будет показано, что данные протоколы не уступают в скорости протоколам аутентификации над кольцами вычетов. В качестве испытуемых используются протокол аутентификации Шнорра и протокол аутентификации на основе задачи о нахождении гамильтонова цикла в графе.

На рис. 3 и 4 соответственно приведены результаты сравнения скоростных характеристики выполнения протоколов Шнорра и протокола на графах с использованием и без использования технологии CUDA. Для протокола на графах применение технологии CUDA (рис. 4, 6) имеет больший эффект за счет того применения матриц смежности.

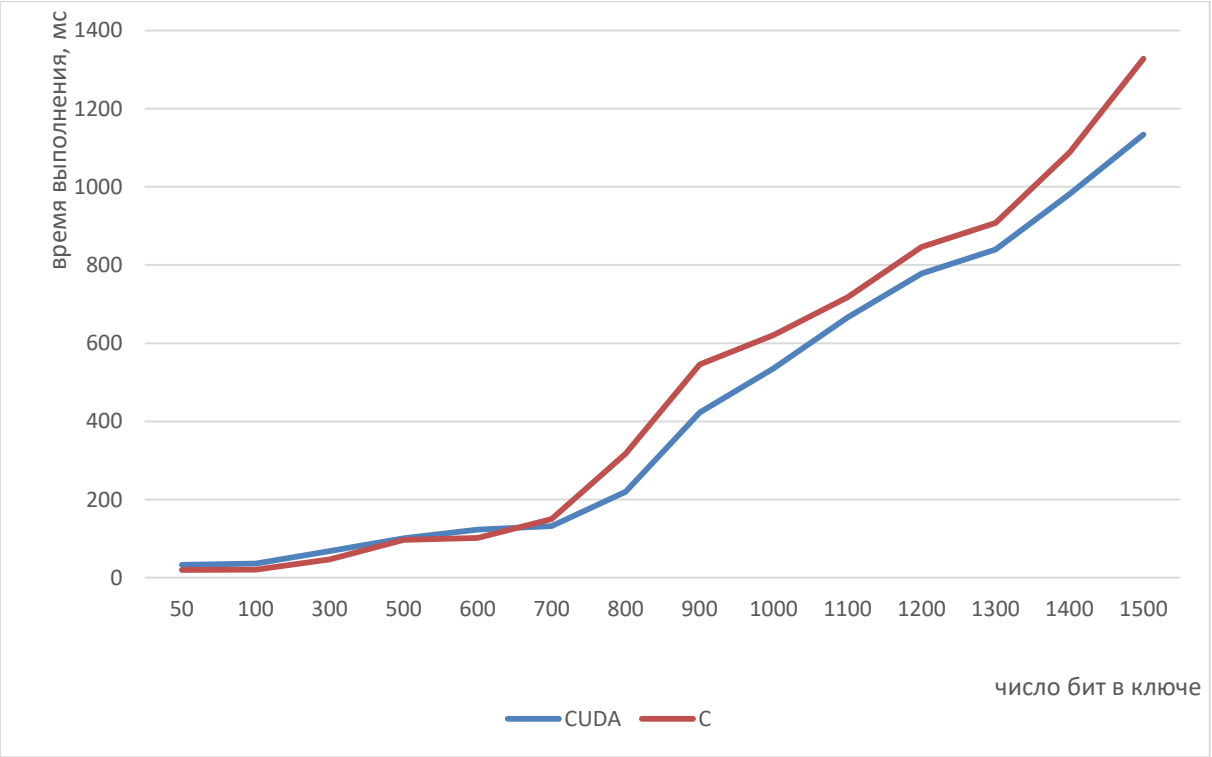

Рис. 3. Графики скоростей выполнения протокола Шнорра с использованием и без использования CUDA

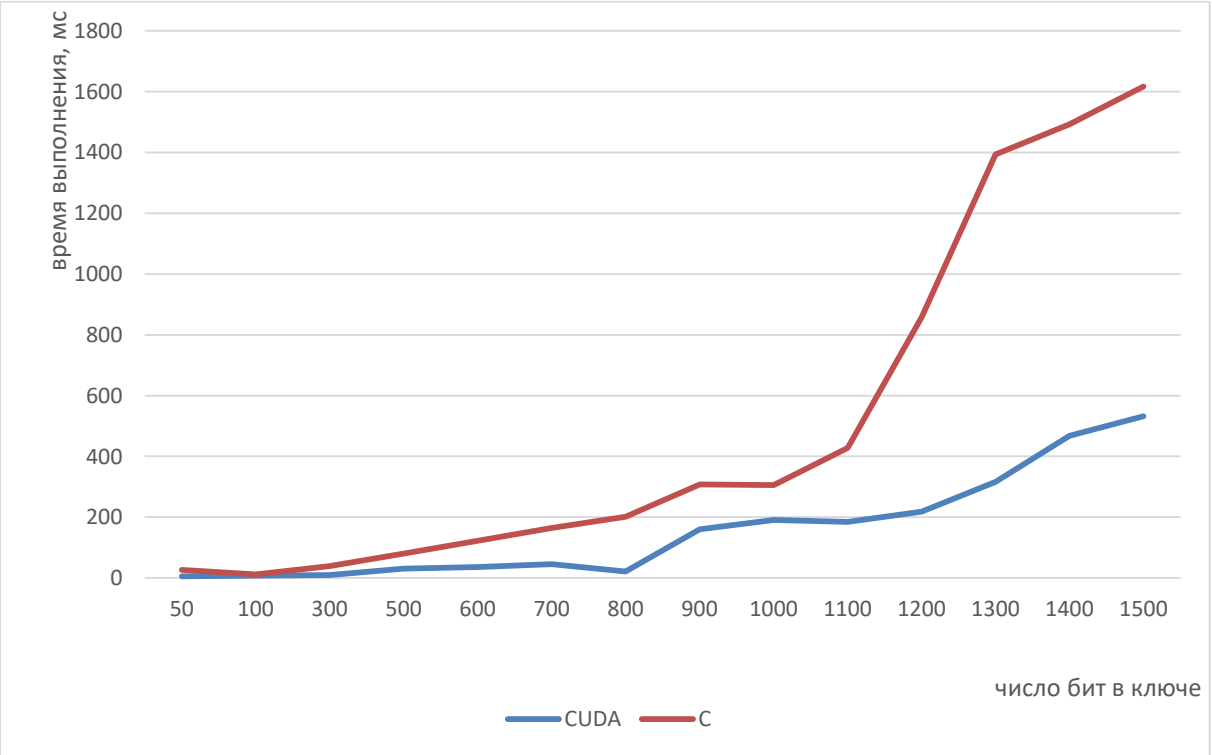

Рис. 4. Графики скоростей выполнения протокола на графах с использованием и без использования CUDA

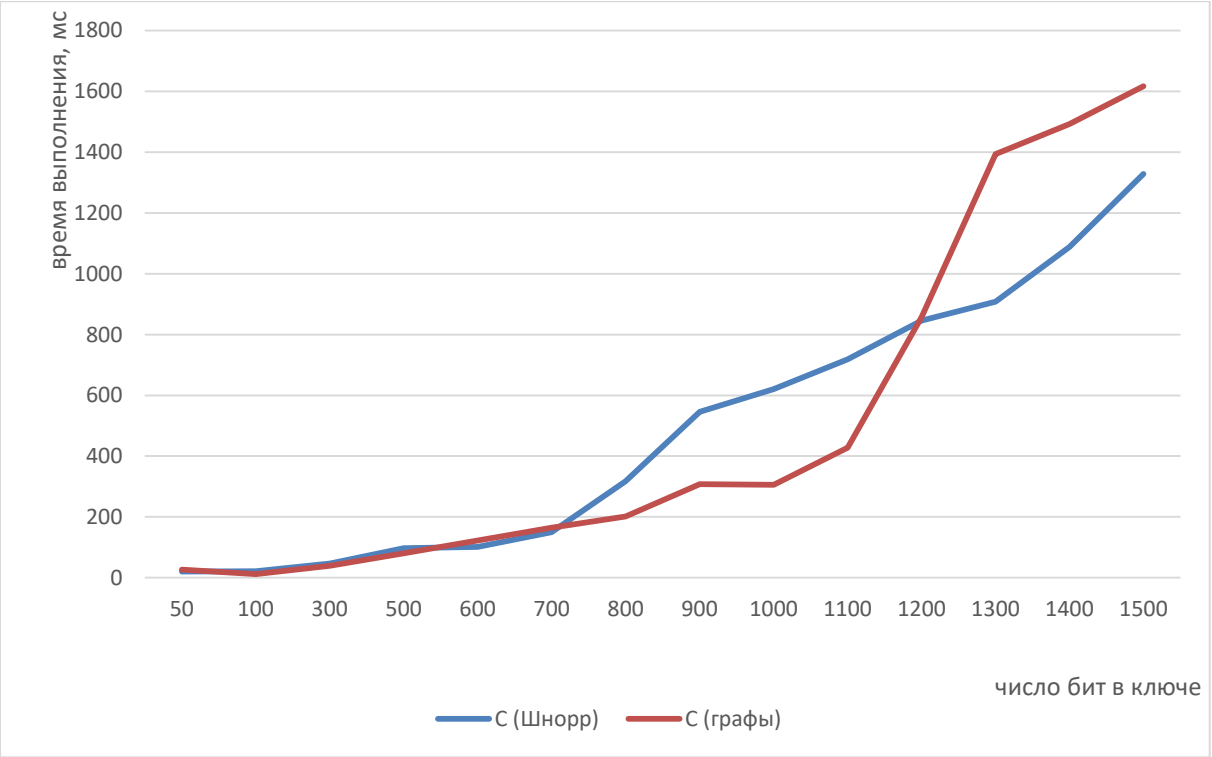

Рис. 5. Графики скоростей выполнения протокола Шнорра и протокола на графах без использования CUDA

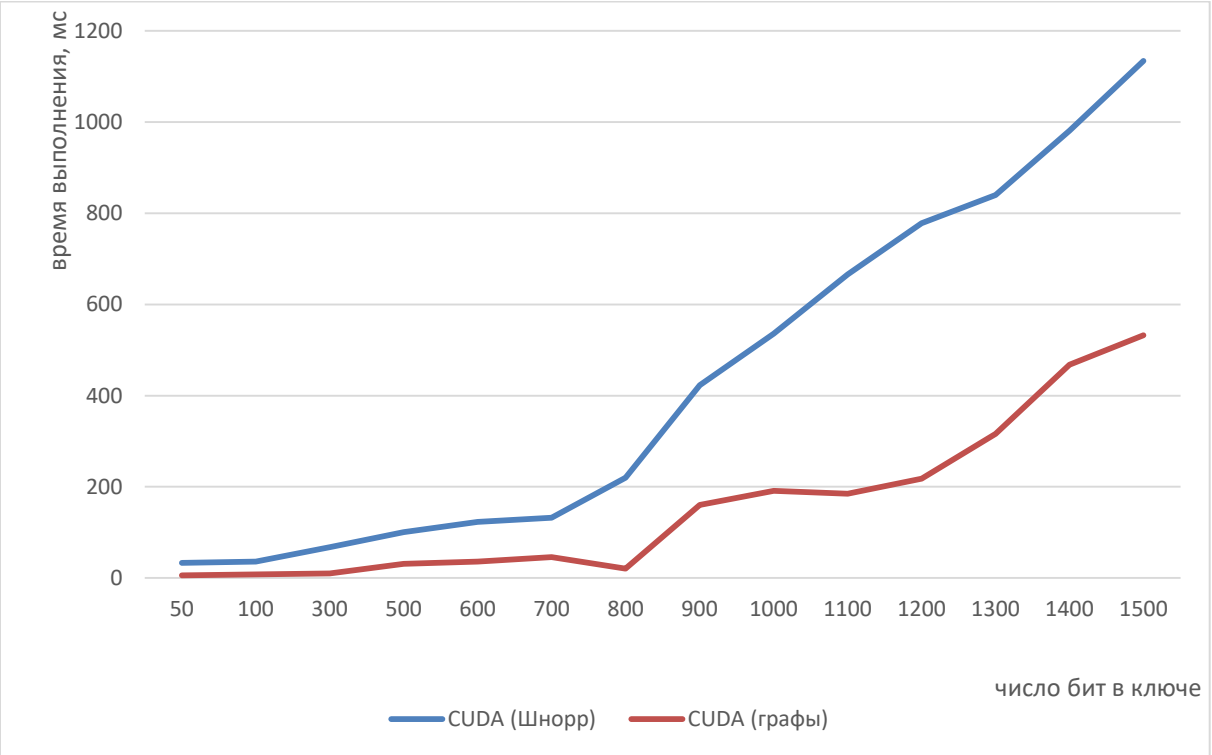

Рис. 6. Графики скоростей выполнения протокола Шнорра и протокола на графах с использованием CUDA

Заключение

Протокол аутентификации Шнорра имеет более простую реализацию и является более быстрым, нежели протоколы аутентификации на графах. Но данный протокол не является постквантовым, так как основан на задаче дискретного логарифмирования. Применение технологии CUDA меняет ситуацию относительно скоростей выполнения протоколов. Теперь уже протоколы на графах показывают лучшую производительность, нежели протокол Шнорра. Похожие результаты были получены в работах [3, 4].

Список литературы

1. Рацеев С. М. *Математические методы защиты информации* : *учеб. пособие для вузов*, *2-е изд., стер*. СПб.: Лань, 2023. 544 с.
2. Рацеев С.М. *Программирование на языке Си* : *учеб. пособие для вузов, 2-е изд., стер*. СПб.: Лань, 2023. 332 с.
3. 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 Белгородского государственного университета. Экономика. Информатика*. 2017, № 16 (265), с. 131-137.
4. Рацеев С.М., Ростов М.А. О протоколах аутентификации с нулевым разглашением знания // *Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика*. 2019, № 1 (19), с. 114-121.
5. Schnorr C.P. Efficient Identification and Signatures for Smart Cards. Advances in Cryptology // *CRYPTO'89. Lecture Notes in Computer Science 435*. 1990. P. 239-252.

On the high-speed program implementation of zero-knowledge authentication protocols

Ratseev, S.M.*[*], *Tarasov, D.A.

[*] ratseevsm@mail.ru

Ulyanovsk State University, Russia

The paper provides a comparative analysis of the capacity of the Schnorr authentication protocol and the authentication protocol based on the problem of finding a Hamiltonian cycle in a graph. It is shown that with the use of CUDA technology the capacity of protocols on graphs is not inferior to the capacity of the Schnorr protocol.

Keywords: authentication protocol, zero-knowledge proof, CUDA technology