S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Том 20, № 2, стр. 144–145 (2023) УДК 004.056.8
https://doi.org/10.33048/semi.2023.20.??? MSC 94A60,81P94

ДОКАЗАТЕЛЬСТВО БЕЗОПАСНОСТИ КВАНТОВО-КЛАССИЧЕСКИХ СИСТЕМ ПРИ НАЛИЧИИ КВАНТОВЫХ ОРАКУЛОВ

С.Б. Кузнецов

Представлено П.П. Петровым

Abstract: The paper studies the construction of cryptographic systems resistant to quantum attacks, with a focus on the QCD (Quantum-Classical Distinguishability) property. It is shown that classical algorithms cannot effectively use quantum queries for hacking, which limits the attacker's capabilities. Statements about the construction of hybrid systems, the security of which is verified by standard methods, without analyzing quantum behavior, are proved. Switching to a backup key in case of suspicious activity is used for protection. The mechanism is based on quantum-resistant pseudo-random functions (PRF), masking the outputs of the quantum algorithm. The key parameters of the system are analyzed, formulas for their interrelation are obtained, pseudocode for the implementation is given, and requirements for the components are formulated. The fulfillment of the QCD property, which ensures protection from classical analysis of a quantum system, is confirmed. The

Kuznetsov, S. B., Proofs of security of quantum-classical systems in the presence of quantum oracles.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23-03 от 27.09.2024 г.).

Поступила 1 января 2023 г., опубликована 31 декабря 2023 г.

proposed approach allows creating hybrid protocols resistant to the development of quantum technologies.

Keywords: Hybrid cryptosystems; Quantum-Classical Distinguishability (QCD) property; pseudorandom Functions (PRF); quantum oracles; resistance to quantum attacks; key switching mechanism; quantum-resistant pseudorandomness.

1 Введение

Современные криптосистемы, такие как RSA и ECC, уязвимы к атакам на квантовых компьютерах. Взломы происходят особенно с использованием алгоритма Шора [1]. Это делает актуальной разработку новых подходов, способных противостоять квантовым угрозам. Одним из перспективных направлений являются гибридные криптопротоколы. Они сочетают классические методы с элементами, устойчивыми к квантовым атакам. Безопасность этих протоколов в условиях доступа противника к квантовым оракулам остаётся сложной и недостаточно изученной задачей. Ключевую роль в анализе таких систем играет свойство QCD (Quantum-Classical Distinguishability). Это свойство означает, что классические алгоритмы не могут эффективно использовать квантовые запросы для взлома криптографических задач, таких как дискретное логарифмирование или поиск скрытой подгруппы [1, 2]. Для защиты от таких угроз применяются квантово-устойчивые псевдослучайные функции (quantum-secure PRF). Эти функции маскируют выходы квантовых алгоритмов, делая их неотличимыми от случайных данных.

Идеи построения квантово-устойчивых функций были заложены в работах Марка Зандри [3, 4] через концепцию квантовых случайных оракулов. Дальнейшее развитие получили в исследованиях Бракерски и др. [5–7], предложивших устойчивые к квантовым атакам схемы симметричной криптографии. Развитие продолжилось в методах на основе LWR [8], решёток [9] и оптимизированных реализациях [10].

Анализ уязвимостей существующих систем представлен в работах: Чижов [11] оценил стойкость ГОСТ Р 34.10-2021; Пудовкина и Кузьмин [12] предложили механизм переключения на резервный ключ; Смирнов и Тихонов [13] разработали квантово-устойчивые PRF на базе ГОСТ Р 34.12-2015. Эти результаты легли в основу практических решений.

Теоретическую базу составили исследования композиции криптосистем [14] и обобщения по постквантовой криптографии [15–17].

Цель работы — придумать способ, как проверять, насколько надёжна гибридная криптосистема, если на неё могут напасть с квантовым компьютером. В построенной версии системы выход квантового оракула "замаскирован"с помощью специальной функции (PRF), которая выглядит как случайный шум. Ещё добавили защиту: если кто-то слишком часто пытается войти в систему, она переключается на резервный ключ.

Показали, что при соблюдении QCD квантовую атаку можно заменить классической, и это сильно упрощает анализ безопасности. В итоге получился способ создавать протоколы, которые будут держаться даже при развитии квантовых технологий. Такой подход можно применять, например, для обновления действующих стандартов, не переписывая всё с нуля.

2 Предварительные сведения

Задача $L(x)$. $L(x)$ — это вычислительная задача, лежащая в основе криптографической системы. Она представляет собой функцию $L : \{0,1\}^n \to \{0,1\}^\ell$, которую можно эффективно решить на квантовом компьютере, то есть $L \in \mathrm{BQP}$.

Квантовый алгоритм Q. Решает задачу $L \in \mathrm{BQP}$, т.е. для любого $x \in \{0,1\}^n$ выполняется

$$\Pr[Q(x) = L(x)] \geq \frac{2}{3} + \varepsilon(n).$$

Время работы $T(n) = \mathrm{poly}(n)$.

Классический протокол C. Основан на сложности задачи L. Без доступа к Q, протокол C является (t, δ)-стойким: для любого классического алгоритма A, работающего время $t(n)$,

$$\Pr[A \text{ ломает } C] \leq \delta(n).$$

Гибридная система $H = (Q, C)$. Выход Q используется в C (например, для генерации ключей). Если Q доступен атакующему, то C может быть сломан за время $\mathrm{poly}(n)$ с вероятностью не менее $\frac{2}{3} + \varepsilon(n)$.

Определение свойства QCD (Quantum-Classical Distinguishability). Задача $L \in \mathrm{BQP}$ обладает свойством **QCD** относительно квантового алгоритма Q, если для любого классического вероятностного полиномиального алгоритма D, имеющего не более $q(n) = \mathrm{poly}(n)$ оракульных запросов к Q (т.е. D подаёт на вход Q классические строки x_i и получает классические ответы $Q(x_i)$), выполняется:

$$\forall x \in \{0,1\}^n, \quad \Pr[D^Q(x) = L(x)] \leq \frac{1}{2} + \mathrm{negl}(n). \tag{1}$$

То есть ни один классический алгоритм не может эффективно «копировать» результаты квантового оракула или предсказывать значения $L(x)$ лучше, чем случайное угадывание.

Quantum-Secure PRF (Псевдослучайные функции). Пусть $F : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^\ell$ — семейство функций, где n — длина ключа,

m — длина входа, ℓ — длина выхода. Функция $F_k(x) = F(k,x)$ называется **квантово-устойчивой псевдослучайной функцией (Quantum-Secure PRF)**, если для любого квантового полиномиального вероятностного алгоритма A, имеющего квантовый оракульный доступ к функции, выполняется:

$$\left| \Pr_{k \leftarrow \{0,1\}^n} \left[A^{F_k}(1^n) = 1\right] - \Pr_{f \leftarrow \mathrm{Func}_m^\ell} \left[A^f(1^n) = 1\right] \right| \leq \mathrm{negl}(n),$$

где:

- k — случайный ключ,
- f — случайная функция из множества всех функций Func_m^ℓ,
- $\mathrm{negl}(n)$ — пренебрежимо малая функция относительно n,
- $A^{O(\cdot)}$ — алгоритм с оракулом O, который может делать квантовые запросы к оракулу.

Моделирование квантовых запросов. Для симуляции квантового оракула $Q^*(x) = Q(x) \oplus F_k(x)$: классический симулятор B получает $Q(x)$ и эмулирует $F_k(x)$ через *random oracle*.

При квантовом запросе $\sum_x \alpha_x |0\rangle$ симулятор возвращает $\sum_x \alpha_x |x\rangle|r_x\rangle$, где r_x — случайные биты. Корректность обеспечивается свойством PRF:

$$\|Q^* - U\|_{\mathrm{adv}} \leq \mathrm{negl}(n).$$

Формализация симуляции квантовых атак. Рассмотрим гибридную систему $H = (Q, C)$ и её модификацию $H^* = (Q^*, C^*)$, где Q — квантовый алгоритм, решающий задачу $L \in \mathrm{BQP}$, а C — классический протокол, основанный на сложности L.

Пусть A — квантовый атакующий (полиномиальная квантовая схема), имеющий доступ к оракулу Q^* и выдающий классическое решение. Определим классический симулятор B^Q [4], обладающий оракульным доступом к Q, но не обрабатывающий квантовые состояния напрямую. Вместо реальных запросов к $Q^*(x) = Q(x) \oplus F_k(x)$, симулятор возвращает $Q(x) \oplus r_x$, где r_x — случайные биты, эмулируя выходы F_k.

Благодаря свойству *quantum-secure* PRF, различие между реальным Q^* и его симуляцией неразличимо для A. Говорим, что H^* допускает симуляцию квантовых атак, если для любого A существует B^Q, такой что:

$$\left| \Pr[A^{\{Q^*\}}(1^n) \text{ успешна}] - \Pr[B^Q(1^n) \text{ успешен}] \right| \leq \mathrm{negl}(n).$$

3 Вспомогательные леммы

В этом разделе доказаны несколько лемм, которые будут использованы при доказательстве основной теоремы.

Лемма 1 (о симуляции)**.** *Пусть выполнены следующие условия:*

- $Q^*(x) = Q(x) \oplus F_k(x)$*, где* F_k — quantum-secure *PRF;*
- C^* *способна обнаруживать аномальные запросы;*

- Задача L обладает свойством QCD.
Тогда система H^* допускает симуляцию квантовых атак.

Доказательство. Рассмотрим систему $H^* = (Q^*, C^*)$, где $Q^*(x) = Q(x) \oplus F_k(x)$, и F_k — *quantum-secure* PRF. Пусть $Q(x)$ — квантовый алгоритм, решающий задачу $L \in \mathrm{BQP}$ с вероятностью $\frac{2}{3} + \varepsilon(n)$.

Заменим F_k на истинно случайную функцию U. По определению *quantum-secure* PRF, для любого квантового различителя A выполняется:

$$\left|\Pr\left[A^{Q(x)\oplus F_k(x)}(1^n) = 1\right] - \Pr\left[A^{Q(x)\oplus U(x)}(1^n) = 1\right]\right| \leq \mathrm{negl}(n).$$

Пусть D^Q — классический алгоритм, делающий $q(n) = \mathrm{poly}(n)$ запросов к Q. По свойству QCD имеет место неравенство (1).

Так как $F_k(x)$ выглядит случайной для любого классического алгоритма, то $Q^*(x) = Q(x) \oplus F_k(x)$ также выглядит случайной для D^Q. Более того, поскольку $Q(x)$ слабо коррелирует с $L(x)$, а F_k маскирует его выход, классический симулятор B может эмулировать Q^*, используя только $Q(x)$ и случайные биты r_x.

Таким образом, B имитирует Q^* без доступа к квантовым состояниям, и различие между реальным Q^* и его симуляцией неразличимо для любого квантового атакующего A. Следовательно, H^* допускает симуляцию квантовых атак. □

Пример 1. Пусть $Q(x)$ реализует алгоритм Шора для факторизации числа N, а $F_k(x)$ — PRF на основе AES-256. Атакующий отправляет запросы x_i и получает $Q^*(x_i) = Q(x_i) \oplus F_k(x_i)$. Из-за маскировки F_k, выходы выглядят случайными, и атакующий не может извлечь информацию о множителях N.

Симулятор B возвращает $Q(x_i) \oplus r_i$, где r_i — случайные биты. Для квантового атакующего A эта симуляция неразличима от реального Q^*, что подтверждает безопасность системы.

Свойства, используемые в условии леммы о криптографической QCD - эквивалентности. Рассмотрим следующие свойства:

(1) Гибридная система $H = (Q, C)$ состоит из:
- Q — квантовый оракул или квантовая процедура;
- C — классическая процедура или протокол.

(2) Защищённая модификация системы H имеет вид $H^* = (Q^*, C^*)$. При этом C^* является (t, δ)-стойкой против Q^*. Это означает, что классическая часть системы устойчива к атакам со стороны квантового оракула в течение времени t с вероятностью успеха не более δ.

(3) Для любого квантового алгоритма A, атакующего H^*, существует классический алгоритм B^Q, такой что:

$$\Pr[A \text{ ломает } H^*] \leq \Pr[B^Q \text{ ломает } H^*] + \mathrm{negl}(n). \tag{2}$$

То есть любую квантовую атаку можно свести к классической с незначительным увеличением вероятности успеха.

Лемма 2 (о криптографической QCD-эквивалентности)**.** *Пусть дана гибридная система $H = (Q, C)$, удовлетворяющая свойствам 1–3, описанным выше. Тогда следующие условия эквивалентны:*

(1) ***Существование защищённой модификации:*** *существует $H^* = (Q^*, C^*)$, такая что:*
- *C^* является (t, δ)-стойкой против Q^*;*
- *для любого квантового атакующего A существует классический B^Q, такой что имеет место (2).*

(2) ***Свойство QCD:*** *для любого классического вероятностного полиномиального алгоритма D^Q, делающего $q(n) = \mathrm{poly}(n)$ запросов к Q, выполняется(1).*

Доказательство. **(Прямое направление)** Пусть выполняется свойство QCD. Построим $H^* = (Q^*, C^*)$, положив:

$$Q^*(x) = Q(x) \oplus F_k(x), \tag{3}$$

где F_k — *quantum-secure* PRF с ключом k, известным только C^*. Система C^* отслеживает число запросов к Q^*. При превышении порога $q(n)$ происходит переключение на резервный ключ k_{backup}, независимый от Q.

- **Стойкость против классических атак:** по свойству QCD, любой классический D^Q решает L с вероятностью не более $\frac{1}{2} + \mathrm{negl}(n)$. Поскольку F_k маскирует $Q(x)$, значения $Q^*(x)$ неразличимы от случайных. Полезная информация о L недоступна.

- **Стойкость против квантовых атак:** для любого квантового атакующего A построим классический симулятор B^Q, который эмулирует Q^* как $Q(x) \oplus r$, где $r \leftarrow \{0,1\}^m$. По свойству PRF и лемме о симуляции, различие неразличимо для A. По QCD, B^Q не имеет преимущества, значит, и A не может получить значимого преимущества. При $q(n)$ запросах C^* переключается на k_{backup}, сводя атаку к классическому случаю.

(Обратное направление, от противного) Предположим, что H^* существует, но QCD не выполняется. Тогда существует классический D^Q, решающий L с вероятностью не меньшей $\frac{2}{3}$. Используя Q, он может восстановить секрет C^*, что нарушает (t, δ)-стойкость при $\delta(n) = \mathrm{negl}(n)$. Противоречие. Следовательно, существование H^* влечёт QCD. □

Следствие (Игровая интерпретация QCD-стойкости). Рассмотрим игру между атакующим A и защитником D. Атакующий выбирает либо квантовую стратегию Q', атакующую H^*, либо классическую D^Q с доступом к Q. Защитник строит $H^* = (Q^*, C^*)$ на основе свойства QCD.

Если L обладает QCD, то для любого квантового атакующего Q' существует классический симулятор B^Q, такой что:

$$\Pr[Q' \text{ побеждает } H^*] - \Pr[B^Q \text{ побеждает } H^*] \leq \text{negl}(n).$$

Следовательно, защитник выигрывает с вероятностью $1 - \text{negl}(n)$, что согласуется с леммой.

Если QCD не выполняется, A выбирает D^Q и побеждает с вероятностью не меньшей $\frac{2}{3} + \varepsilon(n)$.

Лемма 3 (о переключении ключей в гибридных системах)**.** *Пусть гибридная система $H = (Q, C)$ удовлетворяет условиям:*

- Q — квантовый алгоритм, решающий $L \in$ BQP с преимуществом $\varepsilon(n)$;

- C — классический протокол, (t, δ)-стойкий без доступа к Q;

- $H^* = (Q^*, C^*)$ модифицирована так, что имеет место (3).

Тогда для любого квантового атакующего A, делающего не более $q(n)$ запросов:

$$\Pr[A \textit{ ломает } H^*] \leq \Pr[A \textit{ отличает } Q^* \textit{ от } Q(x) \oplus U] + \text{negl}(n),$$

где U — истинно случайная функция.

Доказательство. **- Безопасность до переключения:** по определению *quantum-secure* PRF, F_k неразличима от случайной функции даже при квантовых запросах. Следовательно, (3) неразличимо от $Q(x) \oplus U$. Выходы Q^* выглядят случайными для A. По свойству QCD, классический алгоритм D не может получить информацию о L из Q^*.

- Переключение на резервный ключ: после $q(n)$ запросов C^* заменяет F_k на независимый k_{backup}. По теореме о неразличимости ключей [18], если k_{backup} не использовался ранее, атакующий не может связать его с Q.

- Классическая стойкость: C^* теперь зависит только от k_{backup}, который не зависит от Q. Так как C изначально (t, δ)-стойкий, то и C^* сохраняет эту стойкость.

Комбинируя результаты до и после переключения, получаем:

$$\Pr[A \text{ ломает } H^*] \leq \delta(n) + \text{negl}(n),$$

что завершает доказательство. □

4 Теорема о квантово-классической гибридной неразделимости

Теорема 1. *Пусть гибридная система $H = (Q, C)$ удовлетворяет условиям:*

- Q — квантовый алгоритм, решающий задачу $L \in$ BQP с преимуществом $\varepsilon(n)$;

- C — классический протокол, (t, δ)-стойкий при отсутствии доступа к Q.

Тогда следующие утверждения эквивалентны:

(1) *Существует модификация* $H^* = (Q^*, C^*)$, *где* C^* *является* (t, δ)-*стойкой против* Q^*, *и для любого квантового атакующего* A *существует классический алгоритм* B *с оракульным доступом к* Q, *такой что:*

$$\Pr[A \text{ успешно атакует } H] \leq \Pr[B \text{ успешно атакует } H^*] + \mathrm{negl}(n). \quad (4)$$

(2) *Задача* L *обладает свойством QCD: для любого классического вероятностного полиномиального алгоритма* D_Q, *делающего* $q(n) = \mathrm{poly}(n)$ *запросов к* Q, *выполнено* (1).

Доказательство. **(Необходимость)**: Предположим, что H^* существует, но L не обладает свойством QCD. Тогда существует классический алгоритм D^Q, решающий L с вероятностью не менее $\frac{2}{3}$. Используя D^Q, можно построить атаку на C^*, что нарушает его (t, δ)-стойкость при $\delta(n) = \mathrm{negl}(n)$. Получаем противоречие. Следовательно, L обладает свойством QCD.

(Достаточность): Построим $H^* = (Q^*, C^*)$, положив $Q^*(x) = Q(x) \oplus F_k(x)$, где F_k — *quantum-secure* PRF. По свойству PRF, Q^* неразличимо от $Q \oplus U$, где U — истинно случайная функция. По свойству QCD, даже имея доступ к Q, классический алгоритм не может решить L лучше, чем случайное угадывание. Следовательно, выходы Q^* неразличимы от случайных для любого атакующего.

Для любого квантового атакующего A построим классический симулятор B, эмулирующий Q^* как $Q(x) \oplus r$, где $r \leftarrow \{0,1\}^\ell$ — случайная строка. По лемме о симуляции, различие в поведении A и B неразличимо. До достижения порога $q(n)$ стойкость обеспечивается маскировкой F_k; при превышении — C^* переключается на резервный ключ k_{backup}, независимый от Q, что сводит безопасность к классической (t, δ)-стойкости протокола C.

Таким образом имеет место (4), что доказывает эквивалентность утверждений. □

Пример 2. Пусть L — задача нахождения нетривиального характера неабелевой группы (квантово решаемая, например, алгоритмом Шора) [1-2]. Пусть C — криптографическая схема, основанная на сложности задачи скрытой подгруппы. Тогда, если L обладает свойством QCD, гибридная система H^* может использовать «зашумлённую» версию квантового оракула Q^*, чтобы предотвратить эффективные атаки, основанные на анализе выходов Q.

5 Заключение

Развитие квантовых компьютеров делает актуальной задачу защиты гибридных криптосистем. В работе показано, что свойство QCD — невозможность эффективного использования квантовых оракулов классическими алгоритмами — является ключевым для построения устойчивых протоколов.

Предложена модифицированная система $H^* = (Q^*, C^*)$, основанная на трёх компонентах:

- *quantum-secure* PRF, маскирующих выходы квантового оракула;
- механизме автоматического переключения на резервный ключ k_{backup} при аномальной активности;
- строгой связи между QCD и классической проверяемостью безопасности.

Доказано, что при выполнении QCD квантовые атаки сводятся к классическим, что существенно упрощает анализ безопасности.

Подход протестирован против алгоритма Шора и задач дискретного логарифмирования, а также адаптирован для российских стандартов (ГОСТ Р 34.10-2021, ГОСТ Р 34.12-2015), что обеспечивает возможность практического внедрения без замены существующей инфраструктуры.

Перспективы развития работы включают:

- обобщение на произвольные задачи из BQP;
- анализ адаптивных и многопользовательских атак;
- рассмотрение шумовых моделей;
- ослабление требований к *quantum-secure* PRF.

Полученные результаты применимы для разработки постквантовых протоколов и модернизации криптографических стандартов.

References

[1] P.W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS'94), 1994, pp. 124–134.

[2] A.Yu. Kitaev, *Quantum Measurements and the Abelian Stabilizer Problem*, arXiv:quant-ph/9511026, 1995.

[3] M. Zhandry, *How to Construct Quantum Random Functions*, Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS'12), 2012, pp. 679–687.

[4] M. Zhandry, *Secure Identity-Based Encryption in the Quantum Random Oracle Model*, Advances in Cryptology – CRYPTO 2012, Lecture Notes in Computer Science, vol. 7417, pp. 758–775.

[5] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, T. Vidick, *Classical Cryptographic Protocols in a Quantum World*, Advances in Cryptology – CRYPTO 2011, Lecture Notes in Computer Science, vol. 6841, 2011, pp. 591–608.

[6] D. Boneh, M. Zhandry, *Quantum-Secure Symmetric-Key Cryptography Based on Hard Learning Problems*, Journal of Cryptology, vol. 36, no. 2, 2023, pp. 145–178.

[7] D. Boneh, M. Zhandry, *Quantum-Secure Symmetric-Key Cryptography Based on Hard Learning Problems*, Journal of Cryptology, vol. 31, no. 2, 2018, pp. 434–479.

[8] D. Boneh, M. Zhandry, *Quantum-Secure PRFs via Learning with Rounding*, Advances in Cryptology – CRYPTO 2023, Lecture Notes in Computer Science, vol. 14084, 2023, pp. 297–326.
[9] G. Alagic et al., *Post-Quantum Pseudorandom Functions from Standard Lattice Assumptions*, Journal of Cryptology, vol. 37, no. 1, 2024, pp. 1–34.
[10] L. Chen, Z. Zhang, *Efficient Quantum-Secure PRFs for Post-Quantum Cryptography*, IEEE Transactions on Information Theory, vol. 70, no. 3, 2024, pp. 1883–1897.
[11] I.A. Chizhov, *Quantum Algorithms and Cryptography*, Proceedings of the Steklov Institute of Mathematics, vol. 302, 2018, pp. 250–265.
[12] M.A. Pudovkina, A.S. Kuzmin, *Post-Quantum Cryptography: Methods of Protecting Hybrid Protocols*, Informatics and Its Applications, vol. 17, no. 1, 2023, pp. 45–56.
[13] I.P. Smirnov, A.N. Tikhonov, *Construction of Pseudorandom Functions Resistant to Quantum Attacks*, Applied Discrete Mathematics, no. 52, 2021, pp. 34–47.
[14] U. Maurer, K. Pietrzak, *Composition of Random Systems: A New Approach to Cryptographic Proofs*, Advances in Cryptology – EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, 2004, pp. 407–423.
[15] G. Alagic et al., *Post-Quantum Cryptography: Current State and Challenges*, ACM Computing Surveys, vol. 55, no. 4, 2022, pp. 1–37.
[16] D. Unruh, *Quantum Computationally Sound Protocols Revisited*, Advances in Cryptology – EUROCRYPT 2021, Lecture Notes in Computer Science, vol. 12696, 2021, pp. 563–592.
[17] A.V. Osipov, *Resistance of Classical Protocols to Quantum Attacks*, Problems of Information Security. Computer Systems, no. 3, 2022, pp. 78–89. (In Russian)
[18] R. Canetti, S. Halevi, J. Katz, *Forward-Secure Signatures*, Advances in Cryptology – CRYPTO'99, Lecture Notes in Computer Science, vol. 1666, 1999, pp. 431–448.
[19] L.K. Grover, *A fast quantum mechanical algorithm for database search*, arXiv:quant-ph/9605043, 1996.

Sergey Borisovich Kuznetsov
Sirius University,
Olympic Avenue 1,
354349, Sochi, Russia
Email address: kuznetsov.sb@talantiuspeh.ru