УДК 528.44, 004.9

5.2.2. Математические, статистические и инструментальные методы экономики (физико-математические науки, экономические науки)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ВЕРИФИЦИРУЕМЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В РАСПРЕДЕЛЁННЫХ СИСТЕМАХ

Дьяченко Роман Александрович
Доктор технических наук, профессор
SPIN-код: 4138-8408
Московский физико-технический институт (национальный исследовательский университет) Москва, Россия

Ярутин Сергей Алексеевич
Магистрант, Ассистент кафедры
SPIN-код: 3089-7433
yarutinsa@yandex.ru
ФГБОУ ВО "Кубанский государственный технологический университет", Краснодар, Россия

Довгаль Владислав Витальевич
Магистрант, Ассистент кафедры
SPIN-код: 6126-6650
yarutinsa@yandex.ru
ФГБОУ ВО "Кубанский государственный технологический университет", Краснодар, Россия

Гуляева Анастасия Павловна
Студент
ФГБОУ ВО "Кубанский государственный технологический университет", Краснодар, Россия

Скворцова Александра Андреевна
Студент
ФГБОУ ВО "Кубанский государственный технологический университет", Краснодар, Россия

В работе выполнен комплексный анализ вычислительной сложности криптографических задач с акцентом на различия между классами P и NP и их значимость для построения современных криптографических протоколов. Основное внимание сосредоточено на выявлении фундаментальных свойств вычислительных задач, лежащих в основе асимметричной криптографии, а также на анализе факторов, определяющих возможность их сведения к полиномиально разрешимым случаям. Исследование основано на сочетании методов теории вычислительной сложности и моделирования поведения NP-трудных задач. Рассматривается влияние параметров размерности, устойчивости и структурной неоднородности входных данных на

UDC 528.44, 004.9

5.2.2. Mathematical, statistical and instrumental methods of economics (physical and mathematical sciences, economic sciences)

MATHEMATICAL MODELING OF THE ECONOMIC EFFICIENCY OF VERIFIABLE CLOUD COMPUTING IN DISTRIBUTED SYSTEMS

Dyachenko Roman Alexandrovich
Doctor of Technical Sciences, Professor
RSCI SPIN-code: 4138-8408
Moscow Institute of Physics and Technology (National Research University) Moscow, Russia

Yarutin Sergey Alekseevich
Master's Student, Department Assistant
RSCI SPIN-code: 3089-7433
yarutinsa@yandex.ru
Kuban State Technological University, Krasnodar, Russia

Dovgal Vladislav Vitalievich
Master's Student, Department Assistant
RSCI SPIN-code: 6126-6650
Kuban State Technological University, Krasnodar, Russia

Gulyaeva Anastasia Pavlovna
Student
Kuban State Technological University, Krasnodar, Russia

Skvortsova Alexandra Andreevna
Student
Kuban State Technological University, Krasnodar, Russia

The article provides a comprehensive analysis of the computational complexity of cryptographic tasks with an emphasis on the differences between classes P and NP and their importance for building modern cryptographic protocols. The main focus is on identifying the fundamental properties of computational problems underlying asymmetric cryptography, as well as analyzing the factors determining the possibility of reducing them to polynomial solvable cases. The research is based on a combination of methods from computational complexity theory and modeling the behavior of NP-hard problems. The influence of the parameters of dimension, stability, and structural heterogeneity of input data on computational complexity is considered. It is shown that the complexity of cryptographic

вычислительную сложность. Показано, что сложность криптографических конструкций определяется топологией пространства решений, характером комбинаторного роста и распределением вычислительных ресурсов. Установлено, что указанные характеристики оказывают существенное влияние на надёжность и предсказуемость криптографических систем. Полученные результаты позволяют формализовать границы применимости принятых в настоящее время криптографических допущений безопасности. Отдельное внимание уделено анализу локальной и глобальной сложности криптографических задач и их роли в обеспечении устойчивости вычислительных схем.
В рамках экономико-математического анализа исследовано влияние характеристик вычислительных задач на распределение затрат и рисков при передаче вычислений внешним облачным провайдерам. Использование модели «принципал–агент» с включением механизмов верифицируемых вычислений и доказательств с нулевым разглашением позволяет количественно оценить эффект снижения информационной асимметрии и определить условия минимизации вероятности оппортунистического поведения. На этой основе сформулированы критерии экономической целесообразности аутсорсинга вычислительных процессов. Результаты работы уточняют теоретические основы устойчивости криптографических систем и расширяют методологический аппарат оценки затрат и рисков при использовании облачных вычислений. Полученные выводы могут быть использованы при проектировании криптографических систем, устойчивых к квантовым атакам и недостоверным вычислениям. Работа подчёркивает значимость структурного анализа вычислительной сложности и демонстрирует его роль в разработке алгоритмов нового поколения, обладающих высокой вычислительной и экономической эффективностью

Ключевые слова: ВЫЧИСЛИТЕЛЬНАЯ СЛОЖНОСТЬ, NP-ТРУДНЫЕ ЗАДАЧИ, КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ, ВЕРИФИЦИРУЕМЫЕ ВЫЧИСЛЕНИЯ, ZERO-KNOWLEDGE ДОКАЗАТЕЛЬСТВА, ЭКОНОМИКО-МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, РАСПРЕДЕЛЁННЫЕ ВЫЧИСЛЕНИЯ, УПРАВЛЕНИЕ РИСКАМИ, ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ, ОПТИМИЗАЦИЯ ЗАТРАТ

constructions is determined by the topology of the solution space, the nature of combinatorial growth, and the distribution of computing resources. It has been established that these characteristics have a significant impact on the reliability and predictability of cryptographic systems. The results obtained make it possible to formalize the limits of applicability of currently accepted cryptographic security assumptions. Special attention is paid to the analysis of the local and global complexity of cryptographic tasks and their role in ensuring the stability of computing circuits.
Within the framework of the economic and mathematical analysis, the influence of the characteristics of computing tasks on the distribution of costs and risks when transferring calculations to external cloud providers is investigated. Using the "principal–agent" model with the inclusion of mechanisms for verifiable calculations and zero-disclosure evidence makes it possible to quantify the effect of reducing information asymmetry and determine the conditions for minimizing the likelihood of opportunistic behavior. On this basis, criteria for the economic feasibility of outsourcing computing processes are formulated. The results of the work clarify the theoretical foundations of the stability of cryptographic systems and expand the methodological framework for assessing costs and risks when using cloud computing. The findings can be used in the design of cryptographic systems that are resistant to quantum attacks and unreliable calculations. The work highlights the importance of structural analysis of computational complexity and demonstrates its role in the development of a new generation of algorithms with high computational and economic efficiency

Keywords COMPUTATIONAL COMPLEXITY, NP-HARD PROBLEMS, CRYPTOGRAPHIC PROTOCOLS, VERIFIABLE COMPUTATION, ZERO-KNOWLEDGE PROOFS, ECONOMIC-MATHEMATICAL MODELING, DISTRIBUTED COMPUTING, RISK MANAGEMENT, CLOUD COMPUTING, COST OPTIMIZATION

http://dx.doi.org/10.21515/1990-4665-215-050

1. Введение.

Стремительное внедрение распределённых вычислительных

технологий и облачных сервисов в радиотехнических, телекоммуникационных и информационных системах сопровождается изменением структуры затрат и перераспределением экономических рисков, возникающих при аутсорсинге вычислительных процессов. Увеличение объёмов обрабатываемых данных и рост вычислительной сложности алгоритмов, включая задачи анализа сигналов, спектрального моделирования и мониторинга сложных технических процессов [1,2], приводят к снижению экономической целесообразности локального выполнения вычислений. Для большинства организаций переход к использованию облачных вычислительных ресурсов позволяет сократить капитальные и операционные затраты, а также повысить масштабируемость и гибкость вычислительной инфраструктуры. Вместе с тем данный переход сопровождается возникновением дополнительных рисков, связанных с недостоверностью результатов вычислений и информационной асимметрией между заказчиком и облачным провайдером.

Ключевая проблема облачного аутсорсинга вычислений заключается в отсутствии у заказчика надёжных механизмов подтверждения корректности получаемых результатов без повторного выполнения вычислительных процедур [3]. Такая ситуация формирует информационную асимметрию, приводит к росту транзакционных издержек и снижает предсказуемость поведения поставщика услуг. В результате увеличивается вероятность экономических потерь, обусловленных ошибками вычислений, снижением качества обслуживания или преднамеренными манипуляциями. В высокотехнологичных отраслях, где результаты вычислений оказывают прямое влияние на экономические показатели, качество предоставляемых услуг и устойчивость технических систем, возникает объективная потребность в формализованных механизмах снижения риска недобросовестного поведения провайдера [4].

Методы верифицируемых вычислений, включая NP-верифицируемые модели, доказательства с нулевым разглашением, а также современные криптографические протоколы класса SNARK и STARK, могут рассматриваться как инструментальная основа для уменьшения информационной асимметрии при передаче вычислений облачным сервисам. Применение данных методов позволяет заказчику осуществлять проверку корректности вычислений без доступа к исходным данным и без повторного выполнения ресурсоёмких операций. Это приводит к изменению системы стимулов для облачного провайдера, сокращает возможности оппортунистического поведения и способствует оптимизации структуры издержек в рамках контрактных взаимодействий.

Цель настоящей работы заключается в экономико-математическом обосновании применения механизмов верифицируемых вычислений как инструмента минимизации рисков и оптимизации совокупных затрат при аутсорсинге вычислений внешним облачным провайдерам. Для достижения этой цели решаются следующие задачи:

— анализ структуры затрат и рисков, связанных с переносом вычислений в облачные инфраструктуры;

— построение модели взаимодействия типа «принципал–агент», описывающей стимулы сторон и влияние механизмов верификации на поведение провайдера;

— формирование экономической модели минимизации совокупных издержек, включающей стоимость вычислений, стоимость верификации и ожидаемые потери от ошибок или атак;

— определение условий, при которых применение NP-верифицируемых схем и SNARK/STARK-протоколов становится экономически эффективным;

— оценка влияния внедрения механизмов верифицируемых вычислений на экономическую эффективность, транзакционные издержки

и устойчивость распределённых цифровых сервисов.

Такое смещение фокуса позволяет трактовать криптографические и вычислительные технологии не как цель исследования, а как инструмент экономико-математического моделирования, направленный на повышение эффективности и снижение рисков в современных облачных и распределённых вычислительных системах.

2. Материалы и методы

Материалы исследования включают совокупность методов экономико-математического моделирования, теоретические положения вычислительной сложности, инструменты верифицируемых вычислений и модели взаимодействия между заказчиком и облачным провайдером [5-6]. В качестве исходной предпосылки рассматривается ситуация информационной асимметрии, возникающей при передаче вычислений во внешнюю инфраструктуру: заказчик не имеет возможности непосредственно наблюдать, насколько качественно провайдер выполняет вычисления, и вынужден принимать результаты «на доверии» [7]. Это приводит к экономическим рискам, росту транзакционных издержек и появлению оппортунистического поведения поставщика.

Ключевым методологическим элементом выступает концепция NP-верифицируемости, позволяющая отделить процесс дорогостоящего вычисления от существенно более дешёвой проверки результата. Данное свойство используется как инструмент снижения асимметрии информации в модели «принципал–агент», где облачный провайдер стремится минимизировать свои издержки, а заказчик заинтересован в корректности результата. Пусть C_{prov} — затраты провайдера на выполнение вычислений, C_{verif} — затраты заказчика на проверку, а L_{risk} — ожидаемые потери от недостоверных вычислений. Совокупные издержки для заказчика можно записать как (1):

$$C_{\text{total}} = C_{\text{verif}} + p_{\text{err}} \cdot L_{\text{risk}} \quad (1)$$

где p_{err} — вероятность получения некорректного результата без проверки. Если применяется верификация с NP-верифицируемым доказательством, вероятность ошибки существенно снижается (2):

$$p_{\text{err}}^{\text{verif}} \ll p_{\text{err}} \quad (2)$$

что приводит к снижению совокупных издержек (3):

$$C_{\text{total}}^{\text{verif}} = C_{\text{verif}} + p_{\text{err}}^{\text{verif}} \cdot L_{\text{risk}} \ll C_{\text{total}} \quad (3)$$

Для формализации вычислительных процессов и оценки экономических последствий их делегирования используется представление задач в виде арифметических схем и constraint-моделей, применяемых в системах доказуемых вычислений. Пусть T_{local} — время локального вычисления задачи, T_{cloud} — время выполнения облачным провайдером, а T_{verif} — время проверки результата.

Эффективность делегирования (4):

$$\textit{Эффективность делегирования}: E = \frac{T_{\text{local}}}{T_{\text{cloud}} + T_{\text{verif}}} > 1 \quad (4)$$

где $E>1$ означает экономический выигрыш от аутсорсинга.

В качестве инструментария проверки применяются SNARK и STARK-протоколы. Пусть π — доказательство корректности вычислений, $|\pi|$ — его размер, а δ — вероятность ложного допуска. Тогда экономическая стоимость верификации может быть формализована как (5):

$$C_{\text{verif}} = f(|\pi|, \delta, R_{\text{comp}}) \quad (5)$$

где R_{comp} — стоимость вычислительных ресурсов заказчика для проверки доказательства.

Для оценки совокупных затрат учитываются также задержки распределённой обработки данных τ, влияющие на эффективность работы систем (6):

$$C_{\text{total}}^{\text{net}} = C_{\text{verif}} + p_{\text{err}}^{\text{verif}} \cdot L_{\text{risk}} + \tau_{\text{net}} \cdot C_{\text{op}} \quad (6)$$

где C_{op} — операционные издержки, связанные с задержкой.

Экспериментальная оценка проводится путем сопоставления локальных и делегированных вычислений с учётом затрат на проверку и потенциальных потерь (7):

$$\Delta C = C_{local} - C_{total}^{verif} \quad (7)$$

Положительное ΔC демонстрирует экономическую целесообразность использования верифицируемых вычислений как инструмента минимизации рисков и оптимизации совокупных затрат.

Применение указанного инструментария позволяет интегрировать современные методы проверки корректности вычислений в экономико-математическую модель управления рисками и затратами при аутсорсинге вычислительных процессов, делая подход релевантным для анализа распределённых телекоммуникационных, радиотехнических и цифровых систем.

2. Результаты и обсуждение

Проведённые исследования показывают, что включение механизмов верифицируемых вычислений в состав распределённых систем позволяет сформировать формализованный подход к оценке экономической целесообразности передачи вычислительных задач внешним исполнителям. Практическая апробация разработанной платформы продемонстрировала, что применение криптографических средств подтверждения корректности вычислений способствует снижению транзакционных рисков и уменьшению потенциальных экономических потерь, связанных с получением недостоверных результатов, при этом дополнительные временные и ресурсные затраты остаются на приемлемом уровне.

Сопоставление вычислительных затрат показало, что процедуры проверки корректности результата требуют существенно меньших вычислительных и сетевых ресурсов по сравнению с повторным

выполнением задачи в локальной среде. Данная разница в затратах формирует экономический стимул к использованию механизмов делегирования вычислений: заказчик получает возможность решать ресурсоёмкие задачи без необходимости инвестиций в дорогостоящую инфраструктуру, тогда как облачный провайдер оказывается заинтересован в добросовестном выполнении операций, поскольку искажение результатов ведёт к росту издержек либо утрате доверия со стороны клиентов.

Передача доказательств корректности не оказывает заметного влияния на загрузку каналов связи, что указывает на совместимость рассматриваемой технологии с уже существующими сетевыми решениями. Сохранение устойчивости функционирования при изменениях топологии сети и варьировании задержек позволяет более точно прогнозировать затраты и риски в условиях нестабильной производительности сетевых сервисов, включая мобильные, спутниковые и гибридные радиосети. В экономическом плане это выражается в повышении предсказуемости стоимости вычислений и снижении вероятности неплановых расходов, связанных с повторной обработкой данных.

Полученные экспериментальные данные свидетельствуют о высокой устойчивости механизмов верификации к проявлениям оппортунистического поведения со стороны провайдера. Вероятность получения некорректного результата оказалась крайне низкой, что делает возможным включение данных механизмов в системы управления рисками и экономического контроля качества. Для заказчика это означает сокращение затрат на мониторинг, устранение ошибок и последующую корректировку результатов, а также повышение отдачи от инвестиций и снижение финансовых рисков в критически важных приложениях.

Использование предложенной технологии в распределённых радиотехнических и телекоммуникационных сценариях показывает, что

становится возможной количественная оценка экономической эффективности различных моделей аутсорсинга вычислений. Проверяемость результатов позволяет формализовать функции издержек и потерь, возникающих в процессе выполнения вычислительных операций, интегрировать их в модели типа «принципал–агент» и определить условия, при которых передача задач облачным провайдерам является оптимальной с точки зрения совокупных затрат. Такой подход создаёт основу для сопоставления традиционных схем обработки данных с новыми моделями, ориентированными на проверяемую корректность и снижение рисков недобросовестного поведения.

Таким образом, выполненное исследование показывает, что предложенная архитектура верифицируемых вычислений формирует экономически обоснованную основу для функционирования распределённых систем, способствует снижению транзакционных издержек, минимизации финансовых и операционных рисков и повышению прозрачности процессов обработки данных. Полученные результаты создают предпосылки для развития новых сервисных моделей, в рамках которых надёжность и корректность вычислений выступают не только техническими, но и экономически измеримыми характеристиками.

4. Заключение

В рамках выполненного исследования была показана экономическая оправданность использования механизмов верифицируемых облачных вычислений в распределённых телекоммуникационных и радиотехнических системах. Установлено, что применение криптографических методов подтверждения корректности вычислений способно трансформировать характер взаимодействия между заказчиком и поставщиком облачных ресурсов, уменьшая информационную асимметрию и снижая риск оппортунистического поведения со стороны провайдера. Учет процедур проверки результатов в структуре издержек

свидетельствует о том, что даже при возникновении дополнительной вычислительной нагрузки на стороне заказчика совокупные затраты могут сокращаться за счёт уменьшения числа ошибок, задержек, простоев и связанных с ними экономических потерь.

Проведённый анализ показывает, что затраты на проверку корректности вычислений оказываются значительно ниже по сравнению с расходами на их повторное выполнение в локальной среде. Тем самым формируется экономическое обоснование делегирования ресурсоёмких задач в облако, поскольку риск получения недостоверных результатов становится управляемым и поддаётся количественной оценке. В распределённых системах, где вычислительные ошибки способны приводить к ухудшению качества предоставляемых услуг и повреждению инфраструктуры, внедрение механизмов верификации позволяет существенно снизить вероятностные потери и повысить эффективность управления ресурсами.

Сформулированные выводы подтверждают, что включение механизмов доказуемой корректности в экономико-математические модели принятия решений способствует росту эффективности облачного аутсорсинга вычислений. Предлагаемый подход позволяет выстраивать более устойчивые схемы взаимодействия между участниками, повышать предсказуемость результатов и снижать неопределённость, связанную с качеством обработки данных во внешней вычислительной среде. В этом контексте рассматриваемые методы могут быть охарактеризованы как перспективный инструмент управления рисками и повышения прозрачности в телекоммуникационной сфере и смежных отраслях.

К числу перспективных направлений дальнейших исследований относятся разработка более детализированных моделей типа «принципал–агент» с учётом стратегического поведения сторон, совершенствование методов оценки экономического эффекта от внедрения механизмов

верификации в крупномасштабных инфраструктурах, а также анализ оптимальных стратегий распределения вычислительных задач между локальными и облачными ресурсами с учётом уровня риска и стоимости возможных ошибок. Отдельный интерес представляет исследование влияния данных технологий на долгосрочную устойчивость экосистемы облачных провайдеров и формирование новых моделей ценообразования в условиях гарантированной корректности вычислений.

Благодарность

Авторы выражают признательность канд. техн. наук Тотухову К.Е. за предложенную идею публикации

ЛИТЕРАТУРА

1. Студеникин А. Г., Крыжко И. Б., Токарев А. Б., Ашихмин А. В., Фатеев А. А. Алгоритм предварительной идентификации радиосигналов по спектральным маскам // Системы управления, связи и безопасности. 2021. №4. С. 10-39. DOI: 10.24412/2410-9916-2021-4-10-39.

2. Потапов, А. А. Структурно-параметрический синтез систем оптимальной текстурно-фрактальной обработки многомерных радиолокационных изображений / А. А. Потапов, В. А. Кузнецов, Е. А. Аликулов // Радиотехника и электроника. – 2022. – Т. 67, № 1. – С. 51-67. – DOI 10.31857/S0033849422010077. – EDN FPNUIY.

3. Makhlouf, R. Cloudy transaction costs: a dive into cloud computing economics. *J Cloud Comp* **9**, 1 (2020). https://doi.org/10.1186/s13677-019-0149-4

4. Ellman, J., Lee, N. & Jin, N. Cloud computing deployment: a cost-modelling case-study. *Wireless Netw* **29**, 1069–1076 (2023). https://doi.org/10.1007/s11276-018-1881-2

5. Bontekoe, T., Karastoyanova, D. & Turkmen, F. Verifiability for privacy-preserving computing on distributed data — a survey. *Int. J. Inf. Secur.* **24**, 141 (2025). https://doi.org/10.1007/s10207-025-01047-7

6. Мурлин, А. Г. Исследование и разработка серверной части для учебной мобильной информационной системы / А. Г. Мурлин, С. А. Ярутин, Д. А. Шорвоглян // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2025. – № 205. – С. 183-192. – DOI 10.21515/1990-4665-205-017. – EDN YYGYNJ.

7. Галяев А.А., Бабиков В.Г., Лысенко П.В., Берлин Л.М. Новая спектральная мера сложности и её возможности по обнаружению сигналов в шуме // Доклады Российской академии наук. Математика, информатика, процессы управления. - 2024. - Т. 518. - №1. - С. 80-88. doi: 10.31857/S2686954324040122

REFERENCES

1. Studenikin A. G., Kryzhko I. B., Tokarev A. B., Ashihmin A. V., Fateev A. A. Algoritm predvaritel'noj identifikacii radiosignalov po spektral'nym maskam // Sistemy upravlenija, svjazi i bezopasnosti. 2021. №4. S. 10-39. DOI: 10.24412/2410-9916-2021-4-10-39.

2. Potapov, A. A. Strukturno-parametricheskij sintez sistem optimal'noj teksturno-fraktal'noj obrabotki mnogomernyh radiolokacionnyh izobrazhenij / A. A. Potapov, V. A. Kuznecov, E. A. Alikulov // Radiotehnika i jelektronika. – 2022. – T. 67, № 1. – S. 51-67. – DOI 10.31857/S0033849422010077. – EDN FPNUIY.

3. Makhlouf, R. Cloudy transaction costs: a dive into cloud computing economics. J Cloud Comp 9, 1 (2020). https://doi.org/10.1186/s13677-019-0149-4

4. Ellman, J., Lee, N. & Jin, N. Cloud computing deployment: a cost-modelling case-study. Wireless Netw 29, 1069–1076 (2023). https://doi.org/10.1007/s11276-018-1881-2

5. Bontekoe, T., Karastoyanova, D. & Turkmen, F. Verifiability for privacy-preserving computing on distributed data — a survey. Int. J. Inf. Secur. 24, 141 (2025). https://doi.org/10.1007/s10207-025-01047-7

6. Murlin, A. G. Issledovanie i razrabotka servernoj chasti dlja uchebnoj mobil'noj informacionnoj sistemy / A. G. Murlin, S. A. Jarutin, D. A. Shorvogljan // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta. – 2025. – № 205. – S. 183-192. – DOI 10.21515/1990-4665-205-017. – EDN YYGYNJ.

7. Galjaev A.A., Babikov V.G., Lysenko P.V., Berlin L.M. Novaja spektral'naja mera slozhnosti i ejo vozmozhnosti po obnaruzheniju signalov v shume // Doklady Rossijskoj akademii nauk. Matematika, informatika, processy upravlenija. - 2024. - T. 518. - №1. - C. 80-88. doi: 10.31857/S2686954324040122