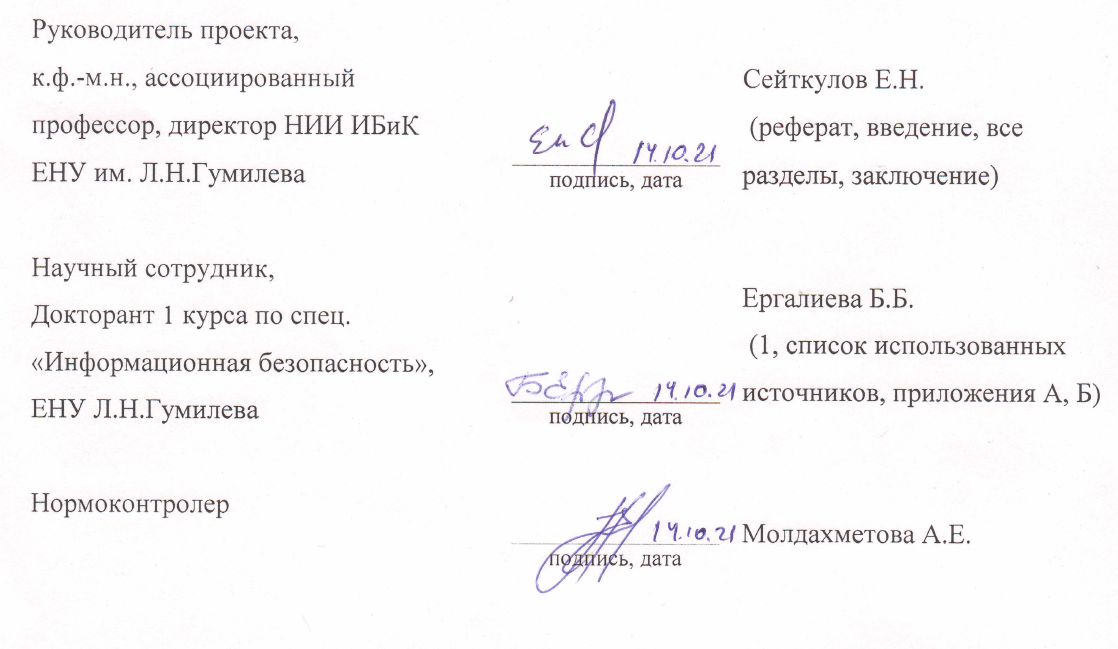


Нур-Султан 2021

**СПИСОК ИСПОЛНИТЕЛЕЙ**



**РЕФЕРАТ**

Отчет 24 с., 1 кн., 24 источн., 2 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, БЕЗОПАСНЫЙ АУТСОРСИНГ, КЛИЕНТ-СЕРВЕРНОЕ ВЗАИМОДЕЙСТВИЕ, БОЛЬШИЕ ДАННЫЕ, ВЫЧИСЛИТЕЛЬНО-СЛОЖНЫЕ ЗАДАЧИ

Объектом исследования являются задачи линейного программирования с секретными параметрами, задачи нахождения экстремума функции с секретными параметрами, задачи нахождения значения аналитической функции на секретном аргументе.

Цель и задачи проекта на 2021 год:

Целью проекта является исследование и разработка методов безопасного использования внешних серверов для решения вычислительно-сложных задач с секретными параметрами.

Задачи:

Разработать новые методы и алгоритмы безопасного использования внешних серверов при решении:

- задачи линейного программирования с секретными параметрами;

- задачи нахождения экстремума функции с секретными параметрами;

- задачи нахождения значения аналитической функции на секретном аргументе.

Область применения: информационная безопасность.

Прогнозные предположения о развитии объекта исследования: результаты работы послужат источником для дальнейшего анализа и исследования в области разработок методов безопасного аутсорсинга вычислительно-сложных задач с секретными параметрами.

В рамках данного малого гранта за 2021 год опубликована 1 статья в зарубежном журнале с процентилем по базе Scopus – 47, а также представлена еще 1 статья в этот же журнал. Сделаны 2 доклада на международной конференции.

В исследовательской работе принимали участие 2 научных сотрудников, один из которых является докторантом 1 курса по специальности «Информационная безопасность».

**РЕФЕРАТ**

Есеп: 24 б., 1 кітап, 24 дереккөз, 2 қосымша.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК, ҚАУІПСІЗ АУЗОРСИНГ, КЛИЕНТ-СЕРВЕРЛІК ӨЗАРА ӘРЕКЕТТЕСУ, ҮЛКЕН ДЕРЕКТЕР, ЕСЕПТЕУІ-КҮРДЕЛІ МӘСЕЛЕЛЕР

Зерттеу нысаны – құпия параметрлері бар сызықтық бағдарламалау есептері, құпия параметрлері бар функция экстремумын табу мәселесі, құпия аргумент бойынша аналитикалық функцияның мәнін табу мәселесі.

Жобаның 2021 жылға арналған мақсаты мен міндеттері:

Жобаның мақсаты - құпия параметрлері бар есептік-күрделі мәселелерді шешу үшін сыртқы серверлерді қауіпсіз пайдалану әдістерін зерттеу және әзірлеу.

Міндеттері:

Шешу кезінде сыртқы серверлерді қауіпсіз пайдаланудың жаңа әдістері мен алгоритмдерін әзірлеу:

- құпия параметрлері бар сызықтық бағдарламалау есептері;

- құпия параметрлері бар функция экстремумын табу мәселелер;

- құпия аргумент бойынша аналитикалық функцияның мәнін табу мәселелер.

Қолдану аясы: ақпараттық қауіпсіздік.

Зерттеу нысанының дамуы туралы болжам жорамалдар: жұмыстың нәтижелері құпия параметрлері бар есептеу-күрделі тапсырмаларды шешудің қауіпсіз аутсорсинг тәсілдерін әзірлеу саласында әрі қарай талдау мен зерттеулер үшін негіз бола алады.

2021 жылға арналған осы шағын грант шеңберінде Scopus дерекқорының 47 пайыздық көрсеткіші бар шетелдік журналда 1 мақала жарияланды, сонымен қатар сол журналға тағы 1 мақала ұсынылды. Халықаралық конференцияда 2 баяндама жасалды.

Зерттеу жұмысына 2 ғылыми қызметкер қатысты, олардың бірі «Ақпараттық қауіпсіздік» мамандығының 1 курс докторанты.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
|  |  |
| ВВЕДЕНИЕ ……………………………………………………………………………… | 6 |
| 1  Методы и алгоритмы безопасного использования внешних серверов для решения вычислительно-сложных задач с секретными параметрами ………………………….. | 8 |
| 1.1 Задачи нахождения экстремума функции с секретными параметрами…... | 8 |
| 1.2 Задачи линейного программирования с секретными параметрами…….. | 13 |
| 1.3 Задачи нахождения значения аналитической функции на секретном аргументе…………………………………….......................................................... | 16 |
| ЗАКЛЮЧЕНИЕ……………………………………………………………....................... | 18 |
| СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ……………………..…………….. | 19 |
| ПРИЛОЖЕНИЕ А Список опубликованных работ за 2021 год……………………... | 22 |
| ПРИЛОЖЕНИЕ Б Календарный план работ на 2021 года………………………..…. | 23 |

**ВВЕДЕНИЕ**

В этой работе мы исследуем методы безопасного использования внешних небезопасных серверов при решении вычислительно-сложных задач с секретными параметрами. Данная проблема является одним из важных научных направлений в сфере обеспечения информационной безопасности облачных вычислений. В работе представлены методы безопасного аутсорсинга для следующих классов вычислительно-сложных задач с секретными параметрами:

- Задачи нахождения экстремума функции с секретными параметрами;

- Задачи линейного программирования с секретными параметрами;

- Задачи нахождения значения аналитической функции на секретном аргументе.

Теория безопасного аутсорсинга научных вычислений бурно развивается в различных областях, так как в современных условиях обработка больших данных уже невозможно представить без использования мощных вычислительных ресурсов. Именно поэтому ведущие ученые в области информационной безопасности предлагают самые разные методики безопасного аутсорсинга научных вычислений [1-24].

Основная идея нового подхода в решении вычислительно-сложных задач с секретными параметрами является использование внешних вычислительных ресурсов. Однако, при этом, на стороне клиента проводятся предварительные преобразования исходной вычислительной задачи. То есть до отправки задачи на сервер, клиенту надо спрятать секретные параметры таким образом, чтобы сервер (или перехватчи информации) не смог определить эти параметры. Потом данная преобразованная вычислительно-сложная задача отправляется на сервер. Решим полученную задачу, сервер возвращает клиенту данное промежуточное решение, а клиент за приемлемое время должен суметь восстановить решение исходной вычислительно-сложной задачи.

Отметим, что наша главная цель это продемонстрировать новые методы безопасного аутсорсинга научных вычислений, поэтому мы моделируем классы задач таким образом, чтобы наглядно показать суть этих методов.

В подразделе 1.1 мы изучим несколько задач нахождения экстремума функции с секретными параметрами. При этом мы предлагаем несколько примеров, поэтапно обобщая их, и переходя к нетривиальным постановкам задач.

В подразделе 1.2 рассмотрены задачи линейного программирования с секретными параметрами. Такие задачи возникают, например, при производственном планировании, которое, как известно, математически может быть представлено в виде задачи определения максимального значения линейной функции при некоторых ограничениях**.** Также представлена одна задача математического программирования, когда целевая функция не является линейной функцией.

В подразделе 1.3 представлено решение задачи нахождения значения аналитической функции нескольких комплексных переменных на секретном аргументе. Для приближенного решения этой задачи с помощью сервера использована лемма Осгуда и обобщенная интегральная формула Коши из теории функций нескольких комплексных переменных.

**1 Методы и алгоритмы безопасного использования внешних серверов для решения вычислительно-сложных задач с секретными параметрами**

**1.1 Задачи нахождения экстремума функции с секретными параметрами**

В этом подразделе мы рассмотрим методы безопасного нахождения экстремума функции с секретными параметрами с использованием внешних серверов. При этом, чтобы показать суть методов, мы продемонстрируем их на конкретных примерах.

Рассмотрим сначала вещественную функцию одной переменной:

(1)

Предположим, что данная функция дважды дифференцируема на некотором интервале . Тогда критические точки , как известно, определяются из условия

Поэтому, основная сложность в нахождении экстремума функции заключается в поиске критических точек, после чего легко можно вычислить значение экстремума функции по формуле (1).

Пример №1. Предположим, что необходимо найти критическую точку для функции

(2)

с помощью небезопасного сервера, при этом некоторые из параметров являются секретными числами клиента.

Вариант 1. Пусть число – является секретом, а остальные параметры не являются секретом. Тогда на небезопасный сервер отправляется уравнение Если решение этого уравнения, тогда клиент находит экстремальное значение, вычислив значение в этой точке.

Вариант 2. Пусть число – является секретом, а числа не являются секретом. Тогда для нахождения критической точки на небезопасном сервере, можно воспользоваться следующим протоколом:

Шаг 1. Клиент выбирает случайное секретное число и вычисляет числа и . И затем отправляет серверу уравнение

Шаг 2. Небезопасный сервер находит решение уравнения , и возвращает это решение клиенту.

Шаг 3. Клиент находит решение уравнения по формуле .

Можно, конечно, привести и другие варианты, например, считать, что число является секретным параметром или сразу все параметры являются секретом, но, по сути, они решаются аналогичным способом.

Пример №2. Предположим, что необходимо найти критическую точку для функции двух переменных

(3)

Критическая точка этой функции находится из решения системы уравнения

То есть необходимо решить матричное уравнение

(4)

Тут тоже могут быть различные варианты, но мы рассмотрим только один вариант, когда числа – являются секретными параметрами клиента. Для решения уравнения (4) с помощью сервера можно воспользоваться следующим протоколом:

Шаг 1. Клиент выбирает случайным образом секретный вектор

и вычисляет вектор

Далее клиент вычисляет вектор

;

и отправляет серверу уравнение

(5)

относительно неизвестных

Шаг 2. Сервер решает уравнение (5), и возвращает решение клиенту. Обозначим это решение .

Шаг 3. Клиент находит решение уравнения (4) по следующей формуле

.

Пример №3. Рассмотрим произвольную дважды непрерывно-дифференцируемую функцию y= на отрезке . Необходимо найти экстремум этой функции, при этом будем считать, что сама функция является секретом.

Произведем следующие виды замены переменных:

- сдвиг вдоль абсцисс: , где – некоторое фиксированное число, обеспечивающее сдвиг графика функции вдоль оси абсцисс;

- сдвиг вдоль ординат: , где – некоторое фиксированное число, обеспечивающее сдвиг графика функции вдоль оси ординат;

- сжатие функции вдоль оси абсцисс: - коэффициент сжатия вдоль оси абсцисс;

- сжатие функции вдоль оси ординат: - коэффициент сжатия вдоль оси ординат.

Теперь произведем последовательно все эти виды замены переменных:

Предположим, что во внутренней точке достигается экстремальное значение , тогда функция достигает своего экстремума в точке

при этом экстремальное значение будет равно

Теперь нахождение экстремума функции можно описать следующим протоколом.

Шаг 1. Клиент преобразовывает исходную функцию , последовательно применяя все вышеперечисленные виды замены переменных, при этом числа держит в секрете. Далее, отправляет серверу функцию и интервал .

Шаг 2. Сервер находит критическую точку и экстремум для функции на интервале и передает пару чисел ( клиенту.

Шаг 3. Клиент находит критическую точку и экстремум исходной функции по следующим простейшим формулам

Пример №4. Рассмотрим теперь общий случай. Заметим, что вместо простого сдвига вдоль оси абсцисс, можно сделать следующую замену переменной:

,

где , а функция любая строго возрастающая непрерывно-дифференцируемая функция на некотором отрезке при этом пусть во всех точках имеет место строгое неравенство

Предположим, что выполняются условия

Далее, так как

,

а , то задача нахождения экстремума функции на отрезке сводится к задаче нахождения экстремума функции

на отрезке .

Итак, нам потребуются следующие виды замены переменных:

- замена зависимой переменной: *,* где новая независимая переменная;

- сдвиг вдоль ординат: , где – некоторое фиксированное число, обеспечивающее сдвиг графика функции вдоль оси ординат;

- сжатие функции вдоль оси ординат: - коэффициент сжатия вдоль оси ординат.

Теперь произведя последовательно все эти виды замены переменных, получим в итоге функцию

Предположим, что во внутренней точке достигается экстремальное значение , тогда функция достигает своего экстремума в точке такое, что .При этом экстремальное значение будет равно

Теперь нахождения экстремума функции можно описать следующим протоколом.

Шаг 1. Клиент преобразовывает исходную функцию , последовательно применяя описанные виды замены переменных, при этом функция , а также числа держит в секрете. Далее, отправляет серверу функцию и интервал

Шаг 2. Сервер находит экстремальную точку и экстремум для функции на интервале и передает пару чисел ( клиенту.

Шаг 3. Клиент находит экстремальную точку и экстремум функции по следующим простейшим формулам

Пример №5.В некоторых случаях, при моделировании экономических задач, мы получаем некоторую задачу оптимизации, где требуется найти экстремум функции при некоторых ограничениях. Рассмотрим следующую задачу определения экстремума функции

|  |  |  |
| --- | --- | --- |
|  |  | (6) |

и наложим условия связи

|  |  |  |
| --- | --- | --- |
|  |  | (7) |

где .

Функция Лагранжа будет иметь вид:

Дифференцируя по каждому переменному функцию Лагранжа и учитывая условие связи, составим следующую систему уравнений:

Обозначим через матрицу

Тогда получим систему линейных алгебраических уравнений

(8)

где - правый столбец, − неизвестный вектор. Как видим, задача нахождения критической точки сводится к решению уравнения (8).

Клиенту необходимо найти экстремум функции (6) при условии связи (7) с помощью вычислительных средств небезопасного сервера. При этом сервер не должен знать следующие секретные параметры клиента: *,* и *P*. И само решение также должно оставаться в секрете.

Для решения этого уравнения можно воспользоваться следующим протоколом:

Шаг 1. Клиент берет случайный образом секретный вектор и секретную обратимую матрицу :

и вычисляет новую матрицу , и отправляет серверу уравнение

|  |  |  |
| --- | --- | --- |
|  |  | (9) |

Шаг 2. Сервер решает систему линейных алгебраических уравнений (9) и возвращает клиенту решение.

Шаг 3. Тогда клиент находит решение уравнения (8) по формуле

То есть находит критическую точку для функции (6) при условии связи (7).

Отметим, что в случае, когда для клиента числа и являются не секретными, тогда вместо матрицы берется единичная матрица.

**1.2 Задачи линейного программирования с секретными параметрами**

Теперь рассмотрим общую задачу производственного планирования, которая, как известно, математически может быть представлена в виде задачи определения максимального значения функции

(10)

с ограничениями (условия связи)

Здесь – некоторые константы.

Предположим, что коэффициенты – являются секретными числами клиента, а числа не являются секретом. Также предположим, что решение также должен оставаться в секрете.

Путь положительная диагональная матрица следующего вида

Сделаем замену переменных

Тогда получим следующую задачу

(13)

с ограничениями (условия связи)

Здесь .

Теперь можно представить протокол решения задачи (10-12):

Шаг 1. Клиент берет случайный образом диагональную матрицу

и делает замену переменных Теперь отправляет на сервер задачу (13-15).

Шаг 2. Сервер решает задачу (13-15) и отправляет решение клиенту.

Шаг 3. Клиент находит решение задачи (10-12) по формуле

Теперь приведем типовую экономическую задачу оптимизации, в которой целевая функция не является линейной, но которую можно будет решить лишь с использованием вычислительных мощностей серверов.

Пусть - положительная матрица, а числа – положительные числа.

Требуется найти вектор , максимизирующий функцию

(16)

с ограничениями

(17)

(18)

Где - выпуклые вверх скалярные функции одной переменной (это нужно чтобы была возможность использовать общие методы выпуклой оптимизации, например, натуральный логарифм является выпуклым вверх функцией).

Итак, предположим, что клиенту необходимо решить задачу (16) – (18). Секретными элементами являются матрица *C,* числа и вектор решение ). Вектор = () секретом не является.

*Протокол*

Шаг 1. Клиент выбирает случайным образом *m* секретных диагональных матриц

и вычисляет Далее, при вычисляет , и отправляет серверу задачу (19) − (21) :

(19)

|  |  |  |
| --- | --- | --- |
|  |  | (20) |
|  |  | (21) |

Шаг 2. Сервер решает задачу (19) − (21) и приближенное решение возвращает клиенту.

Шаг 3. Клиент находит решение задачи (16) - (18) по формуле

|  |  |  |
| --- | --- | --- |
|  |  | (22) |

Легко заметить, что данный протокол решает исходную задачу. Сделаем замену переменных

Тогда, учитывая что

,

тогда (16) - (17) примут вид (19) - (20) соответственно. Далее, так как – положительные числа, то условие (18) можно написать в виде условия (21).

Безопасность протокола. Небезопасный сервер получает систему уравнений

, ,

Так как система уравнений (23) содержит неизвестных, а количество самих уравнений в этой системе , то система (23) разрешима неоднозначно, то есть сервер не сможет однозначно определить секретные параметры клиента.

**1.3 Задачи нахождения значения аналитической функции на секретном аргументе**

Рассмотрим вычислительно-сложную комплексную функцию, определенную в некотором открытом подмножестве , где – декартово произведения n экземпляров комплексной плоскости. Нам требуется приближенно вычислить значение комплексной функции , используя вычислительные ресурсы сервера.

Предположим, что функция непрерывна в открытом множестве и голоморфна по каждой переменной в отдельности, тогда согласно хорошо известной лемме Осгуда, эта функция голоморфна во всей области . Пусть замкнутый полидиск . Тогда, используя многократно интегральную формулу Коши для функции одной переменной, получаем

справедливой для любой внутренней точки .

Не умаляя общности, предположим, что . Тогда значение комплексной функции на секретном аргументе можно вычислить приближенно по следующей интегральной сумме:

где точки равномерно выбраны на границах дисков соответственно, где , , .

Теперь приближенное вычисление значения аналитической функции на секретном аргументе можно представить следующим протоколом:

Шаг 1. Клиент выбирает достаточно большие числа а также точки , равномерно выбранные по границам соответственно, и отправляет на сервер функцию .

Шаг 2. Сервер вычисляет значение функции в каждой точке: , А также вычисляет числа . Значения вычисленных чисел сервер отправляет клиенту.

Шаг 3. Клиент вычисляет приближенное значение функции на секретном аргументе по формуле

Отметим, что в данном методе предполагается, что сервер вычисляет достаточно быстро значения , при каждом Тогда клиент производит достаточно простые арифметические действия.

**ЗАКЛЮЧЕНИЕ**

В работе получены новые методы и алгоритмы безопасного использования внешних небезопасных серверов при решении вычислительно-сложных задач с секретными параметрами. А именно, были представлены методы безопасного аутсорсинга для следующих классов вычислительно-сложных задач с секретными параметрами:

- Задачи нахождения экстремума функции с секретными параметрами;

- Задачи линейного программирования с секретными параметрами;

- Задачи нахождения значения аналитической функции на секретном аргументе.

Отметим, что нашей главной целью было показать новые методы безопасного аутсорсинга научных вычислений именно этих задач, и результаты исследований можно распространить на иные аналогичные задачи.

Уровень научной проработки.Впервые были предложены методы и алгоритмы решения задачи нахождения экстремума функции с секретными параметрами, решения задачи линейного программирования с секретными параметрами, а также решение задачи нахождения значения аналитической функции нескольких переменных на секретном аргументе.

Перспективность использования результатов данного исследования.Результаты исследования могут послужить источником для дальнейшего анализа и исследования в области разработок методов безопасного аутсорсинга вычислительно-сложных задач с секретными параметрами.

Завершенность результатов.Результаты исследовательской работы были опубликованы:

- В индонезийском журнале «Indonesian Journal of Electrical Engineering and Computer Science», который имеет процентиль по CiteScore в базе Scopus – 47, руководитель проекта Е.Сейткулов – первый автор, а также является автором для корреспонденции, ИРН AP09559249 стоит первым в информационной строке о финансировании.

- Два доклада в The III International Turkic World Congress on Science and Engineering.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Seitkulov Ye., New methods of secure outsourcing of scientific computations // The Journal of Supercomputing, 2013. - Vol. 65. - Issue 1. - P. 469-482. Doi: 10.1007/s11227-012-0809-3.
2. Yu Jianhua, Wang Xueli, Gao Wei, Improvement and applications of secure outsourcing of scientific computations // Journal of Ambient Intelligence and Humanized Computing, 2015. - Vol. 6. - P.763–772. Doi: 10.1007/s12652-015-0280-0.
3. Hu Xing and Tang Chunming Secure outsourced computation of the characteristic polynomial and eigenvalues of matrix // Journal of Cloud Computing, 2015. - URL: https://eprint.iacr.org/2014/442.pdf. - Doi: 10.1186/s13677-015-0033-9.
4. Wang C., Ren K., Wang J. Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming // IEEE Transactions on Computers, 2016. -Vol. 65. - Issue 1. - P. 216-229. Doi: 10.1109/TC.2015.2417542.
5. Vyas Ronak, Singh Alok, Singh Jolly, Soni Gunjan, Purushothama B. R. Design of an efficient verification scheme for correctness of outsourced computations in cloud computing // Security in Computing and Communications, Springer*,* 2015. - Vol. 536. - P. 66–77. Doi: 10.1007/978-3-319-22915-7\_7.
6. Atallah M. and Frikken K. Securely outsourcing linear algebra computations // ASIACCS '10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010. -P.48-59. Doi: 10.1145/1755688.1755695.
7. Benjamin D. and Atallah M. Private and cheating-free outsourcing of algebraic computations // Proceedings of 6th conference on privacy, security, and trust (PST), 2008. -P. 240-245. Doi: 10.1109/PST.2008.12.
8. Matsumoto Tsutomu, Kato Koki, Imai Hideki Speeding Up Secret Computations with Insecure Auxiliary Devices // In: Goldwasser S. (eds) Advances in Cryptology — CRYPTO’ 88. Lecture Notes in Computer Science*,* 1990. *-*Vol. 403. –P. 497-506. Doi: 10.1007/0-387-34799-2\_35.
9. Thierry Mefenza, Damien Vergnaud Cryptanalysis of Server-Aided RSA Protocols with Private-Key Splitting // The Computer Journal, 2019. - Vol. 62. - Issue 8. -P. 1194–1213. Doi: 10.1093/comjnl/bxz040.
10. Zhou Kai, Afifi M.Y., Ren Jian ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing // IEEE Transactions on Information Forensics and Security, 2017. - Vol.12. - Issue 11. - P. 2518-2531. Doi:10.1109/TIFS.2017.2710941.
11. Hohenberger S. and Lysyanskaya A. How to Securely Outsource Cryptographic Computations //In: Kilian J. (eds) Theory of Cryptography. TCC, Lecture Notes in Computer Science, 2005. - Vol. 3378. - P. 264–282. Doi: 10.1007/978-3-540-30576-7\_15.
12. Béguin P. and Quisquater J.-J. Fast Server-Aided RSA Signatures Secure Against Active Attacks // In: Coppersmith D. (eds) Advances in Cryptology — CRYPT0’ 95. Lecture Notes in Computer Science, 1995. - Vol. 963. - P. 57-69. Doi: 10.1007/3-540-44750-4\_5.
13. Lim C.H. and Lee P.J. Security and Performance of Server-Aided RSA Computation Protocols // In: Coppersmith D. (eds) Advances in Cryptology — CRYPT0’ 95. Lecture Notes in Computer Science*,*1995. *-* Vol. 963. - P.70–83. Doi: 10.1007/3-540-44750-4\_6.
14. Castelluccia C., Mykletun E., Tsudik G. Improving Secure Server Performance by Re-balancing SSL//TLS Handshakes // ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, 2006. - P.26–34. Doi: 10.1145/1128817.1128826.
15. Chen X., Li J., Ma J., Tang Q., Lou W. New Algorithms for Secure Outsourcing of Modular Exponentiations //In Foresti, S., Yung, M. and Martinelli, F. (eds.) ESORICS, Lecture Notes in Computer Science, 2012. - Vol. 7459. - P. 541–556. Doi: 10.1007/978-3-642-33167-1\_31.
16. Wang Y. and et al. Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage//In Kutylowski, M. and Vaidya, J. (eds.) ESORICS, Lecture Notes in Computer Science, 2014. - Vol. 8712. - P.326–343. Doi: 10.1007/978-3-319-11203-9\_19.
17. Nguyen P.Q. and Shparlinski I. On the Insecurity of a Server-Aided RSA Protocol // In: Boyd C. (eds) Advances in Cryptology — ASIACRYPT 2001. Lecture Notes in Computer Science, 2001. - Vol. 2248. - P. 21–35, 2001. Doi: 10.1007/3-540-45682-1\_2.
18. Merkle J., Multi-round Passive Attacks on Server-Aided RSA Protocols // CCS '00: Proceedings of the 7th ACM conference on Computer and Communications Security, 2000. - P. 102–107. Doi: 10.1145/352600.352616.
19. Pfitzmann B. and Waidner M. Attacks on Protocols for Server-Aided RSA Computation *//*In: Rueppel R.A. (eds) Advances in Cryptology — EUROCRYPT’ 92. Lecture Notes in Computer Science, 1993. - Vol.658. -P. 153–162. Doi: 10.1007/3-540-47555-9\_13.
20. Jakobsson M. and Wetzel S. Secure Server-Aided Signature Generation // In: Kim K. (eds) Public Key Cryptography. PKC 2001. Lecture Notes in Computer Science, 2001. -Vol. 1992. -P. 383–401. Doi: 10.1007/3-540-44586-2\_28.
21. Merkle J. and Werchner R. On the Security of Server-Aided RSA Protocols // In: Imai H., Zheng Y. (eds) Public Key Cryptography. PKC 1998. Lecture Notes in Computer Science, 1998. - Vol. 1431. - P. 99–116, 1998. Doi: 10.1007/BFb0054018.
22. Aono Y. A New Lattice Construction for Partial Key Exposure Attack for RSA // In Jarecki, S. and Tsudik, G. (eds.) PKC, Lecture Notes in Computer Science, 2009. - Vol. 5443. - P. 34–53. Doi: 10.1007/978-3-642-00468-1\_3.
23. Blömer J. and May A. New Partial Key Exposure Attacks on RSA // In Boneh, D. (ed.) CRYPTO, Lecture Notes in Computer Science, 2003. - Vol. 2729. -P. 27–43. Doi: 10.1007/978-3-540-45146-4\_2.
24. Ernst M., Jochemsz E., May A., de Weger B. Partial Key Exposure Attacks on RSA up to Full Size Exponents // In Cramer, R. (ed.) EUROCRYPT Lecture Notes in Computer Science, 2005. - Vol. 3494. - P. 371–386. Doi: 10.1007/11426639\_22.

**ПРИЛОЖЕНИЕ А**

**Список опубликованных работ за 2021 год**

1. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Gulden B. Ulyukova, Banu B. Yergaliyeva, Dina Satybaldina Methods for secure cloud processing of big data // Indonesian Journal of Electrical Engineering and Computer Science, Vol. 22, No. 3, June 2021, pp. 1650-1658, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i3. pp. 1650-1658(**Процентиль по CiteScore в базе Scopus - 47;** **руководитель проекта Е.Сейткулов – первый автор, а также является автором для корреспонденции; ИРН AP09559249 стоит первым в информационной строке о финансировании**).
2. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Banu B. Yergaliyeva Secure Outsourcing a Linear Programming Task with Secret Parameters // Book of abstracts of the III International Turkic World Congress on Science and Engineering 14-15 June 2021, Niğde – Turkey, - p. 29.
3. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Ainur Zhetpisbayeva Secure Outsourcing of Finding the Extremum of a Function with Secret Parameters // Book of abstracts of the III International Turkic World Congress on Science and Engineering 14-15 June 2021, Niğde – Turkey, - p. 30.
4. Banu B. Yergaliyeva, Yerzhan N. Seitkulov, Dina Satybaldina Secure methods for solving computationally-complex problems using auxiliary computers Indonesian // Indonesian Journal of Electrical Engineering and Computer Science (**Процентиль по CiteScore в базе Scopus - 47**; **руководитель проекта Е.Сейткулов – является автором для корреспонденции, на момент утверждения и сдачи отчета (14.10.21) статья находится на стадии рецензирования**)

**ПРИЛОЖЕНИЕ Б**

**Календарный план работ на 2021 год**



