МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

На правах рукописи

Ярмак Анастасия Викторовна

ГРУППОВАЯ АУТЕНТИФИКАЦИЯ И КРИПТОГРАФИЧЕСКИЙ КОНТРОЛЬ ДОСТУПА В СИСТЕМАХ С ИЕРАРХИЧЕСКОЙ СТРУКТУРОЙ НА ОСНОВЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки)

Направленность: 10.06.01_01 – Методы и системы защиты информации, информационная безопасность

Академическая степень **Исследователь. Преподаватель-исследователь**

НАУЧНЫЙ ДОКЛАД

Научный руководитель: д.т.н., доцент, профессор ИКиЗИ,

Александрова Елена Борисовна

Санкт-Петербург, 2022

Научный доклад выполнен в Институте кибербезопасности и защиты информации федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

Научный руководитель: д.т.н., доцент, профессор ИКиЗИ,
Александрова Елена Борисовна

Рецензент: д.т.н., доцент, профессор ИКиЗИ,
Полтавцева Мария Анатольевна

С научным докладом можно ознакомиться в библиотеке ФГАОУ ВО «Санкт–Петербургский политехнический университет Петра Великого» и на сайте Электронной библиотеки СПбПУ по адресу: http://elib.spbstu.ru.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современные крупномасштабные системы представляют собой класс сложных систем с взаимодействующими территориально-распределенными компонентами, построенными на базе технологий Интернета вещей, промышленного Интернета вещей, беспроводных сенсорных сетей и т.п. Большое число узлов системы, их распределенность и избыточность, разнородность вычислительных возможностей и ролей устройств, динамическая топология сети – все эти аспекты накладывают свои ограничения с точки зрения применения традиционных способов обеспечения кибербезопасности. Ключевыми факторами в развитии систем управления крупномасштабными объектами такого типа представляются переход к групповой, многоадресной передаче данных, обеспечивающей возможность одновременной рассылки информации устройствам, входящим в некоторую группу (групповое взаимодействие узлов), а также использование принципа многоуровневого, многослойного и стратифицированного описания архитектуры (в контексте теории многоуровневых иерархических систем М. Месаровича, Д. Мако и И. Такахара) с введённым отношением вертикальной соподчиненности подсистем.

Организация защищенного взаимодействия узлов является одной из актуальных задач в области обеспечения кибербезопасности крупномасштабных систем, так как подделка и несанкционированное изменение потока команд, циркулирующего между устройствами, может привести к нарушению логики работы и согласованности процессов всей системы. Кроме того, для хранения данных крупномасштабных систем все чаще стали использоваться облачные сервисы, что обусловлено отсутствием необходимости развертывания и обслуживания собственной инфраструктуры, меньшими затратами на персонал и ресурсы, возможностью обеспечения быстрого доступа к данным с различных устройств.

Таким образом, с учетом специфики крупномасштабных систем актуальной представляется разработка решений, направленных на защиту от угрозы несанкционированного доступа к данным, в том числе со стороны недоверенного

облачного провайдера, а также обеспечивающих доверие (под которым понимается гарантия целостности, невозможности отрицания авторства и аутентификацию источника данных) к циркулирующей между устройствами информации.

Степень разработанности темы исследования. Изогениям эллиптических кривых и возможности их применения для построения криптографических протоколов посвящены труды таких отечественных и зарубежных специалистов, как О.Н. Василенко, А.Г. Ростовцев, А.Г. Столбунов, Е.Б. Александрова, Э. Чайлдс, Л. де Фео, Д. Кохель, С. Галбрайт, В. Кастрик, Т. Декру. Вклад в развитие направления коллективной цифровой подписи и упорядоченной цифровой подписи внесли Н.А. Молдовян, М. Белларе, Х. Дой, А. Болдырева, С. Митоми, А. Мияги, М. Бурместер. Разработке схем криптографического контроля доступа посвящены работы С.В. Запечникова, С. Акла, А. Кайема, В. Гойяла, Д. Крэмптона. В работах Э. Н. Самохвалова, Г. И. Ревункова, Ю. Е. Гапанюка, А.К. Новохрестова, А. Басу и Р. Блэннинга предложено использование метаграфов для моделирования информационных систем и процессов, оценки их защищенности.

Объектом исследования являются крупномасштабные системы с многоуровневой иерархической структурой участников.

Предметом исследования являются методы групповой аутентификации информации и криптографического контроля доступа к данным.

Целью работы является обеспечение защищенного группового взаимодействия и доступа к данным в иерархических системах.

Для достижения поставленной цели в работе решались следующие задачи:

1. Проанализировать объект исследования: выявить специфику обеспечения защищенного взаимодействия и контроля доступа к данным.
2. Построить модель группового взаимодействия узлов в условиях иерархической структуры участников на основе аппарата атрибутивных метаграфов.
3. Разработать протокол иерархической групповой аутентификации информации на основе изогений эллиптических кривых.

4. Разработать схему криптографического контроля доступа к данным с учетом иерархической структуры участников.

5. Построить архитектуру и реализовать прототип системы иерархической групповой аутентификации и контроля доступа к данным для оценки эффективности предложенных конструкций.

Научная новизна научно-квалификационной работы состоит в следующем:

– впервые разработана метаграфовая модель группового взаимодействия узлов в иерархических системах;

– в отличие от известных предлагаемый протокол групповой аутентификации основан на вычислительно сложной задаче постквантовой криптографии и разработан с учетом специфики крупномасштабных систем;

– предлагаемая схема криптографического контроля доступа отличается сочетанием математического аппарата изогений эллиптических кривых и модели ролевого контроля доступа.

Теоретическая значимость результатов работы заключается в установлении свойств графов изогений суперсингулярных кривых степени 3, разработке классификации упорядоченных схем подписи.

Практическая значимость результатов работы заключается в возможности применения предложенного метода в промышленном Интернете Вещей как примера распределенной системы с многоуровневой иерархической структурой для обеспечения доверия к данным при межмашинном взаимодействии узлов и защиты от угрозы несанкционированного доступа при облачном хранении данных.

Методы исследования. Для решения поставленных задач в научно-квалификационной работе использовались методы теории чисел, алгебры, криптографии, алгебраической геометрии, теории графов.

Положения, выносимые на защиту:

1. Модель группового взаимодействия узлов в условиях иерархии на основе аппарата атрибутивных метаграфов.

2. Протокол иерархической групповой аутентификации информации на основе изогений эллиптических кривых.

3. Схема криптографического контроля доступа к данным на основе иерархической модели сущностей с использованием изогений эллиптических кривых.

4. Архитектура системы иерархической групповой аутентификации и контроля доступа к данным в крупномасштабных системах.

Достоверность и обоснованность результатов, представленных в научно-квалификационной работе, подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными и апробацией результатов в научных публикациях и докладах на конференциях.

Апробация работы. Основные результаты исследований были представлены на следующих конференциях: научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2018-2022 гг.), научно-практическая конференция с международным участием «Неделя науки СПбПУ» (Санкт-Петербург, 2019, 2022 гг.), 5-я международная онлайн-конференция «Алгоритмы и решения на основе компьютерных технологий», ASBC (2021 г.), 2-я международная конференция «Киберфизические системы и управление», CPS&C (2021 г.), международная конференция «World Conference on Smart Trends in Systems, Security and Sustainability WorldS4» (Лондон, 2022 г.), международная научно-техническая конференция «Автоматизация» (Сочи, 2022 г.).

Исследования, лежащие в основе данной работы, победили в конкурсе грантов Правительства Санкт-Петербурга для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, в 2019 и 2021 годах. Результаты работы использованы при выполнении исследований РФФИ № 20-37-90106, при выполнении научного проекта № 12/21-к (грант ИБ).

Публикации. Результаты научно-квалификационной работы отражены в 14 публикациях, в том числе в 4 публикациях в рецензируемых журналах из перечня

ВАК РФ, 5 публикациях в изданиях из перечня Scopus и Web of Science, а также в свидетельстве о регистрации программ для ЭВМ.

Структура и объем научно-квалификационной работы. Научно-квалификационная работа состоит из введения, четырех глав, заключения, списка использованных источников из 98 наименований. Общий объем работы составляет 110 страниц, в том числе 15 рисунков и 15 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приведено обоснование актуальности темы исследования, сформулирована цель работы, а также выполнена постановка задач, необходимых для ее достижения. Отражена научная новизна, теоретическая и практическая значимость результатов работы, сформулированы положения, выносимые на защиту.

В первой главе научно-квалификационной работы выполнено исследование принципов организации и управления крупномасштабными системами. Выделены следующие особенности:

– наличие функциональных подсистем, каждая из которых может решать свои целевые задачи, взаимодействовать с другими подсистемами, а также иметь локальные центры принятия решений;

– использование многоадресной передачи данных, позволяющее снизить нагрузку на сеть и синхронизировать потоки команд;

– упорядочение и снижение количества информационных потоков, а также локализация динамических изменений структуры за счет введения отношения подчиненности, или иерархии, как на множестве узлов внутри подсистем, так и на множестве самих подсистем.

Рассмотрены типовые архитектуры систем управления сложными системами, а также сценарии, демонстрирующие преимущества иерархического подхода. Определены критерии, которые могут быть использованы для кластеризации узлов по группам, а также выделены признаки, используемые при их дифференциации по уровням иерархии. Несмотря на указанные положительные

эффекты, связанные с оптимизацией работы функциональной составляющей, отмечается, что из обозначенной специфики следует необходимость в решении новых задач по обеспечению защищенного группового взаимодействия и контроля доступа к данным. Сделан вывод о целесообразности применения для решения поставленных задач методов криптографической защиты информации.

Для моделирования процессов групповой аутентификации и контроля доступа к данным разработана метаграфовая модель представления узлов в иерархических системах. Метаграф задается тройкой:

$$MG =< V, MV, E >,$$

где:

– V – множество вершин;

– MV – множество метавершин;

– E – множество ребер.

Вершинам и ребрам метаграфа можно сопоставить произвольный набор атрибутов – такой метаграф называется атрибутивным. В атрибутивном метаграфе каждая вершина характеризуется атрибутами $\{attr_{i,j}\}$:

$$v_i = \{attr_{i,j}\},$$

метавершина определяется следующим образом:

$$mv_i = (\{attr_{i,j}\}, \{ev_{i,k}\}), ev_{i,k} \in (V \cup E \cup MV),$$

где $ev_{i,k}$ – фрагмент графа, который может содержать вершины, метавершины и соединяющие их ребра. Ребро метаграфа задается кортежем:

$$e_i = (v_{in}^{(i)}, v_{out}^{(i)}, \{attr_{i,j}\}, eo),$$

где $v_{in}^{(i)} \in V \cup MV$ – исходная вершина (метавершина), $v_{out}^{(i)} \in V \cup MV$ – конечная вершина (метавершина), $\{attr_{i,j}\}$ – атрибуты, $eo = \{True, False\}$ – признак направленности ребра.

Атрибутивные метаграфы позволяют описать защищённое групповое взаимодействие в рамках единой модели, где вершины – это субъекты (узлы) системы, которые агрегируются в метавершину – группу этих объектов в соответствии с определенным критерием кластеризации, ребра характеризуют

отношение подчиненности, атрибуты соответствуют значениям, ассоциированным с ребрами и вершинами метаграфа и определяемым предметной областью (например, криптографическим ключам, меткам доступа и т.п.).

Любые изменения членства в группе (табл.1) и отношений подчиненности можно задавать с помощью операций над метаграфом $MGA =< V, MV, E >$, который преобразуется в метаграф $MGA' =< V', MV', E' >$.

Таблица 1 — Пример операций над метаграфом, характеризующим групповое взаимодействие в иерархических системах

Описание	Операция над метаграфом	Событие при групповом взаимодействии
Добавление ребра e_k между вершинами v_i и v_j	$MGA' \leftarrow add\_edge(MGA, v_i, v_j, \{attr_{k,s}\}, eo)$: $V' = V, E' = E \cup (\{v_i\}, \{v_j\}, \{attr_{k,s}\}, eo)$.	Добавление отношения подчиненности между узлами; установление связи
Удаление ребра e_k между вершинами v_i и v_j	$MGA' \leftarrow delete\_edge(MGA, v_i, v_j,)$: $V' = V, E' = E \backslash (\{v_i\}, \{v_j\}, \{attr_{k,s}\}, eo)$.	Удаление отношения подчиненности между узлами; разрыв связи
Добавление вершины v_i в метаграф	$MGA' \leftarrow add\_vertex(MGA, v_i)$: $V' = V \cup \{v_i\}$, $v_i \leftarrow \{attr_{i,k}\}$, $E' = E$.	Добавление узла в систему
Удаление вершины v_i из метаграфа	$MGA' \leftarrow delete\_vertex(MGA, v_i)$: $V' = V \backslash \{v_i\}$, если $\exists e_j \in E$: $v_i \in invertex\ (e_j)$, то $e'_j \leftarrow (v_{in}^{(j)} \backslash \{v_i\}, v_{out}^{(j)}, \{attr_{j,s}\}, eo) \in E'$; если $\exists e_j \in E$: $v_i \in outvertex\ (e_j)$, то $e'_j \leftarrow (v_{in}^{(j)}, v_{out}^{(j)} \backslash \{v_i\}, \{attr_{j,s}\}, eo) \in E'$.	Удаление узла из системы
Удаление вершины v_i из метавершины mv_j вместе с инцидентными ребрами	$MGA' \leftarrow delete\_v\_from\_mv(MGA, v_i, mv_j)$: $mv'_j \leftarrow (\{attr_{j,l}\}, \{ev'_{j,k}\}) \in MV'$, где $\{ev'_{j,k}\} = \{ev_{j,k}\} \backslash (\{v_i\} \cup \{e_t \in E \mid v_i \in invertex\ (e_t)\} \cup \{e_s \in E \mid v_i \in outvertex\ (e_s)\})$.	Отзыв членства в группе
Включение узла v_i в метавершину mv_j с сохранением	$MGA' \leftarrow insert\_v\_to\_mv(MGA, v_i, mv_j)$: $mv'_j \leftarrow (\{attr_{j,l}\}, \{ev'_{j,k}\}) \in MV'$, где	Добавление узла в группу; переход узла из одной группы в другую

Описание	Операция над метаграфом	Событие при групповом взаимодействии
инцидентных ребер	$\{ev'_{j,k}\} = \{ev_{j,k}\} \cup (\{v_i\} \cup \{e_t \in E \mid v_i \in invertex(e_t)\}) \cup \{e_s \in E \mid v_i \in outvertex(e_s)\})$; Если $\exists\, mv_k = (\{attr_{k,l}\}, \{ev_{k,r}\}) : v_i \in \{ev_{k,r}\}$, то $delete\_v\_from\_mv(MGA, v_i, mv_k)$	

В рамках введённой модели иерархическая групповая аутентификация данных представляется в виде простого пути $h(x, y)$ из элемента x в элемент y, т.е. последовательности ребер $(e_1, \dots, e_m)$ такой, что x принадлежит множеству начальных вершин $x \in invertex(e_1)$, y принадлежит множеству конечных вершин $y \in outvertex(e_n)$, и для любого ребра $e_i, i = 1, \dots, m-1$ из пути выполняется соотношение $outvertex(e_i) \cap invertex(e_{i+1}) \neq \emptyset$. Криптографический контроль доступа задается с помощью атрибутов узлов и вершин. Архитектура системы представлена на рис. 1.

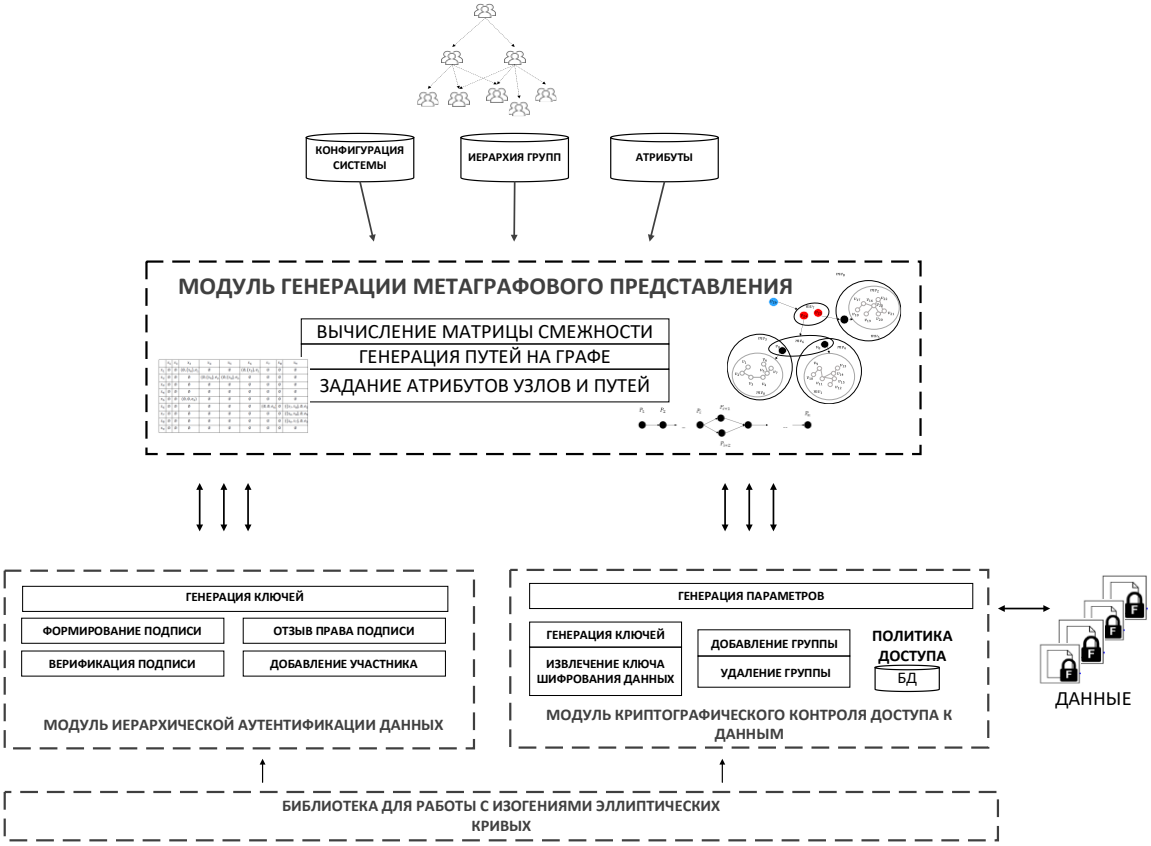

Рисунок 1 — Архитектура системы иерархической групповой аутентификации и контроля доступа к данным в крупномасштабных системах

Во второй главе научно-квалификационной работы выполнено обоснование выбранного математического аппарата для иерархической групповой аутентификации данных и криптографического контроля доступа. Изогении эллиптических кривых позволяют строить гибкие криптографические протоколы, ориентированные на применение в крупномасштабных системах с иерархической структурой.

Криптосистемы с открытым ключом на изогениях эллиптических кривых можно разделить на три семейства: CRS-схемы, SIDH-схемы и CSIDH-схемы. В научно-квалификационной работе представлен сравнительный анализ подходов к построению протоколов на изогениях по критериям сложности задач, длине параметров и ключей, используемым кривым, скорости вычислений изогений.

Процесс построения графа изогений суперсингулярных и несуперсингулярных кривых формализован в виде алгоритма 1.

Алгоритм 1. Вычисление графа изогений суперсингулярных кривых.

Вход: суперсингулярная кривая $E\left(\mathbb{F}_{p^2}\right), j_0 = j(E)$.

Выход: граф $\mathcal{G}_l$ изогений степени l.

1. Инициализировать структуры для хранения вершин (посещенных и вершин на очереди для посещения): $visited \leftarrow \{\emptyset\}, queue \leftarrow \{j_0\}$.
2. Задать структуру графа $\mathcal{G}_l = (\mathcal{V}_l,\ \mathcal{E}_l), \mathcal{V}_l \leftarrow \{\emptyset\}, \mathcal{E}_l \leftarrow \{\emptyset\}$.
3. Пока структура $queue$ не пуста, выполнить следующие шаги:
   3.1. Извлечь первый элемент из множества вершин на очереди: $j_i \leftarrow queue.pop(0)$.
   3.2. Добавить элемент j_i в список посещенных: $visited \leftarrow visited \cup \{ j_i \}$, а также в список вершин графа: $\mathcal{V}_l \leftarrow \mathcal{V}_l \cup \{j_i\}$.
   3.3. С помощью модулярного полинома вычислить всех изогенных с j_i вершин-соседей (вершины указываются с учетом кратности): $j_{nbrs} \leftarrow \{j_{nbrs}^{(1)}, j_{nbrs}^{(2)}, \dots, j_{nbrs}^{(m)}\}$.
   3.4. Для каждой вершины-соседа $j_{nbrs}^{(k)}$ из j_{nbrs} выполнить:

3.4.1. Если $j_i < j_{nbrs}^{(k)}$ или $j_i = j_{nbrs}^{(k)}$, то $\mathcal{V}_l \leftarrow \mathcal{V}_l \cup \{j_{nbrs}^{(k)}\}$, $\mathcal{E}_l \leftarrow \mathcal{E}_l \cup (j_i, j_{nbrs}^{(k)})$.

3.4.2. Если $j_{nbrs}^{(k)} \notin visited$ и $j_{nbrs}^{(k)} \notin queue$, то $queue \leftarrow queue.add\left(j_{nbrs}^{(k)}\right)$.

4. Результат: граф $\mathcal{G}_l$.

Также представлены результаты, расширяющие работы сторонних исследователей о графовой структуре изогенных эллиптических кривых. В частности, рассмотрены свойства графа изогений степени 3 для характеристики поля $5 \leq p < 400000$. Зависимость диаметра графа изогений от длины характеристики поля ближе к известной оценке, полученной для диаметра случайного графа Кэли (рис. 2), что согласуется с утверждением, известным для графа изогений степени 2.

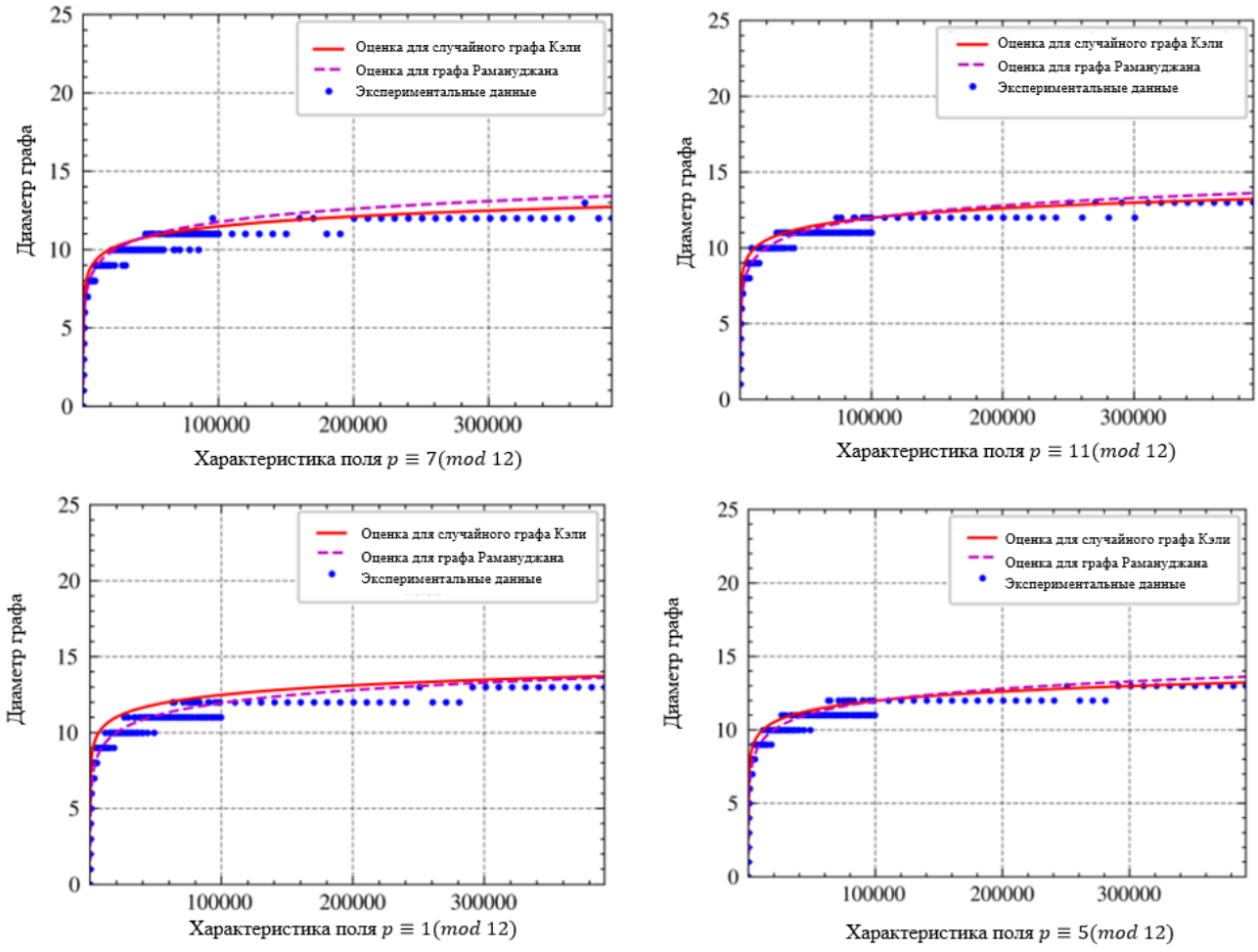

Рисунок 2 — Диаметр графа изогений степени 3

В третьей главе представлен сравнительный анализ протоколов иерархической групповой аутентификации данных, описаны требования к таким конструкциям. Выполнена классификация протоколов упорядоченной подписи по ряду критериев (рис. 3). Предлагаемая схема аутентификации включает в себя четыре процедуры:

– алгоритм генерации параметров;

– алгоритм генерации ключей для участников группы;

– алгоритм формирования подписи;

– алгоритм проверки подписи.

Разработанный протокол коллективной упорядоченной аутентификации данных относится к семейству CSIDH-криптосистем, основан на схеме подписи CSI-FiSh и поддерживает смешанную (как последовательную, так и параллельную) структуру порядка подписи.

Рисунок 3 — Классификация схем упорядоченной групповой аутентификации

Работа схемы иерархической аутентификации была смоделирована с помощью системы компьютерной алгебры SageMath (табл.2) при различном количестве участников группы. Так как в системе SageMath не поддерживается вычисление изогений больших степеней, скорость разработанных прототипов

сравнительно невысока и может быть повышена с использованием низкоуровневых оптимизаций.

Таблица 2 — Результаты тестирования схемы иерархической аутентификации данных

Число участников	Время генерации параметров, с	Время формирования подписи, с	Время проверки подписи, с
5	6,063070	6,357434	0,267946
10	10,586900	13,167771	0,292639
15	14,542996	16,814208	0,290805
20	19,218307	29,324794	0,285047
100	99,185662	147,950126	0,277599
1000	1289,741436	692,340088	0,286423

Размер коллективной цифровой подписи эквивалентен размеру подписи, сформированной одним пользователем и равна 8064, 15806, 20644, 82576 бит при параметре безопасности λ, равном 80, 112, 128, 256 соответственно.

В четвертой главе научно-квалификационной работы описана разработанная схема криптографического контроля доступа, подходящая для иерархической структуры групп пользователей. Пусть $SC = \{SC_1, SC_2, \dots, SC_n\} -$ множество классов доступа, каждый из которых ассоциирован с данными, доступными некоторой группе пользователей $P_i, i = 1,2, \dots, n$. На множестве SC задано отношение порядка $SC_i \leq SC_j$, которое может быть интерпретировано следующим образом: участник группы P_j имеет доступ к данным класса SC_i, однако аналогичное утверждение для пользователей из P_i относительно возможности доступа к данным класса SC_j не выполняется.

Предлагаемая схема подразумевает наличие доверенной стороны, осуществляющей управление криптографическими ключами и, в общем случае, включает три этапа:

– этап инициализации параметров, на котором доверенная сторона выполняет генерацию параметров схемы;

– этап генерации ключей, на котором для каждой группы участников генерируется закрытый ключ и соответствующий открытый ключ, а также осуществляется вычисление ключа шифрования данных, доступных группе.

– этап извлечения ключа, в процессе которого член группы верхнего уровня на основе собственного ключа шифрования и общедоступной информации, связанной с подчиненной группой, вычисляет ключ расшифрования данных, доступных участникам, расположенным по иерархии ниже.

Кроме того, предусмотрены алгоритмы смены ключей группы пользователей, удаления пользователей и добавления пользователей. Результаты моделирования процедур инициализации параметров, генерации ключей, извлечения ключа шифрования при различном количестве групп пользователей (табл. 3) показывают, что время извлечения ключа шифрования не зависит от размера группы. Кроме того, время генерации ключей для членов групп растет по мере увеличения числа участников, однако данный этап может быть распараллелен путем использования нескольких вычислителей, каждый из которых будет взаимодействовать с своим пулом пользователей.

Таблица 3 — Результаты тестирования разработанной схемы контроля доступа

Число участников	Инициализация параметров схемы, с	Время генерации ключей, с	Извлечение ключа шифрования, с
5	0,693784	1,423340	0,005695
10	0,779167	2,650283	0,005794
15	0,842976	2,727988	0,005829
20	0,856158	2,890149	0,005861
100	0,896185	3,264611	0,006499

Проведенный анализ безопасности включал в себя рассмотрение следующих сценариев:

– попытка восстановления ключа шифрования данных, принадлежащих группе, расположенной по иерархии выше;

– сговор участников подчиненных групп для восстановления ключа шифрования данных группы, расположенной по иерархии выше;

– попытка восстановления ключа шифрования данных, принадлежащих группе, имеющей ту же родительскую группу;

– попытка доступа к данным группы исключенным участником.

В заключении приведены основные результаты, полученные в ходе выполнения научно-квалификационной работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Исследованы архитектурные особенности крупномасштабных систем, выделены критерии, используемые при кластеризации участников системы в группы. Описана модель представления узлов в иерархической системе на основе аппарата атрибутивных метаграфов. Разработана архитектура системы групповой аутентификации и криптографического контроля доступа к данным, использующая метаграфовую модель группового взаимодействия узлов в условиях иерархии.

2. Проведен сравнительный анализ криптосистем на изогениях по критериям сложности задач, длине параметров и ключей, используемым кривым, скорости вычислений изогений. Исследованы характеристики графа изогений эллиптических кривых степени 3.

3. Разработана классификация протоколов иерархической групповой аутентификации данных. Предложена схема, в основе безопасности которой используются задачи поиска изогений эллиптических кривых.

4. Проведен сравнительный анализ способов организации криптографического контроля доступа к данным. Предложена конструкция, учитывающая иерархию групп пользователей и обеспечивающая возможность доступа к данным участников, расположенных по иерархии ниже.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из перечня ВАК:

1. Александрова, Е. Б., **Ярмак, А. В.** Иерархическая групповая аутентификация для защищенного взаимодействия узлов в промышленном Интернете вещей //Защита информации. Инсайд. – 2021. – №. 2. – С. 23-27.

2. Александрова, Е. Б., Штыркина, А. А., **Ярмак, А. В.** Генерация эллиптических кривых для криптосистем на изогениях //Проблемы информационной безопасности. Компьютерные системы. – 2017. – №. 1. – С. 50-58.

3. Александрова, Е. Б., **Ярмак, А. В.**, Калинин, М. О. Анализ подходов к обеспечению защищенного взаимодействия в крупномасштабных промышленных системах //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 4. – С. 140-144.

4. Александрова, Е. Б., Штыркина, А. А., **Ярмак, А. В.** Организация криптографического контроля доступа на основе изогений эллиптических кривых //Проблемы информационной безопасности. Компьютерные системы. – 2019. – №. 3. – С. 104-114.

В свидетельствах о регистрации программы для ЭВМ:

Ярмак, А.В. Программа для моделирования графового представления изогений эллиптических кривых, номер свидетельства: RU 2022617504. – зарегистр. 13.04.2022.

В изданиях, индексируемых Scopus и/или Web of Science:

1. Aleksandrova, E. B., Shtyrkina, A. A., **Iarmak, A. V.** Post-quantum primitives in information security //Nonlinear Phenomena in Complex Systems. – 2019. – Т. 22. – №. 3. – С. 269-276.

2. Aleksandrova, E. B., Shtyrkina, A. A., **Yarmak, A. V.** Post-quantum group-oriented authentication in IoT //Nonlinear Phenomena in Complex Systems. – 2020. – Т. 23. – №. 4. – С. 405-413.

3. Alexandrova, E., Poltavtseva, M., **Yarmak, A.** Application of hierarchic authentication to isogenies of elliptic curves for providing safety of data routing in the

systems of analysis of digital production traffic //SHS Web of Conferences. – EDP Sciences, 2018. – Т. 44. – С. 00007.

4. Aleksandrova, E. B., Rekhviashvili, I. S., **Yarmak, A. V.** Lattice-based ring signature with linking-based revocation for industrial Internet of Things //Automatic Control and Computer Sciences. – 2020. – Т. 54. – №. 8. – С. 888-895.

5. Aleksandrova, E., Pendrikova, O., Shtyrkina, A., Shkorkina, E., **Yarmak, A.**, Tick, J. Threshold Isogeny-Based Group Authentication Scheme //Algorithms and Solutions Based on Computer Technology. – Springer, Cham, 2022. – С. 117-126.

Публикации в других изданиях:

1. Федичев, А. В., **Ярмак, А. В.**, Александрова, Е. Б. Оценка быстродействия постквантовых криптографических алгоритмов для маломощных устройств промышленного Интернета вещей //Методы и технические средства обеспечения безопасности информации. – 2021. – №. 30. – С. 47-48.

2. Александрова, Е. Б., **Ярмак, А. В.** Генерация изогенных эллиптических кривых для криптосистем на билинейных отображениях //Методы и технические средства обеспечения безопасности информации. – 2016. – №. 25. – С. 67-69.

3. Александрова, Е. Б., **Ярмак, А. В.** Схема иерархической аутентификации на изогениях эллиптических кривых в сетях динамической архитектуры //Методы и технические средства обеспечения безопасности информации. – 2018. – №. 27. – С. 65-67.

4. Штыркина, А. А., **Ярмак, А. В.**, Александрова, Е. Б. Криптографический контроль доступа на основе изогений эллиптических кривых //Неделя науки СПбПУ. – 2019. – С. 284-286.

5. Александрова, Е. Б., **Ярмак, А. В.**, Штыркина, А. А. Делегирование базиса как механизм построения иерархической схемы аутентификации на решетках в интернете вещей //Методы и технические средства обеспечения безопасности информации. – 2020. – №. 29. – С. 101-103.