«Национальный исследовательский ядерный университет «МИФИ»

На правах рукописи

Макаров Артём Олегович

Способы построения последовательных агрегированных электронных подписей с использованием многомерных квадратичных многочленов и алгебраических кодов

Специальность — 2.3.6

Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени

кандидата технических наук

Москва 2025

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Научный руководитель	**Варфоломеев Александр Алексеевич** кандидат физико-математических наук, доцент, доцент кафедры «Криптология и кибербезопасность» Национального исследовательского ядерного университета «МИФИ»
Официальные оппоненты:	**Логачев Олег Алексеевич** доктор физико-математических наук, доцент, доцент кафедры информационной безопасности Московского государственного университета имени М.В. Ломоносова
	Чеповский Андрей Михайлович доктор технических наук, профессор, профессор кафедры прикладной информатики и информационной безопасности Российского экономического университета имени Г.В. Плеханова
	Коренева Алиса Михайловна кандидат физико-математических наук, заместитель руководителя службы сертификации по научно-техническому сотрудничеству ООО «Код Безопасности»

Защита состоится 15 апреля 2026 г. в 17:00 часов на заседании диссертационного совета «МИФИ.2.05» Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ» (115409, г. Москва, Каширское шоссе, 31).
С диссертацией можно ознакомиться в библиотеке НИЯУ МИФИ и на сайте https://ds.mephi.ru Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ».

Автореферат разослан «___» _____ 2026 года.

Учёный секретарь
Диссертационного совета МИФИ.2.05, _____ / Кессаринский Л.Н.
кандидат технических наук

Общая характеристика работы

Тема диссертационного исследования связана с построением схем постквантовой агрегированной электронной подписи, а также с исследованием их применимости для различных приложений.

Актуальность темы исследования

Системам обеспечения безопасности часто приходится иметь дело с электронными подписями, выработанными различными пользователями для различных сообщений. Например, в инфраструктуре открытых ключей (PKI) глубины n подпись пользователя также содержит цепочку из n сертификатов. Эта цепочка содержит n подписей различных центров сертификации на n открытых ключах. Аналогичная ситуация складывается при использовании протоколов[1] SBGP и BGPsec, являющихся расширениями протокола BGP. Для рассылки информации о доступности автономная система подписывает свой адрес и адрес другой автономной системы, через которую она желает быть доступной. После получения сообщения другими автономными системами производится проверка подписи. Далее эти системы дополняют сообщение своим адресом и адресом следующей системы, которая получит данное сообщение, и затем подписывает это сообщение.

Обе описанные системы могли бы получить выигрыш при использовании алгоритма сжатия списка электронных подписей для разных сообщений, подписанных различными сторонами. Например, цепочка сертификатов может быть сокращена путём агрегации всех подписей в ней в единую подпись, которая может использоваться для проверки всех подписанных сообщений в цепочке.

Основная идея, лежащая в основе агрегации подписей: при наличии n различных электронных подписей для n различных сообщений, выработанных n различными пользователями, должна иметься возможность преобразовать данные подписи в единую электронную подпись. Полученная подпись может быть использована для проверки подписи для каждого из n сообщений. Применение данного вида подписей снижает нагрузку на сеть при передаче данных, что позволяет обеспечить неотказуемость и аутентичность информации в ряде приложений, для которых использование стандартных электронных подписей зачастую нецелесообразно (таких как сенсорные сети).

Последовательные агрегированные подписи, рассматриваемые в данной работе, являются частным случаем агрегированных, для которых объединение индивидуальных подписей возможно только в момент получения очередной агрегированной подписи. В общем случае схемы такого типа требуют проверки предыдущей агрегированной подписи при формировании следующей, что уменьшает их производительность. Схемы последовательной агрегированной электронной подписи, не требующие такой проверки, называются схемами с ленивой проверкой.

Питером Шором был предложен эффективный квантовый алгоритм[2] для решения задачи нахождения скрытой подгруппы конечной абелевой группы, частным

---

[1] **Kent S.** Secure Border Gateway Protocol (S-BGP) — Real World Performance and Deployment Issues / S. Kent [et al.]. – 14 p.; **Lepinski M.** BGPsec Protocol Specification / M. Lepinski, K. Sriram. – Internet Engineering Task Force, 2017. – 45 p.

[2] **Shor P.W.** Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P.W. Shor // SIAM Journal on Computing. – 1997. – Vol. 26. – № 5. – P. 1484-1509.

случаем которой являются задачи факторизации и дискретного логарифмирования. Возможность практического применения данного алгоритма с использованием квантового компьютера ставит под угрозу стойкость криптосистем, в основе которых лежат упомянутые задачи.

В связи с этим ставится вопрос о существовании асимметричных криптосистем, стойких к квантовым атакам. В случае их наличия программные и аппаратные средства обеспечения криптографической защиты с учётом возможности квантовых атак должны быть разработаны задолго до потенциального появления квантового компьютера, так как процедуры стандартизации и замены аппаратных платформ занимают длительное время. К тому же следует учитывать существование информации, которая должна оставаться защищённой даже спустя длительное время, с учётом возможного появления квантовых компьютеров в будущем.

В связи с возможностью появления квантового компьютера в ближайшем будущем криптографическим сообществом активно ведётся разработка и анализ так называемых постквантовых криптографических примитивов, которые будут являться теоретически стойкими даже в условиях квантовой атаки. В настоящий момент существует несколько способов построения асимметричных примитивов, стойких к квантовым атакам. В данной работе рассмотрены два из них — криптосистемы на основе многомерных квадратичных многочленов и теории алгебраического кодирования.

Тема диссертационного исследования связана с построением схем постквантовой агрегированной электронной подписи, а также с исследованием их применимости для различных приложений.

Цель и задачи исследования

Целью исследования является уменьшение размера хранимых и передаваемых данных при использовании схем электронной подписи в информационных системах путём построения и реализации схем последовательной агрегированной электронной подписи с учётом квантового противника.

Научная задача: построение схем последовательной агрегированной электронной подписи на основе односторонних функций с секретом с использованием многомерных квадратичных многочленов и алгебраических кодов.

Для достижения поставленной цели в работе решались следующие задачи:

– анализ потенциального применения схем агрегированной электронной подписи в информационных системах;

– построение схем агрегированной электронной подписи с использованием многомерных квадратичных многочленов и алгебраических кодов, обоснование их стойкости и возможного применения;

– программная реализация предложенных схем агрегированной электронной подписи, получение данных по производительности схем;

– разработка и реализация программной архитектуры системы защищённого аудита с использованием схемы последовательной агрегированной электронной подписи.

Научная новизна диссертационного исследования заключается в следующем:

– впервые предложен способ построения схем последовательной агрегированной электронной подписи SAS-X, являющийся обобщением способа построения схем последовательной агрегированной электронной подписи Лисянской на случай односторонних функций с секретом;

– впервые предложен способ построения схем последовательной агрегированной электронной подписи LSAS-X с ленивой проверкой, являющийся обобщением способа построения схем последовательной агрегированной электронной подписи Гентри на случай односторонних функций с секретом, отличающийся от существующего способа Менегетти-Сигнорини меньшим размером подписи и большей производительностью;

– представлена новая схема последовательной агрегированной электронной подписи SAS-UOV на основе многомерных квадратичных многочленов, а также схемы APCFS/ARCFS на основе теории алгебраического кодирования с использованием кодов Гоппы;

– представлена новая схема последовательной агрегированной электронной подписи с ленивой проверкой LSAS-UOV на основе многомерных квадратичных многочленов, а также схема с ленивой проверкой LARCFS на основе теории алгебраического кодирования с использованием кодов Гоппы.

Теоретическая и практическая значимость работы

Теоретическая значимость работы заключается в получении способов построения схем последовательной агрегированной подписи на основе односторонней функции с секретом, разработке новых схем последовательной агрегированной электронной подписи.

Самостоятельное **практическое значение** имеют следующие результаты работы:

– оценка критичности требований к элементам схем агрегированной электронной подписи для различных приложений;

– данные о производительности схем последовательной агрегированной электронной подписи на основе многомерных квадратичных многочленов и алгебраических кодов;

– программная архитектура системы защищённого аудита, использующая схему последовательной агрегированной электронной подписи.

Методология и методы исследования

Для решения поставленных задач в работе использовались методы теории вероятности, теории алгебраического кодирования, теории чисел, алгебры, доказательной криптографии и теории сложности вычислений.

Положения, выносимые на защиту:

– Способы построения схем последовательной агрегированной электронной подписи с использованием односторонних функций с секретом.

– Схемы последовательной агрегированной электронной подписи на основе многомерных квадратичных многочленов и теории алгебраического кодирования, включая схемы с ленивой проверкой.

– Программная архитектура системы защищённого аудита с использованием схемы последовательной агрегированной электронной подписи.

Соответствие паспорту специальности

Диссертация соответствует паспорту специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность в части п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности»; п. 19 «Исследования в области безопасности криптографических алгоритмов, криптографических

примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов».

Степень достоверности и апробация результатов

Достоверность и обоснованность полученных автором результатов обеспечиваются строгими математическими доказательствами представленных утверждений.

Результаты диссертационного исследования докладывались на следующих конференциях и семинарах:

– IX Всероссийская научно-техническая конференция «Безопасные информационные технологии» (БИТ-2018), 3-4 декабря 2018 г., г. Москва;

– Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, 21-23 октября 2019 г., г. Москва;

– 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 27-30 января 2020 г., г. Москва;

– 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 26-29 января 2021 г., г. Москва;

– Семинар «Математические методы криптографического анализа», ВМК, МГУ им. М.В. Ломоносова, 17 июня 2025 г., г. Москва;

– XIV Всероссийская научно-техническая конференция «Безопасные информационные технологии» (БИТ-2025), 31 октября 2025 г., г. Москва;

– Третья Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность» (КИБ-2025), 3-4 декабря 2025 г., г. Москва.

Внедрение результатов работы. Результаты диссертационной работы использованы при проработке концепции и технических решений систем защищённого аудита в ООО «КРИПТО-ПРО» и АО «НПО «Эшелон». Теоретические результаты исследования внедрены в учебный процесс НИЯУ МИФИ по дисциплинам «Методы и средства криптографической защиты информации» и «Прикладная криптография».

Публикации. Результаты диссертационного исследования опубликованы в 9 печатных работах, из которых 2 опубликованы в изданиях, рекомендованных ВАК Министерства образования и науки Российской Федерации (специальность 2.3.6); 4 — опубликованы в тезисах докладов конференций, из которых 3 индексируются в международной системой научного цитирования Scopus, 1 индексируются системой научного цитирования РИНЦ; 3 являются свидетельствами о регистрации программы для ЭВМ (приравниваются к публикациям в изданиях, рекомендованных ВАК Министерства образования и науки Российской Федерации). Список работ представлен в заключительной части автореферата.

Личный вклад автора. Все результаты, представленные в диссертационной работе, получены автором единолично. В работах, написанных в соавторстве с научным руководителем, лично автору принадлежат: описание подхода к построению расширяемой классификации, соглашение об именовании классов и типов схем, перечисления типов классификации; применение подхода асимметричного выполнения для шифра Эль-Гамаля, анализ полученной схемы асимметричного выполнения, обоснование её стойкости, определение параметров схемы, оценка применимости схемы в протоколе PAKE.

Структура и объём работы

Диссертация состоит из введения, 4 глав, заключения, списка определений, обозначений и сокращений, списка литературы и 6 приложений. Текст изложен на 233 странице, исключая приложения, с 31 рисунком и 17 таблицами. Список литературы включает 213 наименований.

Основное содержание диссертации

Во введении показана актуальность темы диссертационной работы, сформулированы цели и задачи работы, показана научная новизна, теоретическая и практическая значимость, перечислены методы исследования, приведено краткое содержание работы по главам.

В первой главе дано определение схемы агрегированной электронной подписи, рассмотрены различные виды схем агрегированной электронной подписи. Представлен вывод о необходимости построения новой модели классификации схем электронной подписи для получения расширяемой классификации схем с целью добавления в неё новых типов, включая схемы агрегированной электронной подписи.

Представлена расширяемая фасетная классификация схем электронной подписи[3]; классифицированы новые схемы подписи, классификация которых в существующей классификации была невозможна; дана оценка общего числа классов схем электронной подписи; рассмотрены вопросы использования предлагаемой классификации схем электронной подписи для выделения и описания новых типов схем электронной подписи.

Рассмотрены возможные области применения схем агрегированной электронной подписи[4], такие как: протоколы защищённой маршрутизации, сенсорные сети, криптовалюты, быстрые подписи[5], подпись пакетов встраиваемого ПО, инфраструктура открытых ключей, защищённое журналирование[6]. Выделен набор характеристик основных элементов схем агрегированной подписи, значение которых может оказывать влияние на функционирование информационной системы в рамках рассмотренных приложений. Приведена качественная оценка критичности требований к элементам схем.

При использовании агрегированных подписей в указанных приложениях возможно получить такие преимущества, как снижение нагрузки на сеть, повышение производительности, уменьшение размера хранимой и передаваемой информации, повышение безопасности. Таким образом, актуальной является задача построения схем агрегированной электронной подписи, стойких к квантовым атакам.

---

[3] **Makarov A.** Extended Classification of Signature-only Signature Models / A. Makarov, A.A. Varfolomeev // 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – 2021. – P. 2385-2389.

[4] **Makarov A.** A Survey of Aggregate Signature Applications / A. Makarov // Advanced Technologies in Robotics and Intelligent Systems : Mechanisms and Machine Science. – Cham: Springer International Publishing, 2020. – P. 309-317.

[5] **Ozmen M.O.** Fast Authentication from Aggregate Signatures with Improved Security / M.O. Ozmen, R. Behnia, A. Yavuz. – 2019. – P. 686-705.

[6] **Hartung G.** Practical and Robust Secure Logging from Fault-Tolerant Sequential Aggregate Signatures / G. Hartung [et al.] // Provable Security / eds. T. Okamoto [et al.]. – Cham: Springer International Publishing, 2017. – P. 87-106.

Во второй главе рассмотрены способы построения схем последовательной агрегированной электронной подписи на основе многомерных квадратичных многочленов, а также вопросы теоретической и практической стойкости схем данного типа.

Описаны существующие способы построения схем последовательной агрегированной электронной подписи на основе односторонней подстановки с секретом. Кратко рассмотрены вопросы теоретической стойкости существующих постквантовых схем агрегированной электронной подписи MQSAS и MQUOV.

Представлен способ построения схем последовательной агрегированной электронной подписи SAS-**X** с использованием произвольной односторонней функции с секретом **X** на основе модифицированной схемы Лисянской[7]. В отличие от исходной схемы с односторонней подстановкой с секретом, предлагаемая схема может быть реализована с использованием односторонней функции с секретом.

Для описания формальной модели стойкости вводится определение схемы стойкой последовательной агрегированной подписи. Под оракулом, случайным оракулом, адаптивной атакой, эффективным алгоритмом, пренебрежимо малой величиной, игрой, экспериментом и преимуществом противника здесь и далее будем понимать соответствующие термины в игровой модели Белларе-Рогавея[8].

Обозначим $a||b$ — конкатенация векторов a и b, $\emptyset$ — пустая строка.

Определение (PPT-алгоритм). PPT-алгоритмом назовём вероятностный алгоритм, время выполнения $t \in \mathbb{R}_+$ которого для некоторого полиномиально ограниченного входа $i(\lambda) \in \mathbb{R}_+$ от параметра λ является полиномиально ограниченным, где $\mathbb{R}_+$ — множество действительных чисел, больших нуля. PPT-алгоритм назовём эффективным. В дальнейшем полагаем, что для всех PPT-алгоритмов, если явно не указано иное, время их выполнения равно t. Получение величины x как выхода PPT-алгоритма A, имеющего доступ к функции f, будем обозначать как $x \leftarrow_R A^f$.

Для всех определений стойкости в дальнейшем полагаем, что стойкость схем явно зависит от преимущества PPT-противника $\epsilon \in \mathbb{R}_+$ и времени выполнения его алгоритма $t \in \mathbb{R}_+$. Назовём такое понятие стойкости (t, ϵ)-стойкостью. Если величины t, ϵ явно зависят от некоторых параметров $p_1, .. p_k$, то схема называется $(t, p_1, \dots, p_k, \epsilon)$-стойкой, обозначая тем самым, что стойкость данной функции также явно зависит от этих параметров.

Определение ((t, ϵ)-стойкая односторонняя функция с секретом). Пусть X, Y — конечные множества. Пусть $(\boldsymbol{G}, \boldsymbol{F}, \boldsymbol{I})$ — тройка PPT-алгоритмов, таких что: $\boldsymbol{G}$ — вероятностный алгоритм такой, что на входе 1^k для некоторого параметра k он возвращает пару $(pk, sk) \leftarrow_R \boldsymbol{G}(1^k)$, при этом pk называют открытым ключом, sk — закрытым ключом (секретом односторонней функции с секретом); $\boldsymbol{F}$ — детерминированный алгоритм вычисления односторонней функции с секретом,

---

[7] **Lysyanskaya A.** Sequential Aggregate Signatures from Trapdoor Permutations / A. Lysyanskaya [et al.] // Advances in Cryptology - EUROCRYPT 2004 : Lecture Notes in Computer Science / eds. C. Cachin, J.L. Camenisch. – Berlin, Heidelberg: Springer, 2004. – P. 74-90.

[8] **Bellare M.** The Game-Playing Technique [Электронный ресурс]. – URL: https://cr.yp.to/bib/2004/bellare-games.pdf (дата обращения: 20.05.2023); **Bellare M.** Random oracles are practical: a paradigm for designing efficient protocols / M. Bellare, P. Rogaway // Proceedings of the 1st ACM conference on Computer and communications security - CCS '93 the 1st ACM conference. – Fairfax, Virginia, United States: ACM Press, 1993. – P. 62-73.

вычисляющий величину $y \leftarrow \boldsymbol{F}(pk, x)$; $\boldsymbol{I}$ — эффективный детерминированный алгоритм нахождения прообраза односторонней функции с секретом, вычисляющий величину $x \leftarrow \boldsymbol{I}(sk, y)$, $x \in X, y \in Y$; выполняется **свойство корректности**: для всех (pk, sk), полученных как выход $\boldsymbol{G}$, и для всех $x \in X$ справедливо $\boldsymbol{I}\big(sk, F(pk, x)\big) = x$. При фиксации открытого ключа pk алгоритм $\boldsymbol{F}(pk,*)$ определяет функцию $f: X \to Y$. При фиксации закрытого ключа sk алгоритм $\boldsymbol{I}(sk,*)$ определяет функцию $f^{-1} : Y \to X$ нахождения прообраза функции f.

Пусть A — PPT-алгоритм, преимущество в игре которого определяется величиной: $Adv_f^{ow-f}(A) = \Pr[f(x) = y, y \leftarrow_R Y, x \leftarrow_R A^f\ ]$. Тогда $(\boldsymbol{G}, \boldsymbol{F}, \boldsymbol{I})$ определяет (t, ϵ)-стойкую одностороннюю функцию с секретом f, если для всех PPT-противников с временем выполнения t величина $\epsilon = Adv_f^{\mathrm{ow-f}}(k)$ — пренебрежимо малая величина.

Аналогично вводится понятие односторонней подстановки с секретом.

Определение ($(\boldsymbol{t}, \boldsymbol{\epsilon})$-стойкая схема последовательной агрегированной электронной подписи). Схема последовательной агрегированной электронной подписи — тройка алгоритмов *Генерация ключей*, *Агрегированная подпись*, *Агрегированная проверка*: $SAS = (G, AggSign, AggVer)$. Алгоритм *Генерации ключей* G принимает на вход 1^k для некоторого параметра k и выдаёт ключевую пару (pk_i, sk_i). Алгоритм *Агрегированной подписи* $AggSign$ принимает на вход закрытый ключ sk_i, сообщение m_i, текущую агрегированную подпись σ_{i-1}, список пар «открытый ключ — сообщение» $\big((pk_1, m_1), \dots, (pk_{i-1}, m_{i-1})\big)$ и выдаёт новую агрегированную подпись σ_i. *Агрегированная проверка* $AggVer$ принимает на вход список пар «открытый ключ — сообщение» $\big((pk_1, m_1), \dots, (pk_i, m_i)\big)$, агрегированную подпись σ_i и выдаёт результат проверки из множества $\{0,1\}$. Проверка агрегированной подписи осуществляется путём восстановления значений σ_j для $0 \le j < i$ и проверки равенства $\sigma_0 =? 0^t$, $|\sigma_0| = t$.

Пусть A — PPT-алгоритм в игре против схемы последовательной агрегированной электронной подписи SAS. Эксперимент игры $\mathrm{Exp}_{SAS,A}^{\mathrm{sas-uf}}(k)$ состоит из трёх этапов:

инициализация: $(pk, sk) \leftarrow G(1^k)$;

атака: выполнение алгоритма $A^{AggSign(sk,*,*,*),pk}$;

подделка подписи: $\big((pk_1, m_1), \dots, (pk_i, m_i), \sigma\big) \leftarrow_R A$, выдаёт 1, если $AggVer\big((pk_1, m_1), \dots, (pk_i, m_i), \sigma\big) = 1$, $pk_{i^*} = pk$ для некоторого $1 \le i^* \le n$, A не делал запросов к оракулу подписи вида:

$$AggSign\Big(sk, m_{i^*}, \big((pk_1, m_1), \dots, (pk_{i^*-1}, m_{i^*-1})\big)\Big).$$

Преимущество противника A в игре против схемы последовательной агрегированной электронной подписи SAS есть величина:

$$\mathrm{Adv}_{SAS,A}^{\mathrm{sas-uf}}(k) = \Pr\big[\mathrm{Exp}_{SAS,A}^{\mathrm{sas-uf}}(k) = 1\big].$$

Схема SAS называется (t, ϵ)-стойкой, если для любого PPT-алгоритма противника A с временем выполнения t величина преимущества $\epsilon = \mathrm{Adv}_{SAS,A}^{\mathrm{sas-uf}}(k)$ есть пренебрежимо малая величина. Схема SAS называется оптимальной, если размер агрегированной подписи не растёт с ростом числа подписантов.

Предложен новый способ построения последовательной агрегированной подписи SAS-**X** на основе произвольной стойкой односторонней функции с секретом **X**, итерация формирования которой представлена на рисунке 1.

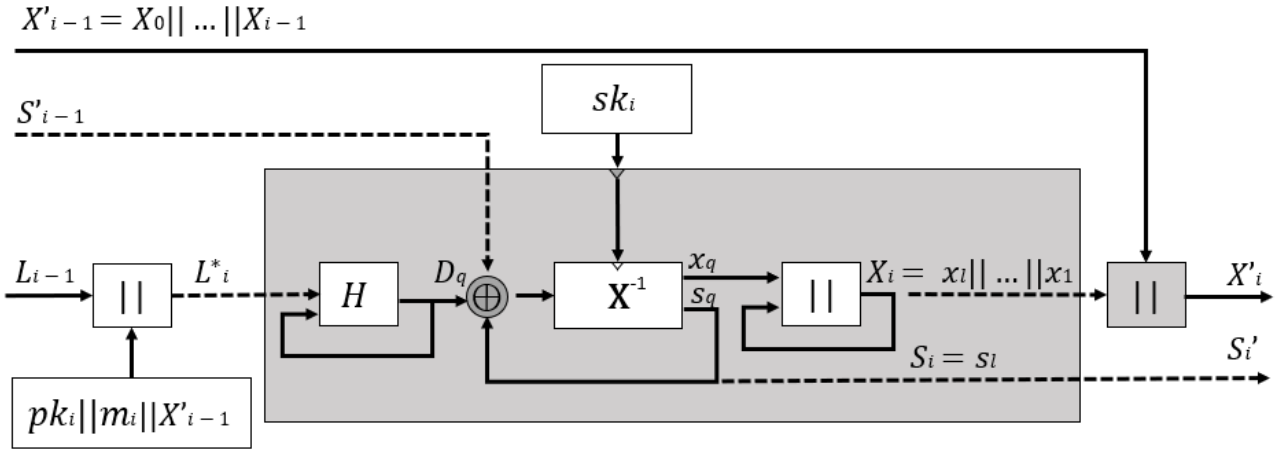


Рисунок 1 — Вычисление итерации агрегированной подписи схемы SAS-**X**, $\sigma_i = (S_i', X_i')$, H — вычисление случайного оракула, $D_q = H^l(L_i^*)$, (pk_i, sk_i) — ключевая пара i-го подписанта, l — параметр повторения, $q = 1..l$, $L_{i-1} = (pk_1, m_1, \ldots, pk_{i-1}, m_{i-1})$; пунктирными линиями обозначена однократная передача одного из значений в цикл или возврат последнего значения из цикла

Доказана теорема о стойкости представленной схемы в сведении к стойкости используемой односторонней функции с секретом **X**.

Теорема (Стойкость схемы SAS-X). Пусть **X**: $\{0,1\}^{z+x} \to \{0,1\}^z$ — (t', ϵ')-стойкая односторонняя функция с секретом, $z, x \in \mathbb{N}$. Тогда схема последовательной агрегированной подписи SAS-**X** с параметром $l \in \mathbb{N}$ с k подписантами является $(t, q_H, q_S, k, l, z, \epsilon)$-стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи для всех PPT-противников с временем работы не более t и преимуществом ϵ, делающих не более q_H запросов к случайному оракулу, не более q_S запросов к оракулу подписи:

$$\epsilon \leq (lq_S + lq_H + 1)\,\epsilon' + lk/2^z;$$
$$t \leq t'/l - 4kl(q_H + q_S).$$

В главе рассмотрены вопросы построения схемы последовательной агрегированной электронной подписи с ленивой проверкой, т.е. схемы, не требующей проверки текущей агрегированной подписи при добавлении подписи для нового сообщения очередным подписантом. Данное свойство позволяет увеличить производительность процедуры формирования подписи и снимает необходимость передачи открытых ключей другими подписантами в процессе формирования агрегированной подписи.

В качестве основы для построения схемы использовалась обобщённая схема Гентри[9], требующая применения идеального шифра π, с произвольным размером ключа и блока, и стойкой односторонней подстановки с секретом f_i.

Представлен способ построения схем последовательной агрегированной электронной подписи с ленивой проверкой LSAS-**X** на основе односторонней функции с секретом **X**. Предлагаемая схема изображена на рисунке 2. В отличие от схем, построенных на основе существующего способа Менегетти-Сигнорини, схемы на

[9] **Gentry C.** A Unified Framework for Trapdoor-Permutation-Based Sequential Aggregate Signatures / C. Gentry, A. O'Neill, L. Reyzin // Public-Key Cryptography – PKC 2018 : Lecture Notes in Computer Science / eds. M. Abdalla, R. Dahab. – Cham: Springer International Publishing, 2018. – P. 34-57.

основе LSAS-**X** обладают меньшим размером электронной подписи, а также более высокой производительностью.

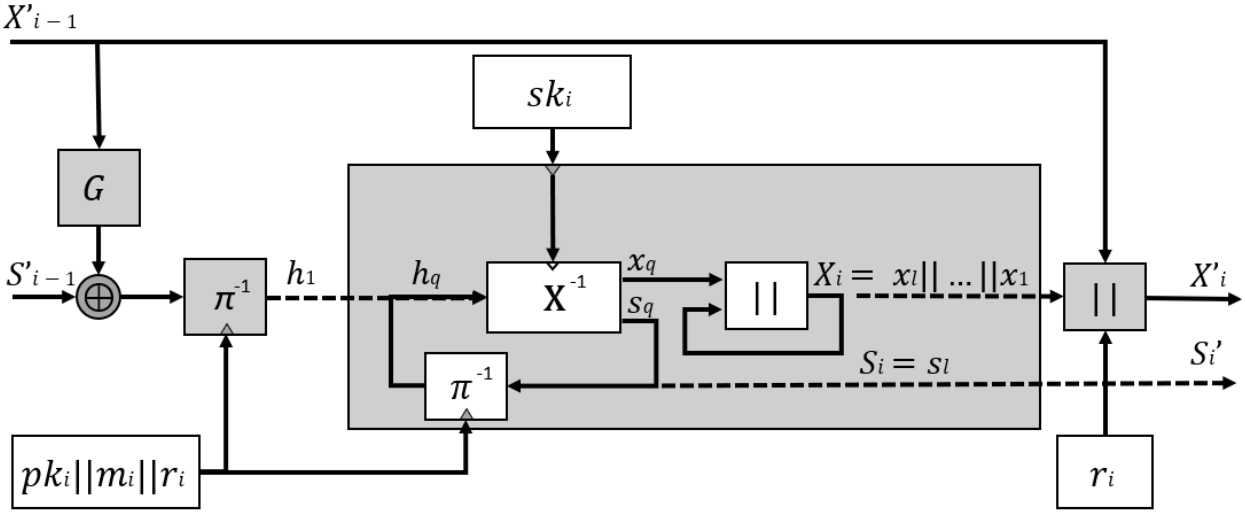


Рисунок 2 — Вычисление итерации агрегированной подписи схемы LSAS-**X**, $\sigma_i = (S_i', X_i')$, π^{-1} — вычисление расшифрования идеального шифра, (pk_i, sk_i) — ключевая пара i-го подписанта, $h_1 = \pi^{-1}_{pk_i||m_i||r_i}\left(S'_{i-1} \oplus G(X'_{i-1})\right), q = 1..l, l$ — параметр повторения; пунктирными линиями обозначена однократная передача одного из значений в цикл или возврат последнего значения из цикла

Алгоритм вычисления функции $G(X'_{i-1})$ с параметрами ρ, x, l представлен на рисунке 3, где запись $V[a..b]$ обозначает получение подвектора V' вектора V с координатами $a,..,b$, $V' = (V_a,..,V_b)$. Фактически функция G вычисляет значение случайного оракула H в точке X_{i-1}, где X_{i-1} — неагрегируемая часть подписи предыдущего подписанта в цепочке без учёта случайной величины r_{i-1}.

if $X'_{i-1} = \emptyset$
  return 0^x
end if
$X_{i-1} \leftarrow X'_{i-1}[\rho + 1..\rho + 1 + lx]$
return $H(X_{i-1})$

Рисунок 3 — Алгоритм вычисления функции $G(X'_{i-1})$ с использованием случайного оракула H, ρ — размер используемой случайной величины r_i в схеме LSAS-**X**, l — параметр повторения схемы LSAS-**X** с использованием односторонней функции с секретом **X**: $\{0,1\}^{z+x} \to \{0,1\}^z$

Теорема (Стойкость схемы LSAS-X). Пусть **X**: $\{0,1\}^{z+x} \to \{0,1\}^z$ —(t', ϵ')-стойкая односторонняя функция с секретом, $z, x \in \mathbb{N}$. Тогда при использовании **X** в *итеративной конструкции с использованием идеального шифра* с параметром $l \in \mathbb{N}$ как стойкой односторонней функции с секретом, схема последовательной агрегированной подписи LSAS-**X** является $(t, q_H, q_\pi, z, \rho, \epsilon)$-стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи для всех PPT-противников с временем работы не более t и преимуществом ϵ, делающих не более q_H запросов к случайному оракулу, не более q_π запросов к оракулу идеального шифра:

$$\epsilon \leq \frac{q_H 2^{z+\rho}}{(2^z - q_\pi^2)(2^\rho - q_H^2)}\,\epsilon' + (q_\pi^2 + z)/2^z;$$
$$t = t'/l$$

для всех t', ϵ', z, где z — размер агрегируемой части агрегированной подписи, $l, \rho \in \mathbb{N}$ — параметры схемы. Использование параметра $l \geq 2$ для ряда схем, имеющих малый размер подписи, позволяет обеспечить защиту от ряда практических атак, таких как атаки на нахождение коллизий.

Схема LSAS-**X** требует наличия идеального шифра, который на практике обычно реализуется с помощью стойкого блочного шифра[10]. Размер блока блочного шифра должен соответствовать размеру агрегируемой части подписи, размер ключа — суммарному размеру сообщения, открытого ключа и используемой случайной величины. Принимая во внимание возможный размер открытых ключей, составляющий для ряда схем величину порядка десятка килобайт, и размер агрегируемой части подписи, потенциально имеющей размер в десятки килобайт, получаем невозможность применения стандартных блочных шифров в качестве идеального шифра в предложенной схеме. Таким образом, нужно решить две задачи — получить идеальный шифр, который:

– имеет размер блока, соответствующий размеру агрегируемой части последовательной агрегированной подписи;

– имеет произвольно большой размер ключа.

Для достижения первой цели (произвольный размер блока) применён метод, описанный в схеме FNR[11]. Основная идея метода — использование сети Фейстеля N_E на основе блочного шифра E в качестве раундовой функции. Для достижения второй цели (произвольный размер ключа) можно использовать 8-раундовую сеть Фейстеля в модели случайного оракула[12]. Комбинируя оба подхода (используя 8-раундовую сеть Фейстеля вместо блочного шифра в схеме FNR на 8 раундов), получаем блочный шифр на основе хэш-функции в модели случайного оракула.

Альтернативный подход — использование непосредственно стойкого блочного шифра $E_b: K \times S \to S$, в модели идеального шифра, и хэш-функции $H: \{0,1\}^* \to K$ в модели случайного оракула для построения шифра $E(k, x) = E_b(H(k), x)$ с ключом $k \in \{0,1\}^*$ произвольной длины.

Представлены схемы SAS-UOV и LSAS-UOV на основе конструкций SAS-**X** и LSAS-**X** с использованием схемы UOV[13] в качестве односторонней функции с секретом при фиксации параметра повторения $l = 1$. Предложен набор параметров схем для достижения параметра стойкости 128-256 бит.

---

[10] **Black J.** The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function / J. Black // Fast Software Encryption / ed. M. Robshaw. – Berlin, Heidelberg: Springer, 2006. – The Ideal-Cipher Model, Revisited. – P. 328-340.

[11] **Dara S.** FNR: Arbitrary Length Small Domain Block Cipher Proposal / S. Dara, S.R. Fluhrer // SPACE. – 2014. – FNR.

[12] **Dai Y.** Indifferentiability of 8-round Feistel networks / Y. Dai, J. Steinberger // Annual International Cryptology Conference. – Springer, 2016. – P. 95-120.

[13] **Beullens W.** UOV: Unbalanced Oil and Vinegar. Algorithm Specifications and Supporting Documentation Version 1.0 [Электронный ресурс]. – URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/UOV-spec-web.pdf.

Выполнена программная реализация предлагаемых схем постквантовой последовательной агрегированной электронной подписи SAS-UOV и LSAS-UOV для процессоров архитектуры x86-64. Данные по производительности схем для сообщений размера 1024 байта представлены в таблице 1 для параметров (q, n, m) схемы OUV.

Схема RSA-SHA256-PSS (в реализации OpenSSL, для параметров, соответствующих параметрам стойкости 128-256 бит[14]) выбрана в качестве базовой схемы для сравнения, так как это наиболее распространённая схема электронной подписи, построенная на односторонней подстановке с секретом. Параметры стенда — процессор Intel Core i5-8300H, частота 2,30 ГГц.

Одним из вероятных приложений предложенных схем являются протоколы защищённой маршрутизации. Так, например, при использовании схемы SAS-UOV вместо схемы электронной подписи DSA в протоколе BGPsec, возможно сократить до трёх раз UPDATE-сообщения за счёт уменьшения размера подписей для стандартной длины пути в 6 узлов[15].

Таблица 1 — Производительность и параметры схем SAS-UOV, LSAS-UOV

Название схемы	Параметры <параметр стойкости, бит>	Размер открытого / закрытого ключа, байт	Размер индивидуальной подписи, бит	Рост размера подписи на одну итерацию, бит	Время на выполнение операции, мкс	
					подпись	проверка подписи
SAS-UOV	16,160,64 <128>	66 576 / 48	768	512	162	54
	256,184,72 <192>	189 232 / 48	1472	896	1 886	453
	256,244,96 <256>	446 992 / 48	1184	1312	3 635	657
LSAS-UOV	16,160,64 <128>	66 576 / 48	1024	672	185	76
	256,184,72 <192>	189 232 / 48	1600	1024	1 909	475
	256,244,96 <256>	446 992 / 48	2080	1312	3 659	680
RSA	3072 <128>	398 / 1769	3072	3072	1 558	42
	7680 <192>	974 / 4364	7680	7680	31 351	193
	15360 <256>	1948 / 8728	15 360	15 360	163 046	708

Другое возможное приложение — использование схемы в системах защищённого журналирования. Благодаря небольшим размерам подписи возможно

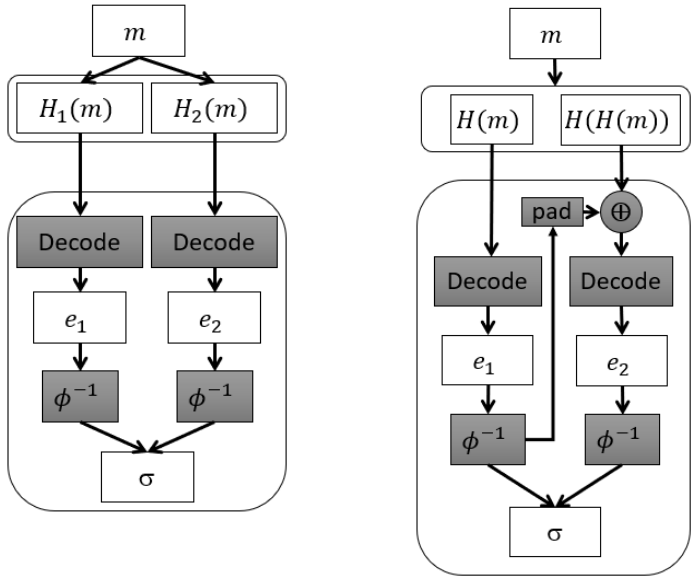
[14] **Barker E.** Recommendation for Key Management: Part 1 – General / E. Barker // National Institute of Standards and Technology. – 2020. – Recommendation for Key Management. – P. 54-55.

[15] BGP in 2018 — The BGP Table [Электронный ресурс]. – URL: https://blog.apnic.net/2019/01/16/bgp-in-2018-the-bgp-table/ (дата обращения: 19.02.2022).

значительно уменьшить размер хранимых данных, обеспечивающих целостность журналов. Учитывая высокое быстродействие процедур формирования и проверки подписи, применение данной схемы не окажет существенного влияния на функционирование системы журналирования.

Третья глава посвящена вопросу построения схем последовательной агрегированной подписи на основе теории алгебраического кодирования. Рассмотрена стойкость существующих схем электронной подписи на основе криптосистемы Нидеррайтера[16] с использованием кодов Гоппы[17].

Предложена схема электронной подписи RCFS, имеющая те же параметры, что и существующая схема электронной подписи Parallel-CFS, но более удобная для построения на её основе схемы последовательной агрегированной электронной подписи с ленивой проверкой в конструкции LSAS-**X**. Стойкость данной схемы эквивалентна стойкости схемы Parallel-CFS (в модели случайного оракула), параметр стойкости составляет 80 бит. Доказана её стойкость в сведении к стойкости односторонней функции криптосистемы Нидеррайтера. Схема RCFS в сравнении с исходной схемой Parallel-CFS представлена на рисунке 4.



(a) (b)

Рисунок 4 — Вычисление подписи Parallel-CFS (a) и RCFS (b) при $l = 2$, Decode — процедура декодирования синдрома кода Гоппы в ошибку e, ϕ — отображение криптосистемы Нидеррайтера вектора фиксированной длины в ошибку e длины n и веса Хэмминга не более чем t, pad — процедура дополнения вектора до размера входа функции Decode

Теорема (Стойкость схемы RCFS). Пусть Ni — (t', ϵ')-стойкая односторонняя функция с секретом. Тогда схема электронной подписи RCFS с параметром повторения $l \in \mathbb{N}$ является (t, l, ϵ)-стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу подписи, причём для всех t', ϵ':

---

[16] **Niederreiter H.** Knapsack-type cryptosystems and algebraic coding theory / H. Niederreiter // Prob. Contr. Inform. Theory. – Vol. 15. – № 2. – P. 157-166.

[17] **Гоппа В.Д.** Новый класс линейных корректирующих кодов / В.Д. Гоппа // Пробл. передачи информ. – 1970. – Т. 6. – № 3. – С. 24-30.

$$\epsilon \le \epsilon', t \le t'/l.$$

Односторонняя функция с секретом схемы Parallel-CFS может быть использована в схеме Лисянской для получения последовательной агрегированной подписи, образуя предлагаемую схему APCFS, представленную на рисунке 5. Схема использует l параллельных вычислений функции зашифрования NI^{-1} криптосистемы Нидеррайтера в качестве односторонней функции с секретом.

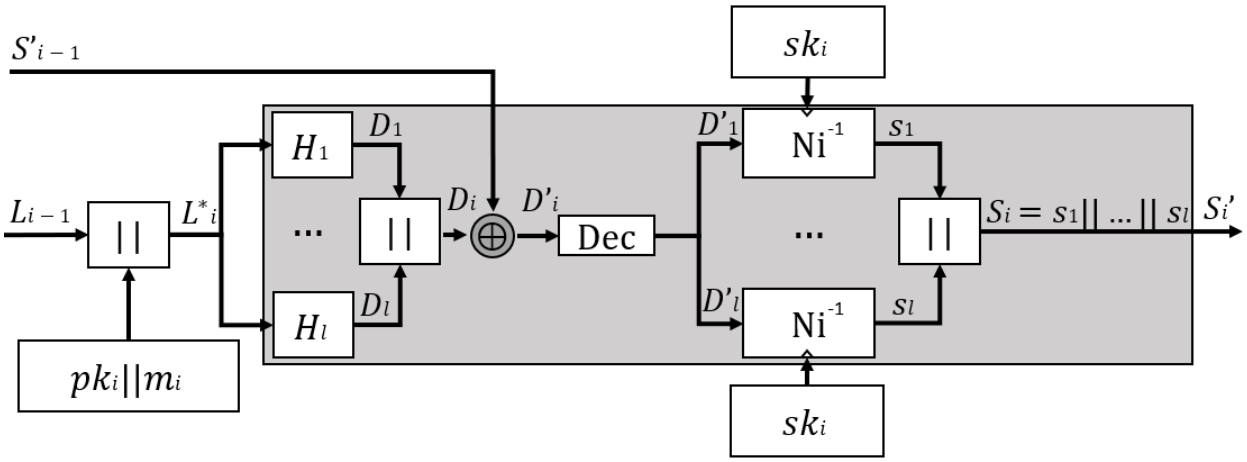


Рисунок 5 — Вычисление итерации агрегированной подписи схемы APCFS, l — параметр схемы, $\sigma_i = S_i'$, $H_1,..H_l$ — вычисление случайного оракула, $l = 1..n$, (pk_i, sk_i) — ключевая пара i-го подписанта, $L_{i-1} = (pk_1, m_1, \dots, pk_{i-1}, m_{i-1})$, Dec — процедура декомпозиции вектора $D'_i = (D'_1||..||D'_l)$ на подвекторы $D'_1, \dots, D'_l$

Предложена аналогичная схема ARCFS, использующая в качестве основы схему RCFS вместо Parallel-CFS, что фактически даёт схему в конструкции SAS-**X** на основе функции зашифрования NI^{-1} криптосистемы Нидеррайтера.

Показана стойкость предложенных схем.

Теорема (Стойкость схемы APCFS/ARCFS). Пусть Ni — (t', ϵ')-стойкая односторонняя функция с секретом. Тогда схема последовательной агрегированной электронной подписи APCFS с параметром $l \in \mathbb{N}$ с k подписантами является $(t, q_H, q_S, k, l, \epsilon)$-стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи для всех PPT-противников с временем работы не более t и преимуществом ϵ, делающих не более q_H запросов к случайному оракулу, не более q_S запросов к оракулу подписи:

$$\epsilon \le (q_S + q_H + 1)\,\epsilon';$$
$$t \le t'/l - (4kq_H + 4lkq_S + 7k + 1).$$

Рассмотрена возможность модификации постквантовой схемы агрегированной электронной подписи ARCFS с целью достижения ленивой проверки при использовании обобщённой схемы агрегации Гентри с применением конструкции LSAS-**X**, где в качестве односторонней подстановки с секретом применяется функция зашифрования криптосистемы Нидеррайтера. Показана стойкость данной схемы, получившей название LARCFS.

Теорема (Стойкость схемы LARCFS). Пусть Ni — (t', ϵ')-стойкая односторонняя функция с секретом. Тогда при использовании Ni в *итеративной конструкции с использованием идеального шифра* как стойкой односторонней функции с секретом, схема последовательной агрегированной электронной подписи LARCFS

является $(t, q_H, q_\pi, z, \rho, \epsilon)$-стойкой против противника в игре на создание новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи для всех PPT-противников с временем работы не более t и преимуществом ϵ, делающих не более q_H запросов к случайному оракулу, не более q_π запросов к оракулу идеального шифра:

$$\epsilon \leq \frac{q_H 2^{z+\rho}}{(2^z - q_\pi^2)(2^\rho - q_H^2)}\,\epsilon' + q_\pi^2/2^z;$$
$$t = t'/l$$

для всех t', ϵ', z, где z — размер агрегируемой части агрегированной подписи, $m, t, l \in \mathbb{N}$ — параметры схемы.

Так как схемы APCFS/ARCFS и LARCFS основаны на схеме Parallel-CFS, в качестве рекомендуемых параметров (включая параметр повторения) были выбраны параметры, предлагаемые авторами Parallel-CFS для защиты от существующих практических атак для соответствия параметру стойкости 80 бит.

Выполнена программная реализация предлагаемых схем постквантовой агрегированной электронной подписи APCFS/ARCFS и LARCFS для процессоров архитектуры x86-64. Данные по производительности схем для сообщений размера 1024 байта представлены в таблице 2 для параметров (m, t, δ, l), где (m, t, δ, l) — параметры схемы Parallel-CFS.

Параметры стенда — аналогичные использованным для измерения производительности схем на основе многомерных квадратичных многочленов SAS-UOV и LSAS-UOV. Схема RSA-SHA256-PSS (в реализации OpenSSL) выбрана в качестве базовой схемы для сравнения, при соответствии параметра стойкости в 80 бит[18]. Заметим, что схемы APCFS/ARCFS являются оптимальными.

Таблица 2 — Производительность и параметры схем APCFS/ARCFS и LARCFS

Название схемы	Параметры	Размер открытого ключа	Размер индивидуальной подписи, бит	Рост размера подписи на одну итерацию, бит	Время на выполнение операции, мс	
					подпись	проверка подписи
APCFS/ ARCFS	20,8,2,3	20 Мбайт	294	0	2 467	76
	18,9,2,3	5 Мбайт	288	0	8 921	120
	19,9,2,2	10,7 Мбайт	206	0	6 648	112
LARCFS	20,8,2,3	20 Мбайт	374	80	2 467	76
	18,9,2,3	5 Мбайт	368	80	8 921	120
	19,9,2,2	10,7 Мбайт	286	80	6 648	112
RSA	2048	270 байт	3072	2048	0,516	0,221

Для рассматриваемых параметров предлагаемые схемы обладают малым размером подписи, но большим размером открытых ключей и медленной процедурой

[18] **Barker E.** Recommendation for Key Management: Part 1 – General / E. Barker // National Institute of Standards and Technology. – 2020. – Recommendation for Key Management. – P. 54-55.

формирования подписи из-за необходимости полного декодирования синдромов, требующего порядка $t!$ операций.

Достижение параметра стойкости 128 бит при использовании кодов Гоппы требует значительного увеличения размера ключевых пар и количества операций (так как размеры ключей экспоненциально зависят от параметров схемы), что делает схемы на основе криптосистемы Нидеррайтера непригодными для практических нужд для данного параметра стойкости. Заметим, что в общем случае возможно построение криптосистемы Нидеррайтера на произвольных линейных кодах, для которых задача декодирования синдромов является вычислительно сложной, с целью достижения параметра стойкости 128 бит для практически значимых параметров схем. Однако такие коды изучены гораздо меньше (применительно к построению криптосистем), чем коды Гоппы и могут являться уязвимыми к практическим атакам.

Среди возможных приложений схем, с учётом некоторых ограничений, можно отметить блокчейн (если в качестве адресов используются хэш-значения, а не открытые ключи, а время подтверждения транзакции составляет десятки минут), а также системы защищённого журналирования и сенсорные сети (при отсутствии жёстких требований к производительности схем электронной подписи).

Четвёртая глава посвящена практической применимости схем последовательной агрегированной электронной подписи в системах защищённого журналирования.

Система журналирования в рассмотренной модели функционирует следующим образом — *служба* (произвольная информационная система), выполняя свои основные функции, формирует пакеты, содержащие записи аудита, которые она передаёт *серверу аудита* в произвольные интервалы времени. *Сервер аудита*, получая пакет записей, при необходимости проверяет его аутентичность и целостность и, в случае успеха данных операций, сохраняет его в своей базе данных. В ходе любого из описанных действий все стороны могут опционально обращаться к *доверенной третьей стороне*.

В рамках описания программной архитектуры представлены процедуры формирования, проверки целостности и удаления промежуточных значений пакетов записей аудита, а также рассмотрены возможные атаки. Предложены форматы хранимых данных, необходимых для проверки целостности пакетов записей аудита. Далее приведены процедуры формирования и проверки целостности пакета аудита, а также процедура удаления промежуточных записей. Прочие процедуры представлены в тексте диссертации.

Определение (Пакет аудита). *Пакет аудита* — упорядоченная по некому признаку последовательность событий аудита одной *службы*.

Определение (Эпоха). *Эпоха* — интервал времени, соответствующий появлению одного или нескольких событий аудита одной *службы.*

Определение (Метка эпохи). T — уникальный строковый идентификатор *эпохи*, называемый *меткой эпохи*.

Процедура формирования пакета событий аудита

Пусть (pk_s, sk_s) — ключевая пара схемы последовательной агрегированной электронной подписи $S = (Gen, AggSign, AggVer)$.

Процедура формирования *пакета* аудита выглядит следующим образом. Если *служба* имеет значение предыдущей *метки эпохи* T^*, то она самостоятельно получает следующую *метку эпохи* $T = T(T^*)$. Иначе — *служба* запрашивает значение последней *метки эпохи* у *сервера аудита*. Если *служба* не имеет предыдущего

значения агрегированной подписи σ^*, то она запрашивает её значение у *сервера аудита*, сообщая значение соответствующей *метки эпохи* T^*. Заметим, что данные запросы необходимо выполнять лишь единоразово при запуске *службы*.

Служба формирует идентификатор *пакета* аудита id_p^T и текущее значение агрегированной подписи σ^* для *метки эпохи* T и *пакета аудита*. При создании событий аудита $a_1, \dots, a_n$, упорядоченных по идентификатору событий id_{a_i}, они добавляются в *пакет аудита* с идентификатором id_p^T. Полученный *пакет* подписывается на стороне *службы* с использованием закрытого ключа sk_S схемы S и передаётся вместе с полученной подписью: $(id_p^T, T, a_1, \dots, a_n, \sigma)$. Подпись *пакета* σ вычисляется как $\sigma = AggSign(\sigma^*, sk_s, (T, a_1, \dots, a_n))$.

Процедура проверки целостности пакетов событий аудита

Для проверки цепочки *пакетов* аудита, начиная с *пакета*, следующего за *эпохой* с *меткой* T_n, до *пакета*, соответствующего *эпохе* с *меткой* T_k включительно, последовательно выполняются следующие действия:

1. получение идентификатора *пакета* id_{p_k} и подписи id_{s_k} для текущего *пакета*, соответствующего *эпохе* с *меткой* T_k, или для следующего доступного *пакета* с подписью, если подпись текущего *пакета* была удалена во время выполнения процедуры удаления промежуточных значений (в этом случае *метка эпохи* T_k принимается равной в дальнейшем *метке эпохи* первого доступного *пакета*);
2. получение значения исходной агрегированной подписи σ_k с идентификатором id_{s_k};
3. получение идентификатора предыдущего *пакета* id_{n-1} и подписи id_{n-1} для *эпохи* с *меткой* T_{n-1} или предыдущего доступного *пакета* с подписью, если подпись предыдущего *пакета* была удалена во время выполнения процедуры удаления промежуточных значений (в этом случае *метка эпохи* T_n принимается равной в дальнейшем *метке эпохи* первого доступного *пакета*);
4. получение значения конечной агрегированной σ_n подписи с идентификатором id_{s_n};
5. получение списка *пакетов аудита* d_{nk}, соответствующих *эпохам* с *метками* с T_n до T_k и упорядоченных по *меткам эпох*;
6. получение списка событий аудита la_i;
7. проверка агрегированной подписи σ_k для упорядоченных *пакетов аудита* и соответствующих упорядоченных событий $(\mathrm{d}ata)$, $s = AggVerify(data, \sigma_k)$, выполняется проверка полученного значения $s =? \sigma_k$.

Процедура удаления промежуточных подписей

Процедура удаления промежуточных подписей для *эпохи* с *меткой* T состоит в нахождении *пакета событий аудита* с идентификатором id_p, соответствующего данной *эпохе*, получении идентификатора подписи id_s, удалении записей о дополнительных сведениях (агрегируемой части) данной подписи, удалении идентификатора id_s из записи о *пакете событий* с идентификатором id_p.

Выполнение данной процедуры позволяет уменьшить размер хранимой информации, однако снижает гранулярность будущих проверок. Так, например, если были удалены все промежуточные подписи *пакетов аудита* начиная с *эпохи* с *меткой* T_1 и заканчивая *эпохой* с *меткой* T_2, при нарушении целостности аудита в событии *эпохи* с *меткой* T^*: $T_1 < T^* < T_2$ при проверке цепочки *пакетов аудита* невозможно определить конкретную *метку эпохи* T^*; таким образом, все события,

соответствующие *меткам эпох* $T_i: T_1 < T_i < T$, должны быть отброшены, так как их целостность скомпрометирована. Частота выполнения процедуры удаления промежуточных значений может являться динамически настраиваемым параметром *сервера аудита* в зависимости от необходимой гранулярности проверок целостности.

Для предлагаемой конструкции системы защищённого аудита рассмотрены особенности защиты от основных типов атак. Использование схем последовательной агрегированной электронной подписи в системах защищённого журналирования позволяет обеспечить целостность и последовательность цепочек пакетов записей, выявлять изменённые пакеты, а также уменьшать размер хранимой информации по сравнению с применением классических схем электронной подписи. Применение схем подписи с ленивой проверкой позволяет выполнять проверку подписей вне периодов высокой нагрузки на сервер аудита, не снижая уровень защищённости записей. Использование схем последовательной агрегированной электронной подписи в общем случае не защищает от атак на удаление последнего пакета аудита в цепочке, однако данные атаки могут быть нивелированы использованием цепочек хэш-значений или кодов аутентичности, вычисленных с использованием доверенной третьей стороны или защищённого аппаратного модуля.

Рассмотрена возможность применения предлагаемых схем последовательной агрегированной электронной подписи в системе защищённого аудита на примере программно-аппаратного комплекса «КриптоПро DSS»[19]. При штатном функционировании системы аудита число индивидуальных событий аудита, получаемых *сервером аудита* за год, составляет величину порядка 90 миллионов (порядка 250 тысяч событий в день). Максимальный размер *пакета аудита* по умолчанию не превышает 50 событий аудита. При этом данные *сервера аудита*, согласно регламенту, должны храниться не менее 10 лет, архивными считаются записи старше 3 месяцев.

При использовании схем последовательной агрегированной подписи частоту построения новых цепочек аудита предлагается принять равной одному месяцу; для событий аудита за последние 3 месяца (13 недель) хранится не более одного значения агрегируемой части агрегированной подписи на каждую неделю; для прочих событий аудита — не более одного значения агрегируемой части агрегированной подписи на каждые 4 недели.

При использовании агрегированных подписей схемы SAS-UOV (параметры 16, 160, 64) суммарный размер хранимых агрегированных электронных подписей составляет 0,29 Гбайта; при использовании схемы LSAS-UOV (параметры 16, 160, 64) — 0,57 Гбайта; при использовании схемы ARCFS (параметры 19,9,2,2) — 3,52 Кбайта; при использовании схемы LARCFS (параметры 19,9,2,2) — 0,05 Гбайта.

При использовании индивидуальных подписей схем-финалистов конкурса NIST по выбору постквантовых схем электронной подписи суммарный размер хранимых электронных подписей составляет: для схемы Falcon-128 — 1,41 Гбайта; для схемы CRYSTALS-DILITHIUM-128 — 5,14 Гбайта; для схемы SPHINCS+ (sha-256-s) — 16,68 Гбайта.

Динамика суммарного размера хранимых подписей сервером аудита в первые 54 недели для предлагаемых схем, а также для схем-финалистов конкурса NIST по выбору постквантовых схем электронной подписи представлена на рисунке 6.

[19] КриптоПро | КриптоПро DSS 2.0 [Электронный ресурс]. – URL: https://www.cryptopro.ru/products/dss (дата обращения: 28.06.2025).

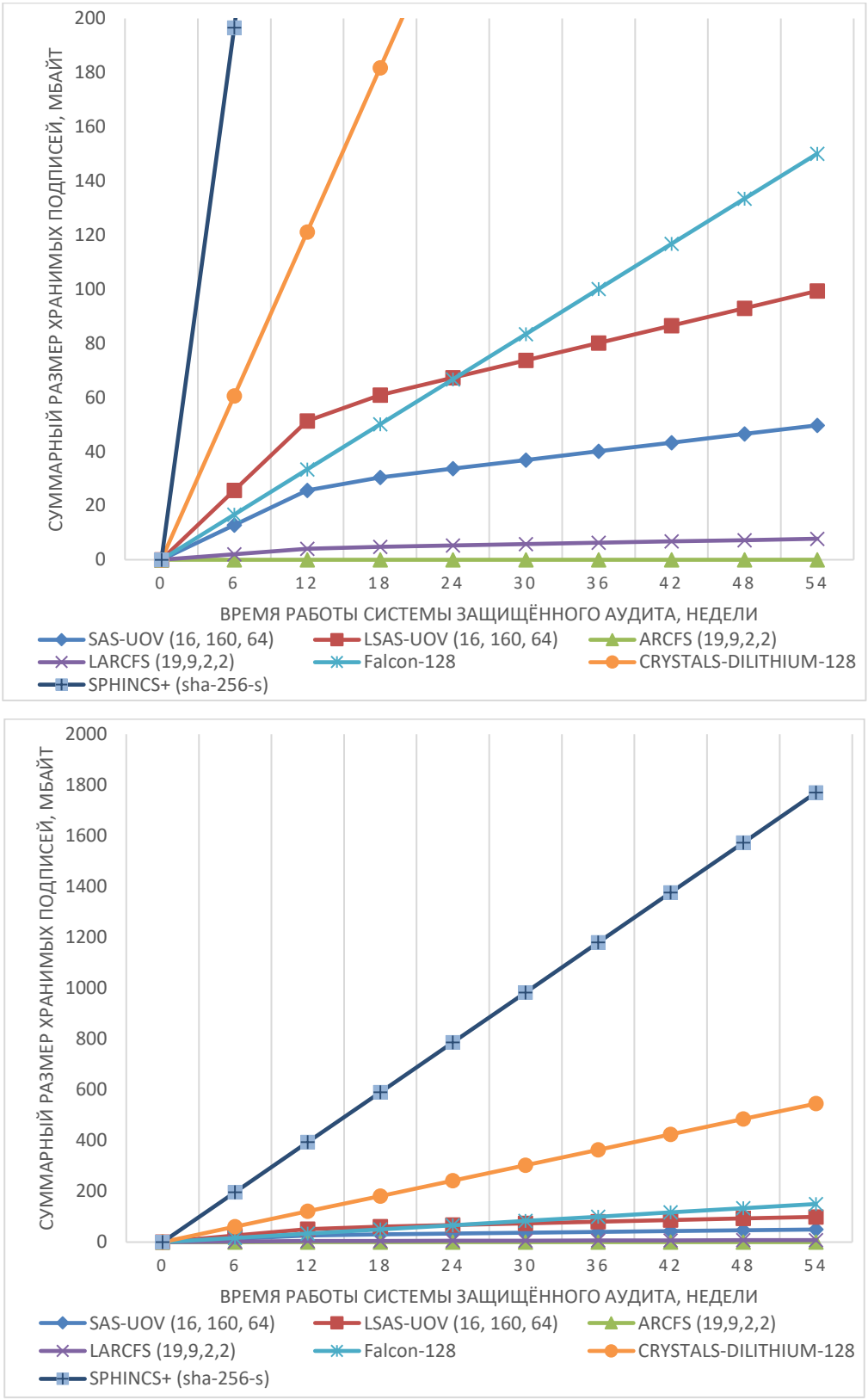


Рисунок 6 — Динамика суммарного размера хранимых подписей сервером аудита для схем SAS-UOV (16, 160, 64), LSAS-UOV (16, 160, 64), ARCFS (19,9,2,2), LARCFS (19,9,2,2), Falcon-128, CRYSTALS-DILITHIUM-128, SPHINCS+ (sha-256-s)

Как можно видеть из представленных данных, использование схем последовательной агрегированной электронной подписи позволяет существенно сократить размер хранимых электронных подписей при использовании в рамках описанной программной архитектуры. Отдельно отметим весьма малый суммарный размер подписей в схеме ARCFS (единицы килобайт), получаемый благодаря свойству оптимальности схемы.

Предложенная архитектура системы защищённого аудита может быть реализована в существующих системах журналирования, так как не требует изменения их структуры, форматов данных или процессов обработки записей журналов. Указанная конструкция может быть реализована с использованием как произвольных схем последовательной агрегированной электронной подписи, обеспечивающих явную зависимость текущей агрегированной подписи от предыдущей, так и с помощью классических схем электронной подписи с целью последующего перехода на схемы агрегированной электронной подписи

В заключении представлены результаты диссертационного исследования:

1. Выделен набор характеристик основных элементов схем агрегированной подписи, значение которых может оказывать влияние на функционирование информационной системы в рамках рассмотренных приложений. Приведена качественная оценка критичности требований к элементам схем.

2. Предложена новая каркасная модель построения классификации электронных схем электронной подписи на основе выделенных свойств. Использование предлагаемой каркасной модели позволяет получить легко расширяемую и удобную классификацию схем. После переноса исходной классификации Цао в новую каркасную модель существующая классификация была расширена добавлением 20 новых свойств, 7 семейств свойств и 1 типа. Предлагаемая классификация легко расширяется любыми свойствами или типами классов. Теоретически можно построить до 11 541 420 классов схем электронной подписи, что должно охватывать практически все существующие схемы. Расширенная классификация должна быть полезной как для классификации существующих схем электронной подписи, так и для предложения новых. Также полученная классификация может быть использована для выбора направлений модификации существующих схем электронной подписи.

3. Разработан новый способ построения схем последовательной агрегированной электронной подписи SAS-**X** на основе произвольной стойкой односторонней функции с секретом. Показана стойкость схемы SAS-**X** в сведении к стойкости используемой односторонней функции с секретом.

4. Разработан новый способ построения схем последовательной агрегированной подписи с ленивой проверкой LSAS-**X** на основе модифицированной конструкции Гентри, использующей идеальный шифр и стойкую одностороннюю функцию с секретом. Показана стойкость схемы LSAS-**X** в сведении к стойкости используемой односторонней функции с секретом.

5. Предложены схемы последовательной агрегированной электронной подписи SAS-UOV и LSAS-UOV, являющиеся реализациями схем SAS-**X** и LSAS-**X** с использованием односторонней функции с секретом схемы постквантовой электронной подписи на основе многомерных квадратичных многочленов UOV. Показана стойкость данных схем в сведении к стойкости односторонней функции с секретом схемы UOV. Представлен набор параметров схем для соответствия параметру стойкости 128-256 бит.

6. Предложена новая схема постквантовой электронной подписи на основе теории алгебраического кодирования RCFS, имеющая те же параметры, что и существующая схема электронной подписи Parallel-CFS, но более удобная для построения на её основе схемы последовательной агрегированной подписи с ленивой проверкой в схеме LSAS-**X**.

7. Предложена новая схема постквантовой последовательной агрегированной электронной подписи APCFS на основе схемы Parallel-CFS в рамках конструкции Лисянской; схема ARCFS на основе схемы RCFS в рамках конструкции SAS-**X**. Данные схемы являются оптимальными.

8. Предложена новая схема постквантовой последовательной агрегированной электронной подписи с ленивой проверкой LARCF на основе конструкции LSAS-**X** и схемы RCFS.

9. Проведён анализ схем RCFS, APCFS, ARCFS и LARCFS на основе теории алгебраического кодирования в сведении к стойкости функции зашифрования криптосистемы Нидеррайтера как односторонней функции с секретом. Предложен набор параметров схем для соответствия параметру стойкости 80 бит.

10. Рассмотрены вопросы программной реализации предложенных схем агрегированной электронной подписи SAS-UOV, LSAS-UOV, APCFS/ARCFS и LARCFS. Получены данные о производительности предлагаемых схем.

11. Предложена программная архитектура системы защищённого аудита, использующая схему последовательной агрегированной электронной подписи для обеспечения целостности журналов аудита. Описаны процедуры формирования, проверки целостности, удаления промежуточных значений пакетов записей аудита, а также возможные атаки. Предложены форматы хранимых данных для проверки целостности записей аудита. Произведена оценка применимости предлагаемых в рамках данной работы схем последовательной агрегированной электронной подписи в системе защищённого аудита. Использование схем последовательной агрегированной электронной подписи в системах защищённого журналирования позволяет обеспечить целостность и последовательность цепочек пакетов записей аудита, выявлять изменённые пакеты, а также уменьшать размер хранимой информации по сравнению с применением классических схем электронной подписи.

Публикации автора по теме диссертации

Статьи в рецензируемых журналах из Перечня ВАК:

Макаров А. Схема Постквантовой Агрегированной Подписи С Ленивой Проверкой На Основе Многомерных Квадратичных Многочленов / А.О. Макаров // Безопасность Информационных Технологий. – 2023. – Т. 30. – № 3. – С. 30-50. (**ВАК**, К2, специальность 2.3.6)

Макаров А. Схема пост-квантовой агрегированной подписи на основе теории алгебраического кодирования / А. Макаров // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 69-76. (**ВАК**, К,1 специальность 2.3.6)

Печатные работы в сборниках трудов международных и всероссийских конференций:

Makarov A. Extended Classification of Signature-only Signature Models / A. Makarov, A.A. Varfolomeev // 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – 2021. – P. 2385-2389. (**Scopus**)

Varfolomeev A.A. About Asymmetric Execution of the Asymmetric ElGamal Cipher / A.A. Varfolomeev, **A. Makarov** // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – St. Petersburg and Moscow, Russia: IEEE, 2020. – P. 2106-2109. (**Scopus**)

Makarov A. A Survey of Aggregate Signature Applications / A. Makarov // Advanced Technologies in Robotics and Intelligent Systems: Mechanisms and Machine Science. – Cham: Springer International Publishing, 2020. – P. 309-317 (**Scopus**)

Макаров А. Схема постквантовой агрегированной подписи на основе теории алгебраического кодирования // Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции / под. ред. М.А.Басараба – М.: МГТУ им. Н.Э.Баумана, 2018. – С. 124-128. (**РИНЦ**)

Свидетельства о регистрации программы для ЭВМ:

Свидетельство № 2025680777 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ «AggreLink Audit» / **А.О. Макаров**. – Заявка № 2025667882 от 15.07.2025; дата гос. регистрации в Реестре 08.08.2025. – Реестр программ для ЭВМ. – 1 с.

Свидетельство № 2023667179 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ «Libuov» / **А.О. Макаров**. – Заявка № 2023666172 от 01.08.2023; дата гос. регистрации в Реестре 10.08.2023. – Реестр программ для ЭВМ. – 1 с.

Свидетельство № 2018613440 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ «ПО "ПАК "КриптоПро DSS" версии 2.0" ("КриптоПро DSS 2.0")» / Горлатых А.В., Смирнов П.В., Усанова Т.И., Хоменко М.В., Корнев Д.К., **Макаров А.О.**, Садофьев Г.А. – Заявка № 2018610515 от 19.01.2018; дата гос. регистрации в Реестре 14.01.2018. – Реестр программ для ЭВМ. – 1 с.