МИНИСТЕРСТВО ОБРАЗОВАНИЯ И ИССЛЕДОВАНИЙ РЕСПУБЛИКИ МОЛДОВА

ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ МОЛДОВЫ

ДЕПАРТАМЕНТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И АВТОМАТИКИ

На правах рукописи

C.Z.U.: 004.056.53/512.54

КУНЕВ ВЯЧЕСЛАВ

СОВРЕМЕННЫЕ ИНТЕРОПЕРАБЕЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ НА ОСНОВЕ АЛГОРИТМОВ ФОРМАНТНОГО АНАЛИЗА

232.02 – ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОДУКТЫ И СИСТЕМЫ

Диссертация на соискание ученой степени доктор информатики

Научный руководитель: Бешлиу Виктор

профессор, доктор

Автор: Кунев Вячеслав

CHIŞINĂU, 2023

**MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
AL REPUBLICII MOLDOVA**

UNIVERSITATEA TEHNICĂ A MOLDOVEI

DEPARTAMENTUL INGINERIA SOFTWARE ȘI AUTOMATICĂ

Cu titlu de manuscris

C.Z.U.: 004.056.53/512.54

CUNEV VEACESLAV

TEHNOLOGII INFORMAȚIONALE INTEROPERABILE MODERNE ÎN SISTEMELE DE PLATĂ ELECTRONICE PROTEJATE, BAZATE PE ALGORITMI DE ANALIZĂ A FORMANȚILOR

232.02 –TEHNOLOGII, PRODUSE ŞI SISTEME INFORMAŢIONALE

Teză de doctor în informatică

Conducător ştiinţific: Beșliu Victor

prof. univ., dr.

Autorul: Cunev Veaceslav

CHIŞINĂU, 2023

© КУНЕВ ВЯЧЕСЛАВ, 2023

Содержание

Аннотация

Диссертации на соискание учёной степени доктор в информатике, с темой «Современные интероперабельные информационные технологии в защищенных электронных платежных системах на основе алгоритмов формантного анализа», Кишинёв 2023, автор: КУНЕВ Вячеслав

Структура работы. Диссертация состоит из введения, четырёх глав, выводов, библиографии из 162 наименований, 110 страниц основного текста, включая 25 рисунков. Полученные результаты опубликованы в 5-ти – и научных работах, 1-й – книги, 1-ом – патенте, 1-й – заявки на патент.

Ключевые слова: интероперабельность систем, информационная безопасность, криптография, криптостойкость систем, алгоритмы формантного анализа.

Область исследования включает в себя теоретические и практические аспекты защиты данных, основные идеи организации, построения и использования криптографических средств в интероперабельных информационных систем.

Цель и задачи работы состоят в разработке методов и алгоритмов защиты информации в интероперабельных платежных системах, с повышенным уровнем крипто защищённости, на основе методов формантного анализа и современной теории чисел.

Научная новизна и оригинальность полученных результатов заключается в предложении модернизированных RSA-алгоритмов на основе формантной алгебры и строковой арифметики сопоставительного и формантного анализа, обеспечивающих заданную временную криптостойкость системы в режиме реального времени, и в предложении способа контролируемого повышения вычислительной сложности криптоалгоритма RSA.

Теоретическое значение заключается в разработке и развитие оригинальных методов и алгоритмов на основе формантного анализа для обеспечения безопасности интероперабельных платежных систем, которые могут быть успешно использованы для защиты данных в режиме реального времени.

Практическая ценность работы заключается в предлагаемой модернизации известных крипто-алгоритмов, позволивших заменить передаваемую информацию защищёнными косвенными данными о ней. Разработанные алгоритмы криптозащиты позволяют наращивать криптостойкость и сложность существующих криптоалгоритмов без существенных затрат на модернизацию уже существующих информационных систем.

Научные результаты работы были запатентованы, а разработанные алгоритмы были приняты для тестирования в составе собственных продуктов компаниями: S.R.L. КВАЗАР-МИКРО S.R.L., QSystems S.R.L., генеральный директор Alfasoft S.R.L.

Adnotare

la teza de doctor în informatică cu tema „Tehnologii informaționale interoperabile moderne în sistemele de plată electronice protejate, bazate pe algoritmi de analiză a formanților", Chişinău, 2023
autor: CUNEV Veaceslav

Structura tezei. Teza de doctor cuprinde introducerea, patru capitole, concluzii, bibliografia cu 162 titluri, 110 pagini text de bază, inclusiv 25 figuri. Rezultatele obţinute sunt publicate în 5 – lucrări ştiinţifice, 1 – carte, 1 – brevet de invenție, 1 – cerere de înregistrare a brevetului.

Cuvinte cheie: interoperabilitatea sistemelor, securitatea informațională, criptografie, crypto-stabilitate a sistemelor, algoritmii de analiza formantă.

Domeniul de studiu îl constituie aspectele teoretice şi practice de asigurare a securității datelor, ideile de bază ale organizării, formării și utilizării instrumentelor criptografice în sistemele informaționale interoperabile.

Scopul şi obiectivele lucrării constau în dezvoltarea metodelor și algoritmilor de protecție a datelor pentru sistemele interoperabile cu un nivel ridicat de securitate criptografică, pe baza metodelor de analiza formantă și a teoriei numerelor.

Noutatea şi originalitatea ştiinţifică a rezultatelor obţinute constă în propunerea algoritmilor modernizați-RSA pe baza algebrei formante și a aritmeticii de șiruri a analizei comparative şi formante, cu asigurarea stabilității criptografice temporale prestabilite a sistemului în timp real și propunerea unei noi metode de creștere controlabilă a complexității de calcul a algoritmilor de criptare.

Semnificaţia teoretică a lucrării constă în propunerea și dezvoltarea unor metode și algoritmi de protecție a datelor bazate pe analiza formantă, care pot fi utilizate cu succes pentru asigurarea securității datelor în timp real în sisteme interoperabile.

Valoarea aplicativă a lucrării constă în modernizarea unor algoritmi criptografici cunoscuți de criptare/decriptare, prin înlocuirea informației inițiale cu date protejate indirecte. Algoritmii criptografici dezvoltați permit creșterea nivelului de stabilitate criptografică și a complexității algoritmilor criptografici, fără costuri semnificative de modernizare a sistemelor informatice existente.

Implementarea rezultatelor ştiinţifice: rezultatele științifice ale cercetării au fost brevetate, iar algoritmii dezvoltați au fost acceptați pentru testare ca parte a produselor proprii de companii: KVAZAR-MICRO S.R.L., Qsystems S.R.L., Alfasoft S.R.L.

Annotation

Of the Ph.D. Thesis in Informatics with title „ Modern interoperable information technologies in the secure electronic payment systems, based on the formant analysis algorithms", Chisinau, 2023
author: CUNEV Veaceslav

Thesis structure. The Ph.D. thesis consists of the Introduction, four Chapters, Conclusions, Bibliography (162 titles), 110 pages of main text, 25 figures. The obtained results have been published in 5 – scientific articles, 1 – book, 1 – patent, 1 – patent application.

Key words: interoperability of the systems, information security, cryptography, cryptographic stability of systems, formant analysis algorithms.

The field of research encompasses theoretical and practical aspects of data protection, the main ideas of organization, design and use of cryptographic tools in the interoperable information systems.

The research objectives focus on the development of methods and algorithms for information protection within interoperable systems with high level of cryptosecurity, based on the methods of formant analysis algorithms and modern number theory.

Scientific novelty and originality of the obtained results consists in proposing the modernized RSA – algorithms, which are based on formant algebra and string arithmetic of comparative and formant analysis, which provide a given temporary cryptographic stability of the system in real time and in proposing the method for controlled increase the computational complexity of crypto algorithms.

Theoretical value of the thesis consists in elaborating methods and algorithms for cipher/decipher data based on formant analysis, that ensure the security of interoperable systems in real time.

Practical value of the thesis consists in the procedure modernization of well-known crypto-algorithms, which made possible to replace the transmitted information with protected indirect data about it. The developed cryptographic protection algorithms allow to increase the cryptographic stability and complexity of existing crypto algorithms without significant costs for the modernization of the existing information systems

Implementation of the scientific results: the scientific results of the work were patented and the developed algorithms were accepted for testing as a part of products developed by the companies: KVAZAR-MICRO S.R.L., QSystems S.R.L., Alfasoft S.R.L.

Список сокращений

API – программный интерфейс приложения

BS – Британский стандарт

DSA – Digital Signature Algorithm

GDR - общий регламент защиты персональных данных (General Data Protection Regulation)

ECC – Elliptic Curve Cryptography

EDI - Electronic Data Interchange

EGSA – El-Gamal Signature Algorithm

ICE – Information and Content Exchange Protocol

IoT – интернет вещей

ITSEC – Information Technology Security Evaluation Criteria

OASIS – Organization for the Advancement of Structured Information Standards

OBI – Open Buying on the Internet

OTP – Open Trading Protocol

RSA – Rivest-Shamir-Adleman

SET – Secure Electronic Transactions

SOAP – Simple Object Access Protocol

SSL – Secure Socket Layer

SWIFT - общество всемирных межбанковских финансовых каналов связи

АЦП – аналого-цифровой преобразователь

БСИ – блок генерирования и обработки служебной информации

ВУ – вычислительное устройство

ИС – информационные системы

ИТ – информационные технологии

МК – микроконтроллер

ПЗУ – постоянное запоминающее устройство

ПС - платежные системы

ПО – программное обеспечение

ФА – формантный анализ

ЭВМ – электронно-вычислительные системы

ВВЕДЕНИЕ

Актуальность и значение темы диссертации. Все существующие финансовые и платежные системы (ПС) выросли из многообразия бумажных систем, при этом для каждой страны мира особенности учета финансовых операций различались. На данный момент, не смотря на значительную унификацию подобных систем, все еще сохраняется значительная разница в построении и бизнес-логике таких систем в разных странах мира. При этом, несмотря на то, что платежные системы вынуждены взаимодействовать друг с другом для осуществления финансовых транзакций, соответствующие интерфейсы взаимодействия уникальны для каждой индивидуальной системы, и поэтому процесс интеграции всегда сложен и трудоемок, в процессе последующей эксплуатации обязательно возникают вопросы как бесперебойной работы в частности, так и безопасности финансовых транзакций, в целом [42]. Именно поэтому стоимость платежных сервисов до сих пор аномально высока и для некоторых сумм финансовых транзакций комиссион за платеж может быть сопоставим с суммой самого платежа.

Под термином «интероперабельность» в контексте платежных систем следует понимать функциональную и информационную совместимость платежных систем — это способность большого количества платежных систем, интерфейсы которых полностью открыты, взаимодействовать и функционировать с друг с другом без каких-либо ограничений доступа и реализации, включая обмен и использование информации о транзакциях, полученной в результате обмена. Иными словами, платежные системы должны действовать по принципу «платежного интернета» - как набор независимых систем, которые используют стандартизированный набор правил, процедур, протоколов [57, 64, 101, 105, 106, 137].

Для обеспечения интероперабельности и необходимого уровня защищенности ПС систем должны обеспечиваться следующие важные свойства системы:

- Гарантирование свойства целостности и неотрекаемости транзакций через механизм цифровой подписи.
- Неотрекаемость любого действия в системе как как пользователя системы, так и ее администратора должна быть гарантирована.
- Уникальность цифрового идентификатора для каждого пользователя или администратора.

- Информационная инфраструктура не должна иметь единой точки отказа – это касается как серверного оборудования, так и информационной системы. По сути, речь идет о децентрализованном классе систем.
- Свойства неотрекаемости, целостности и гарантированности финансовых транзакций и их условий должно основываться на математических принципах, а не на доверии участников сделки друг к другу или посреднику.
- Транзакции между отдельными ПС атомарны, - что означает, что если хотя бы одна операция в транзакции не может быть выполнена, вся транзакция отклоняется.

В интероперабельных ПС должны быть децентрализованы, как минимум, следующие процессы:

- подтверждение целостности транзакций;
- верификация транзакций;
- хранение данных;
- аудит системы (автоматический криптографический аудит);
- принятие решений по ее обновлению.

Необходимость обеспечения информационной безопасности ПС исходит из требования предоставление сохранности и целостности транзакций, достоверности, надежности и секретности хранимой или передаваемой информации, независимо от случайных и умышленных деструктивных воздействий пользователей, или неисправности аппаратуры [107]. Трудоемкости решения этой задачи способствует: факт того, что информация не является жестко связанной с носителем и может легко и быстро копироваться и передаваться по каналам связи [26]; экспоненциальное увеличение объемов - накапливаемой, хранимой и обрабатываемой информации; концентрация в единых вычислительных узлах большого объёма информации различного назначения и принадлежности; увеличения круга пользователей, имеющих доступ к определённым данным, без определения точных уровней доступа; увеличение количества технических средств и коммуникационных связей; распространение сетевых технологий и объединение локальных сетей в глобальные.

Соответственно, обеспечение информационной безопасности представляет собой комплекс действий, который достигается сочетанием ряда методов, а именно: организационных, технических, программных и криптологических [37].

Организационные методы защиты информации предусматривают использование должностных инструкций, регламентаций производственной деятельности и

взаимоотношений сотрудников, регламентаций относительно организационных принципов хранения информации.

Программные методы защиты информации включают в себя программы для идентификации пользователей, обеспечивая дифференцированный доступ к ЭВМ; программы для шифрования информации, удаления временной информации, тестового контроля системы защиты и др. Данные программные средства обладают универсальностью, надежностью, простотой установки, способностью к расширению. Но, как недостаток подчеркивается факт, что незначительная ошибка может вызвать изменения, сводящие на нет всю эффективность защиты системы и принимая во внимание организационные принципы хранения информации, высококвалифицированные специалисты могут получить доступ к любым данным, которые являются не защищенными специальными аппаратными средствами. По этой причине используются криптографические средства, которые обеспечивают защиту данных.

Значение криптографии выходит далеко за рамки обеспечения секретности данных, она используется в таких областях как аутентификация пользователей [38], подтверждения транзакций, смарт-контракты, контроль целостности информации, проверка подлинности цифровых документов, электронная коммерция (e-commerce) [48, 138, 139, 142], реализация технологий blockchain [157, 160-161].

Криптография характеризуется многовековой историей развития и применения, и следует выделить 3 периода развития: период донаучной криптографии (до середины XX века); период классической криптографии (с секретным ключом), где началу этому периоду послужила работа К. Шеннона которая стала основой для развития одно-ключевых симметричных криптосистем [63]; период современной криптографии (с открытым ключом), началу этому периоду положила работа У. Диффи и М. Хэллмана, где было показано, что секретность передачи информации может обеспечивается без обмена секретными ключами [71].

Для современных криптографических систем основной характеристикой криптостойкости является длина ключа, соответственно для симметричных алгоритмов (DES, AES, CAST5, IDEA, Blowfish, Twofish) использования шифрования с ключами длиной 128 бит и выше считается сильным, а для асимметричных алгоритмов (RSA), основанных на проблемах теории чисел, минимальная надёжная длина ключа в настоящее время является 2048 бит (рекомендация RSA Security), и для алгоритмов основанных на использовании теории эллиптических кривых (ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002), минимальной надёжной длиной ключа считается 256 бит [15, 16, 27, 56, 127].

На данный момент криптография является неотъемлемой частью платежных систем и для достижения интероперабельности платежных систем и необходимой безопасности необходимо использовать такие средства криптографии, которые совместимы, масштабируемы с точки зрения криптостойкости и обладают высокой скоростью работы [80, 114, 117, 149, 151, 153]. Исходя из этого, одной из современных тенденций в криптографии является разработка новых методов, обеспечивающих информационную безопасность и криптостойкость, с использованием методов сопоставительного анализа. Метод сопоставительного анализа является разделом теории чисел, позволяющий расширить ее возможности, а именно для криптосистемы RSA [8]. Высокая, практически желаемая, стойкость этой криптосистемы основана на использовании трудностей определения обратных односторонних функций, в частности, при решении задачи факторизации большого составного числа. Решение этой задачи требует реально очень большого времени, не сопоставимого с существующими на сегодняшний день возможностями вычислительных ресурсов самой быстродействующей компьютерной техники.

Однако, реализация криптосистемы RSA весьма медленна для работы в реальном времени, что ограничивает ее использование для защиты в реальном времени информации, циркулирующей в линиях различных коммуникационных и информационно-управляющих систем.

В данной диссертационной работе предлагается технология шифрования данных, основанная не на передаче самой информации, а на отправке косвенных данных об этой информации в режиме реального времени, с требуемой криптостойкостью криптографической системы и без задержки во времени.

Суть предложенной процедуры заключается в использовании числовых формант, с помощью которых любое число может быть представлено в виде простейшей линейной структуры. При этом время выполнения операций разложения чисел при шифровании и восстановлении форманты, при дешифровании будет значительно ниже, чем время, затрачиваемое на прямое использование алгоритмов классической криптосистемы RSA.

Область исследования включает в себя теоретические и практические аспекты защиты данных, основные идеи организации, построения и использования криптографических средств в интероперабельных системах, в условиях перспективы угрозы квантового превосходства, а также зависимость от имеющихся у нарушителей технических устройств.

Объектом исследования являются технологии, в основе которых лежат модели, методы и алгоритмы шифрования/дешифрования данных на базе формантного анализа в контексте применения их для использования в интероперабельных платежных системах и проверке работоспособности данных алгоритмов в режиме реального времени в рамках существенных временных ограничений на базе внедрения в систему защиты голосовой связи.

Цель и задачи исследования. Цель диссертационной работы состоит в исследовании и разработки методов и алгоритмов защиты данных в интероперабельных платежных системах в условиях как кратного роста числа транзакций, так угрозы квантового превосходства.

Из поставленной цели следуют следующие задачи:

1. Анализ архитектур интероперабельных платежных систем и методов обеспечения защиты данных в режиме реального времени.
2. Выявление обязательных свойств и процессов интероперабельных платежных систем, необходимых для обеспечения свойств интероперабельности.
3. Для обеспечения интероперабельности платежных систем и необходимого уровня безопасности, разработка, на основе методов формантного анализа и современной теории чисел, эффективных алгоритмов RSA-mAB (AB1, AB2, AB3) криптографической защиты, обеспечивающих заданную временную криптостойкость систем в режиме реального времени.
4. Разработка алгоритма контролируемого повышения вычислительной сложности криптоалгоритмов, без уменьшения общей производительности и пропускной способности системы.
5. Разработка расширенного алгоритма RSA-mAB шифрование/дешифрование в зависимости от варьируемых параметров алгоритма, который обеспечивает высокую надёжность RSA с малой длиной ключа.
6. Для проверки эффективности разработанных алгоритмов RSA-mAB, предлагается спроектировать систему защиты голосовой связи, где зашифрованные голосовые сообщения передаются в режиме реального времени со скоростью передачи примерно в 64 kb/сек. Это позволит проверить эффективность работы алгоритмов в режиме реального времени в системах, где скорость обработки данных кратно больше, чем в платёжных системах.

Гипотеза исследования. Достижение квантового превосходства может обнулить все текущие результаты в классических системах криптографии и, соответственно, необходимость замены текущей криптографии на что-то принципиально другое приведет к колоссальным издержкам, таким образом, необходимо принципиально усилить существующие криптосистемы, не меняя их принципов работы.

Соответственно, относительно низкая скорость работы криптосистемы RSA, но её высокая криптографическая стойкость заставляют разработчиков искать пути доработки этой системы в условиях возможного квантового превосходства.

Методологическая основа диссертации. При решении поставленных в работе задач использовались методы формантного и сопоставительного анализа теории чисел, объектного проектирования, методы теории множеств, теории графов, теории уточнения спецификаций.

Методологическое обеспечение исследования базируется на теории систем, математическом анализе, теории алгоритмов, методах математического моделирования и объектно-ориентированных технологиях.

Новизна и оригинальность диссертации. Научная новизна и теоретическая значимость полученных результатов заключается в предложении модернизированных RSA-алгоритмов на основе формантной алгебры и строковой арифметики сопоставительного и формантного анализа, что позволяет использовать такой подход для защиты современных платежных информационных систем.

Оригинальность предлагаемых решений состоит в предложении использования формантного анализа в криптографии, а именно для реализации алгоритмов шифрования/дешифрования, обеспечивающих заданную временную криптостойкость системы в режиме реального времени и в предложении способа контролируемого повышения вычислительной сложности криптоалгоритмов, без уменьшения общей производительности и пропускной способности системы.

Решенная научная задача заключается в разработке алгоритмов защиты данных на базе формантной алгебры и строковой арифметики сопоставительного и формантного анализа, обеспечивающих возможность контролируемого повышения вычислительной сложности криптоалгоритмов.

Теоретическая значимость диссертации заключается в разработке и развитии оригинальных методов и алгоритмов на основе формантного анализа для обеспечения безопасности интероперабельных платежных систем, которые могут быть успешно

использованы для защиты данных в режиме реального времени, что особенно важно для постквантовой криптографии**.**

Практическая значимость работы заключается в предлагаемой модернизации известных криптоалгоритмов, позволивших заменить передаваемую информацию защищёнными косвенными данными о ней. Разработанные алгоритмы криптозащиты позволяют наращивать криптостойкость и сложность существующих криптоалгоритмов без существенных затрат на модернизацию уже существующих информационных систем.

Полученные практические результаты были запатентованы РМ №4511 (13) B1, “Устройство и способ криптографической защиты двоичной информации (варианты)” и была подана заявка на патент “Metoda de criptare a informațiilor binare în spațiul spectral și unui dispozitiv de transmisie în baza lui”.

Научные результаты, представленные для защиты:

- Технология, в основе которой предложены алгоритмы передачи зашифрованной информации, путём создания косвенных данных в виде формант на основе формантного анализа.
- Алгоритмы шифрования/дешифрования - RSA-mAB (AB1, AB2, AB3), обеспечивающих заданную временную криптостойкость систем в режиме реального времени.
- Расширенный алгоритм RSA-mAB шифрования/дешифрования, который обеспечивает контролируемое повышение вычислительной сложности в зависимости от варьируемых параметров.

Апробирование результатов работы. Основная концепция, методы и результаты была представлена на 2-х научных форумах:

- Conferinţă Internaţională "Telecomunicaţii, Electronică şi Informatică", ICTEI 2018, Mai 24-27, 2018, Chişinău, Moldova;

- Конференция «Математическая теория управления и ее приложения» (МТУиП-2020), 6–8 октября 2020, Санкт-Петербург, Россия;

а, также врамках чтения лекций мастерантам Технического Университета Молдовы, по специальности: «Технология Информации».

Научные публикации. Основные результаты теоретических изысканий отражены в 6 публикациях, из которых 3 в научных журналах, 2 в тезисных изложениях выступлений на научных международных конференциях и на базе представленного материала была

опубликована книга. Практические результаты изысканий были запатентованы в 2017 году и в 2021 году была подана заявка на патент.

Структура и содержание теоретического исследования. Работа включает в себя: 110 страницы основного текста, состоящего из введения, четырех глав, основных выводов и рекомендаций, библиографии из 162 источников.

Во **Введении** представлена аргументация актуальности темы исследования. Сформулированы цель и задачи исследования, представлены область и объект исследования, представлены элементы научной новизны полученных результатов, теоретическая значимость и прикладная ценность области исследования, а также краткое изложение результатов исследования.

В первой главе – **Современные требования к интероперабельности ИТ-систем,** был сделан обзор характеристик и описаны категории развития интероперабельных систем, была представлена концептуальная модель и обобщённая архитектура интероперабельной ПС системы. Были проанализированы стандарты обеспечения интероперабельности и безопасности информационных систем, был сделан обзор проблем интероперабельности современных платежных систем и были представлены принципы построения перспективных интероперабельных платежных систем. Описаны децентрализованные информационные системы на основе распределенных реестров как основа построения перспективных интероперабельных ПС. В конце главы были сформулированы заключения и направления дальнейшего исследования.

Во второй главе – **Описание и моделирование криптопроцессов** – отображены основные области применения криптографической защиты, принципы стойкости криптографических систем и основные методы шифрования - на базе работы с данными: блочное и поточное шифрования, и на базе работы с ключами: симметричное и асимметричное шифрование.

Для каждого из анализированных методов и алгоритмов шифрование/дешифрование были представлены преимущества и недостатки. В данной главе был сделан обзор формантного анализа и применение сопоставительного анализа для решения диофантовых уравнений применительно к крипто алгоритмам RSA. В конце главы были сформулированы проблемы и направление дальнейшего исследования.

В третей главе – **Защита информации при помощи алгоритмов RSA-mAB на основе формантного анализа,** представлены модернизированные RSA-алгоритмы на

основе формантной алгебры и строковой арифметики сопоставительного и формантного анализа.

Предложен способ контролируемого повышения вычислительной сложности криптоалгоритмов, используемых в ПС без уменьшения общей производительности и пропускной способности системы. Представлен расширенный алгоритм RSA-mAB шифрования/дешифрования в зависимости от варьируемых параметров алгоритма, который обеспечивает высокую надёжность RSA с малой длиной ключа.

В четвертой главе - **Система асимметричного побитного шифрования форманты речевого сообщения** была обоснована необходимость модернизации RSA алгоритма для исправления некоторых его недостатков на основе алгебры нового направления в теории чисел – формантного анализа.

Была рассмотрена процедура реализации модернизированных RSA-алгоритмов в широкополосных каналах связи в качестве основной криптосистемы закрытия информации, при использование малой длины ключа, с частой и быстрой его заменой. В данной главе была подробна описана система асимметричного побитного шифрования форманты речевого сообщения, где были подробно проанализировано шифрование 4096 возможных значений дискрет звука на базе предложенных алгоритмов.

Диссертация снабжена списком литературы на русском, английском, румынском языках.

В **Общих выводов и рекомендациях** представлены наиболее важные достижения и результаты диссертационной работы.

1 СОВРЕМЕННЫЕ ТРЕБОВАНИЯ К ИНТЕРОПЕРАБЕЛЬНОСТИ ИТ-СИСТЕМ

1.1 Интероперабельность систем

Термин «система» был введен в употребление в общей теории систем и представляет собой некую целостность, структуру в которой следует выделить составные части – элементы, а также связи и взаимодействия между ними. Каждый элемент, а следовательно, и вся система в целом демонстрируют поведение в зависимости от заданного алгоритма и взаимодействуют с окружающей средой и другими системами через интерфейсы или протоколы коммуникации. Окружающая среда и другие системы могут влиять на поведение и структуру системы, более того, система может изменять свое поведение, что позволяет системе развиваться, переходя из одного состояния в другое с течением времени.

Системы, при взаимодействии друг с другом, формируют новую, так называемую “систему-систем”, которая может быть проанализирована с точки зрения используемых ресурсов, или с точки зрения протоколов взаимодействия. В настоящее время всё к большему количеству таких структур систем, предъявляются требования в интероперабельности в рамках постоянно формирующегося и развивающегося информационного общества, как совокупности компонентов информационного общества, представленного на Рисунке 1.1.

Рисунок 1.1. Представления информационного общества как совокупность компонентов

Эти требования означают, что системы, взаимодействующие в «системе-систем», могут использовать как свои собственные ресурсы, так и ресурсы и возможности других систем, могут легко подключаться и обмениваться информацией друг с другом, а также могут обеспечивать функциональную совместимость всех взаимодействующих систем без определённых ограничений. Поэтому интероперабельность взаимодействующих систем следует считать одним из главных элементов развития информационного общества [67, 74, 155].

Что касается цифровых систем, интероперабельность означает информационно-логический и интерфейсный механизм, на базе которого каждая система формирует и отправляет данные, а также ими (интероперабельными системами) собираются данные от других систем с последующей их интерпретацией, и в этом случае концепция интероперабельности приобретает два значения [91]:

• **синтаксическая интероперабельность** - относится к соответствию форматов данных, протоколов передачи/получения данных, задействованные системами для успешного обмена данными;

• **семантическая интероперабельность** - относится к способности системы автоматически интерпретировать полученные данные с определённой точностью, что требует использование некой общей модели для интерпретации данных, где очень важно исключить недвусмысленное интерпретирования данных.

Наиболее приемлемое решение для обеспечения интероперабельности данных разных категорий является спецификация модели сопоставления данных между общими понятиями (mappings), которые в данном случае связанны с конкретными данными через метаданные [18]. Например, для инфраструктуры семантической интеропрабельности в рамках построения Электронного правительства необходимо, как минимум, использовать метаданные, онтологии и семантические активы [77].

Различаются **три категории трудностей** развития интероперабельных систем [91]:

- Концептуальная, которая связана с синтаксическими и семантическими различиями информации, которая подлежит обмену между системами.

-Технологическая, которая связана с несовместимостью информационных технологий (архитектура, инфраструктура систем). В данном случае трудности связаны со стандартами представления, хранения, обмена, обработки и передачи данных через компьютерные или мобильные сети.

- Организационная, которая связана с несовместимостью организационных структур (например, матричная или иерархическая) и касаются определения ответственности и полномочий.

В настоящее время развивается множество методологий для обеспечения интероперабельности систем в разных областях деятельности человека, которые регламентируются основоположениями (framework). Таким образом, в 2017 году Европейской Комиссией была разработана Европейское Основоположение по интероперабельности **(European Interoperability Framework (EIF))**, которое предлагает конкретное руководство по созданию интероперабельных цифровых государственных услуг и также предлагаются 47 конкретных рекомендаций о том, как улучшить управление деятельностью по интероперабельности систем, установки межорганизационных отношений, оптимизации процессов, поддержки цифровых услуг [112].

Компоненты и отношения в концептуальной модели EIF представлены на Рисунке 1.2.

Рисунок 1.2. Компоненты и отношения в концептуальной модели EIF [112]

В 2012 году Комиссией Европейского Парламента, Консилиумом, Экономическим и Социальным Европейским Комитетом и Комитетом Регионов было утверждено Основоположения интероперабельности е-правительства (**e-government** Interoperability Framework) для согласованного подхода интероперабельности организаций, которые хотят совместно работать над совместным предоставлением государственных услуг [69].

В 2011, Европейским Союзом было определено руководство для интероперебельности и стандартизации в области электронного здравоохранения (**e-health**) в Европе, которое предлагает структуру терминов и методологий для достижение общего языка, общей отправной точки для анализа проблем и описание решений электронного здравоохранения по всей Европе.

В плане электронного здравоохранения следует отметить научно-исследовательский австралийский проект NEHTA, который предложил архитектуру обеспечения интероперабельности систем электронного здоровья, на базе установления общих понятий из области электронного здоровья, принципов и стандартов, охватывая интероперабельность систем на техническом, семантическом и организационном уровнях.

Разикин в [31] представил архитектуру интероперабельных системы в виде ряда последовательных систем, который представляет каскадную структуру, где каждый новый этап базируется на предыдущем, Рисунок 1.3 [31].

Рисунок 1.3. Обобщенная архитектура интероперабельных систем [31]

Данная архитектура включает в себя пять этапов:

-Этап **Основные положения** (Framework), который содержат в себе концепции по достижению интероперабельности систем. Эти концепции охватывают уровни: концептуальный, контекстный и технологический.

-Этап **Архитектура (Arhitecture)**, который определяет элементы системы и взаимосвязи между ними и с окружающей средой.

- Этап **Эталонная модель (Reference model)**, который определяет многоуровневую модель интероперабельности.

- Этап **Профиль (Profile)**, определяющий набор стандартов, которые расположены в терминах эталонной модели.

- **Реализация (Solution)** — определяет программно-аппаратную реализацию интероперабельных систем.

1.2 Стандарты интероперабельности и безопасности систем

В настоящее время, развитие таких технологий как e-commerce, e-government, e-health, интернет вещей (IoT), облачное пространство (cloud computing) привело к развитию сред, где разнородные системы (компоненты) должны обеспечить взаимодействие друг с другом, с подержанием соответствующего уровня надежности и безопасности данных и систем [44, 67, 82, 94, 134, 109, 159].

Для обеспечения интероперабельности и безопасности были созданы десятки международных и национальных стандартов, которые устанавливает для реальных или потенциальных проблем, положения для общего и многократного использования с целью достижения оптимальной степени порядка [33, 119].

Стандарты, связанные с интероперабельностью делятся на две большие группы:

- непосредственно стандарты по интероперабельности;

- стандарты по безопасности и информационному аудиту.

Стандарты в области интероперабельности

Стандартизация в области интероперабельности систем позволяет различным процессам, системам, производить обмен информацией учитывая *синтактический, семантический и технические уровни* [21]. Данная стандартизация затрагивает следующие области [90 – 91, 130]:

1. Интероперабельность производственных систем и программных модулей, которая регламентирована [60, 73]:

- **ISO 15745** - Системы промышленной автоматизации и интеграция, основные положения для интеграции открытых систем (Industrial automation systems and integration — Open systems application integration frameworks). Стандарт состоит из четырех частей:

Часть 1: Общее справочное описание.

Часть 2: Справочное описание систем управления на основе ISO 1189.

Часть 3: Описание систем управления на основе IEC 61158.

Часть 4: Справочное описание для Системы управления на базе Ethernet.

Этот стандарт описывает Платформу для интеграции систем и включает в себя набор элементов и правил для описания профилей интероперабельных приложений.

-ISO 16100 - Системы промышленной автоматизации и интеграции – стандарт включает в себя профилирование производственных возможностей программного обеспечения для обеспечения интероперабельности (Industrial automation systems and integration — Manufacturing software capability profiling for interoperability).

Стандарт состоит из четырех частей:

Часть 1: Структура (относящаяся к ISO 15745).

Часть 2: Методология профилирования.

Часть 3. Интерфейсные сервисы, протоколы и шаблоны взаимодействия.

Часть 4: Методы, критерии и отчеты испытаний на соответствие.

Стандарт ISO 16100 определяет основополагающие требования для интероперабельности программного обеспечения, используемого в производственной сфере, и для облегчения интеграции в производственные приложения. Стандарт определяет методологию построения профилей производственного программного обеспечения и определяет требования к интерфейсу, сервисам и протоколам.

-ISO/TC 184/SC 5 стандарты для интероперабельности, интеграции производственных систем и приложений автоматизации (Interoperability, integration, and architectures for enterprise systems and automation applications).

2. Интероперабельность информационных и коммуникационных технологий для развития бизнеса и согласования требований производителей и потребителей, которая определена стандартами [84]:

- ISO/IEC JTC 1/SC 32 – стандартизация для управления и обмена данными, включая языки баз данных, управление мультимедийными объектами, управление метаданными, электронный бизнес.

- ISO/IEC JTC 1/SC 38 - стандартизация для интероперабельных распределенных приложений и сервисных платформ, включая веб-сервисы, сервис-ориентированную архитектуру (SOA) и облачную.

3. Интероперабельность данных в Веб – технологиях. Стандартизация веб-технологий регламентируется W3C - организацией, которая разрабатывает и внедряет технологические стандарты для веб-технологий. Многие из разрабатываемых стандартов касающихся веб-технологий решают проблемы присущие процессам работы с большими данными (Big Data).

4. Интероперабельность геопространственных данных и сервисов. Стандартизация в данной сфере определяется Open Geospatial Consortium (OGC) — международной некоммерческой организацией, которая в настоящее время координирует деятельность более 500 правительственных, коммерческих, некоммерческих и научно-исследовательских организаций с целью разработки и внедрения решений в области открытых стандартов для геопространственных данных, обработки данных геоинформационных систем и совместного использования данных.

5. Интероперабельность данных в области электронной коммерции. Стандартизация в данной сфере определяется глобальным консорциумом, который управляет разработкой, конвергенцией и принятием промышленных стандартов электронной коммерции в рамках международного информационного сообщества - OASIS (англ. Organization for the Advancement of Structured Information Standards). Данный консорциум является лидером по количеству выпущенных стандартов, относящихся к веб-службам. Кроме этого, он занимается стандартизацией в области безопасности, электронной коммерции; также затрагивается общественный сектор и рынки узкоспециальной продукции. В OASIS входит свыше 5000 участников, представляющих более 600 различных организаций из 100 стран мира.

6. Интероперабельность данных в области электронного здоровья (e-health), определяется стандартам ISO / IEEE 11073 Personal Health Device (X73-PHD) – решает проблему интероперабельности разных типов устройств в медицинской сфере.

Стандарты в области информационной безопасности и аудита

В области безопасности информационных систем наиболее известные стандарты являются [30, 60, 78, 105, 131, 152]:

1. Стандарт – «Критерий оценки надежности доверенных компьютерных систем «Оранжевая книга» (США)» - который регламентирует **принципы доступа к информации**, только авторизованными лицами или процессами.

2. Гармонизированные критерии европейских стран, принятые в 1991 году – «Information Technology Security Evaluation Criteria, ITSEC», которые определяются следующими критериями:

- конфиденциальности данных;

- целостности данных;

- доступности данных.

Этот критерий различает понятия “система” и “продукт”, и был введен термин «корректность», который подразумевает правильность реализации функций и механизмов

безопасности. Используется семь возможных уровней гарантированности корректности – от E0 (гарантированное отсутствие) до E6 (гарантированное присутствие).

В данных гармонизированных критериях выделяются следующие разделы:

- идентификация и аутентификация;
- управление доступом;
- точность информации;
- надежность обслуживания;
- обмен данными.

3. Германский стандарт BSI - посвящён детальному рассмотрению управления информационной безопасности компании, даны методики управления информационной безопасностью и описаны основные компоненты организации режима информационной безопасности.

4. Британский стандарт BS 7799 - в соответствии с которым любая служба безопасности, отдел, руководство компании должны начинать работать согласно общему регламенту, на данный момент этот стандарт поддерживается в 27 странах мира и с 2005 года Международная организация по стандартизации приняла стандарт BS 7799–2:2002 в качестве международного – ISO/IEC 27001:2005.

Данный стандарт определяет и рассматривает аспекты, связанные с политикой безопасности, организацией защиты данных, управления персоналом, ресурсами, компьютерными системами и др.

5. Международный стандарт ISO 17799 - (Code of practice for information security management – практические рекомендации по управлению безопасностью информации) – стандарт, который был разработан на базе стандарта BS 7799 и включает в себя административные, процедурные и физические меры защиты.

Этот стандарт рассматривает защиту компьютерных систем, сетей, электронных носителей информации, и активы организации такие как: документы на традиционных носителях, недокументированная информация – сведения, которыми располагают сотрудники организации.

6. Международный стандарт ISO 15408 «Общие критерии» - определяют функциональные требования безопасности и требования к адекватности реализации функций безопасности.

7. Российские стандарты информационной безопасности (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 51275 и др.), ГОСТ Р 50922-2006 “Защита информации. Основные термины и определения”.

Стандарты в части платежных систем

Отдельно рассмотрены стандарты в области платежных систем.

1. Стандарт обмена информационными сообщениями [128].

- **ISO20022** – “Финансовые услуги. Универсальная схема сообщений финансовой индустрии”:

Текущая версия стандарта состоит из восьми частей:

- ISO 20022-1: Метамодель (Metamodel).
- ISO 20022-2: UML-профайл.
- ISO 20022-3: Процесс моделирования.
- ISO 20022-4: Формирование схем XML.
- ISO 20022-6: Обратное проектирование.
- ISO 20022-7: Характеристики транспортировки сообщений.
- ISO 20022-8: Формирование ASN.1.

Стандарт включает в себя требования к следующим типам сообщений:

- платежи и расчеты (инициирование платежа, расчеты, управление денежными средствами, ведение переписки);
- ценные бумаги (заключение сделок с ценными бумагами, залоговые операции, клиринг по ценным бумагам, голосование по доверенности);
- торговые операции;
- платежи по дебетовым и кредитовым картам;
- конверсионные операции.

В стандарте также описываются базовые требования к бизнес-процессам в системе передачи сообщений для обеспечения безопасности доставки сообщений.

Уполномоченным органом по сопровождению стандарта ISO 20022 является организация SWIFT (Сообщество всемирных интербанковских финансовых телекоммуникаций).

2. PSI DSS – “Стандарт безопасности индустрии платежных карт” (PCI DSS Requirements and Security Assessment Procedures) является стандартом обеспечения безопасности для карточных платежных систем [46].

Стандарт выделяет шесть областей контроля:

- Построение и сопровождение защищенной сети.
- Защита данных держателей карт.
- Поддержка программы управления уязвимостями.
- Реализация мер по строгому контролю доступа.

- Регулярный мониторинг и тестирование сети.

- Поддержка политики информационной безопасности.

Для шести областей контроля устанавливается 12 основных требований к безопасности:

- установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт;

- неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности;

- обеспечение защиты данных держателей карт в ходе их хранения;

- обеспечение шифрования данных держателей карт в ходе их хранения;

-обеспечение шифрования данных держателей карт при передаче их через общедоступные сети;

- использование и регулярное обновление антивирусного программного обеспечения;

- разработка и поддержка безопасных систем и приложений;

- ограничение доступа к данным держателей карт в соответствии со служебной необходимостью;

- присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре;

- ограничение физического доступа к данным держателей карт;

- контроль и отслеживание всех нюансов доступа к сетевым ресурсам и данным держателей карт;

- регулярное тестирование систем и процессов обеспечения безопасности;

- разработка, поддержка и исполнение политики информационной безопасности.

1.3 Проблема интероперабельности современных платежных систем

Все существующие признанные во всем мире платежные и финансовые системы общаются на разных языках и решают многие важные вопросы, связанные с безопасностью и необходимым уровнем прозрачности и неотрекаемости бизнес-процессов самостоятельно.

Некоторые из ограничений:

- каждая система независимо идентифицирует своих пользователей;

- процессы внутри систем непрозрачны (иногда даже для владельцев этих систем);

- цифровые данные уязвимы так как их защита строится по принципу «периметра безопасности», что провоцирует постоянные атаки на систему;

- даже если API отдельных ПС открыты, у каждой ПС они свои.

Учитывая отсутствие открытых API, современные платежные системы (ПС) не могут беспрепятственно и прозрачно взаимодействовать друг с другом – необходимы постоянные усилия по поддержанию согласованности работы через самостоятельные API. Достижение даже минимальной совместимости между ПС является весьма затратным процессом как по времени, так и финансово, причем как непосредственно для организаций – владельцев ПС, так и для клиентов этих систем. Кроме этого, необходимо поддерживать постоянную работоспособность подобных систем, что приводит к высокой стоимости комиссий за денежный перевод – в системе SWIFT, например, комиссион за транзакцию доходит до 50 долларов.

Безопасность существующих ПС.

Концепция абсолютного большинства современных ПС построены по принципу «периметра безопасности». Предполагается, что для защиты системы от угроз создается «периметр безопасности»: брандмауэры, системы контроля доступа и тд.

Попытки защитить ценные данные, спрятав их за «периметром безопасности» становятся все более и более ущербны по своей сути и чрезвычайно затратны как по людским ресурсам, так и финансово.

Например, в рамках политики BYOD (Bring Your Own Device) сотрудники компаний используют собственное оборудования для работы, причем как дома, так и в офисе компании [70]. Это дает очевидные преимущества: повышение общей производительности сотрудников, сокращение затрат компании на предоставление оборудования сотрудникам, гибкий график работы и т. д. Но при этом, в рамках концепции «периметра безопасности», это порождает очевидные проблемы с обеспечением информационной безопасности, так как получение несанкционированного доступа злоумышленника к личному оборудованию сотрудника компании может привести к потере конфиденциальных данных компании.

Противоположным примером являются криптовалюты – для каждой из них существует публичный распределенный реестр всех транзакций и остатков на электронных кошельках участников системы, который доступен всем, вне какого-либо «периметра безопасности» [55]. Но невозможно изменить ни одну запись в исторических данных этой системы так как все записи в ней защищены криптографическими ключами, а информация разнесена географически.

Таким образом, ключевой момент обеспечения безопасности, целостности и неотрекаемости в ПС это использование криптографических ключей при совершении любых действий - от авторизации до запроса или подтверждения транзакции. Они

используются для подписания каждого запроса или транзакции и, тем самым, обеспечивают целостность и аутентичность данных [99, 100, 102, 104, 110, 113, 116].

Идентификация.

В финансовых системах, в целом, и в ПС, в частности, не поддерживаются единая цифровая идентификация подобная той, которая используется в большинстве мобильных и интернет-приложениях – через свой аккаунт в Facebook, Linkedin или других социальных сетях. Сегодня в каждой ПС участник должен проходить свою, весьма громоздкую процедуру идентификации и регистрации [66, 85, 86, 97, 144]. В результате клиенты имеют свои уникальные идентификаторы и пароли в каждой отдельной ПС. Конечно, каждому пользователю ПС было бы значительно удобнее иметь как единый идентификатор во всех системах, так и единообразную систему входа и подключения.

Прозрачность бизнес-процессов.

К сожалению, абсолютное большинство ПС систем закрыты – их архитектура известна только разработчикам, исходный код программ закрыт. Более того, часто это считается дополнительным уровнем защиты ПС от возможных попыток взлома.

Доверие к ПС в этом случае основано на юридических и надзорных инструментах государства, в чьей юрисдикции работает данная система.

Однако такой подход приводит к следующим очевидным проблемам:

- необходимо слепо доверять разработчику системы как в уровне безопасности системы в целом, так и отсутствии уязвимости на уровне кода;

- внутренние бизнес-процессы неочевидны, хотя могут иметь значительные проблемы как с безопасностью, так и в вопросе их соответствия национальным и международным регламентам и инструкциям;

- невозможность провести внешний аудит работы системы.

Централизованность.

В традиционных ПС все процессы централизованы, т.е.:

- централизованно хранятся все данные;

- централизована обработка данных;

-централизовано система безопасности, через роль главного администратора системы.

В целом это означает, что изначально создаются потенциальные риски и соблазн модификации данных, так как при централизованном характере их хранения и управления, соответствующие манипуляции с данными можно скрыть, а соответствующий факт будет крайне трудно проверить и доказать.

В результате как владельцу ПС, так и ее клиентам необходимо полностью доверять ответственной стороне, которая осуществляет управление данными в соответствующей ПС, при этом постоянно существуют высокие риски мошенничества.

Проблема аудита традиционных ПС.

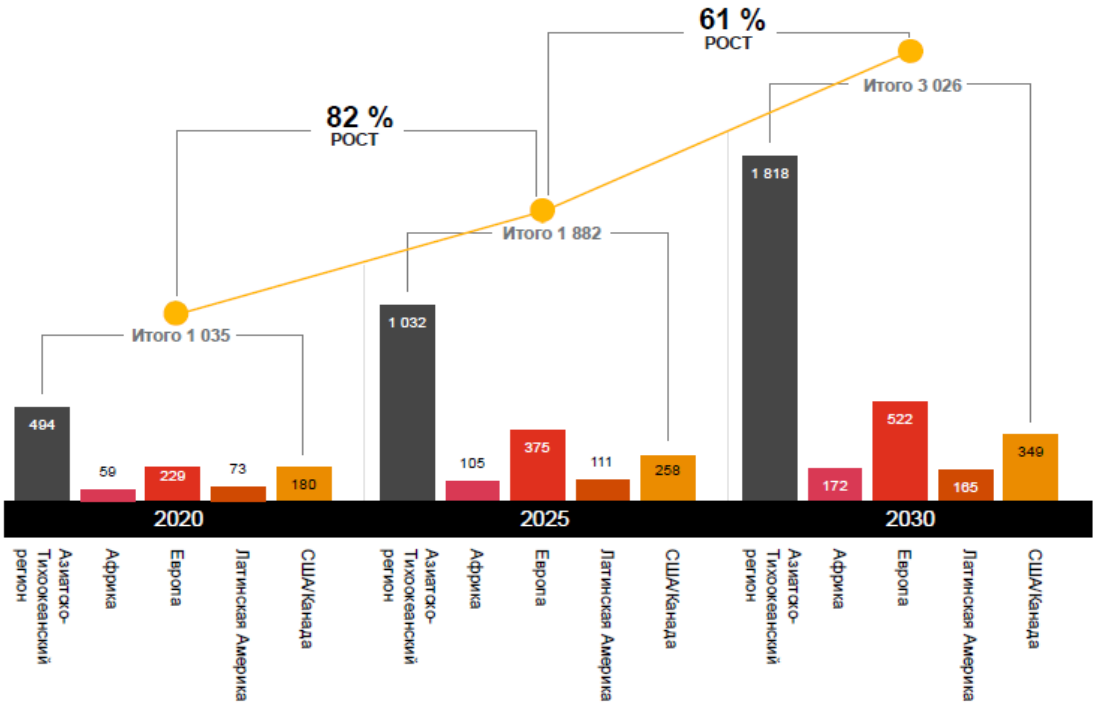
У аудитора нет никакой уверенности что задокументированные и предоставленные ему данные являются подлинными, целостными, полными и актуальными. Он может работать только с представленными ему данными, которые могут отличаться от реальных – как в силу ошибок, так и преднамеренно.

Только использование реестров, где все операции подтверждены криптографическим механизмами может гарантировать целостность и подлинность всех транзакций.

Масштабирование и доступность.

Широкая доступность финансовых сервисов для населения во всем, мире, особенно в развивающихся странах, возможна только через расширение безналичных платежных сервисов [59, 87, 115].

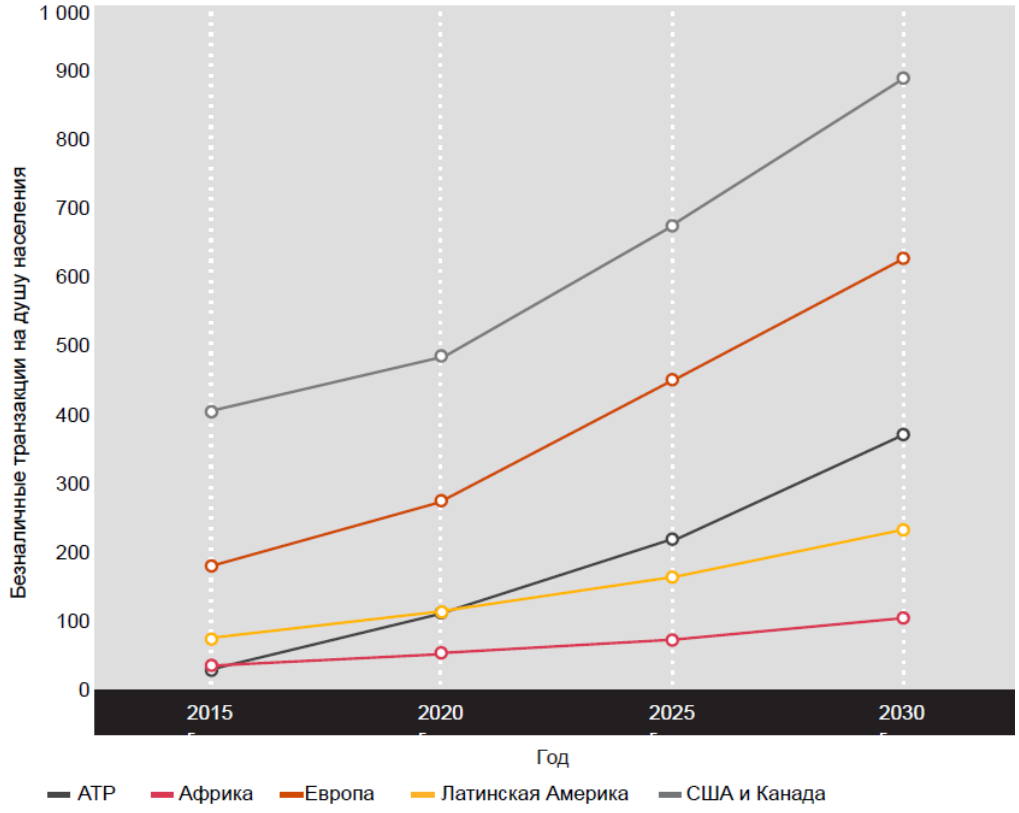
На базе глобального исследования, проведенного в 2021 году консалтинговым подразделением PwC Strategy& компании PriceWaterhouseCoopers прогнозная модель платежей в мире, предполагает, что рост объема безналичных транзакций в мире в денежном выражении вырастет к 2030 году более чем в два раза (Рисунок 1.4, Рисунок 1.5).



Примечание. Общие суммы безналичных транзакций в 2025 г. и 2030 г. являются прогнозными величинами.
Источник: модель платежей в мире, PwC Strategy&, 2021 г.

Рисунок 1.4. Предполагаемый рост объема безналичных транзакций

Проводниками подобных решений обычно выступают небанковские финансовые организации, предоставляющие исключительно платежный сервис особенно в сфере микроплатежей.



Примечание. Количество транзакций в 2025 г. и 2030 г. является прогнозной величиной.
Источник: модель платежей в мире, PwC Strategy&, 2021 г.

Рисунок 1.5. Предполагаемый рост объема безналичных транзакций

На Рисунке 1.6 показано, на базе исследования консалтинговым подразделением PwC Strategy& компании PriceWaterhouseCoopers, с какой скоростью мгновенные платежи набирают популярность с момента запуска в различных регионах мира.

Однако, быстрое внедрение новых безналичных платежных сервисов требует значительных ресурсов для многочисленных интеграций [50, 54, 120, 123, 133, 140], которые, зачастую специально сдерживаются или максимально тормозятся традиционными банковскими организациями, не заинтересованными в наличи конкуренции на рынке платежных сервисов.

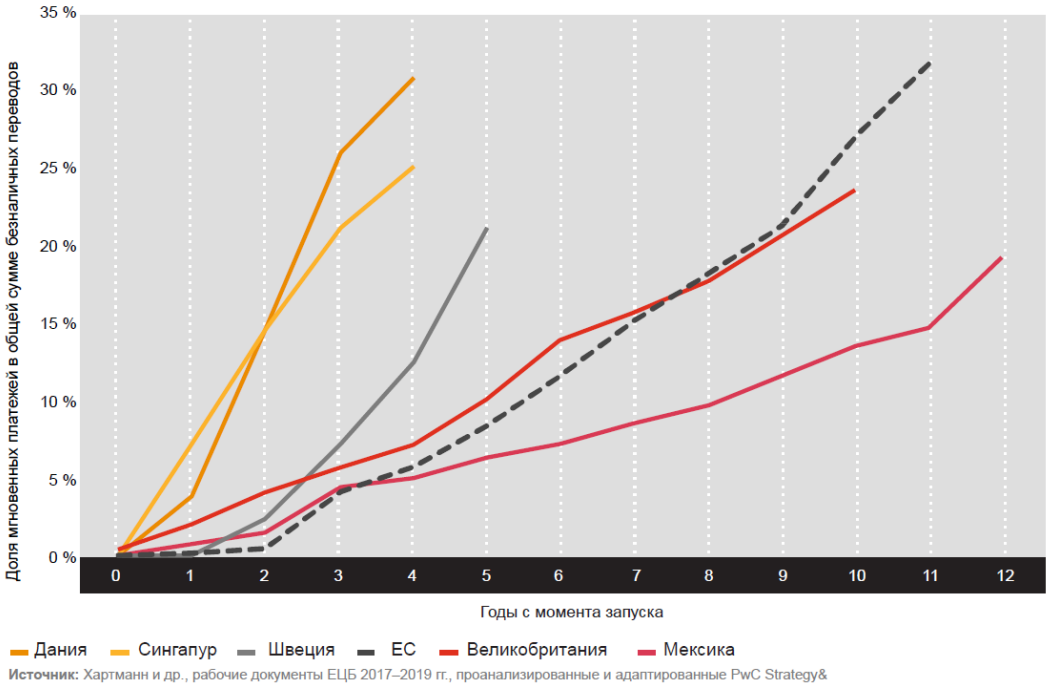


Рисунок 1.6. Рост объема мгновенных платежей

На Рисунке 1.7 показан прогноз развития альтернативных ПС по сравнению с традиционными банками с точки зрения роста валовой выручки (указана транзакционная выручка в млрд долларах США. Совершенно очевидно, что к 2030 году альтернативные системы ПС в совокупности обойдут по валовой выручке банки как традиционные платежные сервисы.

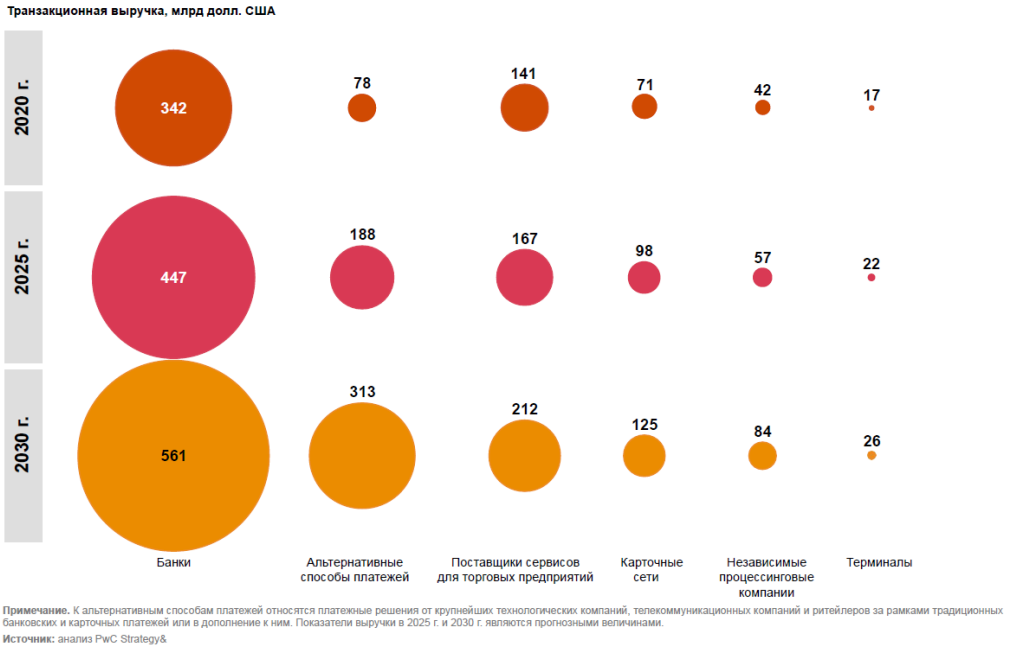


Рисунок 1.7. Прогноз развития альтернативных ПС по сравнению с традиционными банками с точки зрения роста валовой выручки

Единственным реальным способом решения подобной проблемы является сквозная совместимость всех ПС на рынке, что обеспечит возможность появления новых игроков и новых продуктов на рынке с минимальными временными, финансовыми и технологическими издержками.

Но на данный момент, учитывая нарастающую сложность современных ПС они создаются как закрытые системы, для максимального «замыкания на себя» клиентов и всяческому препятствованию появления новых, альтернативных игроков на рынке ПС, с принципиально новыми или с более дешевыми услугами, прежде всего, для массового клиента.

Основные проблемы, стоящие на пути построения интероперабельных ПС.

К основным проблемам, стоящим на пути создания интероперабельных ПС во всем мире, следует отнести следующие:

- **Национальные границы**. Каждое национальное правительство склонно к созданию собственных, суверенных ПС по собственным стандартам. В понимании национального правительства это обеспечивает национальный суверенитет и независимость финансовой системы страны.
- **Персональные данные.** Совместное, трансграничное использование персональных данных требует очень сложного законодательного регулирования этого вопроса между различными государствами.
- **Монополизм**. Сильные национальные или глобальные игроки склонны защищать свое доминирующее положение всеми доступными средствами, зачастую используя для этого нерыночные механизмы.
- **Патенты**. Многие решения в области ПС запатентованы и компании, владельцы патентов, могут не согласиться с передачей прав на их решения для всех игроков финансового рынка.
- **Договорные отношения**. Необходимо уйти от индивидуальных двухсторонних отношений между различными ПС к универсальным типовым договорным отношениям, между любыми ПС во всем мире.
- **Контроль сложности**. Требуется постоянно отслеживать все более увеличивающуюся сложность глобальной международной системы внедряя стандарты интероперабельности для ПС.

1.4. Принципы построения интероперабельных ПС

Построение интероперабельных ПС как совокупности взаимодействующих локальных и глобальных ПС, которые могут неограниченно масштабироваться, должно отвечать следующим принципам:

- каждая ПС имеет единообразное API для взаимодействия с другими системами, а также управления аккаунтами и транзакциями;
- каждое действие в рамках ПС – вход, запрос состояния остатка на счете, инициация операции, изменение текущего баланса счета должно быть криптографически подтверждено;
- каждый инициатор действия ПС в обязательном порядке имеет уникальный идентификатор;
- обязательно шифрование данных во время передачи и хранения для обеспечения требований GDPR (General Data Protection Regulation);
- отказ от механизма аутентификации по паролю, все пользователи ПС подписывают каждый запрос своим личным криптографическим ключом;
- ПС могут\должны связываться друг с другом в режиме реального времени и являются источниками информации друг для друга;
- отношения между ПС основаны не на доверии, а исключительно на математических принципах;
- протоколы для работы ПС унифицированы и стандартизованы, поставляются с открытым исходным кодом и доступны всем;
- все процессы ПС децентрализованы как единственный способ обеспечения реальной отказоустойчивости;
- любая транзакция атомарна. Транзакция считается законченной, когда присутствуют все необходимые подписи, включая валидирующие подписи. Как только валидатор (или валидаторы) определены в соответствии с необходимыми требованиями (такими как KYC/AML) и они подписывают транзакцию, транзакции становятся юридически значимыми. Все балансы корректируются в каждой ПС и соответствующем реестре асинхронно;
- ключевой элемент безопасности ПС – личный криптографический ключ пользователя системы и проведение всех криптографических преобразований, включая подписание транзакций на личном устройстве пользователя.

С точки зрения клиента различных ПС вышеописанные принципы означают что:

- клиент использует одно приложение для доступа к любой ПС, в которой он авторизован;
- подписание транзакций выполняется устройстве клиента;
- использование любой ПС для клиента прозрачно и понятно, так как они работают по единым принципам, как это сейчас происходит, например, при чтении новостных сайтов.

Основные составные части и принципы построения интероперабельных ПС:

- **Реестр транзакций**. Каждая ПС имеет свой реестр операций (транзакций) – частный или публичный, это решает сама ПС в зависимости от целей, задач и требований к данной конкретной ПС, при этом в любом случае обеспечивается прозрачный доступ для целей аудита.
- **Валидаторы**. Для ПС это, как правило - внутренние валидаторы (контролеры), национальные и межнациональные организации (Национальные банки, контролирующие организации и тд). Их набор определяется либо исходя из требований законодательства к каждому типу транзакций, либо исходя из доверия к ним со стороны различных ПС.
- **Консенсус**. Для децентрализованных систем, построенных на основании распределенных реестров, устанавливается обязательное правило консенсуса – те условия или события, при которых, например, транзакция считается завершенной или валидной. Например, транзакция считается завершенной или валидной в случае, если ее подписали любые три из пяти назначенных валидаторов.
- **Идентификация**. Идентификация должна проводиться через независимых национальных\наднациональных поставщиков сервисов KYC\AML [72], которые взаимодействуют между собой по модели web-of-trust, для предотвращения случаев мошенничества, особенно трансграничного мошенничества. Весь обмен информации между ними, так и к ним происходит с использованием криптографических механизмов.
- **Поставщики данных (оракулы)**. Это поставщики внешних по отношению к ПС данных, которые рождаются вне ПС, но важны для проведения транзакции или отказа от ее проведения. Например, это кросс-курсы валют или котировки на биржах или глобальные сервисы метки времени (time stamp). Все запросы к ним также происходят с использованием криптографических механизмов.
- **DNS ПС**. По аналогии с DNS (Domain Name System) для интернета – универсальный реестр адресов для различных ПС.

- **Универсальное клиентское приложение**. Данное приложение должно обеспечивать доступ через DNS ПС доступ ко всем ПС, в которых клиент авторизован.

Таким образом, глобальная ПС система будет состоять из множества самостоятельных ПС, действующих по единым принципам, описанным выше, где для каждой из отдельных ПС прозрачно и доказательно через криптографические механизмы осуществляется:

- Валидация и аутентификация.
- Управление реестрами.
- Управление транзакциями.
- Внешний аудит.

1.4.1 Управление реестрами

Сами по себе реестры, в отличии от централизованных систем не являются основным источником информации, так как они являются результатом выполненных транзакций [24]. Таким образом, совершенные транзакции являются основным источником информации, на основании которого в итоге получается фактическое конечное состояние реестров. Реестр – это таблица, в которой хранится состояние всех учитываемых единиц в ПС. Это состояние является результатом выполненных транзакций с момента запуска ПС до определенного момента.

1.4.2 Управление транзакциями

Транзакции – это набор данных для проведения операции для изменения состояния реестра, каждое последующее состояние которого соответствует последующему набору транзакций [24]. Под управлением транзакциями понимается следующие процессы - инициации транзакции, валидацию и проверку транзакции, а также обновление соответствующего реестра на основании содержания транзакции. Историю транзакций хранят: непосредственно ПС, национальные и наднациональные регуляторы, валидаторы, аудиторы, внешние хранители данных.

1.4.3 Внешний аудит

Для проведения аудита аудитору нужно загрузить всю историю транзакций от валидаторов и, в соответствии с принятыми правилами, сверить с соответствующими данными в реестре данной ПС. Имея конечное состояние учетной системы, аудитор сверяет

его с теми состояниями, которые он получил от валидаторов, и которые используют клиенты ПС. Такой аудит ПС должен быть полностью автоматизированным, выполняться в режиме реального времени в любое время, когда сочтет нужным аудитор. Более того, такой аудит может происходить в полностью автоматическом режиме по заранее заданному графику.

1.5 Децентрализованные информационные системы на основе распределенных реестров как основа построения интероперабельных ПС

Децентрализованные системы предполагают распределение функций информационной системы между ее участниками без единого управляющего центра на основе распределенных реестров. Для таких систем отпадает необходимость в центральном сервере, все узлы (составляющие) такой системы равноправны по отношению друг к другу. Соответственно, атака на часть этих узлов и даже выведение части узлов системы из строя не влияет на работоспособность системы в целом [24].

Типичным примером подобной системы является глобальная сеть Интернет, где выход из строя одного из маршрутизаторов пакетов (узла) не приводит к неработоспособности системы в целом.

В отличии от централизованных систем децентрализованные системы на основе распределенных реестров имеют ряд важных достоинств [24]:

- Все процессы во всех узлах системы прозрачны и однотипны, что обеспечивает возможность функции доверия и контроля, основанной на математических принципах.
- Не существует единой точки отказа.
- Не существует единого механизма контроля за данными и безопасностью в системе, что в централизованных системах является основой и питательной средой для мошенничества и наличия критических уязвимостей.

Децентрализованные системы на основе распределенных реестров всегда избыточны с точки зрения хранения данных таким образом, чтобы при любом выходе из строя части узлов системы, включая те, где хранятся данные, всегда можно было восстановить ключевые данные для данной системы. Принцип работы децентрализованных систем передачи данных состоит в том, что узлы системы сами поддерживают каналы передачи данных и выполняют маршрутизацию пакетов данных. В такой системе узлы «слушают» друг друга, и если один из них выходит из строя, то те узлы, которые были подключены к нему, ищут альтернативные узлы для подключения и передаче данных.

1.5.1. Использование принципов построения децентрализованных систем на основе распределенных реестров при создании интероперабельных ПС

Ниже рассматривается децентрализация ключевых инфраструктрурных элементов ПС для обеспечения функциональной и технологической совместимости:

1. Инфраструктура идентификации.
2. Инфраструктура Public Key Infrastructure (PKI) [39].
3. Инфраструктура Know Your Clients / Anti Money Laundering (KYC/AML) [72].
4. Децентрализованное хранение транзакций.
5. Инфраструктура валидаторов. Подходы к достижению консенсуса.
6. Смарт-контракты.
7. Единая точка входа.

Все вышеуказанные инфраструктурные элементы могут быть как составной частью той или иной ПС, но также и внешними по отношению к ПС элементами. Реализация ключевых инфраструктрурных элементов как внешних по отношению к конкретной ПС имеет ряд неоспоримых преимуществ, а именно:

1. Специализация как возможность повышение качества предоставляемого инфраструктурным элементом сервиса.

2. Повышенная техническая и технологическая надежность инфраструктурного сервиса в следствии изначальной нацеленности на предоставление сервиса большому количеству клиентов по всему миру в режиме 24x7x365.

3. Соответствие предоставляемого провайдером инфраструктурного сервиса международно признанным стандартам и практикам, что обеспечивает высокий уровень унификации технологических решений и их соответствие международной нормативной базе.

4. Обязательный технологический и процедуральный международный аудит провайдера инфраструктурного сервиса.

5. Высокий уровень конкурентности в предоставлении инфраструктурных сервисов, что обеспечивает постоянную необходимость для провайдеров поддержание высокого уровня качества оказываемых услуг.

Исходя из вышесказанного далее будет рассматриваться принципы построения децентрализованных ключевых инфраструктурных элементов как внешних по отношению к ПС, что повышает технологические, функциональные и иные требования к ним, но существенно улучшает качество получаемой интероперабельности ПС.

1.5.2 Распределенные реестры

Различие между централизованными, децентрализованными и распределенными системами.

Прежде чем приступить к обсуждению построения интероперабельных ПС на базе распределенных реестров необходимо предельно четко провести разграничение между понятиями: централизованные, децентрализованные и распределенные системы.

Централизованные\децентрализованные системы характеризуются уровнем контроля. В централизованной системе контроль осуществляется одним субъектом, в децентрализованной – несколькими независимыми или ограниченно зависимыми субъектами.

Распределенные системы характеризуется отсутствием единого субъекта управления и разнесенным географически хранением данных.

Лучше всего различие в централизованных, децентрализованных и распределенных системах демонстрирует графическое изображение всех трех типов систем представленное на Рисунке 1.8 [141].

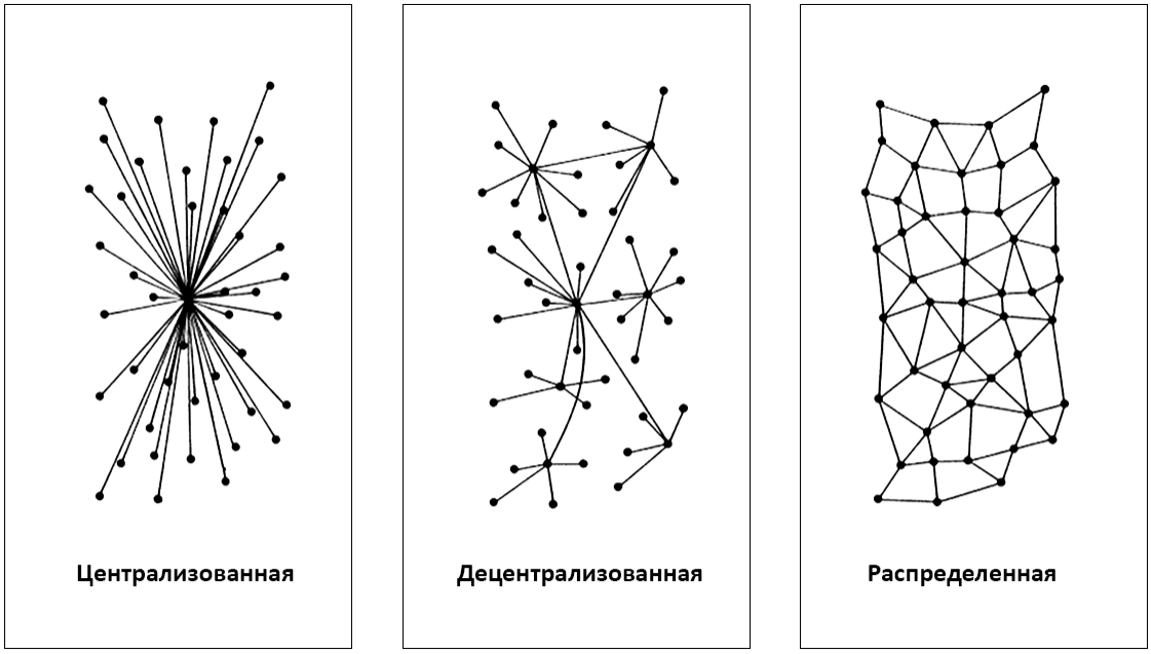


Рисунок 1.8. Представления централизованных, децентрализованных и распределенных систем

Преимущества и недостатки, а также свойства каждой из вышеперечисленных систем перечислены в Таблице 1.1 [141].

Таблица 1.1. Свойства централизованных, децентрализованных и распределенных систем [141]

Свойства	Централизованные	Децентрализованные	Распределенные
Точки отказа	Одна точка отказа	Конечное число точек отказа	Бесконечное
Поддержка	Легкая	Умеренная	Сложная
Стабильность	Высокая нестабильность	Возможность восстановления	Очень стабильная
Масштабируемость	Низкая масштабируемость	Низкая масштабируемость	Бесконечная масштабируемость
Легкость создания	Средняя сложность	Управляемая сложность	Высокая сложность
Возможность развития	Низкая	Высокая	Высокая

В распределенных реестрах данные хранятся не в единой централизованной базе, а в территориально распределенных хранилищах данных. Главные требования к распределенным реестрам - целостность и доступность данных в реестре [24].

Целостность данных обеспечивается путем добавления хэш-значений к соответствующей транзакции, тогда как доступность обеспечивается при помощи резервного копирования данных и хранения их на нескольких территориально разнесенных серверах (Рисунок 1.9).

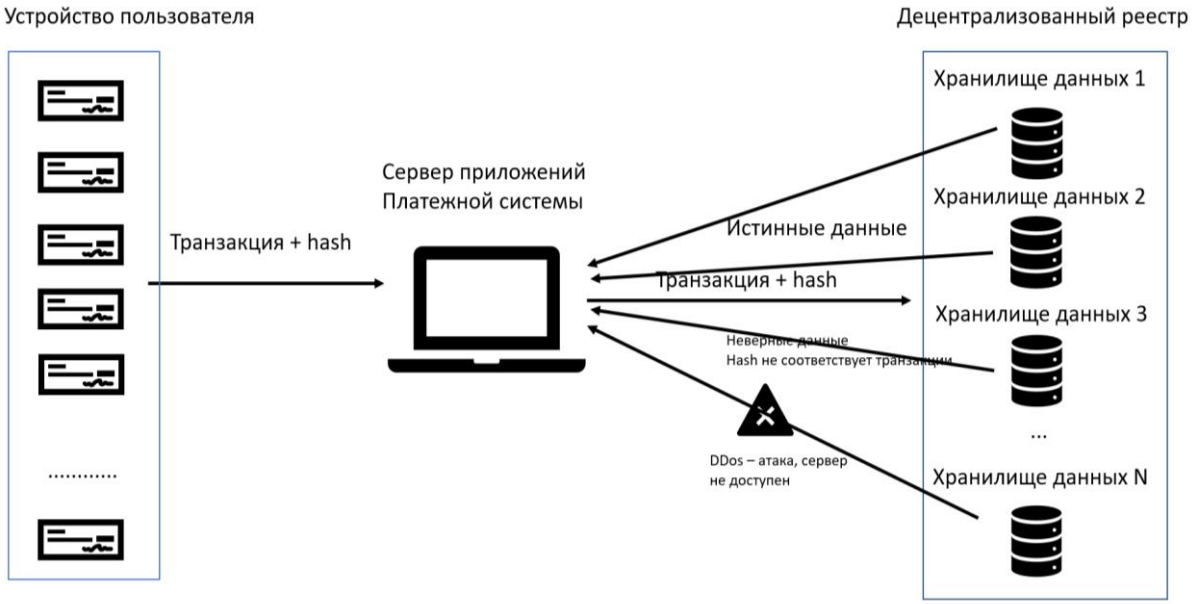


Рисунок 1.9. Обеспечение целостности данных в ПС

Важно отметить, что различная по типу информация в ПС может храниться в различных реестрах. Например, для ПС в разных децентрализованных реестрах можно хранить:

- остатки на счетах;

- транзакции;

- реестр счетов;
- реестр клиентов;
- справочники;
- и тд.

Такой подход, в том числе, позволяет прозрачно для ПС использовать как собственные, так и внешние реестры без появления ограничений на скорость, безопасность или функциональность ПС.

Таким образом, следует констатировать что оптимальным способ построения совокупности глобальных интероперабельных ПС является реализация ПС как децентрализованных систем на базе распределенных реестров.

Также целесообразен аналогичных подход к ряду инфраструктурных элементов ПС, которые могут быть как внутренние, так и внешние по отношению к конкретной ПС, к которым можно отнести инфраструктуру идентификации, инфраструктуру PKI [98], инфраструктуру KYC/AML и инфраструктуру валидаторов.

Необходимо отметить, что все вышеуказанные инфраструктурные элементы ПС функционируют с использованием криптографических алгоритмов. Наличие надежных, высокопроизводительных криптографических алгоритмов, обеспечивающих необходимый уровень надежности и безопасности, является краеугольным камнем возможности построения и успешного функционирования интероперабельных ПС на базе распределенных реестров. Любая угроза надежности и безопасности существующих криптоалгоритмов и их программных и\или аппаратных реализаций ставит под угрозу безопасность платежного документооборота, в принципе. На данный момент увеличение вычислительной мощности компьютеров как потенциальной угрозы для существующих криптографических алгоритмов и их реализаций компенсируется увеличением длины используемого ключа при процессе шифрования\дешифрования.

В разделе 1.2 Стандарты интероперабельности и безопасности систем, первой главы указывалось на стандарты, используемые при построении ПС. Данные стандарты основываются на требованиях к ПС как централизированным\децентрализированным системам, для которых существует «периметр безопасности», который реализуется через брандмауэры, системы контроля и тому подобные системы. Особенно в явном виде на это указывает стандарт обеспечения безопасности банковских карт PCI DSS. Как было указано ранее, данный подход все более ущербен по своей сути и чрезвычайно затратен по финансовым и человеческим ресурсам. Ситуация во время эпидемии COVID19, когда сотрудникам вынужденно приходилось использовать собственное оборудование для

работы дома в рамках политики BYOD (Bring Your Own Device) порождала очевидные проблемы с обеспечением информационной безопасности так как получение несанкционированного доступа злоумышленника к личному оборудованию сотрудника компании могло привести к потере конфиденциальных данных компании [70].

При этом нельзя не приветствовать внедрение стандарта ISO 20022, который является существенным шагом в рамках повышения совместимости и интероперабельности существующих систем.

В рамках идеологии систем распределенных реестров ответственность за обработку и безопасное хранение данных лежит исключительно на владельце хранилища данных. Для обеспечения целостности данных, любая транзакция должна включать соответствующий хэш этой транзакции как гарантия того, что данные были обработаны правильно и не были изменены злоумышленником. Кроме того, такие данные должны реплицироваться и храниться на различных физически распределенных серверах.

Все системы (включая ПС), в которых хранятся перечисленные типы данных, должны иметь свои собственные наборы систем защиты информации в зависимости от выполняемых функций и их политик безопасности.

Распределенный реестр состоит из ядра и слоя, ответственного за реализацию бизнес-логики системы (Рисунок 1.10).

Ядро обеспечивает хранение транзакций в упорядоченном виде, а также хранение цифровых подписей транзакций. Основными функциями ядра системы являются:

- обеспечение распределенного хранения транзакций в виде упорядоченной цепочки блоков;
- контроль достижения консенсуса между узлами сети;
- проверка и настройка прав на добавление, обновление и удаление записей в реестре;
- получение истории изменений.

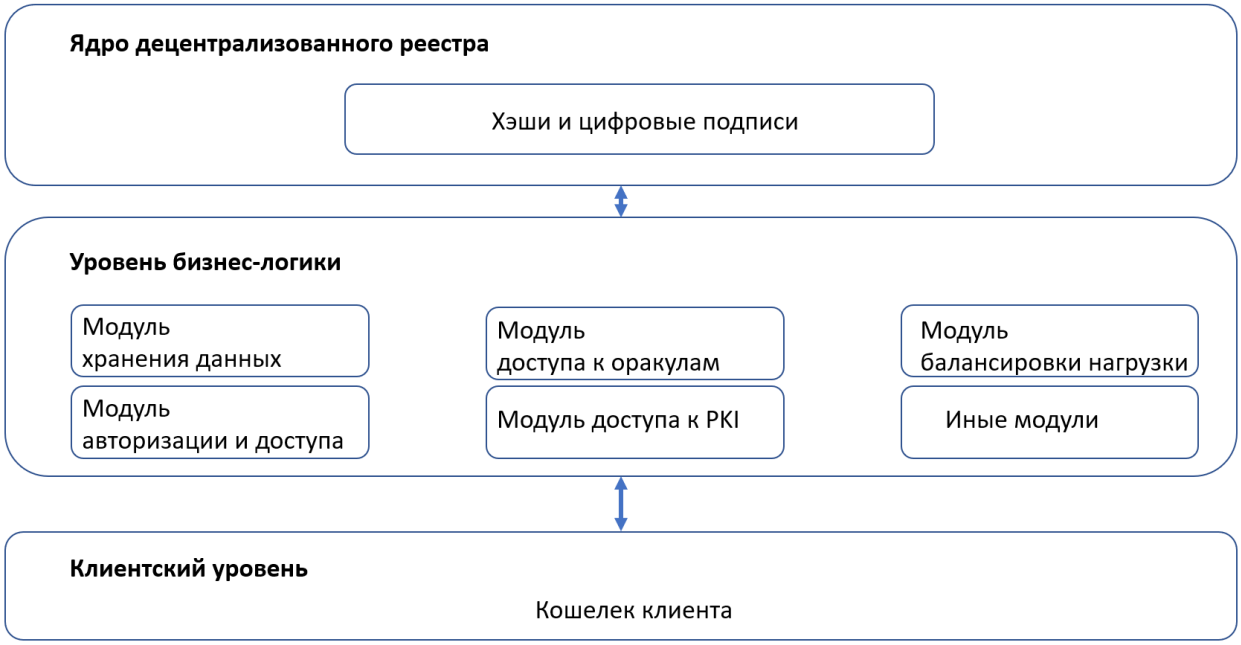


Рисунок 1.10. Архитектура распределенного реестра ПС

Хранение большого количества файлов в цепочке блоков может привести к быстрому ее возрастанию и резкому замедлению скорости работы, что для ПС недопустимо. Выходом является хранение самих данных во внешнем по отношению к распределенному реестру хранилище, а в цепочке блоков указывать хеш-значение транзакции для обеспечения проверки целостности и аутентичности данных.

1.5.3 Инфраструктура идентификации

Децентрализованная система идентификации состоит неограниченного количества центров идентификации, которые действуют друг с другом по единым принципам:

- данные между центрами идентификации синхронизируются в режиме реального времени;
- единый идентификатор клиента (пользователя ПС) для любых ПС;
- доступ в реальном времени ко всем событиям, которые происходят с идентификатором (аудит данных и событий).

Распределенный реестр идентификаторов.

Реестр идентификаторов – это распределенный реестр, который хранит уникальные идентификаторы клиента. Действия с идентификаторами организованы в связанный список транзакций, где каждый следующий набор данных ссылается на предыдущий. Это обеспечивает целостность идентификаторов, которые добавляются в связанный список, и делает невозможным их изменение задним числом.

Реестр идентификаторов – это распределенный реестр, который требует достижения консенсуса между валидаторами системы, в роли которых выступают центры идентификации. Чтобы получить информацию об идентификаторах, клиенты отправляют соответствующие запросы в один из центров идентификации и получают актуальную информацию об идентификаторе и связанных с ним набором данных (Рисунок 1.11) [24].

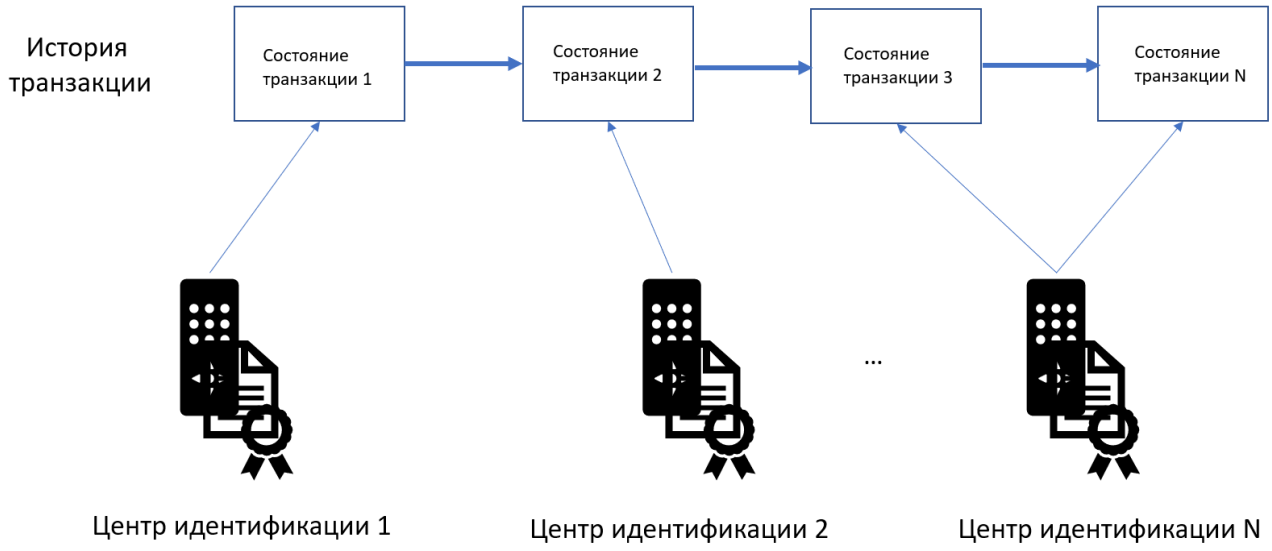


Рисунок 1.11. Формирование реестра идентификаторов

Инфраструктура Public Key Infrastructure (PKI) [39].

Чтобы доказать наличие прав на те или иные действия в системе, обычно используется некоторая информация о клиенте\пользователе и\или требуется использование логинов и паролей.

Наиболее безопасным и надежным способом является использование криптографических механизмов. Чаще всего в такой системе идентификатором выступает открытый ключ пользователя.

Существует два основных подхода к созданию инфраструктуры PKI:

- централизованная иерархической архитектура в соответствии со стандартом X.509 [76];
- децентрализованная архитектура на основе Web-of trust [62].

На данный момент в основном используется централизованная иерархическая архитектура, так как она очень удобна - процессы получения, обновления и отзыва сертификата очень эффективны.

Стандарт X.509 описывает иерархическую модель инфраструктуры PKI. В такой модели сертификаты центра сертификации (ЦС), конечных пользователей, систем и

приложений подписываются вышестоящим ЦС – корневым ЦС. На Рисунке 1.12 отражена иерархическая модель инфраструктуры PKI.

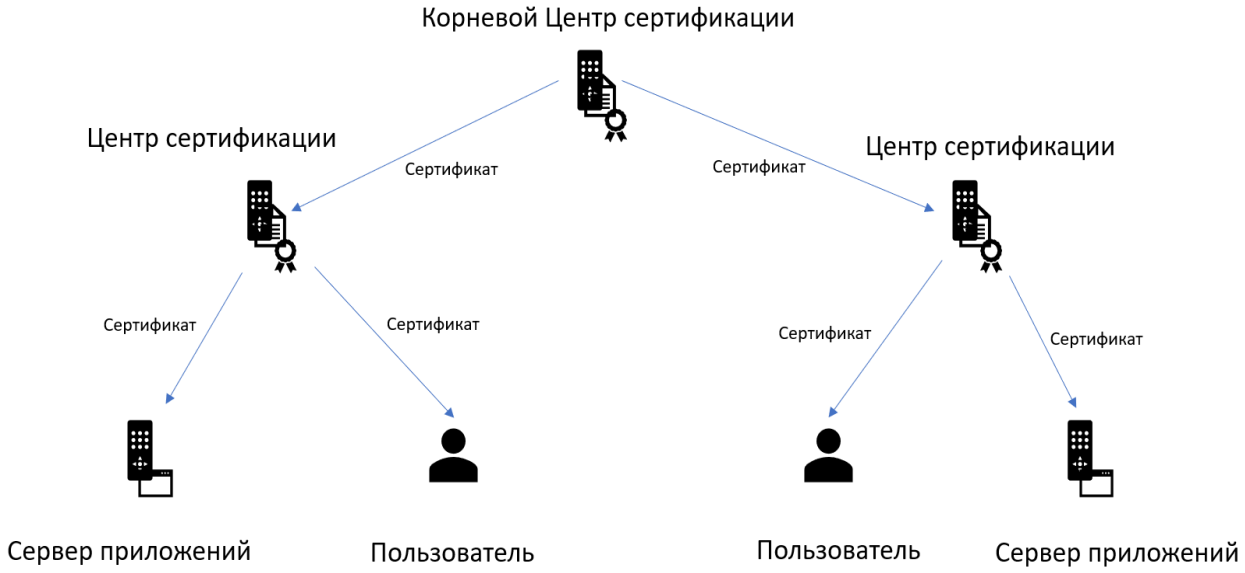


Рисунок 1.12. Иерархическая инфраструктура PKI

К недостаткам иерархической инфраструктуры PKI относится:

- единая точка отказа в виде корневого ЦС;
- единая точка цензуры\компрометации;
- получение сертификатов одним лицом от разных регистраторов (ЦА);
- необходимость проверки всей цепочки сертификатов, вплоть до корневого.

Иерархическая инфраструктура PKI предполагает необходимость прохождения процедуры регистрации пользователю в разных ЦА в зависимости от их обслуживаемой юрисдикции или области применения.

Если система идентификации децентрализована, у пользователя будет только один идентификатор. Этот идентификатор может подтверждается другими независимыми регистраторами и, соответственно, может использоваться в разных юрисдикциях или областях применения.

Децентрализованная архитектура PKI.

Второй подход предполагает построение одноранговой сети доверия.

Инфраструктура PKI, основанная на сети доверия – это архитектура с максимально возможной степенью децентрализации, поскольку каждый регистратор (ЦА) непосредственно занимается сертификацией, а также проверкой сертификатов всех других участников системы (Рисунок 1.13) [39].

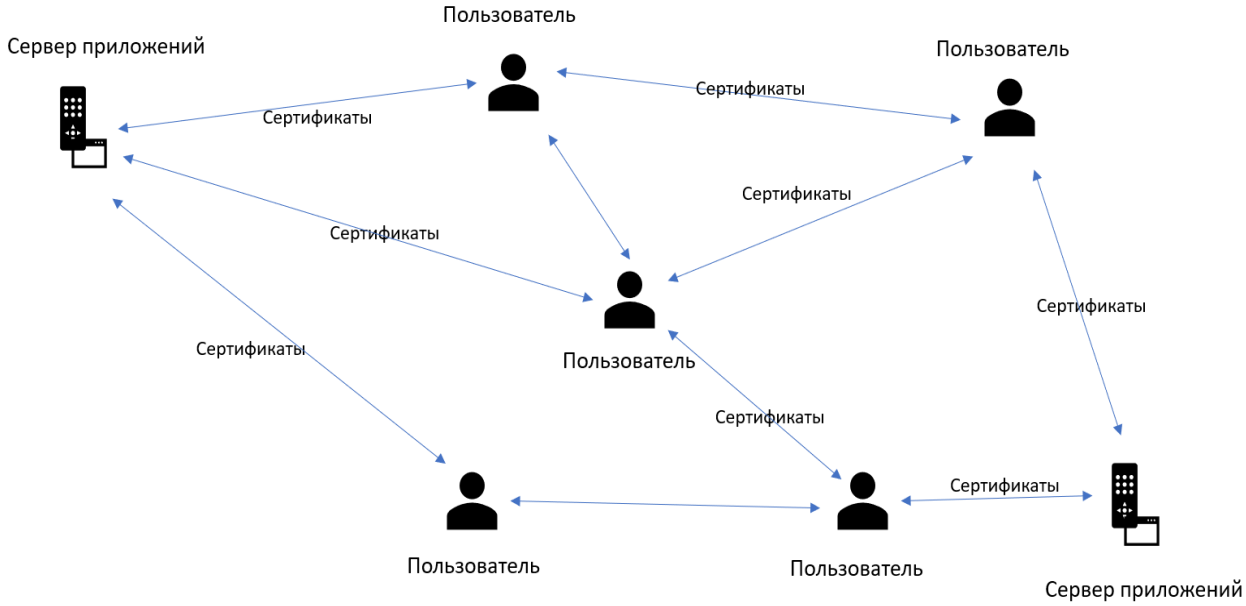


Рисунок 1.13. Подход Web-of-trust [62]

Этот подход позволяет решить проблемы иерархической модели инфраструктуры, а также повысить объективность информации об идентификаторах пользователей. Тем не менее, он гораздо менее гибок, поскольку все действия с валидным сертификатом (обновление, отзыв и т. д.) должны выполняться всеми узлами, хранящими его. Еще одно ограничение – сложность построения путей с высоким конечным уровнем доверия.

Децентрализованная система идентификации и сертификации состоит из следующих компонентов (Рисунок 1.14):

1. Центры идентификации.
2. Модули регистрации.
3. Хранилища персональных данных.
4. Распределенный реестр идентификаторов.
5. Приложения пользователей.

Фактически глобальная система цифровой идентификации является глобальным регистратором всех событий по типу «метки времени» (time stamp), связанных с подтверждениями персональных данных. При этом валидаторам не нужно достигать консенсуса относительно того какие данные проверены и подтверждены.

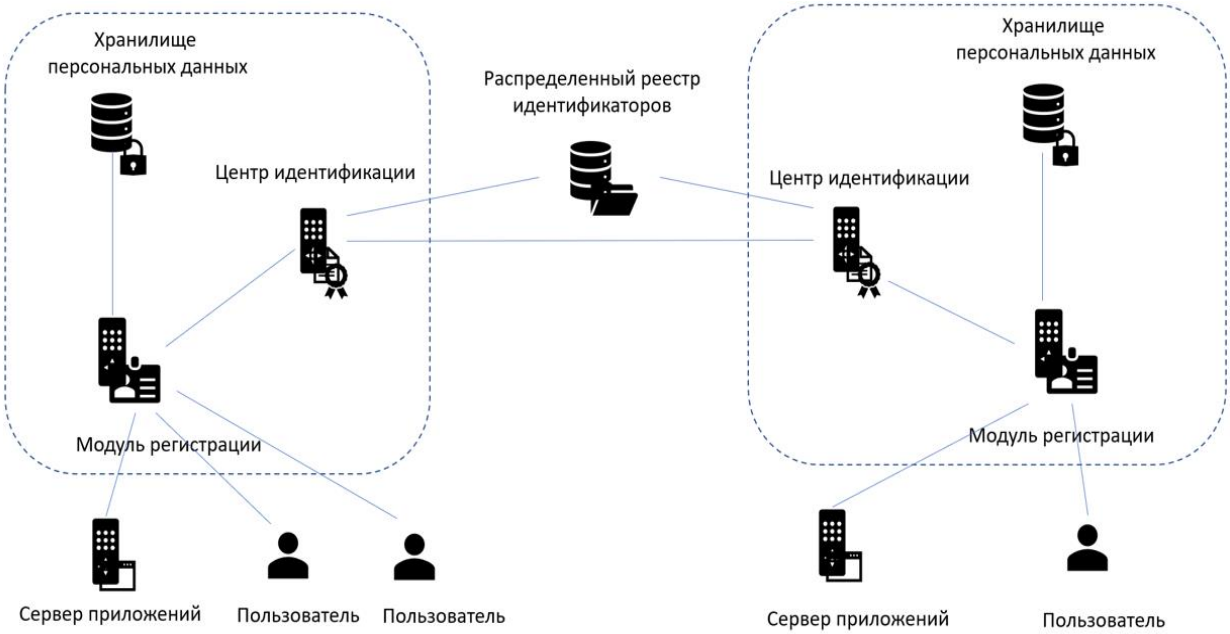


Рисунок 1.14. Компоненты децентрализованной системы идентификации

1.5.4. Инфраструктура KYC/AML

KYC – (Знай своего клиента / Know your clients) — это процесс, с помощью которого банки или другие финансовые организации получают информацию о своих клиентах и проверяют ее достоверность, сравнивая ее с многочисленными внешними списками и общедоступными базами данных. Следует назвать KYC набором процедур и инструментов, принципом в рамках общей политики AML [72].

AML – (Борьба с отмыванием денег / Anti-Money Laundering) процесс, который подпадет под KYC и включает регулярные проверки и постоянный мониторинг клиентов в части противодействия отмыванию денег, полученных преступным путем.

Основной принцип проверок KYC/AML заключается в том, что они не должны быть встроены в логику обработки транзакций, а должны действовать как внешние поставщики данных (оракулы), которые аутентифицируют каждое свое решение посредством совместной подписи транзакций

Сервисы AML\KYC должны быть построены по модели поставщиков данных (оракулов).

1.5.5 Децентрализованное хранение транзакций

После создания транзакции она отправляется ее валидаторам для подтверждения. Как только валидатор получает транзакцию он выполняет начальную проверку: правильно ли создана транзакция, может ли бы совершена данная транзакция в пользу ее участников, достаточный ли размер комиссии для проведения транзакции и т. д. Может существовать

всего один валидатор. В таком случае он самостоятельно проверяет и подтверждает все транзакции. Если валидаторов несколько, то после проверки транзакции одним валидатором она отправляется другому валидатору.

Формирование набора транзакций.

В каждый заданный период времени Валидатор создает набор транзакций, которые были получены с момента последнего согласования состояния реестра. В результате, каждый валидатор имеет свой собственный набор транзакций в любой конкретный момент времени. Затем узлы достигают консенсуса касательно набора транзакций, которые нужно подтвердить.

Принятие транзакций и изменение состояния реестра.

После достижения консенсуса набор транзакций, согласованный Валидаторами, изменяет состояние реестра. Если одна из транзакций не может быть выполнена, весь набор транзакций отклоняется. После согласования и принятия всех новых транзакций Валидаторы формируют новое состояние реестра, с которым согласны все. Транзакции хранятся в связанной форме, что обеспечивает целостность их истории.

Хранилище транзакций.

Главный реестр транзакций реализует связанную структуру наборов транзакций. Каждый новый набор определяет новое состояние ядра по отношению к предыдущему состоянию. Здесь целостность реестра обеспечивается посредством связей между наборами транзакций (каждый следующий криптографически связан с предыдущим). В дальнейшем это позволяет проводить постоянную проверку базы данных и истории всех транзакций, содержащихся в ней, в реальном времени. Первичная база данных хранит все данные, проходящие через ядро.

Как наборы транзакций связываются друг с другом.

Каждый набор транзакций содержит ссылку на предыдущий набор. В качестве ссылки используется уникальный идентификатор (хэш предыдущего набора транзакций) (Рисунок 1.15). Если кто-то попытается изменить один из наборов транзакций, все дальнейшие наборы также должны быть изменены (поскольку они больше не смогут ссылаться на предыдущие наборы).

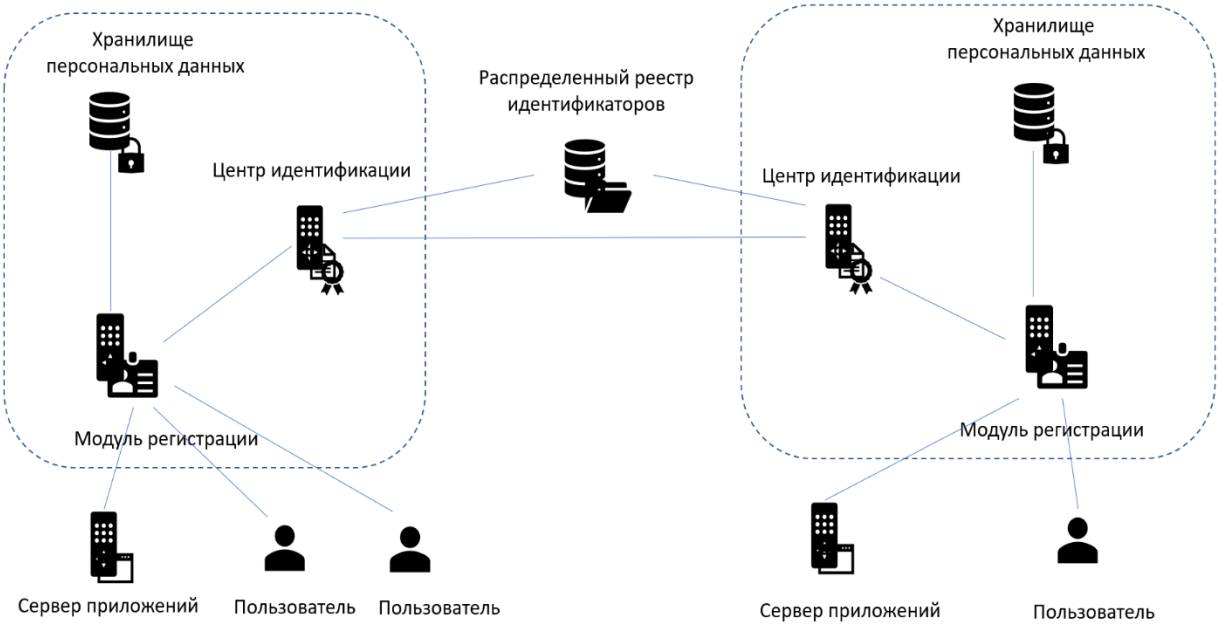


Рисунок 1.15. Связанные наборы транзакций

Изменение хотя бы одной транзакции из прошлого приведет к цепной реакции: все дальнейшие наборы данных будут в конечном итоге изменены. Это обеспечивает целостность данных реестра.

Каждый Валидатор хранит полную историю наборов транзакций. Сохранение этой истории упорядоченной (наборы транзакций связаны друг с другом при помощи хэшей) позволяет валидаторам восстанавливать соответствующее состояние реестра в случае ошибок.

Доступ к состоянию реестра и всем наборам транзакций может получить кто угодно (если система открыта) или только владелец и валидаторы конкретной ПС. Клиенты\пользователи ПС могут связываться с валидаторами через подписанные запросы и получать связанные транзакции и текущее состояние балансов.

1.5.6 Инфраструктура валидаторов. Подходы к достижению консенсуса

Под консенсусом понимается условия, при которых данная транзакция признается валидной и, соответственно, юридически значимой.

Существует различные модели консенсуса для распределенных систем [24]:

- Мультиподпись.
- Proof-of-work.
- Proof-of-stake.
- Byzantine fault tolerance.

– Federated byzantine agreement.

Мультиподпись.

Чтобы подтвердить транзакцию и последующее обновление состояния реестров участвующих сторон на основании этой транзакции, валидатор(ы) должны непосредственно подписать транзакцию, на основании которой будут изменены реестры. Валидатор может быть один или несколько, возможен вариант, когда транзакция является валидной если ее подписало минимально оговоренное количество валидаторов.

Proof-of-work.

Модель Proof-of-work предполагает, что валидаторы для выражения своего мнения (валидации) должны предоставить решение сложной, вычислительно-ресурсоемкой задачи. Факт решения задачи может быть проверен любым участником. В криптовалютных системах для этого используется задача на нахождение хэш-функции с определенными свойствами. Этот подход особенно хорошо подходит для систем с неограниченным количеством валидаторов, кроме этого, он позволяет сохранить анонимность. Каждый участник системы может самостоятельно проверять транзакции [24].

Proof-of-stake.

Модель Proof-of-stake является альтернативным подходом, когда валидаторы должны обладать определенным «весом» в данной системе. Этот алгоритм обеспечивает значительно более высокую пропускную способность системы по сравнению с Proof-of-work [24].

Byzantine fault tolerance (BFT).

Метод (BFT), предполагает работу с предопределенным набором валидаторов, которые всем известны и которые контролируют друг друга.

Для достижения консенсуса валидаторы обмениваются друг с другом подписанными сообщениями, содержащими транзакции, которые они считают правильными. В начале каждого нового этапа выбирается лидер, который предлагает набор транзакций, которые считает достоверными. Дальнейшие итерации представляют собой обмен сообщениями между валидаторами [24].

Federated byzantine agreement (FBA).

Метод FBA построен на достижении консенсуса в пересечении групп, члены которых достигают соглашения только друг с другом, но так как участники могут одновременно принадлежать к нескольким отдельным группам, консенсус достигается во всей сети. FBA избавляет от проблем с масштабируемостью, свойственных BFT, позволяя новым узлам

присоединяться к системе, когда она уже работает. Однако, только те узлы, которым доверяют другие, могут стать валидаторами [24].

1.5.7 Смарт-контракты

Смарт-контракты — это цифровые протоколы для передачи информации, которые используют математические алгоритмы для автоматического выполнения транзакции после выполнения установленных условий и полного контроля процесса.

Другое определение, данное Ником Сабо: смарт-контракт представляет собой «набор обещаний, указанных в цифровой форме, включая протоколы, в рамках которых стороны выполняют эти обещания» [156]. Другими словами, смарт-контракт – это:

- условия в виде компьютерного кода которые могут быть проверены и выполнены программно;
- компьютерный код, который выполняет код смарт-контракта;
- база данных прав собственности на активы сторон договора в виде распределенного реестра, которую все вовлеченные в исполнение смарт-контракта стороны считают достоверным источником данных.

Жизненный цикл смарт-контракта [154]:

- создание контракта, включая установление условий;
- предварительный аудит и тестирование;
- подписание контракта сторонами;
- подтверждение и выполнение контракта валидаторами;
- обновление состояния реестров в учетных системах сторон контракта, в нашем случае - в ПС.

Схематично работа смарт-контракта изображена на Рисунке 1.16.

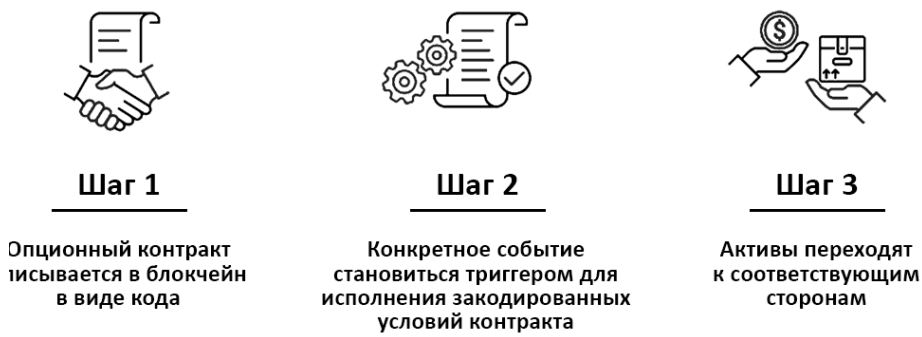


Рисунок 1.16. Этапы работа смарт-контракта [154]

Условия смарт-контракта всеми его сторонами должны приниматься как окончательные и неотрекаемые. По сути, смарт-контракт автоматизирует процесс перераспределения оцифрованных активов. Выполнение контракта зависит от заранее определенных условий, подписанных сторонами контракта, которые проверяются автоматически через механизм оракулов.

Главным преимуществом смарт-контрактов является то, что они устанавливают условия, подтверждаемые третьими независимыми сторонами в автоматическом режиме.

1.5.8. Единая точка входа

Технология единой точки (single sign-on) – это возможность одноразовой аутентификации пользователя с дальнейшим доступом к необходимым ресурсам [129].

На практике это приложение, которое хранит ключи/пароли пользователя и после авторизации пользователя автоматически вводит эти данные в соответствующие поля или подписывает сообщение и проводит аутентификацию пользователя в разных системах, в частности в ПС [147, 150].

Концепция децентрализованной системы идентификации расширяет этот подход. Приложение пользователя должно является хранилищем его приватных ключей, а децентрализованная структура – источником информации о них. Каждый пользователь обладает унифицированным идентификатором и ключами. Для доступа к сервисам, например, ПС он отправляет свой идентификатор и подписывает соответствующий запрос из своего приложения. ПС проверяет, имеет ли клиент соответствующие разрешения и получена ли подпись с использованием соответствующих ключей.

Пользователь запускает приложение, аутентифицируется, получает доступ к своим ключам. Дальнейшие запросы к ПС подписывает приложение, хранящее ключи (Рисунок 1.17).

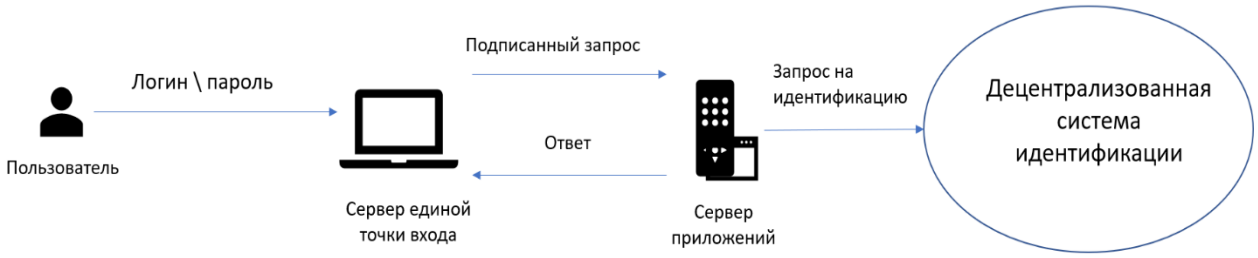


Рисунок 1.17. Технология единой точки входа

1.6 Выводы по Главе 1

В первой Главе дан обзор характеристик интероперабельных систем и были проанализированы стандарты интероперабельности и безопасности интероперабельных систем.

Но данные подходы не удовлетворяют в полной мере требования к перспективной архитектуре платежных интероперабельных систем в части:

- наличия единого механизма идентификации пользователей и всех участников системы;
- наличия единого криптографического механизма для аутентификации, инициирования и подтверждения любых действий в системе;
- распределенное хранение данных в рамках децентрализованных систем;
- возможность внешнего криптографического аудита данных и бизнес-процессов;
- использование унифицированных и стандартизованных наборов протоколов с открытым исходным кодом для обмена и хранения информации о транзакциях. Протоколы должны поддерживать обработку транзакций, совместимы с системами идентификации, поддерживать интеграцию внешних поставщиков KYC/AML услуг и обеспечивать доказуемую завершенность транзакций и свойство неотрекаемости.

Вышеперечисленные требования обеспечивает построение архитектуры построения интероперабельных платежных систем на базе технологии распределенных реестров, что и было предложено в 1-й Главе. Предлагаемая архитектура позволяет решить следующие задачи:

- обеспечить полную функциональную и иную совместимость локальных, региональных и международных платежных информационных систем;
- обеспечить надежность и безотказность функционирования платежной системы, не уступающую традиционной платежной системе, основанной на материальных носителях;
- существенно, в разы, снизить стоимость комиссий для транзакций, что особенно важно – для микроплатежей [146];
- обеспечить онлайновую проверку законности как самой транзакции, так и легитимность ее участников;
- существенно увеличить скорость прохождения транзакций за счет прозрачных методов контроля и достижения консенсуса;
- реализовать возможность проведения регулярных онлайновых, внешних по отношению к платежной системе, криптографических аудитов, гарантирующих

качество и корректность как бизнес-процессов, так и достоверности финансовой информации;

- существенно увеличить скорость вывода на рынок новых платежных сервисов и систем за счет существенного снижения трудоемкости и скорости интеграций как между ПС, так и между внешними критическими инфраструктурными элементами глобального платежного рынка.

Главным инструментом неотрекаемости и достоверности в интероперабельных платежных системах является использование криптографических алгоритмов. Однако, в связи с возможной квантовой революцией возможна компрометация криптографических методов защиты информации в следствии возможной недостаточной вычислительной сложности математической задачи для квантовых компьютеров, лежащей в основе криптографических методов защиты информации.

Для решения данной задачи предлагается:

- рассмотреть криптографические методы защиты информации, с выделением их плюсов и минусов;

- применить подход формантного анализа (ФА) и теории чисел как эволюционный путь для развития средств криптографической защиты на основе модификации алгоритма RSA.

2 ОПИСАНИЕ И МОДЕЛИРОВАНИЕ КРИПТОПРОЦЕССОВ

2.1 Задачи, области применения и основные типы криптографических алгоритмов

Широкое распространения и развития компьютерных технологий, информационных сетей, электронных платежных систем и электронной коммерции привели к возникновению острой необходимости в гарантированной защиты информации и вызвали значительный интерес во всем мире к эффективно лучшим методам защиты и проблемам её стандартизации, как для компаний, оказывающей информационные и другие подобные услуги, так и для потребителей таких услуг [10, 25, 34, 35].

При обработке компьютерных данных криптографическая защита используется в трех практических случаях:

- при передаче данных;
- при хранении информации;
- для аутентификации пользователей информации, ограничения и контроля доступа к ней.

Шифрование данных наиболее часто используется при передаче информации по различным сетям связи и при обработке компьютерных данных в распределенных системах[1]. В этом контексте компьютерная, и другая на ее основе сеть, могут рассматриваться как некоторая универсальная среда для распространения и передачи информации (данные, изображения, речь, звук и т.д.) что, например, привело к развитию IP-телефонии (VoIP – Voice over IP), которая сегодня широко используется в бизнесе различного приложения. Особенности, достоинства и проблемы IP-телефонии заключаются в самом протоколе IP. Потому, что он изначально был разработан, как открытый протокол, сразу же не учитывающий вопросы безопасности и атаки вандального характера, на обычные IP-сети, которые практически без изменений могут быть направлены и на сети VoIP. Поэтому вопросы развития криптографической защиты для развития инфраструктуры IP-телефонии являются одной из важных областей их применения.

Шифрование данных, хранящихся на различных носителях информации, является другой важной областью применения криптографической защиты, которая может

[1] Понятия распределенных, открытых и других типов и классов систем, (сетей), включая информационные, не является предметом наших исследований и считаются изаестными по определению классической или Общей Теории систем и соответствующих научных направлений.

предусматривать и одновременную возможность обработки зашифрованных данных. Поэтому сегодня особенно актуальны и задачи совместного использования как шифрования, так и принципов аутентификации пользователей, и контроля доступа, которые, несомненно, выдвигают дополнительные требования и к криптографическим преобразованиям [2, 47, 49, 52, 61, 98].

Возможность аутентификации пользователей в системе особенно важна, если используются удаленные терминалы и личные устройства. Процедуры аутентификации, защищенные криптографическими методами и средствами, приобретают дополнительную важность в связи с широким развитием электронной коммерции и необходимостью заключения коммерческих и деловых контрактов с помощью компьютеров, которые, как правило, реализуются на базе следующих способов [12, 32, 44, 51, 65, 81, 96, 145]:

– парольная аутентификация;
– аутентификация по OpenID;
– аутентификация с помощью биометрических характеристик;
– аутентификация при помощи одноразовых паролей;
– аутентификация при помощи открытого ключа.

Широкое развитие компьютерных и коммуникационных технологий стало возможным и в ситуациях, когда стороны, обменивающиеся электронными данными, не доверяют друг другу, что привело к созданию механизма электронной цифровой подписи. Началу этой технологии послужило открытие двух ключевой криптографии, сделанное американскими математиками-исследователями Диффи и Хеллмана в 70-е годы прошлого столетия [26, 71].

Криптографические методы защиты информации используются для обеспечения безопасности передачи, воспроизведения и хранения электронных данных [2]. Поставленная цель достигается путем преобразования некоторого «исходного смысла - или командно-содержащего текста» в случайную последовательность данных (т.н. «шифр текст»), причем - таким способом или процедурами, чтобы обеспечивалась невозможность несанкционированного восстановления изначального текста [162].

Криптосистема состоит из элементов, выполняющих преобразования «электронного текста» и множества ключей, являющихся параметрами преобразования. Знание используемых ключей дает возможность дешифровать «шифр текст».

Схема (алгоритм, принцип действия) криптографической защиты.

База современной криптографии была положена работой Шеннона [132], который рассматривает шифрование как отображение исходного сообщения *M* в зашифрованное *Y*, и когда шифрование реализуется на базе функции *E*, таким образом

$$Y=E_K(M), \tag{2.1}$$

где индекс k - соответствует конкретному ключу.

Основное правило криптографии гласит что исходное сообщения должно быть однозначно восстановимо по шифрованному тексту, и это значит, что функция *E* является обратимой и односторонней функцией, то есть, что значит, что (2.1) должна быть простой операцией, а процедуры нахождения *M* по *Y* должны быть трудным процессом. Обратимость функции *E* означает что должно существовать единственное обратное отображение E_k^{-1} такое, что

$$E_k E_k^{-1} = I,$$

где $I = E_k^{-1}(Y)$.

Таким образом, процесс шифрования состоит из выбора ключей $k \in K$ и отображения открытого текста при помощи функции *E* в элементы множества *Y*. Выбранный ключ k является секретным, но множество функций и соответствие между *K* и этим множеством является несекретно.

Шифры – весьма разнообразны и по методам работы с исходными данными в процессе шифрования делится на:

- **блочные шифры**, которые оперируют блоками данных фиксированной длины;

- **поточные шифры,** в которых каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости от используемого ключа, и от расположения в потоке открытого текста [17].

Методы шифрования, по методам работы с ключами следует разделить на два класса - симметричное шифрование (с секретным ключом) и асимметричное шифрование (с открытым ключом) [19, 29].

Симметричный шифр предусматривает передачу информации, в которой зашифровываемый и расшифровываемый ключи совпадают, соответственно стороны обменивающимися зашифрованными данными должны знать общий секретный ключ.

Асимметричный шифр предусматривает передачу информации, в которой зашифровываемый и расшифровываемый ключи не совпадают, причем знание одного ключа не дает практической возможности определить другой.

Самые известные ассиметричные шифры: RSA, DSA, EGSA, ECC [34-36], Ранцевые алгоритмы, ГОСТ Р 34.10-94 (Российский стандарт схожий с DSA), ГОСТ Р 34.10-2001 (Российский стандарт схожий с ECC) [36].

Таким образом, любой шифр можно классифицировать по двум составляющим **блочный\поточный** и **симметричный\асимметричный**.

В 1990-е гг. Наором и Юнгом были разработаны методы шифрования при помощи особого класса функций – хэш-функций (Hash Function) [37]. *Хэш-функция* – это односторонняя функция реализуемая, как правило, средствами симметричного шифрования со связыванием блоков, переводящие произвольную бинарную последовательность данных в последовательность определённой длины. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции. На вход функции подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$– дайджест сообщения. Проверяемые данные обозначается через M' и контроль целостности данных сводится к проверке $h(M)= h(M')$, если равенство выполняется, то $M=M'$. Криптостойкость этого метода состоит в невозможности подобрать M', который обладал бы требуемым значением хэш-функции. Параметры вычисления хэш-функции h являются семейством ключей $\{K\}^N$ [37, 88].

2.2 Алгоритмы шифрования

Алгоритмы блочного шифрования – алгоритмы симметричного шифрования, который преобразуют входные данные в выходные зашифрованные последовательности (блоки), таким образом, что каждый бит выходного блока зависит от каждого бита входного блока [88].

Схема блочного шифрования состоит из двух взаимосвязанных алгоритмов шифрования и расшифрования. Входными данными служит блок размером n бит и ключом размера m бит.

Каждый входной блок X преобразуется в выходной блок Y, размером n бит при помощи функции шифрования E:

$$Y = E_k(X),$$

где индекс k - соответствует конкретному ключу.

Функция дешифрования - обратная E, обозначается через E^{-1}

$$X = E_{k'}^{-1}\big(E_k(X)\big).$$

Очевидно, что шифр будет работать тогда и только тогда, когда каждому ключу K, будет являться однозначным отображения

$$\{E_k, k \in K\} = \{E_{k'}^{-1}, k' \in K\}.$$

В данном случае возможна ситуация, когда для данного k легко вычисляются ключ k' и E_k, или вычисление k' сложно, как восстановление соответствующего открытого текста на основе данного шифртекста Y.

Размер блока n это фиксированный параметр блочного шифра, обычно равный 64 или 128 битам, хотя некоторые блочные шифры могут использовать другие значения [17].

Классические примеры потоковых шифров – DES, 3DES, AES, IDEA, RC5.

Преимущества блочного шифрования:

1. Высокая степень распространения: информация, состоящая из одного символа открытого текста, распространяется на несколько символов зашифрованного текста.
2. Невосприимчивость к взлому: сложно вставить символы без того, чтобы эти действия были необнаруженными.

Недостатки блочного шифрования:

1. Блочные шифры обычно требуют больше памяти.
2. Ошибка в одном символе может повредить весь блок.
3. Процесс шифрования сравнительно медлен: перед началом шифрования/дешифрования должен быть задан весь блок данных.

Алгоритмы поточного шифрования - алгоритмы симметричного шифрования, которые преобразуют каждый символ открытого текста M в символ шифрованного последовательно по 1 биту m_1, m_2,…m_n и зависящий от ключа и расположения символа в тексте.

Генератор ключевой последовательности выдает последовательность бит k_1, k_2,…,k_n и эта ключевая последовательность складывается по модулю 2 с последовательностью бит исходного текста m_1, m_2,…m_n для получения шифрованного текста

$$c_i = m_i \oplus k_i, i = \overline{1,n}.$$

Что бы получить исходный текст, на приемной стороне шифрованный текст складывается по модулю 2 с идентичной ключевой последовательностью:

$$c_i \oplus k_i = m_i \oplus k_i \oplus k_i = m_i, i = \overline{1,n}.$$

Классические примеры потоковых шифров – шифр Вернама, или одноразовый блокнот, Salsa20, ChaCha20, RC4, A5.

Стойкость системы полностью зависит от структуры генератора ключевой последовательности.

Преимущества поточного шифрования

1. Потоковые шифры требуют меньше памяти для вычислений.

2. Поточное шифрования наиболее пригодно для шифрования непрерывных потоков данных.
3. Потоковые шифры работают быстрее, чем блочные шифры, за счет побитной обработки потока данных.
4. Низкое распространение ошибок: ошибка в шифрование одного символа, скорее всего, не повлияет на последующие символы.

Недостатки поточного шифрования:

1. Потоковые шифры не обеспечивают защиту целостности данных и не используются для аутентификации.
2. Восприимчивость к вставкам/модификациям: перехватчик, нарушающий алгоритм, может вставить ложный текст, который выглядит аутентичным.
3. Потоковые шифры труднее реализовать правильно.

2.3 Алгоритмы с открытым ключом

Идея криптографии с открытым ключом была предложена Диффи и Хеллман в 1971 году и основана на применении односторонних функции с секретом, что позволяет двум пользователям обмениваться ключом по уязвимым каналам, не имея никаких предварительных договоренностей [30].

В системах с открытым ключом (ассиметричные криптосистемы) используются два ключа:

- Открытый ключ E_{k1} для шифрования исходного сообщения X:

$$E_{k1}(X)=Y,$$

где Y зашифрованное сообщения, k_1 – открытый ключ.

- Секретный ключ D_{k2} для дешифрования:

$$D_{k2}(Y)= D_{k2}(E_{k1}(X)) =X,$$

где k_2 – секретный ключ.

В системах с открытым ключом пользователи могут эффективно вычислить оба ключа E_{k1} и D_{k2}, но знание E_{k1} не дает возможности также эффективно вычислить D_k.

Асимметричные алгоритмы основываются на ряде известных математических задач высокой сложности, на которых и базируется их стойкость. Но несмотря на все преимущества криптосистем с открытым ключом, эти алгоритмы не могут конкурировать по быстродействию с криптосистемами с секретным ключом.

Наиболее распространённые криптосистемы с открытым ключом: рюкзачная криптосистема (Knapsack Cryptosystem); криптосистема RSA; криптосистема Эль-Гамаля –

EGCS (El Gamal Cryptosystem); криптосистема, основанная на свойствах эллиптических кривых – ECCS (Elliptic Curve Cryptosystems). Кроме того, криптосистемы с открытым ключом используется не только для шифрования, но также и для создания цифровых подписей и других задач.

Преимущества:

1. Асимметричное шифрование обеспечивает платформу для безопасного обмена информацией без необходимости совместного использования и передачи закрытых ключей.
2. Основным преимуществом в асимметричных криптосистемах является повышенная безопасность.
3. В асимметричных криптосистемах пару (*E, D*) можно не менять значительное время.
4. Криптостойкость алгоритмов полагается на вычислительную сложность алгоритмов, а не на конфиденциальность задействованного ключа.

Недостатки:

1. Асимметричные криптосистемы требуют больших вычислительных ресурсов.
2. Асимметричное шифрование проигрывает в скорости симметричному шифрованию.

2.3.1 RSA-алгоритм

Алгоритм шифрования с открытым ключом Ривеста, Шамира и Адельмана (RSA) стоит у истоков стойкой криптографии и основан на том факте, что разложение большого числа на множители является очень сложной вычислительной задачей. RSA- алгоритм используется в самых различных информационных технологиях и продуктах, на различных платформах и во многих отраслях производственной и общественной деятельности людей. Его эффективность базируется на сложности (предполагаемой) задачи факторизации [7, 15, 16, 27, 56, 127].

Для определения RSA-алгоритма необходимо тщательно выбрать два больших простых числа p и q, которые засекречиваются. Их произведение $r=pq$ несекретно и может быть использовано в качестве элемента открытого ключа, но производное число $f(r)=(p-1)(q-1)$, называемое функцией Эйлера $\varphi(n)$, также секретно.

Алгоритм основан на некоторых математических фактах, а именно, функция Эйлера $\varphi(n)$ натурального аргумента n, равна количеству натуральных чисел, не больших n и

взаимно простых с ним, которую представляется в виде так называемого произведения Эйлера:

$$\varphi(n) = n\prod_{p|n}(1-\frac{1}{p}),$$

где p — простое число.

Тогда по формуле Эйлера

$$a = 1 \bmod r, \tag{2.2}$$

где a относительно простое, а $f(r)$– это функция Эйлера.

Выбирается большое случайное число E_k, которое взаимно простое с $f(r)$ и вычисляется секретное число D_k, таким образом что

$$E_k \cdot D_k = 1 \bmod f(r), \text{ где } r \equiv n. \tag{2.3}$$

Числа E_k и n это открытые ключи, а D_k – закрытый ключ.

Чтобы зашифровать сообщения X, отправитель возводит сообщения X в степень E_k по модулю n:

$$Y = X^{E_k}\ (mod\ n).$$

Расшифровка сообщения Y вычисляется по следующей формуле:

$$X = Y^{D_k}\ (mod\ n).$$

Существует ряд математических задач, связанных с использованием RSA-алгоритма [89]:

- числа p, q должны быть большими, обычно порядка не ниже 2^{256};
- выбор чисел E_k и D_k должен соответствовать уравнению (1.3);
- разность $|p\text{-}q|$ -должна быть достаточно большим числом;
- процесс нахождения больших простых чисел является задачей, требующей проверки чисел на простоту [28].

Преимущества системы RSA:

1. Зная только открытый ключ и зная алгоритм шифрования, невозможно расшифровать сообщение.
2. Высокая криптостойкость алгоритма, которая основана на трудностях факторизации большого натурального числа.

Недостатки системы RSA:

1. Скорость шифрования весьма низкая.
2. Алгоритмы шифрования требуют больших вычислительных ресурсов.

3. Данные, передаваемые с использованием алгоритма RSA, могут быть скомпрометированы через посредников, которые могут вмешаться в систему открытых ключей.
4. Длина ключей RSA превышает длину ключей в симметричных криптографических системах.
5. Для генерации ключей RSA требуется больше времени.
6. На данный момент существует проблема что в будущем для алгоритма RSA, возникшая вследствие быстрого развития вычислительной мощности и появления так называемых квантовых компьютеров, реализующих квантовое превосходство, а именно - через некоторое время решение задачи разложения большого составного числа на множители уже перестанет быть нерешаемой для будущего текущего уровня вычислительной мощности компьютеров.

Реальность угрозы применения классической криптографии в финансовой сфере была проанализирована американской компанией ASC X9, разрабатывающая глобальные финансовые стандарты, в том числе в области криптографической защиты данных. В 2019 году организация выпустила информационный отчет «Риски квантовых вычислений для индустрии финансовых услуг» [83] в котором приведен прогноз роста числа кубитов квантовых компьютеров и, соответственно, для какой длины ключа классических криптоалгоритмов это представляет риски для компрометации, Рисунок 2.1 [83].

Данный прогноз показывает, что при достижении числа кубитов квантового компьютера 2500 классическая криптография с длиной 2048 бит оказывается под риском компрометации. В соответствии с прогнозом ASC X9 подобная ситуация может случиться до конца текущего десятилетия.

Более свежие исследования показывают, что время наступления квантового превосходства для классических систем криптографии может произойти еще раньше. В частности, в статье, опубликованной в августе 2022 года [58] учеными Лос-Аламосской национальной лаборатории США теоретически доказана возможность достижения квантового превосходства для целей машинного обучения искусственного интеллекта за счет упрощения Гильбертова пространства до количества точек, равных числу параметров используемой математической модели. Для большинства моделей число параметров приблизительно равно числу кубитов. Это означает что, если в классическом подходе Гилбертово пространство для 30 кубитов состояло из миллиардов состояний что, соответственно, при обучении модели поиска в этом пространстве требовало миллиарда точек данных. При новом подходе для квантового компьютера с 30 кубитами потребуется

около 30 точек данных. Все это означает, что мы все ближе к практической реализации квантового превосходства.

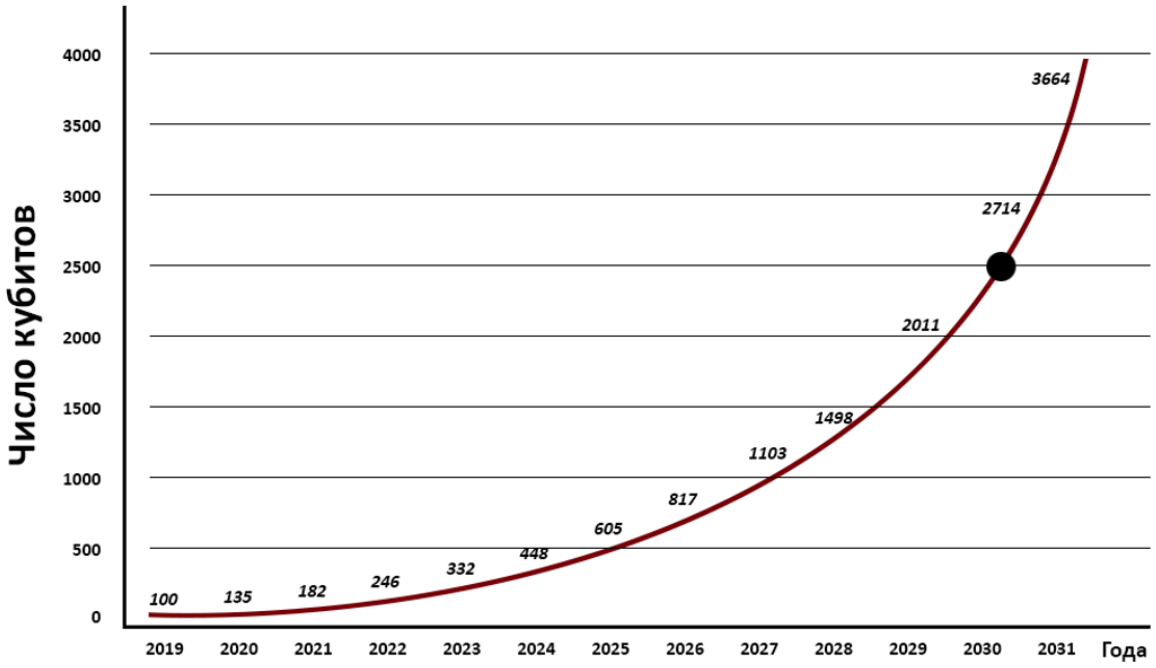


Рисунок 2.1. Прогноз роста числа кубитов в квантовых компьютерах и рисках компрометации алгоритма RSA для разной длины ключа по версии ASC X9

2.3.2 Ранцевый алгоритм

Этот алгоритм был одни из первых алгоритмов с открытым ключом предложенный Мерклом и Хеллманом и основанным на классической задаче теории чисел, но как в последствии оказался не надёжн. Алгоритм базируется на идее шифрования сообщения на основе решения задачи по укладке рюкзака: дан вес рюкзака и вес предметов и нужно найти такой набор предметов, чтобы рюкзак был полностью заполнен [20].

Перед началом шифрования, сообщение сначала разбивается на блоки $X=(x(1),...,x(n))$ по размерам равные числу элементов последовательности в рюкзаке, выбирается открытый ключ $A=(a(1),...,a(n))$ и шифруется сообщения следующим образом:

$$Y = \sum_{i=0}^{n} a(i)x(i) = a(1)x(1) + ... + a(n)x(n).$$

Возможность восстановления X с помощью Y может быть получена благодаря закрытому ключу, который представляет пару чисел (t, r). Расшифровка сообщения Y вычисляется по следующей формуле:

$$tY = \sum_{i=0}^{n} ta(i)m(i)(mod\ r).$$

Преимущества системы заключается в высокой скорости шифрования и дешифрования.

Недостаток системы в том, что она уязвима для атак, имея слабые места в преобразовании, что позволяет восстановить быстрорастущую последовательность рюкзака из нормальной [20, 29].

2.3.3 DSA-алгоритм

DSA (англ. Digital Signature Algorithm — алгоритм цифровой подписи) — разработанный Национальным Институтом Стандартов и Технологий США (NIST) в качестве альтернативы алгоритму RSA, который обеспечивает ту же степень безопасности, но использует другие математические алгоритмы для шифрования [30, 41].

Генерация ключей DSA

При вычислениях используются большие целые простые числа: g и p, длиной L битов каждое ($512 < L < 1024$); q - простое число длиной 160 бит (делитель числа (p - 1)). Числа g, p, q являются открытыми и могут быть общими для всех пользователей сети.

Отправитель выбирает случайное целое число x, $1 < x < q$, которое является секретным ключом для формирования электронной цифровой подписи. Затем отправитель вычисляет значение $y = g^x \bmod p$, которое является открытым ключом для проверки подписи и передается всем получателям документа.

Генерация подписи DSA

Этот алгоритм предусматривает использование односторонней функции хеширования SHA-1. Для того чтобы подписать сообщение M выполняются следующие шаги:

1. Выбирается случайное целое число $к$ в интервале [1, q - 1], которое уникально для каждого сообщения M.

2. Вычисляется $r = (g^k \pmod p) \bmod q$.

3. Вычисляется $k^{-1} \bmod q$.

4. Вычисляется $s = k^{-1}\{h(M) + x.r\} \bmod q$, где h есть алгоритм хеширования SHA-1.

5. Если $s = 0$ тогда возврат к шагу 1.

6. Подпись для сообщения M есть пара целых чисел (r, s).

Проверка подписи DSA

Для проверки подписи (r, s) сообщения M, получатель выполняет следующие шаги:

1. Вычисляются

$$w = s^{-1} (mod\ q).$$

3. Вычисляется значения:

$$u_1 = (w \cdot h(M)) \bmod q,$$

$$u_2 = (w \cdot r) \bmod q.$$

4. Используя открытый ключ *y,* вычисляет значение

$$r' = (g^{u1} y^{u2} mod\ p) mod\ q.$$

5. Если *r*=*r*’ подпись под документом *M* является подлинной.

Преимущества системы DSA:

- Стойкость алгоритма подписи DSA определяется сложностью решения задачи дискретного логарифмирования.

- Только одна сторона может создать подпись, но любая другая сторона может проверить подпись с помощью открытого ключа.

- DSA требует меньше цифровых ресурсов для работы, по сравнению с другими алгоритмами.

- Высокий уровень защиты.

Недостатки системы DSA:

- Скорость вычисления подписи очень низкая, при подписывании и при проверке подписи приходится выполнять сложные операции деления по модулю что не позволяет получать максимальное быстродействие.

- Данные в DSA не зашифрованы.

- DSA зависит от SHA1. Следовательно, любое ограничение или проблема, связанная с этим, отражается в DSA.

2.4 Симметричное шифрование

Системы с симметричным шифрованием — предусматривают шифрованияе/дешифрование данных при использовании одного и того же ключа. Для реализации такого шифрования/дешифрования должен существовать надежный канал, по которому происходит предварительный обмен секретными ключами [36]. Современные симметричные алгоритмы считаются надежными, если отвечают следующим требованиям:

- Выходные данные не должны содержать статистических паттернов исходных данных.
- У одного из его законных участников должен быть генератор, формирующий ключи, обеспечивающие гарантированную стойкость системы.

Современные симметричные алгоритмы для обеспечения надежности, используют комбинацию операций подстановки и перестановки, поочередно повторяя их. Самые известные симметричные шифры: DES, AES, ГОСТ 28147-89, RC5, Blowfish, Twofish.

Преимущества:

1. Симметричная криптосистема работает быстрее чем асимметричная.

2. В симметричных криптосистемах зашифрованные данные могут передаваться по ссылке, даже если есть вероятность перехвата данных.

3. Симметричная криптосистема использует аутентификацию по паролю для подтверждения личность получателя.

4. Только система, владеющая секретным ключом, может расшифровать сообщение.

Недостатки:

1. Обмен зашифрованными данными и ключами. Секретный ключ должен быть передан принимающей системе до того, как фактическое сообщение будет передано и единственный безопасный способ обмена ключами - это обмен ими лично.

2. Невозможно использовать для цифровых подписей.

2.4.1 Алгоритм DES

DES (англ. Data Encryption Standard) — алгоритм для симметричного шифрования, утверждённый правительством США в 1977 году как официальный стандарт шифрования.

Для шифрования DES обычно данные шифруются поблочно, перед шифрованием любая форма представления данных преобразуется в числовую, и на вход шифрующей функции поступает блок данных размером 64 бита и генерируется 64-битовый зашифрованный текст и наоборот, получив 64 бита зашифрованного текста, он выдает 64 бита расшифрованного, в процессе шифрования и дешифрования применяется один и тот же 56-битовый ключ. Процесс шифрования состоит из двух перестановок, которые называют начальной и финальной перестановками, и 16 раундов Фейстеля, где каждый раунд использует различные 48-битовые ключи [88].

Основные этапы алгоритма, следующие:

1. Разделение текста на блоки размером 64 бита (8 октетов).

2. Первичная перестановка блоков.

3. Разбивка блоков на две части: левую и правую, названные L и R.

4. Шаги перестановки и замены, которые повторяются 16 раз (так называемые раунды).

5. Повторное соединение левой и правой частей, затем обратная начальная перестановка.

Преимущества системы DES:

1. Для шифрования и дешифрования используется один и тот же алгоритм, и выполняется путем повторения операций шифрования в обратной последовательности.

2. Достаточно высокая стойкость алгоритма.

Недостатки системы DES:

1. Ограничения данного алгоритма является размер ключа (56 битов), что снижает его стойкость, проявляющуюся в том, что в результате атаки грубой надо проверить всего 2^{56} ключей.

2. DES с программным обеспечением работает медленнее чем аппаратная реализация.

3. В DES только один закрытый ключ, который используется как для шифрования, так и для дешифрования, поэтому, при потере ключа, расшифровать данные на принимающей стороне становится невозможным.

2.4.2 Алгоритм AES

В 2001 году Национальное бюро стандартов США утвердило новый стандарт симметричного шифрования - AES (Advanced Encryption Standard). В результате AES обеспечивает лучшую защиту чем алгоритм DES, так как использует 128-битные ключи (а также может работать со 192- и 256-битными ключами) и имеет более высокую скорость работы, шифруя за один цикл 128-битный блок в отличие от 64-битного блока DES. В настоящее время AES является наиболее распространенным симметричным алгоритмом шифрования [20].

Алгоритм AES оперирует байтами, то есть числами от 0 до 255, все байты в AES интерпретируются как элементы конечного поля $F(28)$, которое представляет собой — множество произвольных элементов, содержащее конечное число членов. Для элементов поля определены две бинарные операции: сложение двух элементов поля и умножение двух элементов поля. В процессе шифрования используется ключ размера 128 бит.

В начале процесса шифрования, входные данные разбиваются на блоки размером 16 байт, которые обычно представляются в виде матрицы 4×4 байта. Операция шифрования каждого блока данных проводится независимо от содержимого других блоков. По окончанию шифрования блока - матрица заполняется порцией данных и процесс повторяется, каждый блок шифруется в несколько этапов. Все преобразования

шифрования однозначны и, следовательно, имеют обратное преобразование, то есть могут быть инвертированы и выполнены в обратном порядке, чтобы выполнить процесс дешифрования.

Преимущества системы AES:

• Поскольку алгоритм реализован как в аппаратном, так и в программном обеспечении, это наиболее надежный протокол безопасности.

• Для шифрования используются ключи большой длины, например 128, 192 и 256 бит, что делает алгоритм AES более устойчивым к взлому.

• Это наиболее распространенный протокол безопасности, используемый для самых разных приложений, таких как беспроводная связь, финансовые транзакции, электронная коммерция, хранение зашифрованных данных и т. д.

• Это одно из самых распространенных коммерческих решений с открытым исходным кодом, используемых во всем мире.

Недостатки системы AES:

• Используется слишком простая (для взлома) алгебраическая структура.

• Каждый блок всегда шифруется одинаково.

• AES в режиме счетчика сложно реализовать в программном обеспечении, учитывая и производительность, и безопасность системы.

2.5 Стойкость криптографических систем

Понятие стойкости шифра в криптографии является центральным элементом, которое зависит от сложности алгоритмов преобразования, методов реализации (программного или аппаратного) и длины ключа. Современные шифры основываются на принципе Огюста Керкгоффса, согласно которому стойкость шифра обеспечивается секретностью ключа, а не секретностью алгоритма шифрования. Это правило отражает тот факт, что надлежащий уровень стойкости шифра может быть обеспечен за счет неизвестных легко сменяемых элементов шифра [13, 14, 20, 43, 45, 92].

Известно [37], что безусловно стойкие криптосистемы могут быть получены только при использовании ключа, длина которого равна длине открытого текста. Это - чрезвычайно дорогие в реализации системы, поэтому на практике используются системы, которые в принципе можно взломать, но за неприемлемое время.

Существует два типа стойкости шифров: теоретическая (математическая) стойкость и практическая. Иногда в рассмотрении стойкости криптосистемы участвует и алгоритмическая стойкость.

Теоретическая стойкость связана с теоретической оценкой вычисления сложности решения задачи криптоанализа в предположении, что доступная злоумышленнику информация недостаточна для определения открытого текста, даже если информация о криптосистеме несекретна. Также, теоретическая стойкость определяется при условии, что не существует временных ограничений на несанкционированное дешифрование.

Под **практической стойкостью** понимается трудоёмкость решения задачи криптоанализа шифров с учетом большого количества факторов, которые имеют место в условиях реального применения криптосистемы и соответственно принимается во внимание число операций, временная сложность определения открытой информации посторонним лицом и организационно – технические условия использования шифров.

Важным элементом для любой криптосистемы является соответствие между её стоимостью и временем её взлома.

Алгоритмическая стойкость определяется требованиями к вычислительным ресурсам и используется для исследования сложности взлома шифров [22, 23, 40, 95, 75, 79]. При этом вычислительная сложность алгоритмов включает в себя:

- временную сложность T, где T – время необходимое для выполнения алгоритма, равное произведению числа элементарных действий на среднее время выполнение одного действия;

- пространственную сложность S, где S - объем памяти используемых алгоритмом.

Параметры T и S являются функциями от входных последовательностей n. Обычно оценку функции $f(n)$ представляется в виде $f(n)=O(g(n))$, где $g(n)$ - вычислимая функция (Рисунок 2.2). Известна следующая классификация алгоритмов в соответствии с их сложностью:

- **постоянные алгоритмы**, где сложность не зависит от n;

- **линейные алгоритмы,** где сложность линейно зависит от n, $O(n)$;

- **полиномиальные алгоритмы** – это алгоритмы, временная сложность которого выражается некоторой полиномиальной функцией размера задачи n - $O(n^m)$, где m – константа;

-**экспоненциальные алгоритмы** — это алгоритмы со сложностью экспоненциального времени;

- **суперполиномиальные алгоритмы** со сложностью $O(c^{f(n)})$, где c – константа, а $f(n)$ – функция, возрастающая быстрее некоторой постоянной, но медленнее линейной функции.

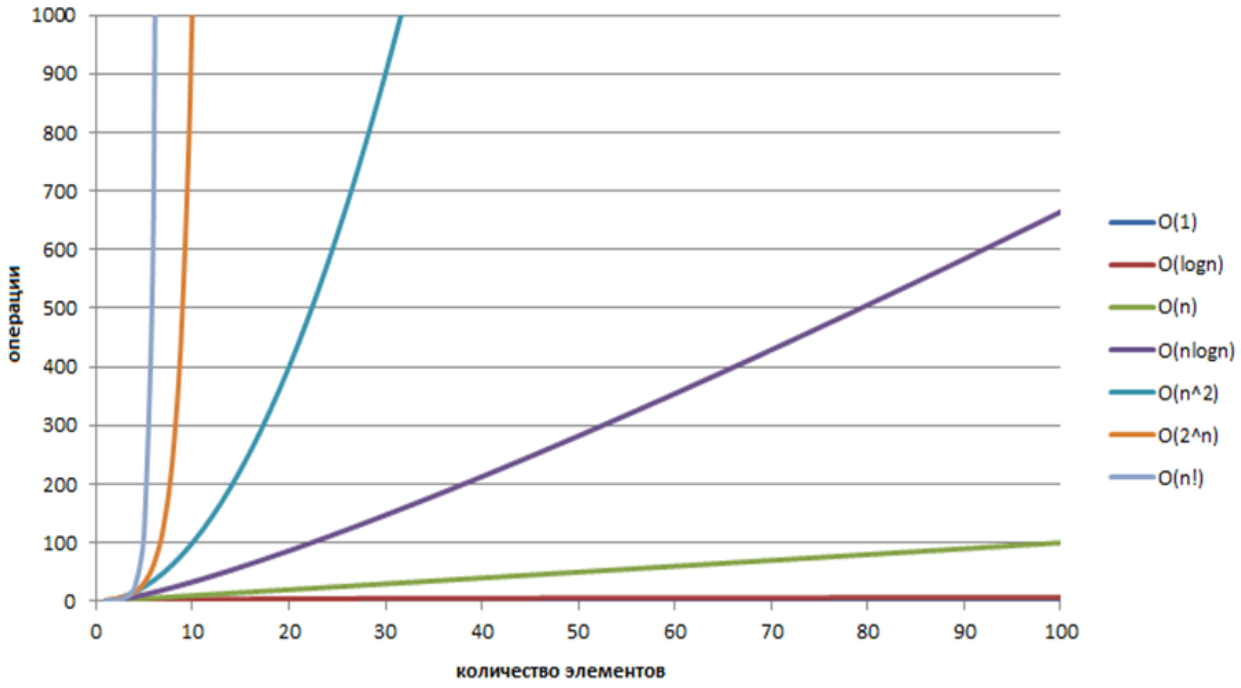


Рисунок 2.2. График роста сложности *f*(*n*)=*O*(*g*(*n*)) в зависимости от алгоритма

2.6 Формантный анализ теории чисел

2.6.1 Введение в сопоставительный анализ

В сопоставительном анализе вместо числовых и алгебраических величин и действий над ними рассматриваются (сопоставляются) имманентные им математические аналоги (в сопоставительных уравнениях – это кратности числа (алгебраического выражения)) по простому основанию (простому числу), а в формантном анализе – это форманта числа или алгебраического уравнения [1, 6, 9, 11]. Ключевым понятием в сопоставительном анализе является понятие кратности $K_P(M)$ числа M (или алгебраического выражения), под которой понимается степень q числа по простому основанию p в разложении числа M на простые множители. Например, число $M = 1350 = 2 \cdot 3^3 \cdot 5^2$. Его кратность по основанию 5 будет $K_5(1350) = 2$, а по основанию 3 - $K_3(1350) = 3$.

Диофантовыми уравнениями, называется уравнения вида

$$F_1(X_1, X_2, .., X_n) = F_2(X_1, X_2, \ldots, X_n),$$

где $F_1(X_i)$ и $F_2(X_i)$, $i=\overline{1,n}$ есть многочлены от переменных X_i с неотрицательными коэффициентами (целые числа) при неизвестных $X_1, X_2, \ldots, X_n$.

Сопоставительное уравнение кратностей — это равенство сопоставлений левой и правой частей, например, диофантового уравнения, как оно представлено в выражении:

$$K_P[F_1(X_1, X_2, .., X_n)] = K_P[F_2(X_1, X_2, \ldots, X_n)].$$

В качестве *Основания (базы)* для записи кратностей *в сопоставительном анализе* берутся только простые числа, в отличие от общего *сравнительного анализа классической теории чисел*, где в качестве оснований допускаются и составные числа [1, 9, 27, 28].

Относительно неразрешимости диофантовых уравнений, различают абсолютную (безусловную) и относительную (условную) неразрешимость. Если ни при каких целых значениях коэффициентов данное уравнение не имеет решений – то этот признак следует считать абсолютной неразрешимостью. Если же решение невозможно при (чётных, нечётных, отрицательных числах, в каком-то интервале значений неизвестных, только положительных значениях неизвестных и т.п.) числах, то это есть относительная неразрешимость. Находить абсолютную неразрешимость – это достаточно просто в сопоставительном анализе, а с относительной неразрешимостью дело обстоит значительно сложнее.

2.6.2 Элементы формантного анализа

Ключевым понятием формантного анализа является понятие форманты (числа или алгебраического выражения).

Формантой $F_P[N]$ по основанию p числа, неизвестного или многочлена N называется его линейное представление в виде трёхчленной (трехмерной) математической конструкции:

$$F_P = pк + q,$$

где p есть база (основание) форманты, $к$ – целая часть от деления N на основание p и q - неотрицательный целый остаток.

Пример обозначения форманты некоторого числа или математического выражения $N = X^2 + 5Y$:

$$F_p[N] = F_p\,[X^2 + 5Y].$$

Конкретное значение или математическое выражение N в форманте заключаются в прямоугольные (круглые или фигурные, в зависимости от сложности записи) скобки. Если, например, $p = 5$, то форманта приведённого выше бинома будет иметь вид:

$$F_5[X^2 + 5Y] = 5к+(1, 4),$$

что означает: «… если X^2 не делится на 5, то при любых целых X и $У$, остаток от деления этого двучлена на 5 будет равным или 1, или 4» и других остатков быть не может.

Не отрицательный остаток (он может быть и ноль) называется **формантной скобкой** (или просто “скобка”), содержащей одно или более целых положительных чисел. Количество чисел в скобке определяет **размерность форманты**.

В структуру форманты добавляется ядро - *к* форманты, то есть целую часть от деления данного числа или алгебраического выражения на базу p. Таким образом, форманта полностью определяется тремя величинами – *p, к* и q.

Различаются несколько типов формант, называемых:

1. Равными, если равны их основания p, ядра k и остатки q.
2. Сравнимыми, если равны их основания p и остатки q.
3. Сродственными, если равны их ядра *к*.
4. Одинаковыми, если у них равны только основания p.
5. Разными (различными), если их основания, ядра и остатки не равны.
6. Несовместимыми, если множество чисел, описываемых каждой из формант, не пересекаются между собою, то есть такие форманты не могут быть равными. Если у двух формант два из главных члена равны между собою, а третьи члены – нет, то такие форманты несовместимые.
7. Ограниченные, если сумма формант равно конечному натуральному числу, в этом случае форманты называются взаимобратными.

Форманта называется [1, 9]:

- простой, если основание p есть простое число;
- составной, если основание p есть составное число;
- единичной, если ядро *к* = 1;
- канонической, если основание p единичной форманты является простым числом;
- полной, если она содержит все возможные остатки;
- неполной, если она содержит не все возможные остатки;
- вырожденной первого вида, если ядро *к* =0;
- вырожденной второго вида, если остаток q =0;
- полновырожденной или нуль-формантой, если и ядро и остаток равны нулю;
- общей или свободной, если на остаток не накладываются никакие ограничения;
- частной или зависимой, если остатки (скобка) связаны ограничением (например, форманта описывает только чётные числа из данного множества);
- кратной другой форманте, если она является произведением целого числа на эту форманту F_1=rF_2 (пример: $F_1 = F_{15}[N1] = 15k + 6 = 3 \cdot F_2[N2] = F_5\ (5k + 2)$);
- связанной с другой формантой, если порядок написания остатков в её скобке строго соответствует порядку написанию остатков в скобке другой форманты, в этом случае остатки заключаются в квадратные скобки;
- предельной, если начиная с некоторого основания, её остаток не меняется.

Свойство формант [1, 9]:

1. Форманта числа по базе p есть само число (константа), записанное в линейной форме. Пример форманты числа:

$$F_3[17] = 17 = 3 \cdot 5 + 2.$$

2. Форманта суммы есть сумма формант.

3. Форманта произведения есть произведение формант.

4. Одинаковые и сродственные форманты можно суммировать. Следствие: форманту всегда возможно представить суммой сродственных формант.

5. Одинаковые и сродственные форманты можно умножать.

6. Одинаковые и сродственные форманты можно возводить в числовую степень. Остатки (скобки) в этих случаях приводятся к виду по модулю основания.

Формантная арифметика

Из теории известно [1, 4, 6, 9], что при сложении (вычитании) формантных скобок по какому-либо основанию p (n-скобка или m–скобка) результирующая скобка будет содержать матрицу из $(n \times m)$ элементов, многие из которых часто одинаковые. Для сокращения объёма вычислений можно использовать аппарат строковой арифметики.

Правило 1. Если в сумме двух скобок к одной скобе добавить какое – то число, а от другой скобки отнять это же число, то сумма скобок не изменится.

Правило 2. Если в разности двух скобок одновременно увеличить или уменьшить все числа, то результат не изменится.

Правило 3. Всякую скобку можно представить как сумму двух нуль-скобок. уль-скобка – это скобка, где присутствует нуль.

Правило 4. К любому числу в скобке можно добавить или отнять основание p, что не меняет величины скобки.

Скобки считаются сравнимыми, если у них имеется хотя бы одно число, равное другому, например скобки [1 2 3 5] = [2 3 4], являются сравнимыми, поскольку числа 2 и 3 у них общие, а скобки [1 3 5] и [2 4] есть несравнимые, т.к. у них нет общих им чисел.

Нелинейные и двумерные форманты

В сопоставительном анализе рассматриваются двусторонние диофантовы уравнения в таком виде [1]:

$$P(X,У) = Q(X,У) + M.$$

Это позволяет исследовать такие уравнения независимо: и левую и правую часть. В этом случае при равенстве частей можно сделать вывод о том, что и кратности этих частей по любому основанию равны. Следует иметь ввиду, что в левой и правой частях уравнения

не может быть ноль, так как ноль не обладает кратностью, соответственно в левой и правой частях уравнения могут быть только суммы натуральных чисел. В этом случае сопоставительное уравнение кратности по основанию *p* принимает следующий вид:

$$Kp(P(X,У)) = Kp(Q(X,У)) + Kp(M).$$

Если же речь идёт о формантах (формантных уравнениях), то остаётся только требование о натуральном значении всех неизвестных:

$$Fp[\,P(X,У)] = Fp[Q(X,У)] + Fp[M].$$

2.6.3 Применение сопоставительного анализа для решения диофантовых уравнений применительно к криптоалгоритмам RSA

В качестве методического примера использования возможностей сопоставительного анализа приведем пример его применения для решения задачи факторизации чисел.

Рассматривается большое составное число в виде произведения двух простых чисел $M = N_1N_2$ (или, как в системе *RSA: n = p·q*). Далее будут рассматриваться, в качестве исходных, квадратичные диофантовые уравнения нулевого порядка в следующих трёх видах (где *M* – факторизуемое число) [1, 6, 9]:

$$X \cdot Y = M = N_1N_2. \tag{2.4}$$

$$X^2 = Y^2 + M = N_1N_2 \rightarrow X^2 - Y^2 = M = (X+Y)(X-Y). \tag{2.5}$$

$$X^2 - 2X \cdot Y = M = N_1N_2\,. \tag{2.6}$$

Во всех этих случаях нужно найти значения неизвестных X и Y. Задача облегчается уже тем, что изначально примерно известен порядок чисел N_1 и N_2. Например, практика работы с ключами RSA показывает, что N_1 и N_2 (полагая $N_1 > N_2$) - числа одного порядка или отличаются на один, максимум на два порядка. От алгебраических уравнений (2.4), (2.5), (2.6) можно перейти к формантным уравнениям следующих трёх видов, записанных следующим образом (после символа форманты *Fp* по основанию *p*, в круглых скобках следует (неизвестная переменная, число, полином или математическое выражение):

$$F_p(X) \cdot F_p(Y) = F_p(M), \tag{2.7}$$

$$F_p(X^2) \cdot F_p(Y^2) = F_p(M), \tag{2.8}$$

$$F_p(X^2) - 2 \cdot F_p(X \cdot Y) = F_p(M). \tag{2.9}$$

Решение задачи факторизации M, очевидно, будет получено после того, как будут найдены значения X и Y, что очевидно при решении обычного алгебраического уравнения. В сопоставительном же анализе, во многих случаях, достаточно найти только форманты неизвестных по какому-либо основанию. Действительно, предполагается, например, для уравнения (2.5) и формантной схемы (2.8), что уже найдены собственные форманты по

некоторому большому основанию p:

$$X = pn + X_0; \quad Y = pm + Y_0.$$

Тогда

$$X + Y = p(n + m) + (X_0 + Y_0) = N_1$$
$$X - Y = p(n - m) + (X_0 - Y_0) = N_2.$$

Если $p > N_1$, то указанные форманты (суммы и разности) по основанию p являются предельными, поэтому находится сразу искомые числа [1, 6, 9]:

$$N_1 = (X_0 + Y_0);\ N_2 = (X_0 - Y_0).$$

2.6.4. Использование алгоритмов формантного анализа для повышения криптостойкости криптосистем RSA в постквантовый период

Наиболее известной и распространённой в мире криптосистемой является упомянутая выше асимметричная криптосистема RSA [1, 4, 9].

Далее предлагается метод и алгоритмы, повышающие криптостойкость и быстродействие модернизированной криптосистемы RSA-m в постквантовый период путем дополнительного использования алгоритмов формантного анализа, позволяющих контролируемо повышать криптостойкость за счет использования различного вида формант с разными основаниями, что влечет создание дополнительных полей неопределенностей при решении задачи криптоанализа, усложняя операционную сложность алгоритма RSA компонентом $O(A^s)$, где $A -$ длина алфавита сообщения, s – длина основания p_i форманты.

Предлагаемый подход, базируется не на шифровании самой информации, а на шифровании некоторой косвенной информации, рабочий объем которой (минимально необходимый для ее передачи и последующего восстановления в исходном виде) существенно меньше исходной. Такой подход естественным образом повышает итоговую криптостойкость криптосистемы RSA-m при той же длине ключа [4, 9].

Суть предлагаемого подхода лежит в использовании свойств числовых формант, которые были введены в [1, 3, 4, 6, 9], с помощью которых любое число можно представить единственным образом. Причём время разложения и восстановления форманты числа на **порядки меньше времени шифрования и дешифрования** того же числа с помощью криптосистемы RSA и, следовательно не влияет на ее производительность. Действительно, шифрование RSA требует выполнения операции возведения в степень по модулю, что при длинном ключе является весьма ресурсоемкой задачей. Поэтому RSA алгоритм считается медленным и не применяется для защиты информации в системах, где требуется высокое

быстродействие системы, в целом. Однако, тем не менее, алгоритмы RSA весьма предпочтительны в системах, где высокие требования к уровню безопасности, а также требуется обеспечение свойства неотрекаемости.

При модернизации алгоритма RSA добавлением быстрых процедур формантного анализа, сводящихся к простому делению с остатком, но при этом создающих для недоброжелателя дополнительные поля неопределенностей, существенно повышается итоговая криптостойкость интегрального алгоритма RSA-m. Количество операций разложения/восстановления форманты числа по сравнению с RSA соотносятся как $1/r \times 100\% = 1/3 = 30\%$ или $1/300 = 0.3\%$. Это обратная величина открытого ключа в процентах. А по сравнению с дешифрацией, так это вообще доли процента, так как закрытый ключ RSA всегда больше открытого. А восстановление форманты – это одна операция умножения, но при этом использование форманты числа создает дополнительное поле неопределенностей, повышающих криптостойкость интегрального алгоритма RSA-m.

Если сложность RSA оценивается формулой $O(exp\{(\alpha+1)\,[\ln n]^r\, ln\,[\ln n]^{n-r}\}$, то для оценки сложности дешифрования поля неопределенностей вводимого формантами можно применить формулу $O(A^s)$, где $A-$ длина алфавита(от 32 до 560 символов, например), $s-$ длина основания форманты (от 3 до 500 10-тичных разрядов или до 624 и более бит). Количество возможных вариантов перебора даже при скромных числовых примерах дает огромные величины:

$$A = 36, s = 5 \; - \rightarrow 36^5 = 60\,466\,175 \text{ вариантов;}$$

а если длина основания 10 цифр $36^{10} = 3\,650\,10^{13}$вариантов. Что при скорости взлома 10^9 вар./сек. даст время перебора 10^7 сек., или около года.

Как известно [1, 3, 4, 9], линейная форманта использует всего три параметра, а нелинейная форманта, в зависимости от её мерности n, в $3n$ раз больше. Достоинством этого подхода является и то, что в качестве основания (базы) форманты можно использовать любое целое число, как простое, так и составное, что значительно расширяет числовое множество неопределенности, как для выбора основания при формантном преобразовании, так и для восстановления форманты при крипто анализе [4, 6, 9].

2.7 Ситуация в сфере информационной безопасности в Республики Молдова

Основным документом в области информационной безопасности в Молдове является Концепция информационной безопасности Республики Молдова (далее – Концепция), утвержденная Законом № 299/2017.

На основе Концепции была принята Стратегия информационной безопасности Республики Молдова на 2019–2024 годы, утверждённая Постановлением Парламента Республики Молдовы №257 (далее – Стратегия) и План действий по ее внедрению. Целью Стратегии информационной безопасности Республики Молдова на 2019-2024 годы является правовая связка и системная интеграция приоритетных областей с обязанностями и компетенцией по обеспечению информационной безопасности на национальном уровне на основе кибернетической устойчивости, мультимедийного многообразия и институциональной конвергенции в области безопасности, направленных на защиту суверенитета, независимости и территориальной целостности Республики Молдова.

В разделе 83 Стратегии отдельно выделена задача борьбы с мошенничествами посредством использования электронных средств оплаты.

Ситуация в сфере информационной безопасности в Молдове, как и во всем мире, является достаточно напряженной. Как указывалось на заседании Координационного Совета по обеспечению информационной безопасности в республике Молдова, которое прошло 18 ноября 2022 года, к основным вызовам в области информационной безопасности в Молдове можно отнести:

- недостаточная нормативная база для расследования инцидентов в области кибербезопасности, в том числе отсутствие методики оценки материального ущерба в следствии киберпреступлений;
- слабое взаимодействие с другими странами на стороне мониторинга и противодействия кибератакам;
- отсутствие оперативного центра кибербезопасности с функциями постоянного мониторинга ситуации в области кибербезопасности и реагирования на атаки хотя бы на уровне государственной инфраструктуры.

В этом контексте директор Службы информационных технологий и кибербезопасности (STISC) Gheorghe PANTAZ отметил, что: «В последнее время активизировались кибератаки на ИКТ-инфраструктуры Республики Молдова. Последние попытки атак были на 100 информационных ресурсов 40 учреждений, а также коммерческий банк, беспрецедентные для нашей страны атаки, со средней мощностью атаки около 130 Гбит/с, а максимальные показатели в отдельные периоды достигали 240 Гбит/с. Имея высокую интенсивность и среднюю сложность, характеризующиеся перегрузкой Интернет-канала, они были направлены на изоляцию государственной сети от глобальной сети Интернет. В основном, атакам удалось противостоять благодаря

значительным усилиям профильных групп STISC в сотрудничестве со специалистами подвергшихся нападению органов власти, что не привело к тяжелым последствиям, таким как потеря данных или длительная недоступность услуг. Видимым эффектом этих атак в этот период было снижение скорости доступа к некоторым сайтам, некоторые ресурсы даже были недоступны в течение коротких промежутков времени. Практически вся телекоммуникационная инфраструктура государства в последнее время работает на пределе, а в некоторые моменты даже в экстремальных условиях с очень критическими ситуациями. Злоумышленники используют разные методы, внедряя интеллектуальные механизмы, имитирующие поведение реальных пользователей, что крайне затрудняет выявление и блокирование таких видов атак. Существуют Ddos-атаки, а также другие новые типы кибератак, целью которых является получение несанкционированного доступа к информации, кража информации и\или ее удаление».

Таким образом, обеспечение необходимого уровня безопасности при осуществлении безналичных онлайновых платежей является актуальной и важной задачей в Республике Молдова.

2.8 Выводы по Главе 2

1. Сделан обзор наиболее распространенных в настоящее время методов криптографической защиты информации и были описаны их достоинства и недостатки. Современные алгоритмы достаточно комплексны и их выбор должен быть основан на анализе криптостойкости тех или иных методов защиты. На данный момент наиболее используемый критерий проверки криптостойкости системы является вероятность и время раскрытия ключа.

2. Относительно низкая скорость работы криптосистемы RSA, но её высокая криптографическая стойкость заставляют разработчиков искать пути доработки этой системы в условиях возможного квантового превосходства.

3. Форманта является математическим образом или точной математической моделью целого числа, что можно использовать для исследования свойств и состава числа, выделяя в нем три параметра: основание, ядро и остаток, что особенно важно при исследовании, обработке и передаче больших целых чисел. При этом база (основание) форманты может быть любым составным или простым числом, что существенно расширяет множество чисел для шифрования и расшифрования данных.

4. В диссертационной работе предлагается технология в основе которой положены алгоритмы передачи зашифрованных данных, основанные не на пересылке самой

информации, а на отправке косвенных данных об этой информации в режиме реального времени, с требуемой криптостойкостью криптографической системы и без недопустимых задержек во времени. Такой подход естественным образом повышает итоговую криптостойкость криптосистемы RSA при той же длине ключа [4, 9].

3 ЗАЩИТА ИНФОРМАЦИИ ПРИ ПОМОЩИ АЛГОРИТМОВ RSA-mAB НА ОСНОВЕ ФОРМАНТНОГО АНАЛИЗА

3.1 Закрытие информации криптографическими способами

Актуальной задачей криптографии является защита информации промышленного или коммерческого характера. Ограничивающим фактором, накладывающим свой отпечаток на способность любой криптосистемы обеспечить закрытие информации от нежелательной утечки или хищения, является длина кода шифрования. При этом не имеет значения, о каких двух криптосистемах идёт речь: с одним ключем (симметричных) или с двумя ключами (асимметричных).

Длина ключа при реальной онлайн передаче закрытой информации от абонента *A* к абоненту *B* по открытым (т.е. доступным к «прослушиванию») каналам связи, напрямую связана с пропускной способностью канала связи, точнее, с полосой пропускания всех элементов системы [11].

Далее, будет рассмотрено только закрытие информации при её передаче, или, что более точно, режим поточного шифрования в реальном масштабе времени как критичного по времени процесса, оставив вопросы блочного шифрования (т.е. шифрования с задержкой во времени) [68].

Полоса пропускания криптосистемы, в свою очередь, зависит от скорости изменения информации, собственно, от полосы пропускания (т.е. от динамических характеристик) источника информации. Один из этих факторов и является критическим для определения конечной величины длины ключа. Если быть более точным, то критическим временным параметром является длительность паузы между выборками при дискретизации аналогового сигнала, подлежащего шифрованию.

Межвыборочная пауза заполняется импульсами, последовательность которых отражает величину сигнала в двоичной форме (коде). Количество импульсов, которые могут быть размещены на этом интервале определяется, главным образом, двумя факторами: возможностью АЦП по быстродействию, дискретностью съёма информации с АЦП и приемлемым соотношением сигнал-шум в линии связи [48, 68].

Так, если выбрать для примера, 12-битное АЦП и принять минимально допустимый по длительности информационный импульс в 0.1 микросекунды, то максимально допустимой длиной ключа будет обладать ключ в те же 12 бит ($12\ \text{бит} \times 0.1\ \mu c = 1.2\ \mu c = 1.2 \cdot 10^{-6}$ сек).

Радиоканал для передачи такой закрытой информации (с длительностью бита в 0.1 микросекунды) может работать только на частотах, не менее 2 ГГц, что означает использование приёмо-передающих устройств сантиметрового диапазона, близких к существующим на сегодняшний день к устройствам сотовой (мобильной) связи.

Соответственно, шифро - ключ, длиною в 12 бит, не может быть препятствием для его раскрытия. Поэтому напрашивается, само собою, идеология быстрой смены ключей для каждой отдельной дискреты сообщения.

Оценим полосу пропускания аналогового сигнала, который может быть закрываем таким образом. Поскольку длительность информационного импульса принята равной 0.1 микросекунды, то промежуток времени, заполненный 12 такими импульсами, будет равным $12\ \text{бит} \times 2 \times 0.1\ \mu\text{c} = 2.4$ микросекунды (с учётом паузы в 0.1 μс между импульсами), что будет соответствовать периоду самой высокой гармоники аналогового сигнала в 4.8 μс, что и определяет (в соответствии с теоремой Котельникова) полосу пропускания в $f_{max} = \frac{2\pi}{\omega_{max}} = \frac{1}{T_{max}} = 1/(4.8\ \mu\text{c}) = 0.208 \cdot 10^6 \approx$ 200 КГц. Такая полоса пропускания может обеспечить передачу данных, или многоканальную речевую связь, или передачу статического изображения (картинки) или рисунков и графиков [68].

Если эти рассуждения применить для промышленных систем, принимается во внимание, что интервал выборки информации занимает, к примеру, 1 секунду. Использование того же, ранее рассмотренного 12-ти битного АЦП, даёт длительность импульса (бита), примерно, в 40 миллисекунд (1/24 s = 0,04 s=40 ms).

Если используется линия связи с пропускной способностью в 100 КГц, то такая линия способна пропускать импульсы гораздо меньшей длительности, а именно, в 20 микросекунд. Таким образом, на интервале выборки в 1 секунду можно разместить 25 000 импульсов. А это эквивалентно работе криптосистемы на базе RSA с ключом в 25 000 бит, что превышает все разумные пределы закрытости информации.

Ясно, что такая криптосистемы может и должна работать с системой связи, имеющей гораздо меньшую полосу пропускания, например, 10 000 Гц, при этом длина ключа останется в пределах 2500 бит, что гарантировано обеспечить высокую крипто стойкость системе защиты информации.

Из сказанного можно сделать следующий вывод по закрытию информации в промышленных системах: промышленные технические системы можно эффективно защитить от несанкционированного проникновения, используя как симметричную, так и асимметричную криптографию для защиты системы.

Если применить аналогичные рассуждения к коммерческим задачам, то здесь следует говорить о двух аспектах: о закрытии самого факта коммерческой сделки (долгосрочное сохранение тайны) и о невозможности подложных сделок, осуществляемых здесь и сейчас.

Когда же речь идёт о закрытии информации по долгосрочной сделке (о документе сделки, финансовом документе), то это относится уже к вопросу защиты базы данных и находится за рамками данного рассмотрения.

Обычно, хакер определяет ключ клиента и делает ложный запрос к банку о снятии денег. Вся процедура (от запроса до выдачи денег банкоматом или перечисления денег на фиктивный счет) занимает несколько секунд (например, 5 секунд). Основное время занимает передача шифрованного сигнала запроса и шифрованной команды на выдачу запрашиваемой суммы, а также время ожидания в очереди к центральному банковскому процессору. Примем, что один акт «запрос-ответ» занимает 2 секунды. Предполагается, далее, что банк располагает в пределах города 100 банкоматами. Тогда на обслуживание запроса с одного банкомата приходится промежуток времени в 20 миллисекунд. В один конец – это 10 миллисекунд.

Поскольку реальные системы закрытия информации банковского характера строго засекречены, то предположительные рассуждения о работе этой системы строится следующим образом: от банкомата к центральному банку поступает информация о клиенте, желающему снять некую сумму со своего счёта, включающая, по крайней мере, идентификационный номер клиента, номер банкомата, и, может быть, дату и текущее время. Если шифруется эта информация единым блоком, то ключ, длиною в 50 бит, способен зашифровать только 16-значное число. Навряд ли указанная информация поместится в данный интервал, и её придётся разбить на несколько пакетов.

Работая в рассматриваемом случае с ключами в 50-90 бит (для симметричных систем), оценивается возможный риск. Риск взлома определится скоростью раскрытия ключа. Скорость раскрытия ключа в симметричных системах зависит от операционной сложности алгоритма вскрытия, которую можно, весьма приблизительно, оценить как $L = 2^n$, где n есть количество десятичных разрядов ключа [48].

В данном случае мы имеем 16-30-значные двоичные коды, что даёт (см. формулу) $L = 2^{16-30}$, или откуда десятичная длина ключа $L = 10^5 \cdots 10^{10}$.

Понятно, что такая операционная сложность не даёт никаких гарантий от вскрытия системы. Даже обычный процессор (2.5 ГГц) сможет отработать программу вскрытия шифра, затратив, в худшем случае, несколько секунд.

Но ситуацию с закрытием канала, в рассмотренном случае, можно легко поправить, например, уменьшив число банкоматов на один центральный процессор (допустим, в два раза, то есть взять их 50 штук) и увеличив интервал обслуживания (до 3 секунд, т.е. в 1.5 раза). Это позволит работать с ключами в 3 раза длиннее (т.е. 150-300) бит [48].

Общий вывод:

Низкоскоростные (промышленные технологические системы) информационные системы весьма просто поддаются закрытию (защите) от кибер атак, ввиду их повышенной инерционности, независимо от того, какое используется шифрование - симметричное или асимметричное [108].

Другая ситуация возникает, когда речь заходит о закрытии высокоскоростных информационных каналов для обработки большого количества транзакций, особенно в виде микроплатежей [53,118].

Ниже рассматривается вопрос закрытия информации в системах речевой связи по линии, имеющей полосу пропускания 100 КГц, что даёт возможность использовать импульсы с длиной не менее, чем 20 микросекунд. Здесь интервал выборки (полоса частот голосовой речи - около 5 КГц) равен 100 микросекунд. По сравнению с ранее рассмотренным случаем, в этом промежутке времени можно разместить всего лишь 5 импульсов. Это означает, что используется только 5-ти битный ключ шифрования, а сама информация занимает только 4 бита (16 уровней силы звука).

Понятно, что работа с таким ключом, даже в одном, например, часовом сеансе связи, приведёт к неминуемому раскрытию информации и выход из данной ситуации может быть только в быстрой и частой смене ключей. Система RSA как раз и позволяет свободно обмениваться (не боясь их раскрытия) так называемыми открытыми ключами.

3.2 Разработка алгоритмов шифрования, генерирование матриц создания криптоключей p, q, e, d, n и параметров p, k, q для формант сообщения

3.2.1 Алгоритм AB1

Любое число в формантном анализе может быть представлено в виде двучленной конструкции [3, 4, 93]

$$N = pk + q, \tag{3.1}$$

где $p -$ основание форманты; $k -$ ядро; $q -$ остаток. Знание всех трёх параметров без труда позволяет достаточно быстро восстановить исходное число.

На основании (3.1) нужно шифровать не одно число N, а всего лишь три небольших числа. Различие в том, что $N -$ большое целое число (порядка $10^{20} \dots 10^{500}$ и более), а

p, k и q - любые целые числа, простые или составные, значения которых существенно меньше и разрядность которых определяется только необходимой скоростью передачи информации по открытому каналу. Основание p рекомендуется выбирать большим числом, порядка длины ключа RSA, для того чтобы остатки форманты находились в множестве достаточно больших чисел, что увеличивает итоговую криптостойкость.

Для повышения скорости работы описываемого алгоритма с использованием формант создаётся динамическая база данных, например, в виде матрицы, в ячейках которой хранятся заранее сгенерированные числа-основания формант. Например, в матрице 100×100 будут находиться числа-основания p_i для 10 000 различных формант. После однократного использования всех оснований p_{ij}, по заранее предусмотренному алгоритму матрица оснований автоматически обновляется, как на передающей, так и на приёмной сторонах.

В зависимости от требований к крипто стойкости алгоритма шифрования, это могут быть заранее созданные матрицы с жёстким или гибким, автоматическим или ручным, переходом от одной матрицы к другой. Либо это может быть одна и та же матрица, в которой у ячеек-оснований форманты меняются индексы. Например, по правилу $p_{ij} = p_{ji}$ $i = j = 0,1 \ldots n.$, или менять процедуру индексирования по произвольному иному закону.

Значения ядра и остатка очередной форманты шифруются ключом алгоритма RSA, что в совокупности повышает итоговую криптостойкость алгоритма.

Зашифрованная (косвенная) информация на приёмной стороне расшифровывается специальной процедурой, которая распознает в посылке адреса ячеек, в которых размещены основание формант и расшифровывает другие их параметры, после чего восстанавливается исходное число-сообщение, т.е. сама форманта числового сообщения или его части. Само сообщение может быть текстом на любом языке, картинкой или изображением любого класса или типа, речью или музыкальным отрывком и т.п.

На Рисунке 3.1 показана блок-схема алгоритма АВ1 [3, 4, 93].

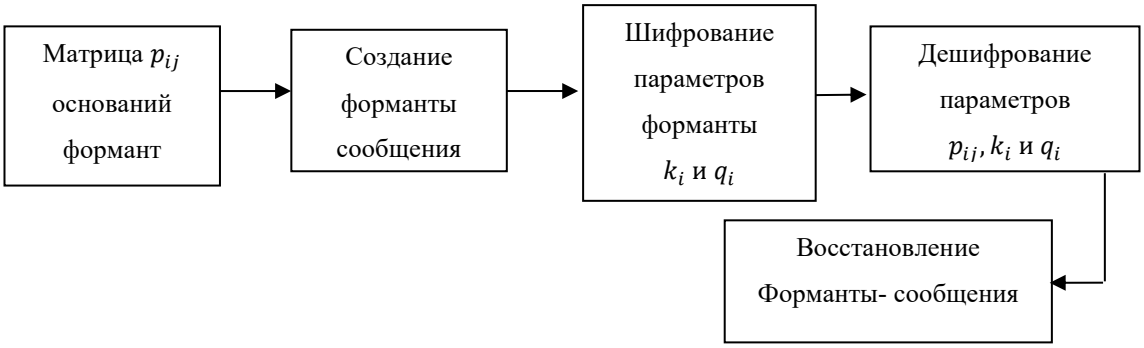


Рисунок. 3.1. Блок-схема алгоритма АВ1

Описание алгоритма [3, 93]

1. Из матрицы оснований случайным образом выбирается номер ячейки, содержимое которой будет равно основанию $p_{ij} = d_1$.
2. Число-блок (открытое сообщение) представляется в виде его форманты по основанию p_{ij}и определяются ядро $k_i = d_2$ и остаток $q_i = d_3$ согласно формуле $F_p[N] = pk + q$.
3. Формируется сообщение $d_1 d_2 d_3$ о форманте открытого сообщения.
4. Зашифровывается сообщение $d_1 d_2 d_3$ о форманте алгоритмом RSA-m.
5. Зашифрованные данные передаются в открытый канал.
6. Принимается блок 64 бита.
7. Из принятого блока извлекаются координаты ячейки из матрицы оснований p_{ij}.
8. Восстанавливается основание p_i.
9. Из блока извлекаются числа k_i и q_i.
10. Восстанавливается сообщение-форманта по формуле (3.1)

$$F = p_{ij} \cdot k_i + q_i = p_i \cdot d_2 + d_3.$$

Далее приводится простой пример использования метода $\mathrm{RSA} - \mathrm{AB1}$ для шифрования сообщения «ЕДА». Для простоты будет использоваться небольшие числа (на практике используются числа намного большие).

Для шифрования алгоритмом RSA-m выбираются два простых числа, например, $p = 3$ и $q = 11$.

Определяется модуль шифрования

$$n = p \cdot q = 3 \cdot 11 = 33.$$

Находится $\varphi(n)$ значение функции Эйлера

$$\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20.$$

Далее, в качестве секретного (т.н. закрытого) ключа d выбирается любое число, являющееся взаимно простым с $\varphi(n) = 20$, т.е. не имеющим с ним общих множителей, например, $d = 3$.

Затем подбирается число для «открытого» ключа e для которого удовлетворяется соотношение

$(\mathrm{e} \cdot \mathrm{d} = 3)\mathrm{mod}20 = 1$, например, $\mathrm{e} = 7$; действительно, $(7 \cdot 3)\mathrm{mod}20 = 1$. (3.2)[2]

Теперь шифруемое сообщение №1 представляется, как последовательность целых чисел в диапазоне $0\ldots32$.

Пусть, для примера, русские заглавные буквы: буква $Е$ изображается числом 6, буква Д - числом 5, а буква А - числом 1. Тогда сообщение ЕДА $= S_1$ представляется в виде последовательности чисел 651.

Далее, пусть генератор случайных чисел компьютера выбрал в качестве номера варианта сессии обмена число 015 и так же случайно - номер ячейки в соответствующей матрице оснований - число 48, для которых нужно выбрать матрицу оснований формант для текущей сессии обмена, например, №71, в которой в ячейке P_{48}, находятся: число − основание $p_i = 23$ и там же уже лежат заранее рассчитанные ключи RSA-m закрытый ключ $d = 3$; открытый ключ $e = 7$ и модуль N=33.

Находим форманту числа 651 по основанию 23:

$$F_{23}(651) = 23 \cdot 28 + 7 \rightarrow p = 23; k = 28; q = 7.$$

Таким образом, был преобразован исходный числовой открытый код 651 текста «ЕДА» в его форманту:

$$651 \rightarrow 23\ 28\ 07.$$

Далее производится шифрование открытого кодо-зашифрованного текста 232807 в закрытое сообщение, используя открытый ключ RSA-m $e = \{7{,}33\}$ согласно известной процедуре: сначала закодированный текст-число возводится в степень 7, после этого результат делится на модуль N. Остаток от деления и есть результат шифрования. Имеем: текст: 48 651 → это номер ячейки оснований формант в матрице P_{ij} №71. Таким подходом экономится время на процедуре генерации сеансовых RSA-ключей. Шифруем форманту ключами RSA:

$$C_0 = 48;$$

$$C_1 = 23^7 \bmod(33) = 3404825447 \bmod(33) = 23;$$

[2] Это выражение в описании алгоритмов RSA называется иногда **крипто замком**

$$C_2 = 28^7 \bmod(33) = 78125 \bmod(33) = 19;$$

$$C_3 = 7^7 \bmod(33) = 823543 \bmod(33) = 28.$$

Теперь сформируется шифрованное сообщение для открытого канала, где С, П, Ш – возможные расшифровки числовых кодов текста:

$$\underbrace{003}_{\text{по 3 разряда}} \quad \underbrace{015}_{\substack{\text{Вариант} \\ \text{сеанса(001…999)}}} \quad \underbrace{048}_{\substack{\text{адрес ячейки} \\ \text{матрицы Оснований}}} \quad \underbrace{023}_{\text{С}} \ \underbrace{019}_{\text{П}} \ \underbrace{028}_{\text{Ш}} \ \ldots \underbrace{[0?\,101\&]}_{\text{Служеб инф}}.$$

Первые три десятичные цифры – это длина разрядов обработки части передаваемого кода, необходимая, чтобы указать длину машинного слова – т.е. надо выделять каждые три десятичных разряда в цифровом сообщении.

2-я группа из трёх десятичных цифр (015 из 999 возможных) – номер матрицы оснований для данного сеанса 015 приёма-передачи информации. Номер варианта сеанса обмена задает (выбирает) вызывающий абонент.

3-я группа из трёх десятичных цифр – номер ячейки матрицы оснований P в ПЗУ на приёмной стороне, которую нужно выбрать из памяти контроллером вызываемого абонента.

4-я группа из последовательности трёхразрядных десятичных цифр – цифровая информация для дешифрования алгоритмом RSA (может содержать любое количество «троек» в зависимости от длины пересылаемого блока бит – 16, 32, 64 бит и т.д.).

Последние, например, 6 цифр – служебная информация: конец отправленного сообщения, проверка чётности и т.д. Таким образом, отправив 64-бит, нужно выбрать первые 6 цифр и последние 6 цифр (чисел), которые содержат всю информацию о расшифровке оставшиеся 52 десятичных знаков. Заметим, что содержимое и место расположения ячейки №48 никому не известно, кроме компьютеров, формирующего содержание соответствующих матриц оснований по номеру варианта сессии обмена.

Далее идет расшифровка этого непонятного сообщения $\{23\ 19\ 28\}$, полученного в результате дешифрования, по известному закрытому ключу $\{3{,}33\}$. На приёмной стороне в ячейке $p_i = p_{23}$ уже лежат числа: $d = 3;\ N = 33$. Получается:

Исходный текст $M_1 = 23^3 \bmod(33) = 23 = \text{основание } p.$

Исходный текст $M_2 = 19^3 \bmod(33) = 4913 \bmod(233) = 28 = \text{ядро } k.$

Исходный текст $M_3 = 28^3 \bmod(33) = 1 \bmod(23) = 7 = \text{остаток } q.$

$$F_p(N) = kp + q = 28 \cdot 23 + 7 = 651 = 06\ 05\ 01 = \text{"ЕДА"}.$$

Таким образом, в результате дешифрования сообщения получено исходное сообщение «ЕДА».

3.2.2 Алгоритм AB2

В отличие от алгоритма AB1 здесь имеется две матрицы - матрица оснований формант и матрица ключей RSA. Для каждого сеанса связи вне зависимости от выбранной ячейки матрицы оснований выбирается случайным образом сеансовые ключи RSA из матрицы ключей RSA.

В отличии от алгоритма AB1 передается:

1. В открытом виде:
   - Адрес ячейки сеансовых ключей RSA.
2. В зашифрованном виде:
   - Адрес ячейки матрицы оснований формант.
   - Ядро форманты.
   - Остаток форманты.

В матрице из 10 000 ячеек (100 строк ×100 столбцов), ячейки пронумерованы в естественном порядке:

00 От 0 до…до 099

01 От 100…. до 199

02 От 200 …до..299

……..

98 От 8000… до 8999

99 От 9000 … до 9999.

Эти же ячейки можно представить и в виде двух-индексной переменной p_{ij}, где $i, j = 00,01, \ldots 99$. Так, например, ячейка №457 имеет адрес (индекс) P_{0457}, а ячейка №$4057 - \mathrm{P}_{4057}$.

Каждая ячейка матрицы $p_{ij}(e, d, n)$ содержит уже зашифрованное по системе RSA число-индекс. Например, в ячейке с номером №0006 находится число 30; в ячейке с номером №0005 находится число 14; в ячейке с номером №0001 находится число 1; что соответствует шифрованию на основе крипто замка $d = 3;\ N = 33;\ e = 7$. Аналогичным образом заполняются все ячейке этой матрицы [3].

При смене крипто замка (путем перемешивания ячеек) суть содержимого матрицы не изменяется, меняются только числовое содержание каждой ячейки, за счёт пересортировки индексов. Для повышения крипто стойкости $\mathrm{RSA} - \mathrm{mAB}$ рекомендуется в процессе

создания шифрованного блока фиксированной длины случайным образом менять матрицы, соответствующие разным крипто замкам[3].

Количество таких матриц и их объем зависят от долгосрочности секретности информации, а также от объёма оперативной и долговременной памяти микроконтроллера, на котором реализуется криптосистема $\mathrm{RSA}-\mathrm{mAB}\,[3, 4, 93]$.

3.2.3 Алгоритм AB3

В отличие от алгоритма AB2 здесь имеется конечный набор матриц оснований формант и матриц ключей RSA. Для каждого сеанса связи выбирается случайная пара матрицы оснований формант и матрицы ключей RSA.

В отличии от алгоритма AB2 передается:

1. В открытом виде:
   - Номера текущих матриц оснований форманты и ключей RSA.
   - Адрес ячейки сеансовых ключей RSA.
2. В зашифрованном виде:
   - Адрес ячейки матрицы оснований формант.
   - Ядро форманты.
   - Остаток форманты.

Данный алгоритм состоит из соответствующих шагов [4, 93]:

1. Формируется блок-сообщение. Из базовой матрицы случайным образом выбирается основание p_{ij} форманты и её номер записывается как сообщение d_1 (в ячейке d_1 хранится основание создаваемой форманты).
2. Начальный номер формируемого информационного блока представляется в виде форманты, все остальные параметры которой ядро $k_i = d_2$ и остаток $q_i = d_3$, определяются выбранным основанием и записываются в сообщения d_2 и d_3.
3. Формируется передаваемое сообщение $d_1 d_2 d_3$.
4. Генерируются крипто ключи для k_i и q_i.
5. Шифруется сообщение о форманте $d_1 d_2 d_3$.
6. Шифрованное сообщение передаётся в канал связи.
7. Принимается блок 64 бит.
8. Из принятого блока извлекается координата-адрес p_{ij}.

[3] Крипто-замок – это алгоритм RSA, включающий ряд процедур по созданию открытого и закрытого ключей шифро- и дешифрования, представленный на стр.85 формулой (3.2) .

9. Восстанавливается значение основания форманты. p_{ij}.
10. Из соответствующего блока извлекаются k_i и q_i.
11. Восстанавливается форманта, по шифрованному сообщению, на основании стандартной формулы.

В качестве примера предлагается рассмотреть шифрование сообщения $S_1 =$ ЕДА, или его числового кода 651. Представляется код числа 651 в виде форманты, то есть в виде суммы произведения и остатка, а в качестве основания выбирается, например, одно из произвольных простых чисел 237, 54, 119 и т.д. Матрица ключей системы варианта 1 заменяется на матрицу оснований формант и образует первый набор выбираемых оснований различной длины и свойств (простые или составные). Итак, наше сообщение: $S_2 = 651$. Случайным образом выбирается основание, например, $p = 54$, таким образом, сообщение $d_1 = 54$. Рассчитывается форманта числа 651 по основанию 54: $F_{54}(651) = 12 \times 54 + 3$. Таким образом определяем остальные сообщения d_2 и d_3: ядро $k_i = d_2 = 12$ и остаток $q_i = d_3 = 3$. Информационный блок сообщения S_0 для шифрования может выглядеть следующим образом:

$$S_0 = 054\ 012\ 003.$$

Из матрицы ключей для ячейки №54 выбирается ключ e шифрования. Шифруется сообщение:

$$C_1 = 54^7 (mod 33 = 24794911296 (mod 33) = 12;$$
$$C_2 = 12^7 (mod 33 = 35831808 (mod 33) = 12;$$
$$C_3 = 3^7 (mod 33) = 823543 (mod 33) = 28.$$

Таким образом зашифрованное сообщение примет вид: 012 012 028. После чего формируется передаваемый блок со служебной информацией и посылается по открытому каналу.

Дешифруется этот блок, и что даёт: $\underbrace{54}_{\text{основание}}\ \underbrace{12}_{\text{ядро}}\ \underbrace{3}_{\text{остаток}}$

Восстанавливается форманта: $S_1 = 54 \times 12 + 3 = 651 \rightarrow EDA$.

Матрица M_1 на 12х12 бит содержит 64х64=4096 десятичных чисел, которые надо зашифровать 64-мя различными крипто замками (крипто ключами). Сначала предлагается работать с 64-х битными числами (ранг - 6 десятичных разрядов). Удвоив число регистров легко перейти на 124-битные (12-ти разрядные, ранг=12) числа.

$2^{10} = 1024$ бит-разрядов и каждое 10-ти битное число располагается в ячейке матрицы $10 \times 10 = 1000 \approx 1024$.

$2^2 = 4$ $2^3 = 8$ $2^4 = 16$ $2^5 = 32$ $2^6 = 64$ $2^7 = 128$ $2^8 = 256$

$$2^9 = 512 \quad 2^{10} = 1024\ 2^{11} = 2048 \quad 2^{12} = 4096.$$

Если в матрице M_1 64x64 10-разрядных десятичных чисел разместить 4096 зашифрованных чисел крипто ключом K_1, в матрице M_2 те же 4096 чисел, но зашифрованных уже другим крипто ключом K_2 и так далее до $Mz \to Kz$, где z – желаемое число криптозамков или длина ключей шифрования, например, 10 или 100 и так далее, то процесс шифрования можно существенно сократить во времени, заменяя вычислительный процесс многократного умножения более простым процессом выборки (Рисунок 3.2). Это позволяет использовать алгоритмы $\mathrm{RSA-AB}$ для защиты информации в системах, критичных по быстродействию, а для повышения крипто стойкости – часто, вплоть до поблочного, менять крипто замок [3, 4, 93]. Матрицы Mz можно создавать отдельно (независимо) различными способами. В алгоритме $AB1$ – это одна динамическая матрица, в которой содержимое ячеек остается неизменным, но меняются адреса ячеек по заранее согласованному алгоритму, [3, 4]. В алгоритме AB2 – это две динамические матрицы оснований и ключей, в которых содержимое ячеек остаётся неизменным, но меняется их адрес. Перемешивание или перераспределение содержания ячеек матрицы M можно выполнять различными способами, например, случайно. Или согласно какому-либо алгоритму обхода ячеек матрицы, например, по формуле $p_{ij} = p_{i+k,j+l}$, варьируя k и l так, чтобы обойти все ячейки, либо только некоторые из них, Рисунок 3.2.

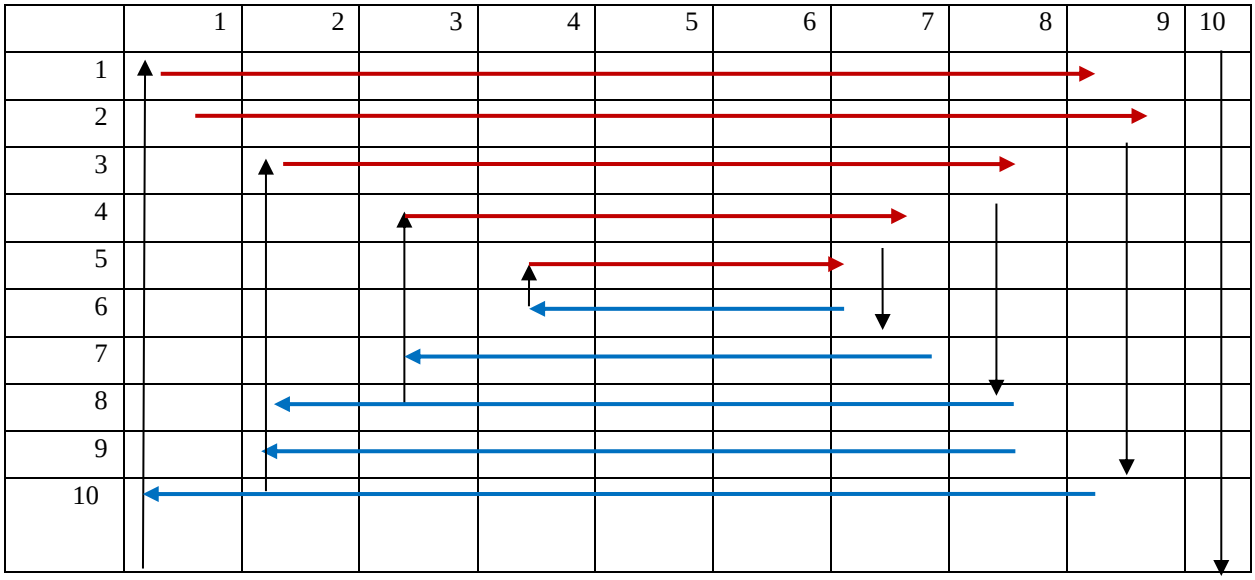


Рисунок. 3.2. Пример перемешивания и сортировки матрицы оснований формант

В алгоритме AB3 используется используется конечный набор динамических пар матриц оснований и ключей. Выбор конкретной пары матриц оснований и ключей для данного сеанса работы также определяется по некоему алгоритму. Итак, на передающей

стороне информация не шифруется в процессе передачи, а формируется поблочно и либо передаётся в открытый канал, либо передаётся информация об этом сообщении, на основе которой восстанавливается на приёмной стороне. На приёмной стороне в памяти дешифратора имеются точно такие же матрицы крипто замков, но содержащие данные, необходимые для восстановления сообщения по данным полученного шифрованного сообщения. В алгоритме АВ1 в соответствующей ячейке находятся данные $\{d, n\}$, позволяющие расшифровать сообщение на приемной стороне. В алгоритме АВ2 по полученной информации на приемной стороне мы обращаемся к ячейкам матрицы ключей, где содержатся уже расшифрованные части блока сообщения. В алгоритме АВ3 в ячейках дешифратора содержится необходимая информация, по которой восстанавливается форманта исходного сообщения. Совершенно очевидно, что такое сообщение весьма трудно вскрыть за реально разумное время. Более того, даже после записи сообщения на внешний носитель оно практически не может быть расшифровано (раскрыто) за разумно короткое время, так как диверсанту не известна ни длина сообщения, ни длина посылки, ни открытый ключ (тем более – закрытый), ни алгоритм шифрования (они известны, но нужно проанализировать слишком большое число комбинаторных перестановок). Каждая посылка внешне может быть одинаковой, но её состав отличается по содержимому начальной, конечной и рабочей части посылки в каждом сеансе связи [3, 4].

3.2.4 Процедура организации сеанса связи при использовании алгоритмов RSA-m

На передающей стороне в программе есть таблица с уже сгенерированными 64-разрядными ключами, которая содержит значения $p, q, n, e, d, \varphi(n)$ для расчёта открытого и закрытого ключей e, d, где p и q имеют 64 разряда. Вводится текст, который переводится в цифры, каждая буква шифруется трёхзначным десятичным числом. Затем для каждой буквы генерируется индекс ключа (адрес ячейки матрицы ключей), и по этому индексу считываются ключи из таблицы, затем по классическому алгоритму RSA шифруется текст. Шифрованные блоки разделяются между собой четырьмя нулями плюс индекс ключа из таблицы, и выводятся на экран (см. Рисунок 3.3) [3, 4, 93].

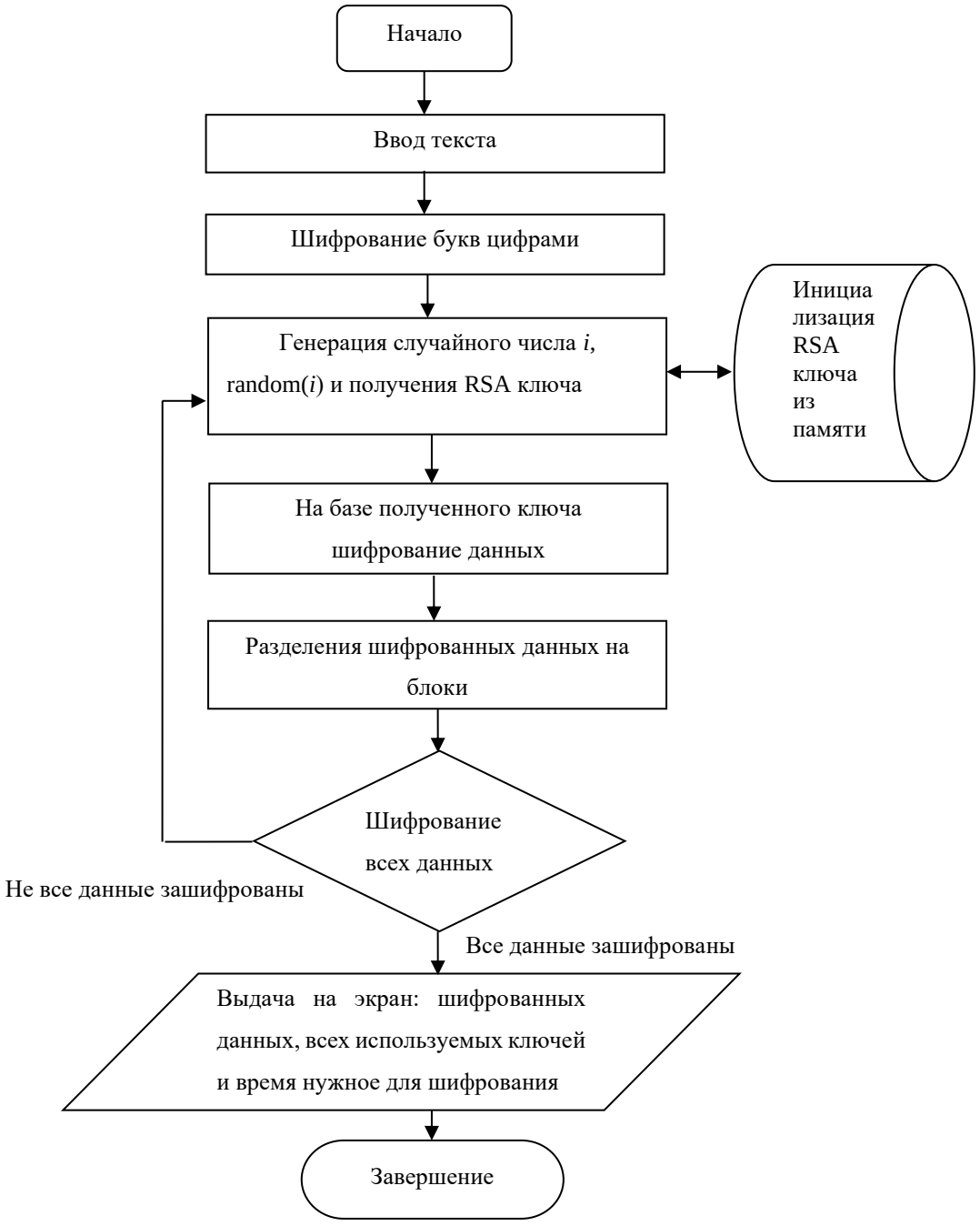


Рисунок 3.3. Алгоритм шифрования на передающей стороне

На приёмной стороне зашифрованный текст анализируется и то место (биты), где находятся, например, четыре нуля, означает для алгоритма, что это начало блока и после 4-нулей, идёт информационный блок, например, адрес или индекс ключа. По этому индексу из соответствующей области памяти (например, массива, таблицы, вектора крипто ключей и т.п.) выбираются ключи RSA, после чего, запускается процедура дешифрования очередного анализируемого блока данных. Получается число, которое представляет какой-

либо символ или его код. Далее это число конвертируется в букву, исходный символ или число (последовательность бит). Дальше продолжается снова поиск нулей в зашифрованном тексте, Рисунок. 3.4.

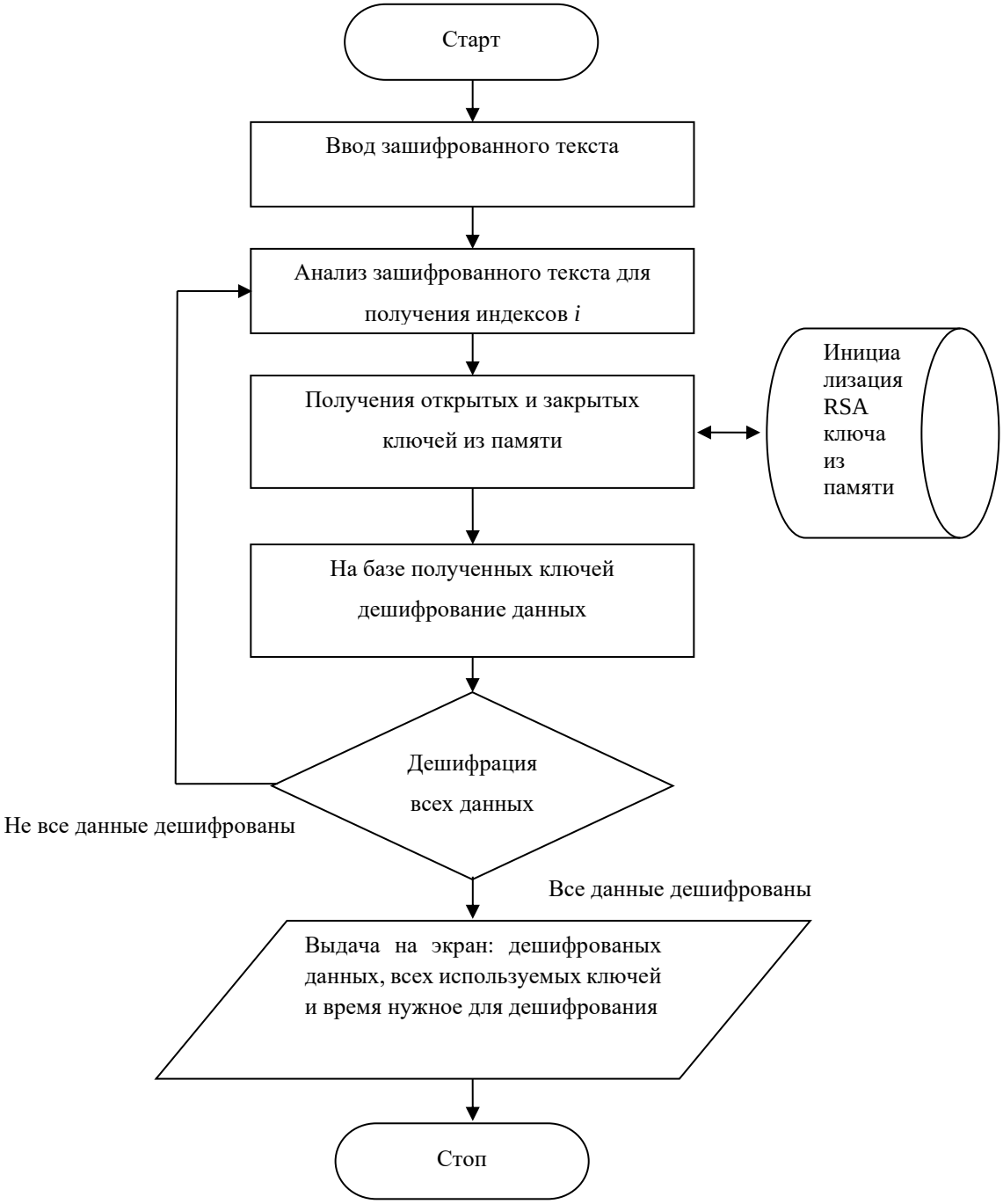


Рисунок 3.4. Алгоритм дешифрования на приёмной стороне

3.3 Расширенный алгоритм RSA-m. Анализ криптостойкости RSA-mAB в зависимости от варьируемых параметров алгоритма

Формантный анализ позволяет вводить дополнительные неопределённости при шифрование/дешифрование, если в уравнение крипто замка RSA (3.3) ввести дополнительно параметр "a". Как известно, асимметричная система RSA использует свойства односторонних функций для целочисленного аргумента, удовлетворяющих условиям существования решения одного из видов диофантова уравнения с параметром $a \in [1,\ldots,5]$, [1, 4].

$$e \cdot d = \varphi(n) \cdot k + 1. \qquad (3.3)$$

При a=1 выражение (3.3) представляет собой крипто замок обычной, классической RSA.

Под расширенным алгоритмом работы (модернизированный «крипто замок» или алгоритм RSA-mAB) понимается следующее диофантово уравнение, связывающее открытый (e, n) и закрытый (p, q, d) ключи RSA:

$$e \cdot d = k \cdot \varphi(n) + a = k \cdot \varphi(p) \cdot \varphi(q) + a = k \cdot (p-1) \cdot (q-1) + a,\ a \geq 1.$$

Пример 1. Приводимый ниже пример показывает, с какими сложностями может столкнуться противник в своей попытке раскрыть ключи RSA-mAB. При этом предполагается, что противник не располагает пока сведениями, касательно введённой модернизации.

Пусть имеется RSA-mAB со следующими параметрами: $p = 1181,\ q = 1193,\ n = pq = 1408933$ и $\varphi(n) = 1180 \cdot 1192 = 1406560$. Тогда, согласно (3.2) следует записать уравнение крипто замка для отыскания закрытого ключа d:

$$17d = 1406560 \cdot k + a = 17d_{a=3} = 1406560 \cdot k + 3, \qquad (3.4)$$

и, полагая a=3, при k=6 находим $d_{a=3} = 82739$.

Противник, найдя разложение n=1408993=1181· 1193 и, предполагая, что имеет дело с классической системой RSA, будет, естественно, «атаковать» крипто замок при a=1, вида:

$$d_1 = 1406560 \cdot k_1 + 1. \qquad (3.5)$$

При этом $d_1 = 496433 > d_{a=3} = 82739$, что, как видно, значительно превышает значение ключа в реальной системе. Этот факт потребует большей операционной ёмкости на реализацию крипто аналитического алгоритма и загоняет противника, таким образом, за пределы возможностей ограниченных ресурсов его вычислительной техники.

Пример 2. Этот пример иллюстрирует, как, несмотря на знание разложения числа n на множители, противник сталкивается с другой проблемой – с неразрешимостью диофантового уравнения. При этом, как и в предыдущем примере, предполагается, что противник не знает о применении модернизированного алгоритма RSA.

Если в уравнении (3.5) левую и правую части уравнения умножить на 5, то получается крипто замок вида:

$$85d_1 = 1406560 \cdot k_2 + 5. \quad (3.6)$$

Противник, зная, что $e_1 = 85$ (открытый ключ) и легко раскладывая, как и в примере 1, число n на сомножители p=1181 и q=1193, получает диофантово уравнение для отыскания закрытого ключа d, но, естественно, при a=1, в виде:

$$85d_{a=3}=1406560 \cdot k_3+1. \quad (3.7)$$

Уравнение (3.7) неразрешимо вообще [1], в то время, как RSA-mAB при a=5 вполне нормально работает в диапазоне чисел вида $N < \sqrt{n}$. Действительно, взяв, например, в качестве открытого сообщения N=13, получается первый остаток по модулю (или открытое, шифрованное сообщение) при $e_1 = 85$:

$$N_1 = N^{85} (\mathrm{mod}\ 1408933) = 1262521 = 1{,}262521 \cdot 10^6,$$

второй остаток (дешифрованное сообщение), после возведения в степень $d_1 = 496433$, противник просто не сможет найти, в силу его промежуточного (в данном примере, возведенного в 5-ю или другую степень) значения, о чем противник не может знать.

Действительно:

$$N_2 = N_1^{496433} (\mathrm{mod}\ n) = 371 \cdot 293,$$

что есть 135 и открытое истинное сообщение $N = \sqrt[5]{N_2} = 13$.

Если потенциальный противник (хотя бы на некоторое время) не знает об использовании в (3.3) значения параметра $a \neq 1$, то есть об использовании расширенного алгоритма RSA-m, то такая модернизация обеспечит высокую надёжность RSA даже с малой длиной ключа [4, 93]. Если передаваемые блоки информации малы (короткие), а необходимо обеспечить высокую крипто стойкость (для чего и выбирается длинный ключ), то в этом случае вместо дополнения текста пустыми битами следует осуществить операцию возведения в степень. Криптостойкость такой системы будет никак не ниже криптостойкости классической RSA с такой же длиной ключа, а неопределённый для противника параметр a затруднит дешифрование. При этом следует учесть, что в случае размещения содержательной информации в M - блоках, нахождение a будет нелёгким делом, особенно, если значения a от блока к блоку будут меняться.

Ниже представлен сравнительный график оценки крипто стойкости различных алгоритмов через сравнение сложности решения задачи разложения числа на простые множители (задача факторизации) для следующих алгоритмов:

- Алгоритм Шора – предназначенный для использования на квантовых компьютерах алгоритм факторизации за полиномиальное от Log(n) время [135].
- Общий метод решета числового поля – наиболее эффективный на данный момент алгоритм факторизации из классических алгоритмов.
- Алгоритм RSA-m AB. Сложность Алгоритма RSA-m AB оценивается формулой:

$$O(exp\{(\alpha+1)\,[\ln n]^{r}\, ln\,[\ln n]^{n-r}\}+ O(A^{s}) \text{ или } \quad O\left(e^{1{,}9lg[N]^{\frac{1}{3}}\, lg([logN])^{\frac{2}{3}}}\right)+O(A^{S}),$$

то для оценки сложности дешифрования поля неопределенностей вводимого формантами можно применить формулу $O(A^{s})$, (где $A-$ длина алфавита, например, от 32 до 560 символов), $s-$ длина основания форманты (от 15 до 700 10-тичных разрядов или до 2048 и более бит). Количество возможных вариантов перебора даже при скромных числовых примерах дает огромные величины, Рисунок 3.5.

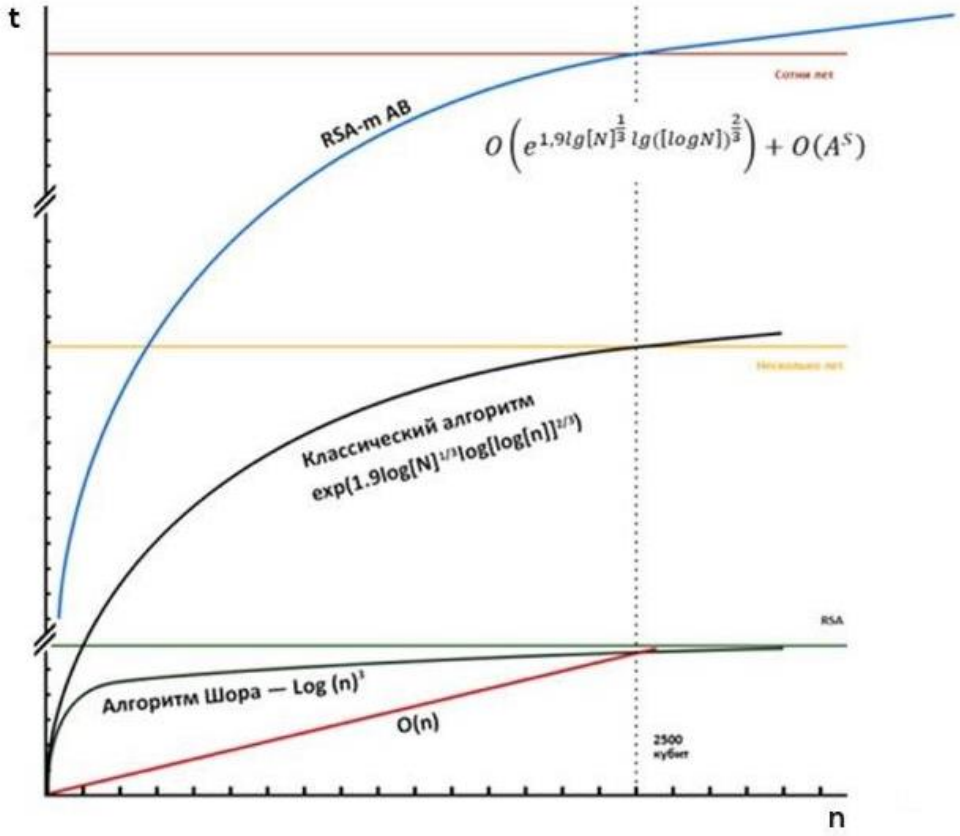


Рисунок 3.5. Сравнительный график оценки крипто стойкости различных алгоритмов к атаке «грубой силой» в постквантовый период (r = 2048 бит)

3.4 Выводы по Главе 3

Сравнительная низкая скорость работы криптосистемы RSA и высокая ее криптостойкость заставляют разработчиков искать пути для эксплуатации этой системы в обычной поточной передаче информации или для защиты информации в реальном времени. Здесь следует предложить подход, базирующийся не на передаче самой информации по открытому каналу, а в передаче некоторой специальной информации, которая может быть передана в зашифрованном виде с необходимой степенью криптостойкости при помощи RSA, без задержек во времени.

Суть предложенного подхода лежит в использовании свойств числовых формант, с помощью которых любое число представляется единственным образом. Причем время разложения и восстановления число на порядки меньше шифрования и дешифрования того же числа с помощью криптосистемы RSA.

Как известно, линейная форманта использует всего три параметра, а нелинейная форманта, в зависимости от ее мерности n – в $3n$ раз больше. Достоинством предложенного подхода является и то, что основанием (базой) форманты может быть любое число, как простое, так и составное, что значительно расширяет числовое множество, как для выбора базы при шифровании, так и ее вскрытия при криптоанализе.

В данной главе были предложены несколько алгоритмов использования формантного подхода для шифрования/дешифрования информации любой срочности секретности с существенным уменьшением времени прямой и обратной операций шифрования.

Применение расширенного алгоритма RSA вводит дополнительный неопределённый параметр a, подлежащий определению, что потенциально увеличивает время «взлома» и в случае шифрования краткосрочной (по секретности) информации может служить средством повышения крипто стойкости системы (например, при оперативных переговорах).

Введение дополнительного неопределённого параметра возможно и увеличило бы крипто стойкость, будь он достаточно большим, то есть не «поддающимся» так называемой «атаке грубой силы», то есть элементарному подбору, но поскольку в предлагаемом подходе на его размер налагаются определённые ограничения, то увеличение стойкости он даёт только при частой смене ключей.

4 СИСТЕМА АСИММЕТРИЧНОГО ПОБИТНОГО ШИФРОВАНИЯ ФОРМАНТЫ РЕЧЕВОГО СООБЩЕНИЯ

4.1 Преимущества систем, использующих алгоритм RSA-mAB с быстрой сменой ключей

Одной из современных тенденций в криптографии является разработка новых методов, обеспечивающих информационную безопасность, даже если ожидаемые квантовые компьютеры преуспеют в разрушении (взломе) традиционных методов и криптосистем, таких как RSA [103, 121, 122, 132, 148].

Применение формантного анализа - эволюционный способ разработки средств криптографической защиты на основе модифицированных алгоритмов RSA-mAB. Это объясняется тем, что они позволяют использовать уже существующие подходы к защите информации на фоне экспоненциального роста вычислительной мощности быстро развивающихся квантовых компьютеров. Проблема с алгоритмом RSA уже ясна - через некоторое время задача факторизации большого числа перестанет быть неразрешимой проблемой для вычислительной мощности компьютеров [125-126]. Но увеличение вычислительной сложности проблемы может быть решено уже сегодня, например, путём изменения одного и/или введением новых дополнительных параметров в предлагаемую реализацию алгоритмов формантного анализа для шифрования / дешифрования данных.

Предложенные алгоритмы в третей главе далее будут использованы в отношении защиты данных в системах голосовой связи, где, с одной стороны, существуют значительные временные ограничения на процесс шифрования / дешифрования данных, и с другой стороны существует требование обеспечить гарантированную криптографическую стойкость. Включение в процесс шифрования дополнительных параметров криптографирования, связанных с использованием формант, усложняют задачу взлома, требуя на эти операции дополнительное время, которое очень велико. При скоростях дискретизации голосовой связи от 4-до 12 кГц это время превышает все мыслимые величины здравого смысла. Поэтому такой крипто системе с комбинированным и модернизированным алгоритмом RSA-mAB не страшен надвигающийся кризис современной криптографии, связанный с появлением фантастически скоростных квантовых компьютеров.

Квантовые компьютеры будут уничтожать (взламывать) самые популярные криптографические системы с открытым ключом, включая RSA, DSA и ECDSA. Но уже разрабатываются криптографические алгоритмы и системы следующего поколения, которые будут противостоять атакам с использованием квантовых компьютеров: в

частности, системы пост-квантового шифрования и системы подписи с открытым ключом [5, 111, 158].

Ключи шифрования и дешифрования постоянно изменяются, причём они генерируются (или выбираются из матриц ключей) случайно, что исключает возможность предугадать следующую пару ключей. За период времени, который необходим для факторизации открытого ключа, крипто ключи успеют измениться, причём неоднократно, как и значение плавающего кода [126]. Более того, чтобы вскрыть систему взломщик должен знать число N и открытый ключ. Он не имеет возможности определить даже длину (разрядность) числа N, то есть, он не знает, какое число надо факторизовать. В то же время все изменяемые параметры достижимы и легко реализуются в существующем оборудовании и не приводят к критическим временным задержкам вычисления параметров в реальном времени, а именно скорости шифрования / дешифрования.

Устраняется основной недостаток систем, основанных на RSA: недостаточное быстродействие. Ведь предлагаемые алгоритмы не гарантируют крипто стойкость на очень долгое время, достаточно гарантировать, что ключ не будет расшифрован в течение некоторого временного промежутка, достаточного для того, чтобы коды сменились. В этом случае достаточно удовлетвориться довольно короткими ключами, генерация которых не займёт много времени.

4.2 Описание системы асимметричного побитного шифрования форманты речевого сообщения

Система относится к области криптографических преобразований и защиты передаваемой побитно или пакетами конфиденциальной и хранимой информации для использования в вычислительных и информационных системах, в онлайн платёжных системах, в локальных корпоративных сетях, в системах радиосвязи, информационно-управляющих комплексах, в системах массовой мобильной (сотовой) телефонии, конфиденциальной телефонной цифровой связи государственных, коммерческих, охранно-сигнальных предприятий и финансовых структурах [48, 68].

Особенностью данной системы является применение в режиме реального времени (он-лайн) асимметричного побитного (потокового или блок-фонемного, блочного 32-битного) шифрования форманты речевого сообщения то есть адекватного ему аналога в виде модели (образ, свёртка) алгоритмами RSA-mAB с сохранением присущего алгоритму RSA высокого уровня крипто стойкости, но используя с высокой частотой смены короткие длины крипто-ключей, достаточных для обеспечения краткосрочного уровня защиты

переговоров (3-10 мин.), а при увеличении уровня долгосрочности (до нескольких месяцев и лет) предусматривают изменение и длины крипто ключей до величин, обеспечивающих заявляемый уровень криптостойкости при повышенных временных интервалах секретности [3, 4].

Заявляемый способ предполагает реализацию статистически независимого кодирования шифрованием форманты то есть уменьшенного (сжатого) объёма исходной информации и её избыточности, а также повышение её энтропии (среднее количество информации, приходящееся на один символ, фонему или дискрету), так как в сжатом контексте будут отсутствовать статистически часто повторяющиеся буквы, слова, фонемы и даже дискреты, что существенно затруднит дешифрование для противника, то есть криптоанализ. Задачи, решению которых способствует заявляемый способ и возможные на его основе системы защиты информации, передаваемой по каналам связи, это - повышение качества криптографической обработки информации различной длительности секретности, то есть скорость и стойкость, повышение быстродействия процедуры шифрования/дешифрования за счёт уменьшения объёма информации в шифрованном сообщении, а также расширение функциональных возможностей и областей применения заявляемого способа защиты двоичной информации [48, 68].

Опираясь на правило О. Керкгоффса (1835-1903): «стойкость шифра должна быть обеспечена в том случае, когда известен весь алгоритм шифрования, за исключением секретного ключа», в заявляемом способе для шифрования двоичной информации при её передаче по открытому каналу передают не исходную информацию, а её образ, адекватную модель, т.е. некоторые не очевидные сведения о ней, известные только принимаемой стороне, или внутреннему ПО шифрующего устройства, на основании которых исходную информацию легко восстановить. Для этого используют, например, одну или многомерную числовую форманту (в классической теории чисел — это широко известная линейная форма, используемая совсем в других целях и применениях, не имеющих ничего общего с крипто- алгоритмами, да и вообще с преобразованием информации), значения параметров которой (форманты) изменяются во времени в зависимости от значения цифрового представления защищаемой информации. Саму форманту передают в зашифрованном виде с помощью алгоритма $RSA - mAB$ [3, 4].

Известны десятки патентных методов и соответствующих им устройств криптографической защиты информации, а также Российские патенты Молдовян А.А., М.А.,Н.А. RU №№2188513, 2211541, 2172075, 2212108 и 2206182 (Клепов А.В.), которые можно рассматривать, как аналоги. Известные системы характеризуются сложностью

алгоритмов, эксплуатации, достаточно громоздким исполнением и недостаточной криптостойкостью закрытия данных при приёме/передаче в режиме он-лайн.

Предлагаемый способ выгодно отличается от известных шифрующих устройств (например, RU 209/2096918(Волков С.С. и др.), RU 209/2099885 (Аверин С.В. и др.), RU 209/2091983 (Чижухин Г.Н.), или системы Lucifer фирмы IBM и стандарта шифрования данных национального бюро стандартов США) возможностью побитного шифрования двоичной информации с использованием неизвестного пользователю ключа необходимой длины. Это делает способ удобным при решении конкретных задач скрытия информации в системах радиосвязи [48].

Известен способ асимметричного шифрования RSA (патент США № 4405829, разработанный в 1977 году в Массачусетском технологическом институте (США)), который получил название по первым буквам фамилий авторов (Rivest, Shamir, Adleman), предназначенный для криптографической защиты информации в вычислительных и информационных системах и заключающийся в шифрование цифровых, обычно 64-битовых блоков, с помощью двух ключей – открытого и закрытого, основанный на использовании односторонних функций и арифметики больших чисел, больше 10^{12} и более, $10^{60} \dots 10^{150}$, и на вычислительной сложности задачи разложения большого числа на простые множители (отыскания делителей большого числа) за разумно короткое время. Существенным недостатком этой криптосистемы является её низкая скорость работы.

Известен российский патент RU 2108002, авт. Федоров и др. «Шифрующее-дешифрующее устройство», содержащее на передающей стороне последовательно соединённые генератор ключа и шифрующий блок, другой вход которого соединён с выходом источника информации, а также генератор случайных чисел, а на приёмной стороне - приёмный блок, выполненный в виде дешифрующего блока, выход которого соединён с потребителем информации, а также канал связи, с введёнными на передающей стороне последовательно соединённые умножитель на открытый ключ, первый вход которого соединён с выходом шифрующего блока, а второй вход соединён с выходом генератора ключа, и сумматор по модулю два, второй вход которого соединён с выходом генератора случайных чисел, а выход соединён с первым входом канала связи, а на приемной стороне - блок формирования открытого ключа, передаваемого в канал связи, выполненный в виде умножителя матриц, декодера, принимающего шифрованный сигнал и дешифратора.

Недостатком устройства является сложность формирования открытых ключей, необходимость генерирования псевдослучайных последовательностей, недостаточное быстродействие для работы в режиме реального времени.

Требуемый технический результат заключается в повышении криптостойкости.

Известен, также способ и система защиты информации, передаваемой по каналам связи, включающая связанные в единую сеть оконечное оборудование данных, прибор криптографической обработки информации оконечного оборудования данных, каналы связи (патент РФ № 59921 на полезную модель «Система защиты информации, передаваемой по каналам связи, и прибор криптографической обработки информации оконечного оборудования данных», МПК H04L 9/00, H04K 1/06, опубл. 27.12.2006 г.)

Известная система также характеризуется ограниченными функциональными возможностями и низкой производительностью, поскольку не обеспечивает возможности одновременной работы с несколькими ПЭВМ и не позволяет обрабатывать более двух файлов (информационных пакетов) - один из которых является входящим, а другой - исходящим. Кроме того, система не защищена от случайного вмешательства в работу прибора криптографической обработки информации.

Также из известных наиболее близким аналогом (прототипом) по своей технической сущности заявленному способу шифрования является по патенту Российской Федерации 209/2096918 «Способ шифрования двоичной информации и устройство для его осуществления» (авторы Волков С.В и др.) и по патенту Российской Федерации (19) RU (11) 2091983 (13) C1 (51) 6 H04L 9100, G06F 12/16 автор Чижухин Г.Н «Способ шифрования двоичной информации и устройство для его осуществления». В устройстве по этому способу открытую информацию на передаче шифруют в виде M −разрядного блока зашифрованной информации с помощью N −разрядного ключа путём суммирования и преобразования, а на приёме принятый M −разрядный блок зашифрованной информации расшифровывают в открытую информацию с помощью N −разрядного ключа путем суммирования и преобразования, то есть формируется K групп по n бит, где $n-$ длина части обрабатываемого текста, причём каждая из групп обрабатывается в зависимости от значения N −бит секретного ключа, с перемешиванием поточного шифра по случайному закону. Поточный шифр суммируют по модулю 2 с порцией сообщения. Устройство содержит регистр секретного ключа, блок управления, четыре последовательно-параллельных регистра, регистр показателей степени, блок перемешивания бит, логический блок с сумматором по модулю 2, элементы «И», «ИЛИ» и др [48].

По существу, в устройстве по патенту № 2091983 сделана попытка для каждой порции информационного сообщения на основе единственного секретного ключа построить «индивидуальный», как они называют, поточный шифр с учётом значения самой порции сообщения. Недостатком этого устройства является использование в его структуре весьма сложного устройства возведения n −битного кода $(i-1)$ группы поточного шифра в степень m по модулю P, а также использование одного фиксированного секретного ключа с числом бит, равным разрядности одной «порции» сообщения. Недостатком также является сложность формирования открытых ключей, необходимость генерирования псевдослучайных последовательностей, недостаточное быстродействие для работы в режиме реального времени [48].

Известны способы защиты информации по Российскому патенту RU 140/2325695 «Система защиты информации», авт. Хренов В.П. и по патенту RU 220/2206182 «Способ криптографической защиты информации в информационных технологиях и устройство для его осуществления», авт. Клепов А.В. В этих патентах заявляется Способ генерации ключей для защиты информации, где в качестве указанных ключей используют последовательность простых чисел подряд, каждому из ключей ставят в соответствие индекс, присвоенный персональному номеру пользователя, при этом по сигналам точного времени осуществляют регулярный сдвиг всех ключей, получая, таким образом, для каждого одноразового ключа новое простое число из указанной последовательности простых чисел, соответствующее заданному персональному номеру пользователя и являющееся персональным ключом пользователя на заданный промежуток времени, полученные одноразовые ключи с заданным персональным номером пользователя предназначают для использования в криптографических протоколах.

Недостаток заключается в использовании одной и той же регулярной последовательности простых чисел для крипто ключей, а для повышения сложности (стойкости) их вскрытия используют случайную точку отсчёта для случайной выборки чисел, регулярность которой сохраняется. Кроме того, нужен генератор простых чисел и тестирование их на простоту, что занимает достаточное время, не позволяющее в совокупности всех необходимых операций по защите информации, использовать данный способ для защиты речи в онлайн режиме [48].

Близкими по совокупности технических признаков к заявляемым способу и устройству (прототипом) являются Российский патент 8/83861 (авторы Трушкин О.В и др. «Мобильное устройство защиты информации с повышенным уровнем защищённости» и патент 8/83862 тех же авторов «Мобильное устройство защиты информации»,

предназначенные для осуществления криптографически защищённого информационного взаимодействия пользователя с информационными и телекоммуникационными сетями и системами, содержащие энергонезависимую память, адаптер интерфейса и процессор, о снабжённый встроенным аппаратным генератором случайных чисел, выполненным, по меньшей мере, на одном шумовом диоде, а во втором патенте последний выполнен на многофункциональном микроконтроллере, аппаратно реализующем ряд используемых в мировой практике криптографических алгоритмов, и построен так, чтобы все ключи шифрования использовались только внутри него и никогда не передавались бы через интерфейс, и доступ к критичным данным, хранящимся в энергонезависимой памяти процессора, был бы возможен также только изнутри него.

Недостатки этих способов заключаются в том, что они, как и все выше перечисленные изобретения, работают с исходной информацией, а не с её уменьшенными по объёму адекватными аналогами - образами моделями или свёртками и поэтому скорость их работы не соответствуют тому, чтобы эти способ и устройство могли быть применены для передачи речевой информации в реальном времени из-за большого запаздывания, вносимого процедурами шифрования речи.

4.3 Системы защиты речевого канала связи с использованием методов криптозащиты на базе RSA-mAB

Предлагается рассмотреть процедуру реализации идеологии RSA в широкополосных каналах связи в качестве основной криптосистемы закрытия информации, но при этом используется малая длина ключа, с весьма частой и быстрой его заменой. Так как диалог по защищённой линии необходимо обеспечивать в реальном времени, то защита информации основывается на потоковом шифрование (алгоритм RSA-mAB1), в отличие от RSA, когда формируются и шифруются блоки информации [3, 4, 48, 68].

Выигрыш этого метода защиты речевого канала связи состоит не в использовании длинных ключей, требующих при «взломе» неразумно много времени на факторизацию очень большого числа, а в частой смене относительно коротких ключей, каждый из которых предназначен для шифрования отдельной дискреты. Это потребует от противника дополнительных затрат машинного времени на раскрытие каждой дискреты в отдельности. Заметим, что «взлом» речевых дискрет существенно отличается от взлома текстовой информации. В последнем случае при дешифровании текста допустимы пропуски не только отдельных букв, символов, но даже и слов, тем не менее, скрытый текст можно будет

восстановить, если его рассматривать как некоторую осмысленную информацию, но совсем другое дело со звуком.

Звук – это достаточно большой набор дискрет в цифровом представлении речевой или звуковой информации. Если звук имеет постоянную интенсивность и частоту – то это монотонное звучание. А в человеческом голосе присутствует огромное количество обертонов и тонов (дискрет различной квантованности или просто высоты, амплитуды). Именно это обстоятельство и создаёт трудности при раскрытии закрытой речевой информации «по одной дискрете», которые лежат в основе высокой криптостойкости предложенного способа шифрования.

4.3.1 Описание действия полностью открытой криптосистемы RSA-mAB1, mAB2

Перед сеансом связи обеими сторонами переговоров будет запущена процедура инициализации, инициирующая указатели адресов всех матриц в начальное (исходное) положение, при котором на приёмной и передающей сторонах все содержимое матриц абсолютно одинаковы по содержимому ячеек и по их адресам.

При установлении связи сторона «инициатор» (A) отправляет приёмной стороне ($Б$) первое зашифрованное сообщение, содержащее случайно выбранный из своей базы данных открытый ключ $\{e, n\}$ (заранее сгенерировав закрытый ключ $\{d, n\}$). Полученный открытый ключ, будет использован стороной ($Б$) для шифрования своего сообщения, содержащего, в свою очередь, пару собственных открытых крипто-ключей, стороне (A). Таким образом, основная идея организации защищённой он-лайн передачи информации между сторонами переговоров заключается в постоянной смене открытых ключей (достаточно коротких по длине для поточной передачи данных), что является альтернативой использованию длинных ключей, так как потребует от крипто-аналитика постоянных затрат машинного времени на определение и факторизацию базового числа n для компрометации новых ключей [3, 4, 48, 68].

В другом альтернативном варианте ключи не будут передаваться в зашифрованном виде, а передаваться будет кодовая информация о них, например, об адресах их расположения на каких-то серверах (алгоритм RSA-mAB3) или в ПЗУ приёмника.

Приведённый пример показывают, что шифрование голосовой связи происходит без непосредственного участия абонентов в процессе обмена ключами. В канале связи не фигурируют явно параметры форманты или алгоритма RSA-mAB. В патенте авторов [48] заявлены разные алгоритмы, требующие передачи либо всех сразу параметров форманты,

либо по отдельности. Если передаются только индексы ячеек, где находится информация для восстановления форманты, то для взлома такого шифра потребуется атака сплошного перебора (англ., brute-force) из n дискрет (где n – частота дискретизации), которая оценивается огромной временно́й величиной в миллиарды миллиардов лет.

Действительно, при частоте дискретизации голосового сигнала 8-10 кГц (с максимальной частотой гармоник в сигнале 4-5 кГц , см. п. 4.3.2) злоумышленнику для восстановления даже хотя бы секундного разговора, который дает мизерную информацию о сути переговоров и абонентах, понадобится выполнить $(8 \cdot 10^3)!$ операций сопоставления очерёдности следования дискрет за 1 сек., ну пусть за 10 сек. (тогда рассекречивание мобильного разговора будет идти с существенным запаздыванием и выйдет за границы гарантированного срока секретности). И это только на одном периоде, за 1 сек. А чтобы узнать голос, разобрать смысл сказанного, надо обработать, как минимум, 10 периодов (10 секунд низкочастотных периодов колебаний, то есть огибающей несущей частоты). Считаем: чтобы это сделать при сплошном переборе (угадывание или подбор речи по голосу или по смыслу – это разные временные задачи), нужно предыдущую оценку проделать не менее 10 раз, то есть даже при 1000 это очень большое число. Действительно, зная, что $1\ \text{год} = 3{,}15 \cdot 10^7\ сек$:

$$10 \cdot \left((8 \cdot 10^3)!\right) \gg 1000! = 4{,}023872600770937735437024339 23\text{E} + 2567\ \text{сек} =$$

$$= 1{,}275961631396162397081755561653 4\text{E} + 2551 \approx 10^{2551}\ \text{млрд лет}$$

огромное число, которое трудно оценить сразу и выходит за рамки здравого смысла при оценке реального времени взлома. При быстродействии 10^9 и даже больше операций умножения в секунду выполнение такого количества сравнений перестановок потребует даже при более низкой скорости дискретизации в 1 кГц уже 10^{2551} миллиардов лет. И с ростом частоты дискретизации f, Гц или, что то же самое, числа дискрет $n = \frac{1}{T} = f$ это время взлома экспоненциально растет.

Так, при увеличении полосы частот голосового сигнала с 8 до 12 кГц число лет, необходимых для взлома 10-ти секундного разговора или передачи аналогового сигнала вырастет и будет больше, чем при $n = 1000$ для частоты 1 кГц и 10 секундах прослушивания. Действительно: при частоте дискретизации $n = 1$ кГц односекундный разговор потребует с учетом скорости обработки и перевода секунд в года делением на 10^{-16} 1000!=1,27596163139616239708175556165 34E+2560 сек, или при скорости работы компьютера до $10^9\ \frac{\text{умнож}}{\text{сек}} = 1{,}275961631396162397081755561653 4E + 2560$ сек. или будет равно $1{,}3 \cdot e^{2544}$ млрд лет.

При $n = 12$ кГц число вариантов перебора за 10 секунд = 120 000! И время взлома вырастет в десятки тысяч и миллионы раз по сравнению с 1,3E+2551 млрд лет.

Такие оценки криптостойкости алгоритмов формантного анализа получаются, если будет увеличивается частота дискретизации голосового или аналогового сигнала или длина алфавита при передаче символьного текста.

4.3.2 Работа и стойкость алгоритма шифрования и защиты передачи данных

Оцифрованный сигнал в виде набора последовательных значений (дискрет) амплитуды в случае, когда записываются абсолютные значения амплитуды, называется формат записи PCM (Pulse Code Modulation). Стандартный аудио компакт-диск (CD-DA), применяющийся с начала 80-х годов 20-го столетия, хранит информацию в формате PCM с частотой дискретизации 44.1 кГц и разрядностью квантования 16 бит. Согласно теореме Котельникова для того, чтобы однозначно восстановить исходный сигнал, частота дискретизации должна минимум в два раза превышать наибольшую частоту в спектре сигнала [48].

Так как верхний предел слуха 20 кГц, то в идеале частота дискретизации должна быть не меньше 40 кГц. Именно поэтому стандартная частота дискретизации, использующаяся при записи компакт-дисков, составляет 44,1 кГц (так называемое CD-качество). Впрочем, частота дискретизации может быть и выше, но такое качество звука используется лишь в звукозаписывающих студиях.

Частота дискретизации 44,1 кГц — это не всегда достижимый идеал, на практике обычно используются частоты дискретизации в два, четыре и восемь раз меньшие, чем 44,1 кГц:

22,05 кГц — радио-качество, используется при кодировании звука FM-радиостанциями.;

11,025 кГц — телефонное качество, частота дискретизации, подходящая для передачи человеческого голоса, которая используется в IP −телефонии;

5,5 кГц — звук на грани потери информационной составляющей.

Итак, частоту дискретизации выбирают равной $2f_{max}$ в частотном спектре голосового канала. Считая, что граничная частота звукового канала сотовой связи 40 кГц, примем для модельного варианта частоту квантования 12 кГц $\rightarrow T_{\text{выборки}} = 12\,000\,\frac{\text{дискрет}}{\text{сек}}$. То есть, при передачи речи или звука шифруется каждая дискрета оцифрованной амплитуды аналогового сигнала, со скоростью 12 000 дискрет в секунду.

При разрядности АЦП 12 бит или $2^{12} = 4096$ чисел и частоте дискретизации 4 ... 50Гц, период выборки оказывается в пределах от 250 мкс до 20 мкс, что предъявляет повышенные требования к обработке числовой информации при работе в режиме реального времени.

Так, при частоте выборки в 12 кГц значения дискрет речевого звука при IP −телефонии и 12-разрядном АЦП представляют случайный набор натуральных чисел в интервале чисел от 1 до $4096 = 2^{12}$. Чтобы, например, 3-х минутный разговор, не прерывался вынужденными «паузами молчания», затрачиваемыми на обработку миллиардов битов, скорость обработки и пропускная способность канал связи и микроконтроллерной и компьютерной техники должны быть весьма высокими.

Суть способа шифрования двоичной информации лежит в использовании свойств форманты [48], с помощью которых любое число представляется единственным образом в виде трёх небольших чисел, существенно меньших по абсолютной величине, чем исходное большое число.

Для реализации формантного подхода в подготовке исходного сообщения для шифрования в заявляемом устройстве формируют матрицы KN размером $n \times n$ для хранения чисел-модулей $N = p'q'$, вычисленных в соответствии с алгоритмом Эйлера на основе простых чисел p' и q' криптопреобразования RSA и заранее подобранных к ним пар крипто-ключей e_i и d_i с различной длиной $\mu(s_i)$ бит, а также матрицу PF для хранения оснований p_i, ядер k_i и остатков q_i формант, соответствующих открытому коду сообщения и матрицу R, размером $n \times n$ для хранения M −разрядных случайных битовых последовательностей для кодирова-ния шифрованных блоков информации.

В процессе трансляции разговора по каналу связи (радио, мобильный телефон, интернет и др.) каждую дискрету на выходе АЦП с амплитудой $A_d(t_i)$ бит рассматривают, как адрес расположения крипто-ключей, размещённых в ПЗУ в матрицах PF объёмом 2^{32}, где крипто-ключи распределены по адресам случайным образом, т.е. адрес матрицы не совпадает со значением дискреты.

Шифрование производится в два этапа: 1) нахождение параметров форманты – ядра k_i и остатка q_i для очередной амплитуды $A_d(t_i)$ дискреты (или блок-фонемы) по основанию p_i; 2) шифрование алгоритмом $RSA - m$ параметров форманты k_i и q_i по модулю N_i своим индивидуальным крипто-ключом e_i, (i −номер шифруемой/дешифруемой дискреты или информационного блока, причём, согласно алгоритму криптосистемы RSA $e_i d_i (\mathrm{mod}\, N) = 1$). После каждого сеанса связи адресация ключей в ПЗУ автоматически

меняется согласно алгоритму ПО. Таким образом, заявляемый способ фактически эквивалентен шифрованию сообщения одноразовым ключом со случайной длиной, в зависимости от длины сообщения в виде дискреты или блока (согласно выбранному алгоритму), что соответствует выполнению условий теоремы Шеннона о невозможности расшифровки [124].

Действительно, информация передаётся через накопительный буфер, откуда формируются пакеты (блоки) по 32 бита или 4 байта. Эти блоки содержат также информацию о восстановлении реальной информации и способе её воспроизведения в режиме реального времени (или как её записать в память: как зашифрованную, или как восстановленную информацию). Формат блока данных содержит и служебные биты о составе и структуре передаваемого пакета информации.

4.3.3 Различные алгоритмы шифрования

1 вариант (алгоритм RSA-mAB1) - самый простой и самый не защищённый – по закрытому каналу передаётся адрес ячейки, в которой находится значение очередной дискреты, в виде форманты (p, k, q), зашифрованной с помощью алгоритма RSA – m [3, 4].

Понятно, что в связи с ограниченным числом возможных дискрет (их всего 4096) их всех можно заранее упорядоченно расположить в памяти. Первый способ – значение дискреты – это и есть её адрес в ПЗУ приёмного или передающего устройств.

Дальнейшая главная задача – зашифровать этот адрес. Например, путём какой-нибудь маски или с помощью RSA-m.

Шифрование путём простого перемешивания. Исходное состояние – значение содержимого ячейки и есть адрес хранения этого содержимого в матрице. Например, число 3253. Оно должно храниться в ячейке № 3253. Но, кроме этого, там же хранятся и значения всех параметров для её шифрования и дешифрования [48, 68].

Перемешиваются случайным образом адреса матрицы дискрет. Например, №3253 стал №1900. Последний адрес шифруется в системе формант (p, k, q) с помощью RSA − m и передаётся в открытый канал. Хотя дискрета – прежняя, её значение по-прежнему равно 3253, но теперь она будет храниться в ячейке №1900, который зависит от форманты чисел 1900 (или 3253, в зависимости от перемешивания адресов).

2 вариант (алгоритм RSA-mAB2). Шифруется каждая форманта дискреты (то есть p, k, q - основание, ядро и остаток) с помощью RSA − m, шифрованные числовые параметры которой передаются он-лайн в открытый канал [48].

4.3.4 Шифрование 4096 возможных значений дискрет звука

Для каждой дискреты выбирается, например, 10000 разных пар ключей RSA (матрица KN 100×100) для различных оснований N_i. Создают для каждой дискреты свой шифр-текст или крипто-дискрету. Поэтому для 4096 реальных дискрет понадобится $4096 \cdot 10^4 \approx 4 \cdot 10^7 \approx 2^{21} = 524288$ 32-битных ячеек памяти для хранения вариантов шифр записей дискрет (полагая, что $10 \approx 2^3$) что равно $524{,}288$ кБайт ячеек памяти, т.е. чуть больше 0,5 мБ памяти ПЗУ.

А при выборе для каждой дискреты 10 000 разных пар ключей крипто замка RSA (матрица 100×100) для 4096 реальных дискрет понадобится $4096 \cdot 10000 = 4096 \cdot 10^4 \approx 4 \cdot 10^7 \approx 2^{23} = 8388608$ бит или 8,5 мБ ячеек памяти для хранения вариантов шифр-записей дискрет [48].

Хранение шифрованных дискрет (M1)

Пусть имеется матрица $M1$ $300 \times 300 = 900\,000$ ячеек, что в два раза больше необходимых для размещения $409600 \approx 410\,000$ чисел длиной до 32 двоичных разрядов. Расположить их надо так, чтобы время поиска случайного числа в этом диапазоне было минимальным.

Содержимое ячеек $M1$ – это форманты дискрет, точнее их параметры ядро k, остаток q и основание p в «чистом виде» или зашифрованные каким-либо шифром.

Длина ключей RSA-m

Длина ключей выбирается из расчёта минимального времени затрат на крипто-обработку. Поэтому длины открытого и закрытого ключей примерно одинаковы. Часто открытый ключ выбирают на порядок или даже два порядка меньше закрытого ключа. В системах краткосрочной секретности передачи данных ключи можно выбирать в диапазоне до 2-х байт.

Подготовительная работа с памятью

Создается набор матриц: $MAD -$ матрица адресов дискрет, $MADE -$ матрица шифрованных дискрет, $PF -$матрица текущих оснований формант, $PN -$ матрица крипто-замков и все матрицы заполняются, то есть записываются в память ПЗУ в виде целых чисел все значения дискрет из 4096 возможных, то есть ряд $\overline{1, 4096}$ для MAD, ряд $\overline{1, 409600} -$ для шифрованных значений дискрет матрицы $MADE$ и ряд значений простых и составных оснований для матрицы PN.

Вычисляются форманты всех дискрет по 10000 основаниям и записываются в матрицу 5000×100. Всего 500 000 формант.

Последовательность расположения дискрет в ячейках матрицы 5000×100 шифруется путём перемешивания (100×100 вариантов: 100 по строкам и 100 по столбцам. Всего 10000 перемешиваний-вариантов расположения дискрет в матрице). Всего будет 100 матриц типа $M1 \ldots M100$.

Шифруются все дискреты тройкой параметров формант p, q, k и записываются в память в виде индексов матриц $M1$. Таким образом у одной и той же дискреты в ПЗУ будет существовать 10000 различных индексов-адресов в матрице типа $M1$.

Такое же распределение ПЗУ формируется и на приёмной стороне [48, 68].

Работа на передающей стороне

1. Оцифровывается звук, речь при помощи АЦП.

2. Работа с очередной дискретой которая записывается в буфер:

а) переводится значения дискреты в целое битовое число;

б) вычисляется форманта (или ищется такое число в ПЗУ) и записывается его адрес в память ОЗУ (по этому адресу в ПЗУ будут находиться все сведения о текущем целом числе).

3. Формируется сигнал-текст посылки: передаются 4 адреса: 3 адреса для p, q, k и 4-й адрес для контроля переданной информации в контрольной ячейке.

Работа на приёмной стороне

1. Приём сигнала и его анализ. Читаются адреса p, q, k и сравниваются их значения с данными в контрольной ячейке.

2. Собирается речевой сигнал по адресам дискрет.

3. Воспроизводится сигнала с помощью РПУ.

На рисунке 4.1 представлена передача данных, которая происходит следующим образом: Микрофон → АЦП → Вычисление форманты очередной дискреты (в виде целого числа) → нахождение адреса ячейки очередной форманты → запись в память (буфер) → формирование шифрованного сигнала-текста посылки: → передача шифрованного адреса ячейки в эфир → .... → приём шифрованного сигнала-текста посылки → декодирование → дешифрование → декомпозиция принятой посылки → воспроизведение речи [48].

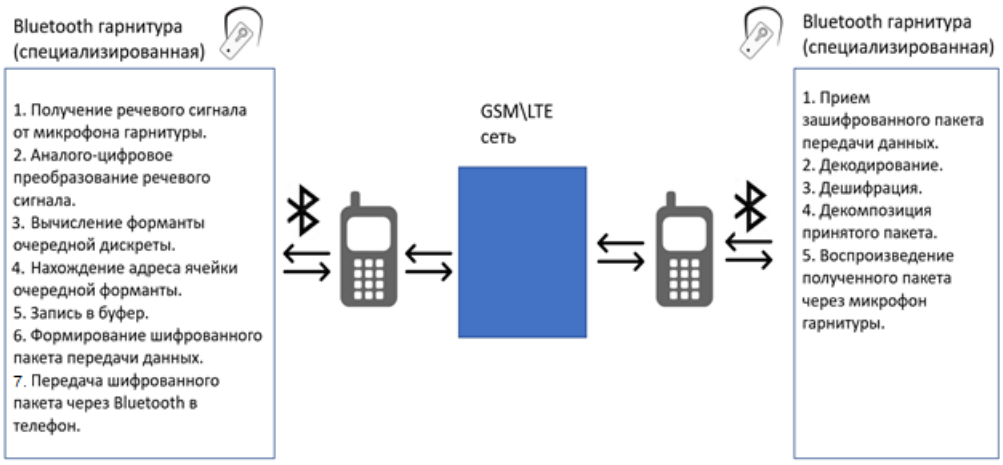


Рисунок 4.1. Инфограмма устройства защищённой мобильной передачи данных

4.4 Выводы по Главе 4

В этой главе были рассмотрены и выделены достоинства и недостатки наиболее популярной крипто системы RSA.

Была обоснована необходимость модернизации RSA для исправления некоторых недостатков на основе алгебры нового направления в теории чисел – формантного анализа.

Сформулирован, опробован и исследован алгоритм защиты информации, базирующийся на платформе RSA с использованием преобразования исходной информации на основе методик формантного анализа.

Все рассмотренные выше примеры подчеркивают, что зашифрованные голосовые сообщения, передаваемые в режиме реального времени со скоростью передачи примерно 64 kb/сек возможны при использовании коммуникационных каналов, таких как Телеграм или Мессенджер. Совершенно ясно, что возможны и другие варианты использования формант для передачи не только речи.

Практическая значимость работы подтверждается реальным интересом к предложенному решению по защите данных со стороны компаний, предлагающих решения в различных областях экономики. В Приложении №1 приведены письма от компаний, которые сейчас уже используют, либо планируют использовать разработанный криптоалгоритм RSA-m в собственных проектах.

Компания Kvazar-Micro SRL, специализируется на разработке и внедрение систем контроля и мониторинга технологических процессов в рамках концепции интернета вещей для промышленных предприятий (IoT), включая предприятия агропромышленного комплекса. Подобные решения характеризуются большим объемам обмена данными, при этом каждый пакет передачи данных является сравнительно небольшим. Для многих

предприятий, в которых внедряются системы мониторинга и управления техпроцессом, основанные на передачи данных в сети Internet/Intranet, защита передаваемых данных становится вопросом первостепенной важности (целостность данных, несанкционированный доступ и коммерческая тайна). При этом актуальна задача минимизации размера трафика обмена данными, особенно через мобильные сети. Для этой задачи решено использовать алгоритм RSA-m для пакетного шифрования данных в гибридных сетях в рамках поставляемых решений.

Компания Alfasoft разрабатывает и внедряет информационные системы для государственного сектора, в частности для судебных инстанций. Решения компании внедряются и используются в десятках стран мира. Ключевой задачей для создаваемых компанией систем документооборота является вопрос информационной безопасности в части передачи и обмена данных с учетом экспоненциального роста объема электронного документооборота и существенно возросших рисках кибертерроризма во всем мире. В качестве одной из опций по обеспечению информационной безопасности компанией принято решение предлагать клиентам использование алгоритма RSA-m. Одно из важнейших преимуществ предложенной реализации алгоритма является возможность использования RSA-m без внесения каких-либо существенных изменений в существующие информационные системы заказчика.

Компания QSystems специализируется на создании современных платежных систем, которыми пользуются физические и юридические лица в более чем 8 странах мира. Одним из таких проектов является проект Мрау в Молдове, через который ежегодно проходит свыше 5 млн. платежей в год. В создаваемых системах компания использует реализации классических RSA алгоритмов. С учетом резкого ежегодного повышения числа платежей, прежде всего, микроплатежей, компания постоянно отслеживает новые методы и инструменты обеспечения необходимого уровня надежности и безопасности финансовых транзакций. Компания планирует использование алгоритма RSA-m после проведения внешнего аудита предлагаемого криптосредства по требованию платежных систем.

ОБЩИЕ ВЫВОДЫ И РЕКОМЕНДАЦИИ

Данная работа является целенаправленным исследованием оригинальных методов, процедур и алгоритмов, используемых для защиты информации в интероперабельных платежных системах. Разработанные в диссертационной работе методы могут быть успешно использованы для защиты информации краткосрочной и долгосрочной временной секретности в интероперабельных платежных системах, где обработка и передача данных происходит в онлайн режиме.

Анализируя результаты, полученные в диссертационной работе, следует сделать следующие выводы:

1. Для обеспечения интероперабельности платежных систем и необходимого уровня безопасности необходимо использовать такие средства криптографии, которые совместимы, максимально масштабируемы с точки зрения криптостойкости и обладают высокой скоростью работы в свете ожидаемого экспоненциального роста количества транзакций в ПС. Достижения квантового превосходства может поставить под угрозу безопасность всех текущих платежных систем, которая основана на текущих криптографических механизмах. Замена текущей криптографии на что-то принципиально другое приведет к колоссальным издержкам и потерям, таким образом есть острая необходимость в усилении крипто стойкости существующей криптографии, не меняя её принципов работы. (1-я Глава, Параграф 2.5)
2. С учетом требований стандартов интероперабельности и безопасности платежных систем в электронной коммерции была разработана технология в основе которой положены алгоритмы передачи зашифрованных данных на основе использования числовых формант, которые основываются не на пересылке самой информации в реальном времени, а на отправке косвенных данных об этой информации битовая длина которой намного меньше и, следовательно, она может быть передана в зашифрованном формате с требуемой скоростью и криптостойкостью криптографической системы при помощи модернизированной системы RSA-m без задержки во времени. (3-я Глава, Параграф 3.2)
3. Был модернизирован алгоритм RSA в RSA-m на основе алгебры нового направления в теории чисел – формантного анализа. Таким образом, были введены дополнительные неопределённые параметры, подлежащие

определению при попытках взлома, что потенциально увеличивает время «взлома» и в случае шифрования краткосрочной (по секретности) информации может служить средством повышения крипто стойкости системы (например, при оперативных переговорах или транзакциях в режиме реального времени). (3-я Глава)

4. На основе алгоритмов формантного анализа были разработаны алгоритмы шифрования/дешифрования - RSA-mAB (AB1, AB2, AB3), обеспечивающих при необходимой скорости заданную временную крипто устойчивость платежных систем в режиме реального времени, когда время разложения и восстановления чисел на порядки меньше времени шифрования и дешифрования того же числа при помощи классической криптосистемы RSA. (Параграфы 3.2.1, 3.2.2, 3.2.3)
5. Расширенный алгоритм RSA-m позволяет существенно уменьшить время генерирования новых криптографических ключей очередного пакета данных и, таким образом, позволяет в процессе работы оперативно менять криптографические ключи неограниченное число раз, что также существенно затруднит задачу взлома передаваемых сообщений, что является слабым местом в классической RSA. Криптографическая устойчивость алгоритма RSA-m может существенно выше всех существующих криптографических алгоритмов и может увеличиваться на порядки по мере роста требований к уровню защиты только путем изменения параметром работы алгоритма без значимого снижения скорости работы. (Параграф 3.3)
6. Предложенные алгоритмы были проверены для закрытия информации в системах речевой связи, где передаются зашифрованные голосовые сообщения, в режиме реального времени со скоростью передачи примерно в 64 kb/сек. Особенностью разработанной системы является применение в режиме реального времени (он-лайн) асимметричного побитного (потокового или блок-фонемного, блочного 32-битного) шифрования форманты речевого сообщения (то есть адекватного ему аналога в виде модели - образа, свёртки) алгоритмами RSA-mAB с сохранением присущего алгоритму RSA высокого уровня крипто стойкости, но используя его с высокой частотой смены коротких крипто-ключей, достаточных для обеспечения краткосрочного уровня защиты переговоров (3-10 мин.), а при увеличении уровня долгосрочности (до нескольких месяцев и лет) предусматриваются изменение и длины крипто ключей до величин, обеспечивающих заявляемый уровень криптостойкости при повышенных

временных интервалах секретности. В этом случае при использовании быстро сменяющихся ключей, каждый из которых имеет длину 19 десятичных цифр (≈152 бита), система обеспечит сохранность сеанса переговоров длиною в 24 часа сроком на три года, а при длине ключа 9 десятичных цифр (≈ 72 бита) – порядка несколько недель. (Параграф 4.3)

В качестве будущих направлений исследований предлагается:

1. При определенной доработке (модернизации) алгоритмы могут быть использованы в других предметных областях самого различного назначения – аутентификации, блокчейн, карточные платежные системы и т.д.
2. Полная аппаратная реализация данных алгоритмов на базе микропроцессоров, что обеспечит более высокую скорость шифрования, и тем самым предлагается исследовать данную область аппаратной реализации, поскольку интероперабельнные системы включают в себя как программные, так и аппаратные системы, реализованные на микропроцессорах, где есть ограничения на используемую память и скорость обработки данных.
3. Внедрение данных алгоритмов в процесс автоматической аутентификации на базе уникальных биологических характеристик человека, где нужно четко распознавать объекты в режиме реального времени, с обеспечением требуемой криптостойкости системы.

БИБЛИОГРАФИЯ

На русском языке

1. АГАФОНОВ, А. *Научные труды по математике, физике и социологии истории. Математические начала в исследовании исторических процессов*. Избранное / А.Ф. Агафонов. Научный редактор академик РАЕН – А.А. Балабанов. К. : ТУМ, 2011, 227 с. ISBN 978-9975-45-177-2.
2. АЛФЕРОВ, А. П., ЗУБОВ, А.Ю., КУЗЬМИН, А. С., ЧЕРЕМУШКИН, А. В. *Основы криптографии: Учебное пособие*. М.: Гелиос АРБ, 2001. 480 с.
3. БАЛАБАНОВ, А., **КУНЕВ, В. В.** Современное применение алгоритмов формантного анализа для криптозащиты IT-систем. В: *Журнал: Вестник Российской Академии Естественных Наук РАЕН*, том 19, № 3, 2019, с. 25-35.
4. БАЛАБАНОВ, А., **КУНЕВ, В. В.** *Защищённые IT-системы на основе алгоритмов формантного анализа: Новые направления и перспективы*. LAP LAMBERT Academic Publishing, 2016, 220 с. ISBN 3659948268, 9783659948268.
5. БАЛАБАНОВ, А., **КУНЕВ, В. В.** Криптографическая защита цифровой информации в частотной и спектральной областях на основе алгоритмов форматного анализа (ч.1. основы теории) В: *Материалах Конференции «Математическая теория управления и ее приложения» (МТУиП-2020)*, Санкт-Петербург, 6–8 октября 2020, с. 228-233.
6. БАЛАБАНОВ, А. А., АГАФОНОВ, А. Ф. Методы сопоставительного анализа и формантных уравнений теории чисел в задачах криптографии. В: *Вестник Российской Академии Естественных Наук*,Том 14, № 4, 2014, кат. Б, с. 47-53. ISSN 1682-1696.
7. БАЛАБАНОВ, А., АГАФОНОВ, А., РЫКУ, В. Агоритм быстрой генерации ключей в криптографической системе RSA. В: *Вестник научно-технического развития*, 2009, №7(23), с.11-17. http://www.vntr.ru/ftpgetfile.php?id=323.
8. БАЛАБАНОВ, А. А., АГАФОНОВ, А. А., КОЖУХАРЬ, И. Б. Возможности создания новых и модернизированных алгоритмов для системы RSA. В: *Вестник научно-технического развития* №9(37) 2010, с.3-17. http://www.vntr.ru/nomera/2010-937/
9. БАЛАБАНОВ, А. А., АГАФОНОВ, А. А. *Сопоставительный анализ и его приложения. Классические и современные задачи теории чисел и криптографии*. LAP LAMBERT Academic Publishing, 2016, 200 с. ISBN 978-3-659-92621-1.
10. ВАРФОЛОМЕЕВ, А. А. *Современная прикладная криптография*. Учебное пособие. М.: Рудн, 2008. 218 с.

11. ВАСИЛЕНКО, О.Н. *Теоретико-числовые алгоритмы в криптографии.* М.: МЦНМО, 2003. 328 с.
12. *Введение в криптографию* / Под общ. ред. ЯЩЕНКО, В.В.. М.: МЦНМО, 2012. 348 с.
13. ВЕЛЬШЕНБАХ, М. *Криптография на Си и Си++ в действии*. М.: Триумф, 2004.
14. ВЕНБО, М. *Современная криптография. Теория и практика*. М.:Вильямс, 2005,768 с.
15. КОУТИНХО, С. *Введение в теорию чисел. Алгоритм RSA*. М.:Постмаркет, 2001,328 с.
16. ВИНОГРАДОВ, И.М. *Элементы высшей математики*. М.:Высшая школа,1999,518 с.
17. ГАТЧЕНКО, Н. А., ИСАЕВ, А. С., ЯКОВЛЕВ, А. Д. *Криптографическая защита информации*. СПб: НИУ ИТМО, 2012, 142 с.
18. ГУЛЯЕВ, Ю. В., ЖУРАВЛЕВ, Е. Е., ОЛЕЙНИКОВ, А. Я. Методология стандартизации для обеспечения интероперабельности информационных систем широкого класса. Аналитический обзор. *Журнал АДИОЭЛЕКТРОНИКИ,* No. 3, 2012, 40 с.
19. ЗУБОВ, А. Ю. *Криптографические методы защиты информации. Совершенные шифры*. М.: Гелиос АРВ, 2005.
20. ИВАНОВ, М. А., ЧУГУНКОВ, И. В. *Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие*. Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012, 400 с.
21. КАМЕНЩИКОВ, А. А., ОЛЕЙНИКОВ, А. Я., ШИРОБОКОВА, Т. Д. Стандарты интероперабельности в высокопроизводительной среде. В: *Программные системы: теория и приложения* т. 9, №4(39), с. 383–397.
22. КНУТ, Д. *Искусство программирования, том 2. Получисленные алгоритмы*. М.: Издательство Диалектика, 2019. 832 с. ISBN: 978-5-8459-0081-4.
23. КОРМЕН, Т., ЛЕЙЗЕРСОН, Ч., РИВЕСТ, Р., ШТАЙН, К. *Алгоритмы: построение и анализ.* М.: Вильямс, 2005. 1296 с. ISBN 5-8459-0857-4.
24. КРАВЧЕНКО, Б., СКРЯБИН, Б., ДУБИНИНА, О. *Блокчейн и децентрализованные системы учеб. пособие для студ. заведений высш. образования: в 3 частях*. Ч. 1. Харьков, 2019, 488 с.
25. МАСЛЕННИКОВ, М. Е. *Практическая криптография*. СПб.: БХВ-Петербург, 2003. 464 с.
26. МОЛДОВЯН, А. А., МОЛДОВЯН, Н. А. *Введение в криптографию с открытым ключом*. СПб.: BHV-Санкт-Петербург, 2005. 288 с.
27. НЕСТЕРЕНКО, Ю. В. Алгоритмические проблемы теории чисел. В: *Матем. просв.*, сер. 3, 2, МЦНМО, М., 1998, с. 87–114.

28. ОЛЕЙНИК, В. Л. *Методы получения простых чисел – текущее состояние*. Chişinău.:Akta Akademia All, 1999.
29. ОНАЦКИЙ, А. В., ЙОНА, Л. Г. *Асимметричные методы шифрования. – Модуль 2 Криптографические методы защиты информации в телекоммуникационных системах и сетях: Учеб. Пособие*. Под ред. Н. В. Захарченко – Одесса: ОНАС им. А. С. Попова, 2010, 148 с.
30. ПЕТРОВ, А. А. *Компьютерная безопасность. Криптографические методы защиты*. М.:ДМК, 2000. 448 с.
31. РАЗИНКИН, Е. И. Концепция обеспечения интероперабельности в области электронной коммерции. В: *Управление в Социально-Экономических Системах, Информационно Управляющие Системы*, № 5, 2012, с. 82-88.
32. РОСТОВЦЕВ, А. Г. *Алгебраические основы криптографии*. СПб: Мир и Семья, 2000.
33. СНЫТНИКОВ, А. А. *Лицензирование и сертификация в области защиты информации*. М.: Гелиос АРВ, 2003. 192 с.
34. ФЕРГЮСОН, Н., ШНАЙЕР, Б. *Практическая криптография*. М.: «Диалектика», 2004, 432 с.
35. ЧЕРЕМУШКИН, А. В. *Лекции по арифметическим алгоритмам в криптографии: Учебное пособие для студентов, обучающихся по специальности "Компьютерную безопасность"*. М.: МЦНМО, 2002. 104 с.
36. ШНАЙЕР, Б. *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*. М.: Триумф, 2002. 816 с.
37. ЯКОВЛЕВ, А. В., БЕЗБОГОВ, А. А., РОДИН, В. В., ШАМКИН, В. *Криптографическая защита информации: Учебное пособие.* Тамбов: Издательство ТГТУ, 2006, 140 с.

На английском и румынском языке

38. ABADI, M. Explicit Communication Revisited: Two New Attacks on Authentication Protocols. In: *IEEE Trans. on Software Eng., Ma*r. 1997 – 23(3), 1997, p.185-186.
39. ALBARQI, A., ALZAID, E. , GHAMDI, F., ASIRI, S. AND KAR, J. Public Key Infrastructure: A Survey. In: *Journal of Information Security*, 6, 2015, pp. 31-37. doi: 10.4236/jis.2015.61004.
40. AHO, A. V., HOPCROFT, I. E., ULLMAN, I. D. The design and analysis of Computer Alghorithm. *Los Angeles: Addison – Wesley*, 1975, p. 20 - 45.

41. AKASH, NAG, SUNIL, KARFORMA. DSA Security Enhancement through Efficient Nonce Generation. In: *Journal of Global Research in Computer Science (JGRCS)*, Vol.5(10), 2014, p. 14-19.
42. ALHOTHAILY, A., ALRAWAIS, A., CHENG, X. et al. A novel verification method for payment card systems. In: *Pers Ubiquit Comput* 19, 2015, p. 1145–1156. https://doi.org/10.1007/s00779-015-0881-9.
43. ANDERSON, R., NEEDHAM, R. Robustness Principles for Public Key Protocols. In: *Proc. Of CRYPTO'95. Lecture Notes in Comp. Sci. Springer-Verlag*, 1995, v. 963.
44. ASHISH, KR. LUHACH, SANJAY, K., DWIVEDI, JHA, C. K. Designing a logical security framework for e-commerce system based on SOA. In: *Proceedings International Journal on Soft Computing (IJSC)* Vol. 5, No. 2, May 2014, p. 1-10.
45. BAASE, S. Computer Alghorithms. Introduction to Design and Analysis. *Los Angeles: Addison - Wesley*, 1992, p. 37 -75.
46. BAHTIYAR, Ş., GÜR, G., ALTAY, L. Security Assessment of Payment Systems under PCI DSS Incompatibilities. In: Cuppens-Boulahia N., Cuppens F., Jajodia S., Abou El Kalam A., Sans T. (eds) *ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology*, vol 428. Springer, Berlin, Heidelberg, 2014, p. 395-402. https://doi.org/10.1007/978-3-642-55415-5_33.
47. BALABANOV, A., **KUNEV, V**., COLESNIC, V. Spectral Space as a Method for Data Crypto Protection Using the Fast Fourier Transform. In: *Journal of Engineering Science* Vol. XXVIII (1) 2021, p. 75 – 82. ISSN 2587-3474/ eISSN 2587-3482. https://doi.org/10.52326/jes.utm.2021.28(1).07.
48. BALABANOV, A., AGAFONOV, A., **CUNEV, V**. Dispozitiv și procedeu de protecţie crypto-grafică a informaţiei binare (variante). Brevet de invenție 4511 (13) B1, Int. Cl.: H04L 9/14 (2006.01) H04L 9/28 (2006.01) H04L 9/30 (2006.01) G06F 1/00 (2006.01) G06F 12/16 (2006.01) G11B 20/00 (2006.01); a 2016 0046; 2016.04.20, 31 august 2017.
49. BANGDAO, C., ROSCOE, A.W. Mobile Electronic Identity: Securing Payment on Mobile Phones. In: *Ardagna C.A., Zhou J. (eds) Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication. WISTP 2011.* Lecture Notes in Computer Science, vol 6633. Springer, Berlin, Heidelberg, 2011, p.22-37. https://doi.org/10.1007/978-3-642-21040-2_2.
50. BAO, F., DENG, R., ZHOU, J. Electronic Payment Systems with Fair On-line Verification. In: *Qing S., Eloff J.H.P. (eds) Information Security for Global Information Infrastructures.*

SEC 2000, IFIP — The International Federation for Information Processing, vol 47. Springer, Boston, MA, 2000, p. 451-460. https://doi.org/10.1007/978-0-387-35515-3_46.

51. BASU, AMIT, MUYLLE, STEVE. Authentication in E-Commerce. In: *Communications of the ACM*, December 2003, Vol. 46 No. 12, p. 159-166.
52. BLAZE, M. Key Management in an Encrypting File System. In: *Proc. Of the Summer USENIX Conference*, USENIX Association, 1994, p. 27-35.
53. BO, Y., DONGSU, L. & YUMIN, W. An anonymity-revoking e-payment system with a smart card. In: *Int J Digit Libr* 3, 2002, p. 291–296. https://doi.org/10.1007/s007990100047.
54. BOLY, JP. et al. The ESPRIT project CAFE —High security digital payment systems. In: *Gollmann D. (eds) Computer Security — ESORICS 94. ESORICS 1994. Lecture Notes in Computer Science*, vol 875. Springer, Berlin, Heidelberg, 1994, p. 217-230. https://doi.org/10.1007/3-540-58618-0_66.
55. BOUDKO, S., ABIE, H., BOSCOLO, M., FERRARIO, D. Predictive Analytics Service for Security of Blockchain and Peer-to-Peer Payment Solutions. In: Kim H., Kim K.J., Park S. (eds) *Information Science and Applications. Lecture Notes in Electrical Engineering*, vol 739. Springer, Singapore, 2021,p.71-81. https://doi.org/10.1007/978-981-33-6385-4_7.
56. BURNET, S., PAINE, S. *RSA Security`s Official Guide to Cryptography*. NY.: The McGraw-Hill Companies, 2001. 419 p.
57. CAI, XQ., WEI, CY. Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature. In: *Quantum Inf Process* 12, 2013, p. 1651–1657. https://doi.org/10.1007/s11128-012-0477-5.
58. CARO, M.C., HUANG, HY., CEREZO, M. et al. Generalization in quantum machine learning from few training data. In: *Nat Commun* **13**, 4919 (2022). https://doi.org/10.1038/s41467-022-32550-3
59. CARDOSO, S., MARTINEZ, L.F. Online payments strategy: how third-party internet seals of approval and payment provider reputation influence the Millennials' online transactions. In: *Electron Commer Res* 19, 2019, p. 189–209. https://doi.org/10.1007/s10660-018-9295-x.
60. CARNAHAN, D., MARTIN, R., DORI, D. ISO TC184/SC5: Standards to Enable Interoperability of Manufacturing Automation Solutions. In: *INSIGHT*, 17(1), 2014, p. 17-19.
61. CARONNI, G., RABSHAW, M. Exhausting is Exhaustive Search? In: *Cryptobytes*, v.2, №3, Winter 1997, p. 1-6.

62. CARONNI, G.Walking the Web of trust. In: P*roceedings IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2000)*, 2000, pp. 153-158. doi: 10.1109/ENABL.2000.883720. 153-158. 10.1109/ENABL.2000.883720.
63. CLAUDE, SHANNON. Communication theory of secrecy systems. In: *The Bell System Technical Journal*, vol. 28, no. 4,1949, p. 656-715, Oct. 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x.
64. CHEN, D., CHUNG, J.Y. OBI&XML standard based business to business electronic business solution. In: *Proceedings of the International Symposium on Government and E-commerce Development (ISGED*), Ningbo, China, 23-24 April 2001, pp. 35-41.
65. CHEN, X., CHOI, K. & CHAE, K. A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service. In: *Wireless Pers Commun 97*, 2017, p. 1–17. https://doi.org/10.1007/s11277-017-4261-9.
66. CHIN, A.G., HARRIS, M.A. & BROOKSHIRE, R. An Empirical Investigation of Intent to Adopt Mobile Payment Systems Using a Trust-based Extended Valence Framework. In: *Inf Syst Front*, 2020. https://doi.org/10.1007/s10796-020-10080-x.
67. COSTAȘ, I. Factorii de influenţă asupra dezvoltării infrastructurii informaţionale a societăţii. În: *Culegerea de articole şi teze ale comunicărilor prezentate în cadrul Conferinței Științifice Internaționale "Rolul investițiilor în dezvoltarea economiei digitale în contextul globalizării financiare*" consacrate celei de-a 25 aniversări de la fondarea ASEM, Chişinău, 22-23 decembrie 2016, p. 27-34.
68. **CUNEV, V.** Secure Voice Data Transmission Based on the Formant Analysis Algorithms. In: *Proceedings of the 6th International Conference "Telecommunications, Electronics and Informatics"* ICTEI 2018, Chisinau, 24-27 mai 2018, pp. 34- 39. ISBN 978-9975-45-540-4.
69. DAVIES, J., HARRIS, S., CRICHTON, Ch., SHUKLA, Aa., GIBBONS, J. Metadata Standards for Semantic Interoperability in Electronic Government. In: *Proceedings International Conference on Theory and Practice of Electronic Governance*, Cairo, 2008, p. 67-75. 10.1145/1509096.1509111
70. DISTERER, Georg, KLEINER, Carsten. BYOD — Bring Your Own Device. In: *HMD Praxis der Wirtschaftsinformatik*, 50, 2014, pp. 92-100. 10.1007/BF03340800.
71. DIFFIE, W., and HELLMAN, M.E., New Directions in Cryptography. In: *IEEE Transactions on Information Theory*, vol. 22, no. 6, November 1976, p. 644-654.
72. De SMET, D., MENTION, A. Improving auditor effectiveness in assessing KYC/AML practices. In: *Managerial Auditing Journal*, 26(2), 2021, pp. 182–203. doi:10.1108/02686901111095038

73. DELAHOSTRIA, Emmanuel. Manufacturing application integration scheme using ISO 15745 and IEC 62264. In: *IFAC Proceedings*, Volume 38, Issue 1, 2005, p. 52-57. https://doi.org/10.3182/20050703-6-CZ-1902.01527.
74. FAST-BERGLUND, Fasth, ROMERO, Åsa, ÅKERMAN, David, HODIG, Magnus, BJÖRN, PICHLER, Andreas. Agent- and Skill-Based Process Interoperability for Socio-Technical Production Systems-of-Systems. In: *APMS - Towards Smart and Digital Manufacturing*, Volume: B. Lalic et al. (Eds.), IFIP, AICT 592, Part II, Springer, 2020, p. 46-54.
75. FOSTER, C. L. Alghorithms, Abstraction and Implementation. *Los Angeles: Academic Press*, 1992, p. 17 – 36.
76. GERCK, Ed. Overview of Certification Systems: X.509, PKIX, CA, PGP & SKIP. *The Bell Newsletter*, Vol. 1. 2000, p. 8.
77. GRECU, M., COSTAȘ, I. Active de interoperabilitate semantică în infrastructura de date a sistemului de e-guvernare. În: *"Competitivitatea şi inovarea în economia cunoaşterii*" Vol. 1, 2015, Chișinău, Moldova, 25-26 septembrie 2015, pp. 69-74.
78. HOFFMAN, L. (Ed.) *Building in big Brother: the cryptography policy debate*. Springer-Verlag NewYork. Inc., 1995. 560 p.
79. HOFRI, M. Analysis of Alghorithms. Computational Methods and Mathematical Tools. *Oxford: Oxford Press*, 1995, p. 10-42.
80. HONG, SP., KANG, S. Ensuring Privacy in Smartcard-Based Payment Systems: A Case Study of Public Metro Transit Systems. In: *Leitold H., Markatos E.P. (eds) Communications and Multimedia Security*, CMS 2006, Lecture Notes in Computer Science, vol 4237. Springer, Berlin, Heidelberg, 2006, p. 206-215. https://doi.org/10.1007/11909033_19.
81. HORN, G., PRENEEL, B. Authentication and payment in future mobile systems. In: *Quisquater JJ., Deswarte Y., Meadows C., Gollmann D. (eds) Computer Security — ESORICS 98. ESORICS 1998. Lecture Notes in Computer Science*, vol 1485. Springer, Berlin, Heidelberg, 1998, p. 277-293. https://doi.org/10.1007/BFb0055870.
82. HUANG, Jianni. Application of E-commerce System Based on ebXML. In: *Proceedings of 2009 Second International Conference on Future Information Technology and Management Engineering*, 2009, p. 613-616.
83. *Informative Report. ASC X9 IR 01-2019. Quantum Computing Risks to the Financial Services Indutry.* By the ASC X9 Quantum Computing Risk Study Group, 1st edition, 2019, 42 p.
84. ISO/IEC JTC 1 Information technology. Big data preliminary Report 2014, ISO/IEC 2015.

85. JIANG, X., WANG, X., HUANG, Y. One Way to Enhance the Security of Mobile Payment System Based on Smart TF Card. In: He X., Hua E., Lin Y., Liu X. (eds) *Computer, Informatics, Cybernetics and Applications. Lecture Notes in Electrical Engineering*, vol 107. Springer, Dordrecht, 2012, p. 961-970. https://doi.org/10.1007/978-94-007-1839-5_104.
86. JÜRJENS, J. Modelling Audit Security for Smart-Card Payment Schemes with UML-Sec. In: Dupuy M., Paradinas P. (eds) *Trusted Information. SEC 2001. IFIP International Federation for Information Processing*, vol 65. Springer, Boston, MA, 2001, p. 93-107. https://doi.org/10.1007/0-306-46998-7_7.
87. KAI, F., JUN, Z., WEIDONG, K. et al. Electronic payment scheme to prevent the treachery. In: *Wuhan Univ. J. Nat. Sci. 11,* 2006, p. 1745–1748. https://doi.org/10.1007/BF02831865.
88. KNUDSEN, L. R. *Block Ciphers-Analysis, Design, Applications*. Ph. D. dissertation. Aarhus University, Nov., 1994.
89. KOC, C. K. *High-Speed RSA Implementation. Version 2.0. RSA Laboratories*. Nov., 1994.
90. KOSANKE, K. ISO Standards for Interoperability: a Comparison. In: Konstantas D., Bourrières JP., Léonard M., Boudjlida N. (eds) *Interoperability of Enterprise Software and Applications. Springer*, London, 2006, p. 55-64. https://doi.org/10.1007/1-84628-152-0_6.
91. KONSTANTAS, D., BOURRIÈRES, J.-P., LÉONARD, M., BOUDJLIDA, N. *Interoperability of Enterprise Software and Applications*. London: Springer, 2006, 474 p. doi:10.1007/1-84628-152-0.
92. KOZEN, Dexter, C. The Design and Analysis of Algorithms. *San Francisco: Springer Verlag*, 1992, p. 48 -72.
93. **KUNEV, V**. Extended RSA-M Algorithm as a Way of Increase Computational Complexity of Cryptosystems. In: *Journal of Engineering Science* Vol. XXV(2) (2018), pp. 45-56. ISSN 2587 3474/ eISSN 2587-3482. DOI: 10.5281/zenodo.2564486. Microsoft Word - JES 2-2018 (utm.md)
94. KÜTZ, Martin. *Introduction to E-Commerce: Combining Business and Information Technology 1st edition*. Bookboon, 2016, 209 p.
95. LASSAIGNE, R., ROUGEMONT, M. Logique at Complexite. In: *Paris : Editions Hermes,* 1996, p. 38 -53.
96. LAVANYA, D.L., RAMAPRABHA, R., THANGAPANDIAN, B. et al. Novel Privacy Preserving Authentication Scheme Based on Physical Layer Signatures for Mobile Payments. In: *SN COMPUT. SCI.* 2, 2021, p. 119 (11 pages) . https://doi.org/10.1007/s42979-021-00509-8.

97. LAWAL, O.M., VINCENT, O.R., AGBOOLA, A.A. et al. An improved hybrid scheme for e-payment security using elliptic curve cryptography. In: *Int. j. inf. tecnol*. 13, 2021, p.139–153. https://doi.org/10.1007/s41870-020-00517-6.

98. LAYEGHIAN, Javan, S., GHAEMI, Bafghi, A. An anonymous mobile payment protocol based on SWPP. In: *Electron Commer Res* 14, 2014, p. 635–660. https://doi.org/10.1007/s10660-014-9151-6.

99. LIN, IC., CHANG, CC. A Practical Electronic Payment System for Message Delivery Service in the Mobile Environment. In: *Wireless Pers Commun* 42, 2007, p. 247–261. https://doi.org/10.1007/s11277-006-9176-9.

100. LIN, MM., XUE, DW., WANG, Y. et al. A New Quantum Payment Protocol Based on a Set of Local Indistinguishable Orthogonal Product States. In: *Int J Theor Phys* 60, 2021, p. 1237–1245. https://doi.org/10.1007/s10773-021-04749-5.

101. LUHACH, ASHISH, DWIVEDI, SANJAY, JHA C. Designing and Implementing the Logical Security Framework for Ecommerce Based on Service Oriented Architecture. In: *International Journal of Advanced Information Technology (IJAIT)* Vol. 4, No. 3, June 2014, pp. 25-34. DOI : 10.5121/ijait.2014.4303

102. MANDAL, S., MOHANTY, S. & MAJHI, B. Design of electronic payment system based on authenticated key exchange. In: *Electron Commer Res* 18, 2018, p. 359–388. https://doi.org/10.1007/s10660-016-9246-3.

103. MARAND, C., TOWNSEND, P.D. Quantum Key Distribution Over Distance as Long as 30 km. *Optics Letters*, 1995, p. 1659-1697.

104. MARTÍNEZ-PELÁEZ, R., TORAL-CRUZ, H., RUIZ, J. et al. P2PM-pay: Person to Person Mobile Payment Scheme Controlled by Expiration Date. In: *Wireless Pers Commun* 85, 2015, p. 289–304. https://doi.org/10.1007/s11277-015-2738-y.

105. MATSUI, M. The First Experimental Cryptanalyst of the Data Encryption Standard. In: *Proc. CRYPTO'94. Lecture Notes in Comp*, Sci. Springer-Verlag, 1996.

106. MEHLENBACHER, A. Multiagent System Simulations of Treasury Auctions. In: *Comput Econ* 34, 2009, p. 67 -117. https://doi.org/10.1007/s10614-008-9165-z.

107. MENEZES, A. J., PAUL, C. VAN OORSCHOT, and SCOTT, A., VANSTONE. *Handbook of applied cryptography*. Boca Raton: CRC Press, 1997. 816 p.

108. MERKLE, R. C. Secury communication over insecure channels. In: *Communications of the ACM*, Volume 21, Issue 4, April 1978, p. 294–299. https://doi.org/10.1145/359460.359473

109. MILLS, D.C., HUSAIN, S.Y. Interlinkages between payment and securities settlement systems. In: *Ann Finance* 9, 2013, p. 61–81. https://doi.org/10.1007/s10436-012-0198-x.

110. MJØLSNES, S.F., RONG, C. On-Line E-Wallet System with Decentralized Credential Keepers. In: *Mobile Networks and Applications* 8, 2003, p. 87–99. https://doi.org/10.1023/A:1021175929111.
111. MOLOTKOV, S.N., NAZIN, S.S. *Quantum Cryptography Based on the Time-Energy Uncertainty Relation.* Manuscript, 1996.
112. *New European interoperability framework. Promoting seamless services and data flows for European public administrations*. Luxembourg: Publications Office of the European Union, 2017. 48 p. doi:10.2799/78681.
113. NGUYEN, S.T., RONG, C. Electronic Payment Scheme Using Identity-Based Cryptography. In: Lopez J., Samarati P., Ferrer J.L. (eds) *Public Key Infrastructure. EuroPKI, 2007. Lecture Notes in Computer Science*, vol 4582. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-73408-6_24
114. NIU, XF., ZHANG, JZ., XIE, SC. et al. A Third-Party E-payment Protocol Based on Quantum Multi-proxy Blind Signature. In: *Int J Theor Phys* 57, 2018, p. 2563–2573. https://doi.org/10.1007/s10773-018-3778-3.
115. ONDRUS, J., PIGNEUR, Y. Near field communication: an assessment for future payment systems. In: *Inf Syst E-Bus Manage* 7, 2009, p. 347–361. https://doi.org/10.1007/s10257-008-0093-1.
116. OOI, S.K., OOI, C.A., YEAP, J.A.L. et al. Embracing Bitcoin: users' perceived security and trust. In: *Qual Quant*, 2020, p. 1219-1237. https://doi.org/10.1007/s11135-020-01055-w.
117. OU, CM., OU, C.R. Adaptation of proxy certificates to non-repudiation protocol of agent-based mobile payment systems. In: *Appl Intell* 30, 2009, p. 233–243. https://doi.org/10.1007/s10489-007-0089-4.
118. PATIL, V., SHYAMASUNDAR, R.K. E-coupons: An Efficient, Secure and Delegable Micro-Payment System. In: *Inf Syst Front* 7, 2005, p. 371–389. https://doi.org/10.1007/s10796-005-4809-1.
119. PEREIRA, António, CUNHA, Frederico, MALHEIRO, Pedro, AZEVEDO, Américo. EBXML – Overview, Initiatives and Applications. In: *IFIP International Federation for Information Processing*, Volume 266, Innovation in Manufacturing Networks; ed. A. Azevedo, 2008, p. 127-136.
120. PFITZMANN, B., WAIDNER, M. How to Break and Repair a "Provably Secure" Untraceable Payment System. In: *Feigenbaum J. (eds) Advances in Cryptology — CRYPTO* '91. CRYPTO 1991. Lecture Notes in Computer Science, vol 576, Springer, Berlin, Heidelberg, 1992, p. 338-350. https://doi.org/10.1007/3-540-46766-1_28.

121. PHOENIX, S.J.D., BARNETT, S.M., TOWNSEND, P.D., BLOW, K.J. Multi-User Quantum Cryptography on Optical Network. In: *Journal of Modern Optics*, 1995, 42, p. 1155-1163.
122. PHOENIX, S.J.D., TOWNSEND, P.D. Quantum Cryptography: Protecting our Future Networks with Quantum Mechanics. In: *Proc. of Cryptography and Coding. Lecture Notes in Comp. Sci, Springer-Verlag*, v.1025, 1995, p. 112-131.
123. PILLER, G., ZACCARIOTTO, E. Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organizations. In: *Transit Stud Rev* 16, 2009, p. 62–76. https://doi.org/10.1007/s11300-009-0048-3.
124. PRICE, E., WOODRUFF, D. P. Applications of the Shannon-Hartley theorem to data streams and sparse recovery. In: *Proceedings of the 2012 IEEE International Symposium on Information Theory*, 2012, p. 2446-2450. doi: 10.1109/ISIT.2012.6283954.
125. RAGHUNANDAN, K.R., DSOUZA, R.R., RAKSHITH, N., SHETTY, S., AITHAL, G. Analysis of an Enhanced Dual RSA Algorithm Using Pell's Equation to Hide Public Key Exponent and a Fake Modulus to Avoid Factorization Attack. In: Chiplunkar N., Fukao T. (eds) *Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing*, vol 1133. Springer, Singapore, 2021, p. 809-823. https://doi.org/10.1007/978-981-15-3514-7_60.
126. RICKEY, V. Euler's E228: Primality Testing and Factoring via Sums of Squares. In: Zack M., Schlimm D. (eds) Research in History and Philosophy of Mathematics. CSHPM 2016. In: *Proceedings of the Canadian Society for History and Philosophy of Mathematics/La Société Canadienne d'Histoire et de Philosophie des Mathématiques. Birkhäuser*, Cham., 2017, p. 97-116. https://doi.org/10.1007/978-3-319-64551-3_7.
127. RIVEST, R. L., SHAMIR, A., ADLEMAN, L.A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 26(1), 1983, p. 96–99. doi:10.1145/357980.358017.
128. Relebook PH-ISO20022 Standard on Payment Messages. Bangko Sentral ng Pilipinas, 2021.
129. RADHA, V., REDDY, D. H. A Survey on Single Sign-On Techniques. In: *Procedia Technology*, 4, pp. 134–139. doi:10.1016/j.protcy.2012.05.019
130. SANSONE, SUSANNA-ASSUNTA, ROCCA-SERRA, PHILIPPE. Interoperability standards – Digital Objects in Their Own Right. In: *Journal contribution*, p. 1-24. https://doi.org/10.6084/m9.figshare.4055496.v1
131. SCHNEIER, B. The GOST Encryption Algorithm. In: *Dr. Dobb's J.,* v. 20, № 1, Jan, 1995, p. 123-124.

132. SHANNON, C. E. Communication theory of secrecy systems. In: *The Bell system technical journal* 28 (4), p. 656-715
133. SHAO-BIN, W., XIAN, Z. & FAN, H. ACSEPP on-line electronic payment protocol. In: *Wuhan Univ. J. Nat. Sci.* 9, 2004, p. 717–721. https://doi.org/10.1007/BF02831669.
134. SHIM, S. S. Y., PENDYALA, V. S., SUNDARAM, M., GAO J. Z. Business-to-business e-commerce frameworks. In: *Computer*, vol. 33, no. 10, 2000, p. 40-47. doi: 10.1109/2.876291.
135. SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, p.124-134. doi:10.1109/sfcs.1994.365700.
136. STERN, J. A. New Identification Scheme Based on Syndrome Decoding. In: *Proc. Of EUROCRYPT '93. Lecture Notes in Comp. Sci. Springer-Verlag*,1994, v. 773, p.13-21.
137. SUNA, Alexandru, LEMAITRE, Christian, EL FALLAH SEGHROUCHNI Amal. E-commerce using an agent oriented approach. In: *Revista Iberoamericana de Inteligencia Artificial*, vol. 9, núm. 25, 2005, p. 89-98.
138. TAKYI, A., GYAASE, P.O. Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce. In: Khachidze V., Wang T., Siddiqui S., Liu V., Cappuccio S., Lim A. (eds) *Contemporary Research on E-business Technology and Strategy* iCETS 2012. *Communications in Computer and Information Science*, vol 332. Springer, Berlin, Heidelberg, 2012, p. 232-239. https://doi.org/10.1007/978-3-642-34447-3_21.
139. TAMBAG, Yusuf. EIOP: an e-commerce interoperability platform. In: *Proceedings of the 13th international conference on World Wide Web - Alternate Track Papers & Posters*, WWW 2004, New York, NY, USA, May 17-20, 2004, p. 230-231.
140. TÉLLEZ, Isaac, J., ZEADALLY, S. & SIERRA, J.C. Implementation and performance evaluation of a payment protocol for vehicular ad hoc networks. In: *Electron Commer Res* 10, 2010, p. 209–233. https://doi.org/10.1007/s10660-010-9052-2.
141. TRUONG, Nguyen, JAYASINGHE, Upul, UM, Tai-Won, LEE, Gyu Myoung. A Survey on Trust Computation in the Internet of Things. In: *The Journal of Korean Institute of Communications and Information Sciences (J-Kics)*, 33, 2016, pp. 10-27.
142. URECHE, O., PLAMONDON, R. Digital payment systems for Internet commerce: The state of the art. In: *World Wide Web* 3, 2000, p. 1–11. https://doi.org/10.1023/A:1019217210183.

143. VINCENT, O.R., LAWAL, O.M. A key agreement authentication protocol using an improved parallel Pollard rho for electronic payment system. In: *J Supercomput* 74, 2018, p.1973–1993. https://doi.org/10.1007/s11227-017-2204-6.
144. VINCENT, O.R., OKEDIRAN, T.M., Abayomi-Alli, A.A. et al. An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security. In: *SN COMPUT. SCI*. 1, 2020, p. 112 (12 pag.). https://doi.org/10.1007/s42979-020-00122-1.
145. VON GRAEVENITZ, G.A. Biometric authentication in relation to payment systems and ATMs. In: *DuD* 31, 2007, p. 681–683. https://doi.org/10.1007/s11623-007-0223-9.
146. WANG, CT., CHANG, CC. & LIN, CH. A New Micro-Payment System Using General Payword Chain. In: *Electronic Commerce Research* 2, 2002, p. 159–168. https://doi.org/10.1023/A:1013360606669.
147. WARD, M. Developments in Electronic Payment Systems Security. In: Gertz M., Guldentops E., Strous L. (eds) Integrity, Internal Control and Security in Information Systems. IICIS 2001. *IFIP — The International Federation for Information Processing*, vol 83. Springer, Boston, MA, 2001, p. 103-111. https://doi.org/10.1007/978-0-387-35583-2_7.
148. WEN, X., CHEN, Y. & FANG, J. An inter-bank E-payment protocol based on quantum proxy blind signature. In: *Quantum Inf Process* 12, 2013, p. 549–558. https://doi.org/10.1007/s11128-012-0398-3.
149. WESTERMANN, B. Security Analysis of AN.ON's Payment Scheme. In: Jøsang A., Maseng T., Knapskog S.J. (eds) Identity and Privacy in the Internet Age. NordSec 2009. *Lecture Notes in Computer Science*, vol 5838. Springer, Berlin, Heidelberg., 2009, p. 255-270. https://doi.org/10.1007/978-3-642-04766-4_18.
150. WÓJTOWICZ, A., CHMIELEWSKI, J. Payment Authorization in Smart Environments: Security-Convenience Balance. In: Hammoudi S., Śmiałek M., Camp O., Filipe J. (eds) Enterprise Information Systems. ICEIS 2018. *Lecture Notes in Business Information Processing*, vol 363. Springer, Cham, 2019, p. 58-81. https://doi.org/10.1007/978-3-030-26169-6_4.
151. XIE, SC., NIU, XF. & ZHANG, JZ. An Improved Quantum E-Payment System. In: *Int J Theor Phys* 59, 2020, p. 445–453. https://doi.org/10.1007/s10773-019-04338-7.
152. YANG, C., TIAN, G. & WARD, S. Security systems of point-of-sales devices. In: *Int J Adv Manuf Technol* 34, 2007, p. 799–815. https://doi.org/10.1007/s00170-006-0638-8.
153. YANG, JH., CHANG, CC. A Low Computational-Cost Electronic Payment Scheme for Mobile Commerce with Large-Scale Mobile Users. In: *Wireless Pers Commun* 63, 2012, p. 83–99. https://doi.org/10.1007/s11277-010-0109-2.

154. YU, L., TSAI, W.-T., LI, G., YAO, Y., HU, C., & DENG, E. Smart-Contract Execution with Concurrent Block Building. In: *IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2017, 160-167. doi:10.1109/sose.2017.33
155. ZAMFIROIU, A., DRAGOS, N. Consideraţii generale asupra interoperabilitaţii aplicaţiilor utilizate în E-Guvernare. În: *Revista Română de Informatică şi Automatică*, vol.27, nr. 1, 2017, p. 33-40.
156. ZHAO, Wenbing. (2021). *Cryptocurrency and Blockchain*. Chapter in Book: From Traditional Fault Tolerance to Blockchain, pp. 295-348. 10.1002/9781119682127.ch8.
157. ZHANG, JL., HU, MS., JIA, ZJ. et al. A Novel E-payment Protocol Implented by блокhain and Quantum Signature. In: *Int J Theor Phys* 58, 2019, p. 1315–1325. https://doi.org/10.1007/s10773-019-04024-8.
158. ZHANG, JZ., YANG, YY. & XIE, SC. A Third-Party E-Payment Protocol Based on Quantum Group Blind Signature. In: *Int J Theor Phys* 56, 2017, p. 2981–2989. https://doi.org/10.1007/s10773-017-3464-x.
159. ZHIZHONG, ZHANG, CHUAN, WU AND DAVID, W.L., CHEUNG. A survey on cloud interoperability: taxonomies, standards, and practice. In: *SIGMETRICS Perform. Eval*. Rev. 40, 4, 2013, p. 13–22. DOI:https://doi.org/10.1145/2479942.2479945.
160. ZHONG, L., WANG, H., XIE, J., QIN, B., LIU, J.K., WU, Q. A Flexible Instant Payment System Based on Blockchain. In: Jang-Jaccard J., Guo F. (eds) *Information Security and Privacy. ACISP 2019. Lecture Notes in Computer Science*, vol 11547. Springer, Cham, 2019, p.289-306. https://doi.org/10.10 07/978-3-030-21548-4_16.
161. ZHOU, T. An Empirical Examination of Initial Trust in Mobile Payment. In: *Wireless Pers Commun* 77, 2014, p. 1519–1531. https://doi.org/10.1007/s11277-013-1596-8.
162. ZGUREANU, A. Information encryption systems based on Boolean functions. In: *Computer Science Journal of Moldova*, vol.18, no.3(54), 2010, pp. 319-335.

ПРИЛОЖЕНИЕ 1. Акты внедрения результатов работы

MD2001, Moldova, Chisinau, str. C.Brincus 124/1, et.6, of.3
phone: (+373 22) 54-54-45, fax: (+373 22) 500 876
e-mail: info@kmm.md , www.kmm.md

Кому:
Г-ну Куневу Вячеславу.

01 апреля 2022

Отзыв
на использование криптоалгоритма RSA-m в системах IoT (интернет вещей).

Одним из направлений деятельности компании Kvazar-Micro SRL является разработка и внедрение систем контроля и мониторинга технологических процессов в рамках концепции интернета вещей для промышленных предприятий (IoT), включая предприятия агропромышленного комплекса. Подобные решения характеризуются большим объемам обмена данными, при этом каждый пакет передачи данных является сравнительно небольшим. Для многих предприятий, в которых внедряются системы мониторинга и управления техпроцессом, основанные на передачи данных в сети Internet/Intranet, защита передаваемых данных становится вопросом первостепенной важности (целостность данных, несанкционированный доступ и коммерческая тайна). В связи с этим, требуется гарантированная защита передаваемых данных через сети общего доступа при обмене сообщениями между многочисленными устройствами (датчиками), контролирующими производственный процесс и системой мониторинга предприятия. Не менее важным критерием является скорость обмена данными так как для многих техпроцессов этот параметр является критичным.

Используемые на данные момент алгоритмы и протоколы защиты данных могут привести к резкому замедлению работы внедряемых нашей компанией систем мониторинга, в случае экспоненциального роста обмена данными, что более чем актуально при постоянном расширении контролируемых параметров техпроцесса и увеличении числа датчиков.

В связи с вышесказанным, нас заинтересовала возможность использования предложенного алгоритма RSA-m для пакетного шифрования передачи данных в гибридных сетях, обеспечивая нашим клиентам безопасный круглосуточной мониторинг.

В частности, нас заинтересовали следующие преимущества предлагаемой реализации алгоритма RSA-m:

1. Возможность контролируемо повышать криптостойкость через изменение параметров, а не самого программного модуля;
2. Высокая производительность предлагаемой системы при работе с большим количеством сравнительно малых пакетов данных;
3. Низкая стоимость решения.

На данный момент совместно с г-ном Куневым В. мы обсуждаем реализацию алгоритма RSA-m в поставляемых нами комплектах систем мониторинга как нативное решение. Мы планируем запуск решения в опытную эксплуатацию до конца 2022 года.

Генеральный директор
Kvazar-Micro SRL

_____Рыков А.Б.

QSystems
S.R.L.
Generatorul Soluțiilor Performante

Moldova, MD-2001
Chișinau, bd. Ștefan cel Mare, 73/1
(373 22) 838425, office@qsystems.md
c/f 1002600023541 cod TVA 0204879

Nr. 02/01-22 **11 января 2022**

Кому: Куневу Вячеславу

Компания QSYSTEMS специализируется на создании современных платежных систем, которыми пользуются как физические, так и юридические лица. За время работы компании внедрены десятки платежных систем в 8 станах мира. Одним из таких проектов является проект MPay в Молдове, через который ежегодно проходит более 5 млн. платежей.

Особенностью современных платежных систем для физических лиц является экспоненциальный рост количества платежей на небольшие суммы на фоне все возрастающих рисков киберпреступлений. Это требуем максимально возможного уровня обеспечения безопасности каждой транзакции и платежных систем, в целом, включая обеспечения свойства неотрекаемости. Классическим способом обеспечения безопасности и неотрекаемости финансовых транзакций является использование ассиметричных алгоритмов, например, RSA.

С другой стороны, потенциальной опасностью для платежных систем является проблема «квантового превосходства», когда развитие квантовых компьютеров позволит взломать существующие алгоритмы ассиметричного шифрования.

В связи с этим для нас показалось чрезвычайно интересным рассмотреть Ваше предложение по использованию алгоритма RSA-m в поставляемых нами платежных системах, что дает нам следующие важные преимущества:

1. Отсутствие необходимости использовать принципиально новые средства криптозащиты, по сравнению с уже использующимися;
2. Возможность повышения криптозащиты путем изменения параметров работы алгоритма RSA-m, а не внедрением новых средств защиты. Криптостойкость повышается исходя из текущего и/или прогнозируемого уровня крипто-угроз либо исходя из требований заказчика к криптостойкости;
3. Низкая стоимость решения;
4. Высокая производительность.

Нами принято решение провести всестороннее тестирование предложенного криптоалгоритма включая нагрузочное тестирование и тесты на проникновение (penetration test) для получения объективной картины реальной криптостойкости предлагаемых решений.

В случае подтверждения заявленных характеристик, мы планируем предложить данное решение для своих клиентов начиная с 2023 года.

С уважением,

Андрей Айдов

Директор

alfasoft
agile software company
Chișinău, Str. Alba Iulia 75, of.910, Republica Moldova, MD-2071
Email: office@alfasoft.md Web: www.alfasoft.md

08 Декабря 2021

Компания Alfasoft разрабатывает и внедряет информационные системы для государственного сектора. Из последних внедрений в Молдове это "система судебного делопроизводства" для всех судебных инстанций Молдовы. Наша компания работает не только на рынке Молдовы но и на международном, наши решения внедрены во множестве стран, таких как: Albania, Antigua and Barbuda, Armenia, Barbados, Belize, Gambia, Iraq, Jamaica, Kosovo, Kyrgyzstan, Malawi, Mongolia, Nigeria, Rwanda, Somaliland, South Africa, St. Lucia, Tanzania and Zambia.

Одной из ключевых задач, для создаваемых компанией системах автоматизации документооборота является вопрос информационной безопасности, в части передачи и обмена данных с учетом экспоненциального роста объема электронного документооборота и существенно возросших рисках кибертерроризма во всем мире. В качестве решения, которое позволит предложить своим клиентам качественное и надежное решения мы рассматриваем использование алгоритма RSA-m, которое нам предложено для использования Вячеславом Куневым. В предлагаемом решении нас привлекают следующие важные моменты:

- Отсутствие необходимости внесения каких-либо существенных изменений в существующие информационные системы, использующие классические криптосредства на базе RSA.
- Передача не зашифрованных данных, а метаданных, что существенно повышает общую криптостойкость.
- Возможность увеличения уровня безопасности до необходимого параметрически, меняя параметры для криптоалгоритма RSA-m, без замены софта.
- Высочайшая скорость работы алгоритма, позволяющие использовать данный алгоритм без какой-либо значимой потери общей производительности разрабатываемых компанией информационных систем для любого объема данных, типичных для данного класса систем.

Считаем что предложенный алгоритм RSA-m является крайне перспективным решением, обеспечивающее нам конкурентное преимущество по сравнению с существующими аналогами на рынке как по заявленным характеристикам, так и по стоимости.

Предполагаемое использование предложенной технологии в планируется в третьем квартале 2022 года для одного из зарубежных клиентов в Malawi, в частности внедренной нами в 2021 году системе управления автодорогами.

С уважением,
Юрий Коробан
CEO Alfasoft srl Moldova

ПРИЛОЖЕНИЕ 2. Описания программы представления чисел через форманты

Была разработана программа **Numbers Ciphering** которая состоит из двух модулей:

1. Первый модуль имеет цель кодирования числа N, где N представляется при помощи форманты в следующим виде

$$N=pk+q.$$

Число N представляе собой большое число до 32-х разрядов. Каждое число N было полученно при умножение двух простых чисел.

Выбор чисел p и q и генерация числа N может быть сделана в автоматическом режиме при нажатии клавиши **Autofilling,** или в ручную при нажатии клавиши **Manual filling.**

При нажатии **Autofilling** все три матрицы автоматически заполняются данными.

В программе реализована опция где пользователь может сам выбрать p, k и q для представления числа N. Для этого пользователь должен выбрать число с первой таблицы сделав клик на соотвествующем числе N, потом во второй таблице выбрать число k, числа p и q будут автоматически сгенерированыи представлены, если выбирается число p то автоматически будут расчитаны числа k и q. Все полученные данные выводятся внизу таблиц и для каждого числа выводится его индекс в таблице.

Числа N с первой таблицы могут быть отсортированны двумя спосабами, используя модуль сортировки **Type of sorting.**

2. Второй модуль используется для востановления числа N на базе чисел p, k и q или их индексов, востановления числа N происходит при введение чисел p, k и q и нажатии кнопки **Calculate**.

Кнопка **Clear Fields** очищает поля а **Clear matrix** очищает все матрицы.

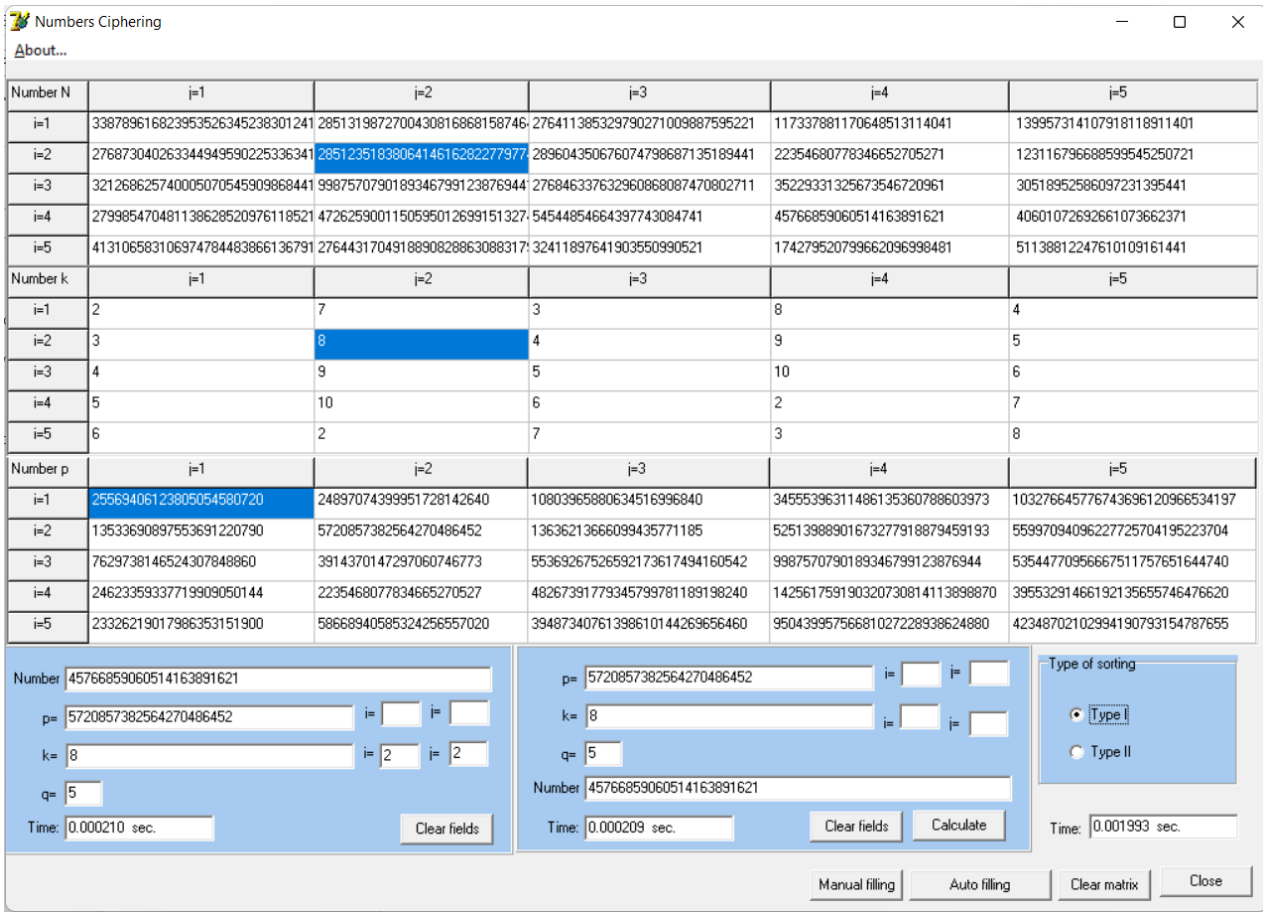


Рисунок 1. Интерфейс программы

ПРИЛОЖЕНИЕ 3. Патент РМ №4511 (13) B1, “Устройство и способ криптографической защиты двоичной информации (варианты)”

MD 4511 C1 2018.03.31

REPUBLICA MOLDOVA

(19) Agenţia de Stat pentru Proprietatea Intelectuală

(11) 4511 (13) C1

(51) Int.Cl: *H04L 9/14* (2006.01)
H04L 9/28 (2006.01)
H04L 9/30 (2006.01)
G06F 1/00 (2006.01)
G06F 12/16 (2006.01)
G11B 20/00 (2006.01)

(12) BREVET DE INVENŢIE

(21) Nr. depozit: a 2016 0046
(22) Data depozit: 2016.04.20

(45) Data publicării hotărârii de acordare a brevetului:
2017.08.31, BOPI nr. 8/2017

(71) Solicitant: BALABANOV Anatoli, MD
(72) Inventatori: BALABANOV Anatoli, MD; AGAFONOV Anatolii, MD; CUNEV Veaceslav, MD
(73) Titular: BALABANOV Anatoli, MD

MD 4511 C1 2018.03.31

(54) Dispozitiv şi procedeu de protecţie criptografică a informaţiei binare (variante)

(57) Rezumat:

1

Invenţia se referă la domeniul convertirilor criptografice şi al protecţiei informaţiei confidenţiale care este transmisă pe bit sau pe pachete.

Dispozitivul şi procedeele de protecţie criptografică a informaţiei binare constau în convertirea semnalelor vocale în formă digitală, codarea lor pe baza unui algoritm de compresie a vorbirii, urmată de criptarea pe pereche de chei cu cifru liniar şi transmiterea în forma cifrată pe canalul duplex de transmitere a datelor de la un abonat la altul.

2

Revendicări: 9

Figuri: 1

COPIE

БЛАГОДАРНОСТЬ

Выражаю глубокую благодарность **Балабанову Анатолию Александровичу**, академику РАЕН, секция информатики и кибернетики, профессору кафедры «Программная Инженерия и Автоматика» Технического университета Молдовы за его неоценимый вклад в подготовку данной работы.

Теоретические исследования г-на Балабанова в области разработки и использования математического аппарата сопоставительных уравнений формантного анализа явился необходимой научной базой для разработки практических методов реализации модернизированных алгоритмов криптозащиты в условиях квантового превосходства.

Благодаря плодотворным дискуссиям с г-ном Балабановым были выявлены и сформулированы возможности использования модернизированных криптоалгоритмов на основе формантного анализа не только в платежных интероперабельных системах как ключевого элемента обеспечения безопасности платежных систем в условиях квантового превосходства, что являлось изначальной задачей автора, но и в системах защиты голосового трафика в рамках жестких ограничений на требуемый уровень производительности криптографических средств защиты информации.

Огромный опыт г-на Балабанова позволил не только сформулировать и реализовать идеи, предложенные автором в рамках данной работы, но и рассмотреть дальнейшее развитие и возможности применения методов формантного анализа в самых разных областях сферы информационных технологий.

Автор Кунев Вячеслав

ДЕКЛАРАЦИЯ ОБ ОТВЕТСТВЕННОСТИ

Нижеподписавшийся, заявляю под личную ответственность, что материалы, представленные в докторской диссертации, являются результатом личных научных исследований и разработок. Осознаю, что в противном случае, буду нести ответственность в соответствии с действующим законодательством.

Фамилия, имя Кунев Вячеслав

Подпись

Число 25.05.2023

DECLARAŢIA PRIVIND ASUMAREA RĂSPUNDERII

Subsemnatul, declar pe răspundere personală că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări şi realizări ştiinţifice. Conştientizez că, în caz contrar, urmează să suport consecinţele în conformitate cu legislaţia în vigoare.

Numele de familie, prenumele **Kunev Veaceslav**

Semnătura

Data 25.05.2023

CURRICULUM VITAE

Вячеслав КУНЕВ

Дата рождения: 06/06/1968

Образование:

1986-1991. Московский Государственный Университет им. Баумана, Москва

Специальность: инженер-системотехник

1997-1998. Академия Государственного Управления при Президенте России

Специальность: финансы и кредит

Работа:

2000 – настоящее время. *Компания/Организация*: Deeplace.

Должность: Директор

2005 – настоящее время. *Компания/Организация*: Технический Университет Молдовы

Должность: Лектор

2009 – настоящее время. *Компания/Организация*: Ассоциация IT-компаний Молдовы

Должность: Председатель Совета Директоров

1997-2000 *Компания/Организация*: Банк “Banca Sociala”.

Должность: Заместитель Руководителя IT-департамента

1992-1997 *Компания/Организация*: Банк “Banca Sociala”.

Должность: Программист

Титулы:

«Maestru in IT» - награда, присуждаемая Министерством Информационного Развития Республики Молдовы

«Honorary Member» - Ассоциация ИТ-компаний Молдовы